Defence Innovation and the UK
Responding to the Risks Identified by the US Third Offset Strategy

John Louth, Trevor Taylor and Andrew Tyler
Defence Innovation and the UK
Responding to the Risks Identified by the US Third Offset Strategy

John Louth, Trevor Taylor and Andrew Tyler

RUSI Occasional Paper, July 2017

Royal United Services Institute
for Defence and Security Studies
185 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world’s oldest and the UK’s leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today’s complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 185 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2017 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution — Non-Commercial — No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Occasional Paper, July 2017. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>v</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>vii</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>I. The Third Offset Strategy</td>
<td>5</td>
</tr>
<tr>
<td>II. The Reality of Vulnerabilities</td>
<td>9</td>
</tr>
<tr>
<td>III. An Emerging UK Response</td>
<td>13</td>
</tr>
<tr>
<td>IV. The SDSR, the UK’s Role in the World, and Innovation</td>
<td>21</td>
</tr>
<tr>
<td>Conclusion</td>
<td>27</td>
</tr>
<tr>
<td>About the Authors</td>
<td>31</td>
</tr>
</tbody>
</table>
Foreword

Lord Arbuthnot of Edrom

As both a former defence minister and chairman of the House of Commons Defence Select Committee, I have spent much of my public life focused on the strategic issues of defence. How much should we spend on our national security and where should we focus our investment? Who are the potential adversaries who could challenge our future wellbeing and safety, and which states are our strategic partners? Are the supposed certainties associated with defence, deterrence, operations and wider geopolitical considerations constant or subject to profound disruption and change?

In seeking a response to these questions, we need to stretch our thinking beyond the confines of our military instrument, important though it is, and consider the security of our critical national infrastructure, the internet of things that frames our lives and the transformative technologies that appear increasingly indispensable to society and individual citizens. This dependency brings with it acute vulnerabilities. I believe this paper goes a long way towards prompting the strategic thinking necessary to embrace all of these challenges, fears, forces and factors.

It was a privilege to be the independent chair of the series of colloquia that provided much of the material and arguments that feature in this paper. Senior colleagues from the UK and US militaries and administrations, commercial executives, engineers, scientists, consultants and thinkers all contributed to an excellent programme of events, framed around a number of positional papers and an early literature review. I need to thank Northrop Grumman for sponsoring this work. I also wish to thank my colleagues at RUSI, where I am a Senior Associate Fellow, for developing the positional papers, capturing the literatures relevant to this topic and constructing a body of knowledge that can only be helpful as the UK grapples with some complex defence and security questions.

The world now is more complex, interdependent and downright dangerous than I can ever remember. If we are to stay safe we need to remain relevant in a military sense, flexible and adaptable in terms of our thinking and innovative in the way in which we nurture and exploit a whole range of current and new technologies. Biomedicine, artificial intelligence, the internet of things and quantum computing are changing our lives in ways we can only just begin to imagine. It would be naive to assume that they will not change our constructs of defence and notions of the secure society. This paper prompts a response from policymakers to ensure that our balance of investment and capability generation addresses these complex, modern and quite revolutionary conditions. I commend its contents and I admire the women and men who gave so much of their time in bringing it to publication. It is important work.

Lord Arbuthnot of Edrom
Former Chairman of the House of Commons Defence Select Committee
Executive Summary

The Third Offset Strategy (TOS), announced by the US in November 2014, stressed the need for a step-level change in American military capabilities to counter the increasing anti-access/area denial systems being developed by potential adversary states. The TOS emphasis was on the potential for innovation at many levels of defence, but technological change was to have a particularly significant role.

This paper examines the implications of the TOS for the UK. It is based on a mixture of desk-based research and three day-long workshops, from November 2016 to March 2017, which brought together senior stakeholders from the governments and private sectors of the UK, the US and continental Europe. Participants in the workshops were directed and challenged through the chairmanship of Lord Arbuthnot of Edrom.

The paper endorses the core assertion of the TOS – that potential adversaries have developed or are developing threats to major Western platforms on the sea, in the air and on land that significantly increase the risks of deploying such platforms in strategic areas, including the Baltics and the North Sea, East Asia and the Gulf. Moreover, these potential adversaries continue to develop offensive cyber capabilities and technologies that threaten the Western use of space for surveillance, communication, navigation and other purposes. It would not be accurate to assert that potential adversaries have ‘caught up’ across the full range of defence capabilities, but they have effectively focused their efforts, particularly on sensors, space denial, many extended-range precision missiles able to attack targets on land, at sea and in the air, as well as cyber. There are thus growing challenges for UK as well as US forces, especially those concerned with force projection.

This paper also recognises that, in any major future conflict, an important part of the battle will be threats to the UK’s critical national infrastructure from hostile cyber operations. In the US, while the Third Offset label may not be adopted by Donald Trump’s administration, we expect Washington’s emphasis on the need for innovation and increased defence effort to be sustained.

In response to the US’s TOS, the British Ministry of Defence (MoD) launched its own Defence Innovation Initiative in September 2016 and has committed £800 million over a decade for basic research purposes, as well as maintaining the assurance that the MoD’s core science and technology budget will be a minimum of 1.2% of the defence budget. These positive steps will need to be supplemented by significant changes to encourage a stronger innovation culture within government defence. These should involve:

- Establishing an appetite for risk in the public and private parts of the UK defence enterprise that recognises the need for experimentation and the inevitability of regular
failure. Clearly, work that is not going to succeed needs to be identified quickly, so that failure is early and comparatively inexpensive.

- Managing innovation on a programme-by-programme, case-by-case basis, by being ready to prioritise valued areas, and searching for technology demonstrators and prototypes with potential in a range of capability applications. The potential of a system or piece of equipment to impact positively the UK’s exports and prosperity should be taken into account. A range of technologies (including those at low, medium and high technology readiness levels) should be supported, and the balance managed between upgrading existing assets and the development of novel capabilities and systems.

- Reinforcing government readiness to work closely with the private sector, taking forward such arrangements as Niteworks and the UK Defence Solutions Centre. If the MoD is to incentivise firms – including small and medium-sized enterprises – to bring their best thinking to defence, it may have to put aside an instinctive preference for competitive tendering and the desire to acquire control over the intellectual property it will use.

- Reviewing the Defence Equipment Plan published in January 2017 to ensure that innovation is a guiding principle for capital investment.

The political stances and developing capabilities of potential adversaries require that the UK consider its role in the world, not least its military links with the Middle East and East Asia. The UK must also, in conjunction with its allies, review thinking about how deterrence and conflict avoidance can be strengthened. The readiness of NATO to explicitly consider escalation to the nuclear level in the face of losses at the conventional level seems like a hangover from the Cold War and looks less appropriate and credible in the contemporary world.

As the UK reacts to the changing vulnerability of many of its forces, an overarching claim of the paper is that, of the seven categories in the Defence Capability Framework (prepare, project, inform, command, operate, sustain and protect), most emphasis should be placed on the last of these: protect.

The paper also offers a four-category approach to the analysis and treatment of specific capabilities and the hardware on which they are based. Summarised as Tolerate, Treat, Transform or Terminate, it is argued that capabilities that face only acceptable risks can be left in place (Tolerate). Other capabilities can be rendered less vulnerable by modest changes (Treat), which is broadly the agenda of the Strategic Capabilities Office in the US. More drastic additions to capabilities, probably taking longer to introduce, fall into the Transform category. Treat and Transform depend significantly on innovation success. Finally, it is recognised that some areas may have to be abandoned (Terminate) and alternative arrangements made, including possible increased reliance on allies.

The effective management of defence has never been easy and has arguably never been so demanding, given the range of challenges on the agenda, the importance of agility in the use of armed forces, and the prevalence of uncertainty and incidence of surprises. The capacity to innovate is a significant aspect of being able to deal with these issues. To maximise the UK’s potential in this area, financial changes, as well as a range of behavioural changes, will be needed.
Introduction

NOTWITHSTANDING THE HUGE improvements in human development and security that mark the contemporary world – most notably the long-term trend of declining numbers of conflict-related deaths,¹ Western states are clearly faced with profound defence and security issues, risks and uncertainties. These include challenges from Russia, China, North Korea, migration, terrorism, low economic growth, rapid change and unforeseen conflicts.

First, Russia’s economic performance since the end of the Cold War has been disappointing. However, President Vladimir Putin’s government has been determined to sustain the country’s ‘great power’ status through the use of the military instrument in Ukraine and the Middle East, and through the exercise of political pressure on the Baltic States, including through cyber operations. The optimism about a ‘new world order’ based on Russian cooperation with the West, articulated by President George H W Bush just after the end of the Cold War, has dissipated.

Second, China has been growing in economic capacity for decades and is now seeking to have that growth reflected in its political power. It has made extensive territorial claims in the East and South China Seas, and its defence efforts underline its ambition to override the US military dominance in East Asia.

Third, North Korea seems set on a confrontation with its southern neighbour and the US, and the potential for miscalculation or misadventure appears significant.

Fourth, the democracies of Europe are faced with major migration challenges as a result of multiple ongoing crises in the Middle East, as well as poverty in Africa.

Fifth, the rise of identity politics associated with extremist Islam is an established security condition in Western cities.

Sixth, Western economies have not regained the confidence or consistent growth patterns that were lost in the 2007–08 financial crisis, and the British decision to leave the EU has increased economic uncertainty, not just in the UK but in the EU as a whole. Meanwhile, the weight of Asian states in the world economy continues to grow.

Seventh, in important parts of the civil, commercial world, rapid change and innovative products have become everyday occurrences, whereas major defence projects continue to take decades to come to fruition and are typically accompanied by inter-generational cost increases.²

Finally, it is important to remember that the world since 1990 has demonstrated a capacity to surprise Western governments, the public and academics with unexpected conflicts. A year before it occurred, who would have forecast UK and international involvement in Kuwait, the former Yugoslavia, Afghanistan, Libya or even Sierra Leone? Thus to assume that there will be no surprise events or operations in the near future would be to disregard the experience of the past 25 years.

Given these challenges, there is a pressing need for decision-makers and commanders to look to the condition of a country’s military, which is, as ever, the final guarantor of a state’s security. The UK is no exception in this regard, and an informal process is already underway for refreshing the country’s Strategic Defence and Security Review (SDSR) following the 8 June general election.

The US response to these external security challenges, and the potential opportunities they could create within the country’s economy and society, manifested itself as the Third Offset Strategy (TOS). In November 2014, then US Secretary of Defense Chuck Hagel made an impactful policy speech to the Reagan National Defense Forum in California and issued a defence memorandum launching the Defense Innovation Initiative.³ These developments were significant because they articulated national imperatives to pursue innovative ways to sustain and advance US military superiority in the twenty-first century in the face of the increasing defence capabilities of potential peer competitor states and the proliferation of disruptive capabilities across the spectrum of conflict. To recover US strategic comparative advantage, Hagel stated that:

> The US changed the security landscape in the 1970s and 1980s with networked precision strike, stealth and surveillance of conventional forces. We will identify a third offset strategy that puts the competitive advantage firmly in the hands of American power projection over the coming decades.⁴

There was no clear blueprint for the TOS. Indeed, in many ways it was more a challenge to US government and business than a comprehensive national strategy. The stated aspiration was to drive and accelerate innovation in defence technology, military practices and organisation, and in capability generation processes. Implicit within the TOS was the notion that wide-ranging global technological advances presented significant opportunities for US defence.⁵

---

⁴ Hagel, ‘The Defense Innovation Initiative’.
Since early 2016, when the research for this paper began, a new president has been elected, and a new administration installed, in the US and so it is unclear whether the term ‘Third Offset Strategy’ will survive in US government parlance. However, we do anticipate that, once gaps in readiness and a policy update have been addressed, the Trump administration will turn its attention to widening the narrowing gap between its military capabilities and those of its potential adversaries. The new president’s enthusiasm for higher defence spending is clear and we assess that an ongoing initiative that builds on TOS principles is highly probable.

This paper addresses the implications of the TOS critique and prognosis for the UK, and explores how Britain might react to the developing capabilities of potential adversaries in the areas where its technological superiority is being eroded.

The Research Approach

Reflecting developments in the governments of Russia, China and others, the TOS was centrally concerned with peer-to-peer deterrence and with conflict in contested environments where manoeuvre or access is denied or restricted. This paper shares that limited focus, and so it does not consider counterinsurgency (COIN) or counterterrorist (CT) operations. In undertaking their research, the authors adopted the following three-tiered approach:

- A review of US policy relating to the TOS.
- A literature review of commentaries and analyses relating to TOS.
- A series of colloquia that involved discussion and analysis relating to defence innovation and technological exploitation.

The initial focus was on the policy narrative emanating from the US suggesting that its technological advantage in defence had been eroded across a number of key capability areas – that peer and near-peer adversaries could or would soon match certain US – and thus Western – capabilities on the battlefield, thereby denying Western forces the freedom to operate. Specifically, it raised concerns that key Western military assets had become vulnerable to targeting and disruption/destruction by long-range precision missiles to a degree that had hitherto been unthinkable, and that the space-denial capabilities of peer and near-peer adversaries risked threatening critical navigation and communication capabilities. The extensive study by Robert Martinage, of the Center for Strategic and Budgetary Assessments, addressed these issues in depth. Attention then turned to a systematic review of the generalist and specialist literature relating to defence innovation, technology insertion and the TOS, much of which informs this analysis.


The subsequent focus was on capturing and analysing the outcomes of a series of three full-day colloquia, organised by RUSI, that addressed the ‘why’, ‘what’ and ‘how’ of the TOS. The significance of the workshops was that they provided the first expert review of the considerations and consequences of TOS-type thinking for UK defence planning and capability generation. The workshops were held between November 2016 and March 2017 and each built upon the outcomes of the preceding event. They were held in plenary session with a combination of discussions and commentaries addressing a structured set of stated aims. There were 32 participants, representing stakeholder interests from across the UK government, the military and industry, with specific high-level representation from the US. Participants were chosen for their thought leadership, knowledge and influence, with the series being independently chaired by Lord Arbuthnot of Edrom.

The issues associated with this approach revolve around the following areas. First, while the work has been informed heavily by government officials and military leaders, both from the UK and the US, there is no official government endorsement of the approach or findings. Second, the work is limited to the insights and suppositions of those involved, and so there is a risk that certain views have not been aired. Third, the work is located in a very particular moment of the debates relating to force generation, technology insertion and capability sustainment. Despite these limits, the research led to some novel findings, insights and suggestions, and brought home the urgency of the need for the UK to deal with the challenges of potential adversary states.

The paper first gives a brief summary of the dimensions and implementation to date of the TOS, before proceeding to its first major finding: that the vulnerability of many British platforms and capabilities is real and growing. This leads into an analysis of the UK’s own Defence Innovation Initiative (DII), which came out of the 2015 SDSR, followed by an examination of the challenges associated with sustaining the ‘innovation culture’ in the British defence enterprise, which is viewed as necessary for the success of the DII.

The paper then offers a series of suggestions for the future development of UK policy and practice, including the value of greater clarity on conventional deterrence, and of increased emphasis on protection for major platforms. Finally, in terms of how the UK should deal with the increasing threat context, the paper offers a four-stage process in which capabilities, and the hardware they rest on, can be addressed: it discusses the options of tolerating any vulnerability, treating a capability with modest change and transforming a capability. Terminating a capability is the fourth and final option.

I. The Third Offset Strategy

THIRD OFFSET IS an odd term, and it comes out of a particular historical context. ‘Offset’ is the term used in the context of nullifying an adversary’s advantage. The US First Offset Strategy was developed by President Dwight Eisenhower in the 1950s and emphasised enhancing tactical and strategic nuclear weapons to deter the stronger conventional forces of the Warsaw Pact.¹ The Second Offset Strategy referred to Secretary of Defense Harold Brown’s initiative in the mid-1970s, which provided the impetus for the procurement of the majority of the US capabilities that are fielded today, as an offset to the defeat in Vietnam. So the TOS today, in the middle of the current decade, has a claimed lineage that can be traced back to just after the Second World War.²

The transformation envisaged by Secretary Hagel implied the prospect of a step change in strategic capability over a decade or so. This would, potentially, reinforce and enable the US to maintain its global military hegemony in the face of the ambitions and rivalries of other powers. This change was to be based on much more than anticipated technological developments. Indeed, technology was just one of five areas seen as having the need and chance to change: in addition to R&D, Hagel referred to leadership development, wargaming, operational concepts and business practices. Expanding on this at a RUSI event in September 2015, Deputy Secretary of Defense Robert Work outlined how TOS implementation could strengthen conventional deterrence and operations in Europe:

Large units aren’t going to survive on those battlefields. They’re going to have to disaggregate … Smaller units are going to seek sanctuary where possible that try to operate outside the major guided weapon ranges of the enemy. But when they can’t, they’re going to have to disperse over wider areas.³

Moreover, the US Department of Defense committed to increasing its efforts in the area of innovative wargaming in order to gain insights into the future requirements associated with disruptive technologies. In parallel, the manner in which new leaders are developed, so that they demonstrate the ability to innovate instinctively, remains a key focus for future training and education programmes.⁴

A doctrinal or strategic basis for the TOS was, in part, the 2014 study by Robert Martinage of the Centre for Strategic and Budgetary Assessments, an independent think tank. Martinage discussed the threat of (conventional) deterrence and denial approaches to US policies and options, most

---

² Martinage, ‘Toward a New Offset Strategy’.
obviously by adversary states.⁵ He saw US forces as too oriented towards operating in low-threat environments, warning that the future need was to be able to operate within the context of medium- and high-threat scenarios. He recognised that asymmetric approaches should be an element of US strategy and advocated in very broad terms that current systems, which were increasingly vulnerable to a capable adversary, should either be significantly hardened in terms of defences or should have less reliance placed upon them.

The TOS was compatible with, and even situated within, the overall framework for improving defence acquisition in the US – the Better Buying Power (BBP) programme, which dated from 2010. Originally stressing the need to improve the professional knowledge and skills of acquisition professionals and the importance of affordability and cost control, BBP 3.0 added a commitment to strengthening innovation and technology:

> The technological superiority of the United States is now being challenged by potential adversaries in ways not seen since the Cold War ... We will continue our work to improve productivity and efficiency, but we must also turn our attention increasingly to our ability to innovate, achieve technical excellence, and field dominant military capabilities.⁶

Overall TOS thinking focuses on perceived growing vulnerabilities associated with land bases, surface ships, aircraft and space systems. It offers a prompt to reform the way the US delivers defence capabilities to meet the perceived challenges of a profoundly changed threat environment. The implication is that the US and its allies may find that their current systems, hi-tech though they may be, to be of limited relevance. It suggests that tomorrow’s threat response may be offered by capabilities that look very different to today’s (costly) maritime, land and air platforms and their associated networks.

The US recognises that its close allies cannot commit the level of investment necessary to match the funding of American defence and security research. It thus sees them as potential customers for US-funded advances, although it has also recognised that there is no American monopoly on military-applicable advanced technologies: in principle, the US is open to offers of contributions from allies, but retains a strong general preference for domestic supply. However, the changing threat context identified by US decision-makers extends to UK and other allied forces, which face a comparable future operating threat context.⁷

---

Any external reaction to the TOS has to address its two key assertions: first, about the projected advanced capabilities attributed to Russia, China and other potential adversaries; and, second, about the feasibility of innovation generating step-level changes in capabilities. It is to the first of these issues that this paper turns next.
II. The Reality of Vulnerabilities

This paper finds that the advancing capabilities of potential adversaries of the UK should be a genuine concern. As underlined by the former director of policy planning for the office of the NATO secretary general, Fabrice Pothier, the weight of evidence in the public domain supports the view that Russia and China have developed the surveillance and precision strike capabilities to put at serious risk Western surface ships, large military aircraft and arguably any land system, even the most heavily armoured.1 This was also the view of the participants at the RUSI workshops held as part of the research for this paper. Moreover, the range of Russia’s anti-ship and anti-air missiles is extending.2 The Russians have been focused on developing their ground-based anti-air defences for a long time, and the sensor and missile ranges are now able to reach the areas where large Western aircraft – such as command and control and surveillance assets – have traditionally operated. It seems therefore that the main driver behind the TOS was not the need to secure more defence funding from the US Congress.3

These developments should not be a surprise since Western countries acquired similar capabilities almost 20 years ago. Indeed, China’s recent claims to have developed a J-20 stealth fighter4 must be seen in the context of the US operational use of the F-117 stealth fighter in 1991, by which date the US also had long-range cruise missiles and the Patriot anti-aircraft system. It would be naive to expect that Russia and China are not where leading NATO states were three decades ago.

The UK’s potential adversaries have also focused on developing relatively inexpensive weapons that can disable or destroy expensive assets. Western governments have become acutely aware of the problems of this financial imbalance in the counterinsurgency context, when they found themselves using weapons costing $70,000, sometimes fired from aircraft that cost $30,000 an hour to fly, to destroy a Toyota pick-up vehicle that might be optimistically valued at $10,000.5 But in the inter-state context similar considerations are present: missiles costing (much) less...

---

3. For instance, in his TOS launch speech in November 2014, Hagel appealed to Congress to work with the administration on financial matters and take away the possibility of sequestration. See Hagel, ‘Reagan National Defense Forum Keynote’.
5. Quoted by a US official at the RUSI workshop in March 2017.
than half a million pounds a unit could at least disable a British aircraft carrier that costs more than £3 billion. Indeed, a salvo of ten such missiles would cost less than $5 million. There has been a growing imbalance within the attack–defence military equation, driven by the spread and speed of applicable technologies. For example, Iran has long held anti-ship missiles from Russia and has claimed to have developed its own Hormuz-2 supersonic, ballistic anti-ship missile. These weapons must be seen as a key contextual element of British naval deployments in and near the Gulf. In summary, China and Russia appear to have focused many (but not all) their efforts on being able to put at risk the key Western assets that are large, few in number and expensive.

A core point is that the US and the UK are powers that must deploy their forces away from home in order to provide assurance to their friends and allies, to deter aggression and prevent conflict. In contrast, their potential adversaries operate largely from their home territory. Certainly since 2010, the Russian government has been seeking to roll back Western influence, most obviously in Ukraine and the Baltic States but from, principally, home bases. In the Gulf, Iran is working to reduce the presence and influence of the West and has land-based anti-ship missiles. In Asia, the US dominance now being challenged by China has been a framework in which the whole region save North Korea has experienced sustained development. Thus, although the US spends much more on defence technology development than its potential adversaries, its better technology does not necessarily translate to proportionate military advantage in a specific theatre.

The potential adversaries of the US and other NATO states are also concentrating on being able to disrupt the collection and exploitation of information by Western governments, through cyber and even anti-satellite capabilities. Cyber is particularly appealing to the West’s rivals since the development of significant capabilities does not require a large capital investment or the wide-ranging knowledge base needed, for instance, for the development of a new combat aircraft. Clearly, the actual distribution of cyber capabilities across the world among governments, private bodies, criminal organisations and motivated individuals (who may act in groups) is not known. It may well be that the US and even the UK governments are much more powerful than any potential adversary, but evidence in the public domain about the incidence and success of some attacks strongly implies that there is no room for complacency. The cyber threat spectrum is not only relevant to defence but to government as a whole, especially to critical national infrastructure and the broader economy. As such, it requires different management and investment arrangements than those associated with the traditional defence portfolio.

Then there is space, where the UK has a significant satellite-building capability and makes extensive military use of space for surveillance, communication, intelligence and navigation, including the control of missiles flying within the atmosphere. The Outer Space Treaty of 1967 puts few constraints on what can be done in space: it only commits its signatories not to base

---

weapons of mass destruction there.\textsuperscript{8} Space assets are vulnerable to electromagnetic and physical attack that could – for example – destroy or degrade navigation and communication systems. The most prominent demonstration of a desire for anti-satellite capabilities was the Chinese test destruction of a satellite in 2007. Since then, there have been multiple reports of Russia seeking anti-satellite capabilities, including an airborne laser system.\textsuperscript{9} There are some fears that China would launch a mass attack on US satellites as the initial step in a major war.\textsuperscript{10} In basic terms, the development of exo-atmospheric anti-ballistic missiles is inevitably generating a capacity to destroy satellites, as the US showed when it destroyed its own malfunctioning satellite with an SM-3 missile in 2008.\textsuperscript{11} Whether any state would use an anti-satellite system in anger is debatable, but the inherent vulnerability of satellites, including those of the UK, is not.

The increasing vulnerability of surface ships and large airborne platforms, not to mention land force formations, has to be viewed in the context of not just what would happen in an all-out war, but also in the more likely scenarios of crisis and confrontation. Despite the vulnerability of surface ships, China and Russia are, after all, continuing to construct them. In its current confrontation with Japan over the Senkaku/Diaoyu Islands, key Chinese assets are very low-technology fishing boats crewed by militias, backed up by offshore patrol vessels from the China Coast Guard.\textsuperscript{12} The Chinese-built islands in the South China Sea could easily be destroyed by Western forces, but their presence continues to have strategic value for Beijing. Therefore responses to Russian and Chinese challenges must embrace diplomatic and commercial themes as well as the components of actual warfighting capabilities.\textsuperscript{13}

In short, while inter-state confrontations have a primarily political nature, in which the psychology of deterrence and dissuasion must be addressed, the increasing physical vulnerability of many platforms and systems needs to be noted and responses generated, not least for the US with its role of security guarantor for a large number of countries.

\textsuperscript{11} Ibid.
\textsuperscript{12} Example offered by UK contributor at the workshop in November 2016. See also Ryan Pickrell, ‘China Has a Covert Naval Fleet Disguised as Fishing Boats’, Business Insider, 8 June 2017; Megha Rajagopalan, ‘China Trains “Fishing Fleet” to Sail into Disputed Waters’, Reuters, 30 April 2016; Simon Denyer, ‘How China’s Fishermen are Fighting a Covert War in the South China Sea’, Washington Post, 12 April 2016.
\textsuperscript{13} See Jerry Hendrix, ‘Retreat from Range: The Rise and Fall of Carrier Aviation’, Center for a New American Security, October 2015.
III. An Emerging UK Response

During the course of their research, the authors found no public admissions by the Ministry of Defence (MoD) about the current or emerging vulnerability of UK platforms and large systems. Privately, among some senior military personnel, the narrative is very different. Moreover, so far in twenty-first century defence, R&D, a key enabler of technological innovation for improved protection, has not been a priority for the MoD. In real terms, the defence budget as a whole was almost the same size in 2015/16 as it was in 2002/03. In that period, R&D spending was halved, research spending alone fell by 27% and development spending by 56%.1

However, the 2015 SDSR called for ‘greater innovation and efficiency’ and featured commitment to the Defence Innovation Initiative (DII) backed by £800 million of investment over a ten-year period.2 When launched in September 2016, the British DII comprised the following:

- A new Innovation and Research InSight Unit to ‘draw on horizon scanning and market intelligence from across government, academia, industry and international partners’.3
- A Defence and Security Accelerator organisation to ‘accelerate ideas from conception through to application’, by linking suppliers and inventors with users and investors.4
- An Innovation Fund ‘of around £800 million over 10 years, to provide the freedom to pursue and deliver innovative solutions’.5

Since the UK’s equipment procurement plan for the decade from March 2016 totalled £82 billion,6 the innovation budget of £800 million was about 1% of the procurement spend.7 Consequently, ensuring that this innovation fund is meaningfully invested is an important challenge for the MoD and the broader defence community. The hope is that the £80 million a year could act as a trigger for greater exploitation of the annual defence science and technology (S&T) budget

5. Ibid., p. 13.
7. This section of the paper was informed by independent research undertaken by Simon Jewell, Managing Director of Niteworks.
of about £400 million. This, in turn, could trigger a greater focus on technology earlier in the equipment plan. The UK's S&T and innovation effort, in this model, would underpin capability development investment within the equipment plan (see Figure 1), rather than sitting aside it as a parallel activity. So each component triggered by the Innovation Fund – the MoD investment in science and technology, the MoD Equipment Plan and the vast and unquantified commercial R&D expenditure – is leveraged, potentially, by the preceding, smaller investment. These four financial strands of innovation become symbiotic within the UK defence enterprise unlocking future capabilities.

**Figure 1:** Spend Figures Per Annum

![Diagram showing financial strands](image)

Source: Authors.

The MoD, like the US Department of Defense, aspires to exploit technology from other government departments and businesses, where the volume of R&D spending is much greater. There is also an international dimension in the MoD's aspiration to be an 'open innovator'. The

---

key here will be to deliberately leverage R&D investment and innovation from the private sector, wherever a company is headquartered, through a focus on experimentation and technology demonstrators and prototypes\(^9\) within the equipment plan.

The MoD should not hope for the private sector to lead on very early stage innovative work: as Mariana Mazzucato, of the University of Sussex, has demonstrated, even in the civil world businesses rely heavily on government spending for the basic research that cannot be associated with a profit opportunity.\(^10\)

The private sector of interest to defence can be divided broadly into two: businesses currently serving defence; and those that are civil and commercial in orientation but which have products of potential for defence. With regard to the latter, the MoD must be aware that the technology involved might also be available for exploitation by potential adversaries. The MoD also needs to be clear on how it is to attract such firms into the defence sector, especially if adoption by defence may result in the application of export controls and possible constraints on future business opportunities. Also, MoD commercial staff in particular needs to be aware that the increasing insistence by the ministry that it secure the use of intellectual property rights from suppliers is a real disincentive for either private sector investment in defence science and technology or for commercial firms to make their innovations available to defence. In the civil world, business customers would not make such demands on their suppliers.\(^11\)

Next, as was emphasised by the RUSI working group members from industry, in all commercial organisations, investments in S&T and R&D require a business case presenting a significant prospect of a rate of return. That private S&T and R&D spending from the defence industrial sector is limited is an indicator that industry is either receiving limited information from its main customer, or it has little confidence in the information it does get.\(^12\) With these qualifications, the UK DII could be a smart response to the recognised need for innovation, but it has to work programmatically as well as conceptually. The programme perspective has several implications, of which the first is the readiness to prioritise effort: an organisation with an adaptive, innovative culture prioritises and settles on key capabilities where it wishes to excel, while having partners to assist with, enable and provide less critical components.

\(^9\) The Oxford English Dictionary defines a prototype as ‘[a] first or preliminary version of a device or vehicle from which other forms are developed’, <https://en.oxforddictionaries.com/definition/prototype>, accessed 6 July 2017. In defence and the wider economy they are used to reduce risk and generate confidence that a set of components can be assembled and integrated to deliver performance of a desired standard. With a prototype, manufacturing costs and challenges as well as reliability performance are often not well understood, and a prototype is usually required to be capable in just a few key and risky areas. For instance, when Boeing and Lockheed built competing prototypes for what is today the F-35, their machines had to demonstrate a capability to take-off vertically, but there was no emphasis on the performance and integration of their envisaged sensor suites. For more detail see PBS, *Nova*, ‘Battle of the X Planes’, 4 February 2003, <https://www.youtube.com/watch?v=B7-LQDueYIk>, accessed 5 July 2017.


\(^11\) Input from RUSI workshop participants, January and March 2017.

\(^12\) Input from RUSI workshop participants, March 2017.
An elegant idea is meaningless unless it is owned by the many and can be implemented. In particular, there needs to be funding so bright ideas from S&T research can be carried through development and into products. This will require a collaborative culture and mindset: characteristics that are easy to articulate but very difficult to engender.

An Innovation Culture

The government has recognised the place of organisational culture in support of, or as a hindrance to, innovation. The UK MoD states that its core principles of innovation are:

- A broad and systematic approach that seeks to embed innovation throughout the Department’s organisation, workforce, process and culture and includes better integration of military concepts, emerging technologies and capability development.
- A culture that is ‘innovative by instinct’ by incentivising and rewarding innovative behaviours that we value. Such a culture emphasises the willingness – indeed expectation – to accept risk responsibly across the enterprise.
- An open innovation “ecosystem” that capitalises on innovative expertise at the MOD and other national security departments and builds effective, efficient and fertile partnerships with innovators in industry and academia, as well as with key allies and partners.
- The ability to accelerate promising innovations from idea to solution, quickly and affordably.
- A strategy-driven approach that provides clear strategic direction to the Department, the component parts of which will remain primarily responsible for delivering innovation.¹³

These are important principles – but innovation is not a management intervention but a mindful and permanent state of being more akin to an organism than a manufactured item. It is disruptive and messy, so that speed and partnership with others can require acceptance of the risks of giving up options of competition among suppliers in some, perhaps many cases. It will also require the MoD to talk openly with trusted suppliers about the nature and severity of emerging threats.

An organisation can set the conditions for innovation but it can never ‘deliver’ it on demand.¹⁴ This is critical, since the MoD is relying on innovation to meet what it perceives to be near-term threats. The stated UK defence challenges are to:

- Project military power against sophisticated adversaries.
- Influence potential adversary choices on terms favourable to the UK.
- Deliver non-traditional and novel ways to have effect beyond traditional weapons systems against sophisticated adversaries.
- Understand and take effective decisions in the Information Age.
- Adapt with agility to anticipated changes in the strategic environment.
- Maintain robust strategic deterrence into the future.
- Optimise the future workforce to meet anticipated needs.¹⁵

Building on this, Defence Equipment and Support, the MoD’s trading body, published a document on innovation strategy in October 2016 stressing the organisation’s role in bringing technological change quickly into defence, and also its responsibility to demonstrate a readiness to change its own ways of doing business in order to become more efficient and effective. It thus addresses both technological and process innovation.\(^{16}\)

While the 2015 SDSR acknowledged the importance of innovation and the MoD has issued its innovation initiative, other key documents give it but a modest place. First, the MoD’s Global Strategic Trends document, covering the period to 2045, has forecasts about the development of laser, directed energy and even biologically targeted weapons, but there is little sense that an era of rapid innovation may be underway or needed.\(^ {17}\) Second, the official How Defence Works guide mentions innovation once but in the context of process rather than technology: it refers to ‘a culture of innovation and efficiency, removing needless process and flushing out bureaucracy’.\(^{18}\) Finally, the UK Defence Doctrine discusses innovation on just three of its 70-plus pages, the first of which treats the conceptual dimension as a solved problem, arguing that ‘the conceptual component is also updated by conceptual innovation, capturing how our thinking changes over time in response to new technologies, structures and challenges’.\(^{19}\) The second reference, in the context of the stressed centrality of the adaptability of the human being, simply asserts that ‘commanders should also champion innovative practice’,\(^ {20}\) while the third, in order to support dealing with the unexpected, makes clear that UK forces should be able to ‘adopt the latest technology and systems’. The overall tone of BDD is that people are normally more important than technology.

As the MoD moves to embrace innovation more prominently, there is a need for recognition, perhaps at the public policy level, that innovation usually involves losers as well as winners, since the change it engenders disrupts existing organisations and people. Such disruption is one of the reasons why history shows many cases of militaries – including the UK’s – being reluctant to adapt to new possibilities.\(^ {21}\) At present, the fact that the desired sizes of the armed forces are laid down in legislation places limits on how the MoD can seek to shape the Whole Force and the balance of spending on people and other elements of defence. Should the size of the armed

---

20. ibid., p. 38.
forces be freed up, the MoD would be liberated to innovate, but obviously some long standing organisations would find themselves losing out. Similarly, the UK wants its forces to be ‘full spectrum’ by 2025, but innovation could – and perhaps should – involve more specialisation and explicit dependence on allies for some functions. Indeed, what ‘full spectrum’ means today may well change by 2025 and will definitely have a different meaning by 2040: a state may not be able to field all capabilities that are important for a particular operation and so may well be dependent on allies at a particular moment.

Innovation also usually involves a good deal of experimentation and failure, with the body of literature seeming to suggest that organisations should aim to experiment a lot, diagnose prospects at an early stage, abandon the failing before too much money has been spent and always learn lessons. This involves a greater readiness to write off public money than appears to be present in UK political culture. Policy disclosure of governmental readiness to accept the risks of an emphasis on innovation would be a prior condition for changed attitudes across the defence enterprise and broader society, and especially perhaps within the House of Commons Public Accounts Committee.

Next, if the MoD is to build a sense of both the need and opportunity for innovation across the defence enterprise, it needs to build confidence among current and potential suppliers that funding will be available to take ideas through to production. As of 2017, the limited unallocated defence funds – those not allocated to a particular project – cannot be a source of assurance that the MoD will have the funding to take an idea through to deployment. As one of the RUSI workshop members observed: ‘In a dynamic business, operating in a competitive environment, I’d expect to see far more capital expenditure flexibility built in the future years’.

The difficulties of building an innovation culture across defence should not be underestimated, not least because the armed forces rely so significantly on tradition and past practice for the construction and maintenance of motivation and commitment. Private companies often find it hard to move from established ways and products, as the extensive literature on ‘change management’ reflects. The fact that the risks in the military include asking people to put their lives at risk may also strengthen soldiers’ wariness of radical change.

---

23. For the UK’s reliance on US assets in the Libya campaign of 2011, see The Economist, ‘A Troubling Victory’, 3 September 2011; Chris Brown, ‘While the UK and Europe can be Proud of their Role in Libya, there was a Dependence on US Support and this Cannot be Relied upon in Future Conflicts’, LSE British Politics and Policy Blog, 2 September 2011.
24. For a discussion on innovation and agility within this context, please see Maritza van de Heuvel, Joanne Ho and Jim Benson, Beyond Agile: Tales of Continuous Improvement (Seattle, WA: Modus Cooperandi, 2013).
However, a disciplined programmatic approach – looking at a series of activities and projects as a whole as well as individually – can reduce some of the hazards intrinsic to a focus on innovation. In particular, this promotes a readiness to prioritise and to manage risks: a body with an adaptive innovative culture assesses and decides on key capabilities where it wishes to excel, relying on partners to source and provide less critical components. Concern with exports and the potential for defence contribution to the prosperity agenda should be part of the prioritisation process. There must be a readiness to experiment and prototype in areas where technical demonstrators can feed multiple areas of capability. This is a particularly visible approach in the pharmaceutical and material extraction sectors, from which defence can learn. Prudence directs that investment is balanced across a range of younger and more mature technologies. Currently, the MoD concentrates on technologies with high readiness levels, but a balance with emerging and adaptive technologies might offer greater utility. The programme perspective also suggests that defence, even with prioritisation, should not put too many eggs in a single basket. For example, in the US there has been some warning against focusing excessively on artificial intelligence and the man–machine interface as the basis for the TOS. It has been argued that innovation requires a readiness to explore more widely. Balance is also significant in looking both to enhance extant assets and the development of entirely novel capabilities and systems. Finally, users of decision-making processes must be ready to demonstrate agility. For example, the formal sequential Initial and Main Gate processes may not always be quick enough.

To summarise the argument so far, changing threats to US military platforms and capabilities have prompted Washington to accelerate innovation in defence, which seems likely to continue into Trump’s presidency. The threats to US forces are extremely relevant also to those of the UK, which has responded with its own Defence Innovation Initiative. This has been launched with some funding, but there is also recognition that the UK government defence establishment, and arguably the wider defence extended enterprise, must strengthen the place of innovation in organisational culture if change is to be optimised and delivered.


29. Initial Gate occurs in the MoD to release funds for the Assessment Phase of a Capability. By the end of this phase, through which up to 15% of the initial procurement costs of a system might be spent, a Main Gate Approval is required before any resources can be committed to a Demonstration Phase. For Main Gate, a single technological and procurement option should be recommended.
The paper now turns to more specific fields of activity and to a comprehensive approach to dealing with capability development in the future.
IV. The SDSR, the UK’s Role in the World, and Innovation

The UK’s need for defence innovation should reflect the role the country chooses for itself in the world and the demands of its corresponding defence policy. A 2017–18 refresh of the SDSR would have dealt with this, but the June 2017 election result has resulted in disruption for many areas of government planning. It is argued here that the British ambition to be an international, even global, military actor has been explicit since the 1998 Strategic Defence Review. The same applies to the UK’s established aspiration to be the major international military partner of the US, able to operate alongside the US from the first stage of a major operation. The UK commitment to NATO could be viewed as set in concrete, which implies that the UK must be concerned about any Russian threat to other NATO members, most problematically in the Baltic region, including in the waters of the North Sea. With regard to Russia and other potential adversaries, it is important to think primarily about deterrence rather than forecasting ‘how the next war will be fought’, as though such a conflict were inevitable. However, deterrence, as a concept, must address explicitly what would happen if fighting broke out.

During the Cold War, the West always saw the threat of escalation to the nuclear level as the key element in the deterrence of the Soviet Union and the Warsaw Pact. That was acceptable to most of NATO’s populations because the threat was that the USSR would seek rapidly to overrun Western Europe. Today, that ambition is not apparent in Moscow, and Western concerns in Europe are more about Russia’s threat to the Baltic States and Poland than to Europe as a whole. In this situation, Western deterrence and dissuasion now rely overwhelmingly on conventional forces and even non-military instruments. It also leaves a space for uncertainty in the minds of adversaries over what would happen if fighting broke out. The concept for deterring Russia is obviously a matter for NATO as a whole, but that needs to be reconciled with the UK’s view of its nuclear force’s role.

Of course, in international politics, deterrence is a much analysed and considered topic. Deterrence policy needs to be cognisant of the following points:

- Since deterrence involves the psychology of an adversary, each targeted state or government should be countered by a bespoke package of threats and capabilities. What would deter China might not work with Iran.
- Any increased reliance on the threat to escalate to the use of nuclear force is likely to provoke strong opposition from within the UK and Western populations. A deterrence stance needs to be continually in the public domain and command a broad base of popular tolerance.
- Uncertainty about the eventual outcome of a conflict should reside in the minds of adversaries. Enemy states should not be allowed confidence that they can control the
order and drumbeat of conflict. In the modern epoch, capabilities that deny an adversary the likelihood of a quick victory or a conflict fought on his terms might be expected to contribute significantly to notions of deterrence.

- Effective deterrence should be based on the threat to destroy or degrade the key assets of an adversary, be they military, economic, societal or personal. Intelligence on the identity, location and significance of these key components should be highly valued.

However, conventional deterrence, not involving nuclear threats, is recognised as a difficult subject, both conceptually and in practice. Its precise formulation needs to be done on a case-by-case basis. Deterrence relationships that are one-sided, with only one side feeling inhibited, are less likely to be stable than in a mutual deterrence construct (such as that which operated at the nuclear level during the Cold War). Deterrence of a significant, but limited, form of Russian aggression would arguably require Moscow to believe that its forces would be highly likely to suffer conventional damage. However, it would also require them to believe that there was a real risk that the conflict might escalate and spiral out of control.¹

**Defence Capabilities Framework**

If the need to innovate is accepted, a subsequent question arises: what should the focus of innovation efforts be? Improved protection has a strong claim to be the answer.

Clearly, systems that cannot easily be destroyed by an adversary have stronger and more direct deterrence impact, and it is important that UK systems have their vulnerability minimised. At the conceptual level, the Defence Capabilities Framework (DCF) has been a valuable aid to capability-based defence thinking, which, in turn, supports the optimum exploitation of technological opportunities and reduces the likelihood of inappropriate ‘replacement thinking’, in which it can easily be assumed that one ageing system should be replaced by something better but similar.² The DCF in British Defence Doctrine classifies all defence capabilities into seven domains: the ability to *project* to the needed area, and then to *inform*, *command* and *operate*. There must also be a capacity to *sustain* activity. None of this is possible without the opportunity to *prepare* forces. Finally, all these elements must be as invulnerable as possible to hostile action, so the requirement to *protect* should be seen as an overarching – rather than just another – element of capability.³ This would be to put into defence as a whole the recommendation for the cyber sphere made by Alec Ross, a former adviser to the US secretary of state: ‘With the evolution of more of our life into zeros and ones and the rise of the Internet

---

2. See MoD, *British Defence Doctrine*.
of Things, cybersecurity needs to be accounted for as a central feature in all the products being developed and commercialized for tomorrow.\textsuperscript{4} In many ways, this stress on protection could be recognised as the subtext of all TOS-type thinking. As a reflection of the neglect of the protect function in at least elements of the US, Colin Clark has claimed that US Transport Command has not factored into its plans ‘the possibility that transport ships would be sunk and transport planes would be shot down’.\textsuperscript{5} Thus the ‘protect’ function in the DCF should be given increased priority in the direction and development of military requirements.

**Achieving Protection**

How is protection to be attained and what should be the main focus of the TOS response? Protection can be achieved in many ways, not least by being more mobile and agile and by being less conspicuous. One possibility is to accelerate development of rapid-fire defensive weapons that can deal with a large number of targets and do not require extensive ammunition stores. Lasers and electromagnetic railguns top the list of candidates, but Deputy Secretary of Defense Robert Work has argued that the key to overall effective defence will be the teaming of people and intelligent machines to survey, track and destroy threats.\textsuperscript{6}

Networks, their integration and dominance on the battlefield, are to be strengthened still further. The argument that an information-based approach to operations should be driven to an even higher level must address how cyber and anti-satellite capabilities – that are the focus of Russian and Chinese efforts – are to be interdicted. Assuming that the UK wishes to maintain its forces as interoperable with those of the US from the early stage of a major operation, there is a need to think about how British forces can join in with, and even contribute to, American networks.

This paper now turns to four particular forms of defence change associated with adaptation to the emerging threat situation.

**Tolerate, Treat, Transform, Terminate: Deliver the Effect to Meet the Threat**

A government needs to maintain and amend its defence capabilities so that they are both effective against adversary behaviour and relevant to the evolving security context. In recent decades the focus on COIN and CT operations has seen the rapid evolution of UK capabilities to maintain effectiveness against a dynamic insurgency and terrorist threat. Arguably, this meant less focus on high-end warfighting capabilities, including those capabilities identified by TOS-type thinking as potentially vulnerable to today’s evolving peer threat environment. However, today, peer challenges are increasingly prominent and, as noted previously, the UK’s conventional deterrence posture relies inextricably also on maintaining credible capabilities

---


\textsuperscript{5} Clark, ‘Not Enough C-17s, Tankers or Ships for Hot War: TRANSCOM’.

that are not regarded by adversaries as being easily overmatched in a contested anti-access/area denial (A2/AD) environment.

This paper explores a T4ET framework (Tolerate, Treat, Transform, Terminate: deliver the effect to meet the threat) that might provide a means of assessment and action across the capability spectrum. The framework presupposes that the objective is to maintain credible effect against the threat, both today and into the foreseeable future, while considering all Lines of Development required for the delivery of a credible capability. The framework examines capabilities on the basis of two factors located in the thinking articulated earlier in the paper: the survivability/protection of a capability in a modern and future contested A2/AD environment against a peer adversary and the ability of a capability to deliver meaningful effect in that threat environment. The framework posits four potential courses of action: Tolerate; Treat; Transform; and Terminate following the Effect to Threat assessment.

The first course of action and the most straightforward is ‘Tolerate’. This describes capabilities judged to be maintaining their effectiveness against peer threats today and require little or no change to be able to maintain superiority into the foreseeable future. In some cases, these will already have the ability to evolve intrinsically built into the capability – for example, the envisaged ability of the F-35 to adapt over time to new threats with new weapons and its software-defined, fused sensor systems.

The second course of action, ‘Treat’, is a key area for consideration and one in which the US has invested significantly through the Strategic Capabilities Office. This category acknowledges some deficiencies in a capability today against the peer threat, but is able to envisage changes or enhancements that may be made to the current capability to either re-establish its superiority or change its function in the battlespace. The Treat action is particularly apposite for platform capabilities that may be becoming increasingly vulnerable. An obvious area is the improvement of self-defence capabilities. Maritime platforms, for example, may need to consider greatly enhanced abilities to defeat salvos of incoming precision missiles through the use of directed energy weapons. Networking may provide the key to building self-forming, self-healing multi-layer networks to combat the compromise of space-borne communications. The possibilities arising from manned–unmanned teaming or ‘combat teaming’ could adapt the utility of platforms unable to penetrate an A2/AD environment, allowing them to remain effective – for example, remote mine countermeasures delivered by unmanned underwater vehicles, or the control of unmanned air vehicles by manned command platforms.

‘Transform’ refers to the adoption of novel emerging technologies. This category links very closely to the science and technology programme, and harnessing of advanced commercial

---

technologies. While the Treat category might be seen as adapting what already exists to maintain relevance, ‘Transform’ focuses on new capabilities designed specifically to deliver decisive change in the contemporary contested A2/AD environment. Central to this is the need to ensure that sufficient resources can be reallocated within constrained budgets to fund transformational capabilities. The nature of transformational capabilities is such that their development requires the more experimental and innovative mindset and suitably adjusted risk-appetite outlined above.

Areas that are widely considered to be key areas for future transformation include artificial intelligence, autonomy, cyber and electromagnetic capabilities, electronic warfare, signature reduction, ISR (Intelligence, Surveillance and Reconnaissance) gathering and associated processing, exploitation and dissemination, directed energy weapons, hypersonics, resilient networking and secure communications. All these areas require significant resources to mature lower Technology Readiness Levels (TRLs), experiment in military application and further mature into a deliverable capability. The transformational nature of these technologies often challenges existing concepts, doctrines and force structures, and so they require a holistic approach across all the Lines of Development. It is not enough simply to acquire a new piece of hardware – the right sort of people who can be trained to use and maintain it must be recruited and prepared; existing infrastructure may not be adequate; the use of one equipment must be linked into how other assets are used in concepts of operations; new organisational structures may be needed and so on. As a specific illustration, in 2017 the make-up of the Royal Signals branch of the British Army is being re-thought to take account of the added importance of the information and cyber aspects of contemporary and future operations.

The final ‘Terminate’ action area is understandably the most difficult, requiring an alignment of stakeholder interests and decisive action. In all organisations, be it in the public or private sector, the allocation of constrained resources where they can best deliver the organisation’s objectives is the difference between success and failure. The organisations’ governance should be fundamentally empowered and supported in making the difficult decisions to take a resource from one area and apply it to another that will deliver greater effect. The most mature organisations are able to anticipate where to do this and so do it early, avoiding unnecessary costs. In the defence and security environment the expedient for change has too often been on the battlefield – the last place where a lack of superiority against an adversary is wanted. The challenge posed by TOS thinking assists considerably in this anticipation.

There are a number of reasons why it might be appropriate to terminate a source of capability. The first is that the capability has unequivocally become redundant in the threat environment, and other courses of action, such as Treat, are not credible either from an effect point of view and/or financially. A capability that was once effective in a peer-contested environment might still have utility in a non-contested environment. The judgement here will be whether it is the most cost-effective means to deliver that effect, or whether a less sophisticated capability might be more appropriate. Second, while desirable, the capability could be rapidly reconstituted should the need arise. Third, while still a credible capability, other partners can be relied upon to provide it. In dealing exclusively here with peer conflicts, it would seem highly unlikely that the
UK would be engaging a peer adversary alone, and therefore Britain can rightly and justifiably rely on others to deliver certain capabilities while it focuses on others. However, this statement should be qualified by the need to take account of the UK’s sole responsibility for the defence of its overseas territories. Finally, and a reason that would likely combine with one of the others, is that there are higher priorities for the allocation of resources. Given the justification for doing so, the challenge is to build the narrative and consensus among stakeholders that redistribution of resources is appropriate in the context of the UK’s overall defence and security. Clearly, the choice among the four possible courses of action depends significantly on calculations of where technological and other sources of innovation can make a significant impact at an acceptable cost in the Treat and Transform domains.

Running through all of the above is the theme of adaptability and agility. The messiness and dynamics of today’s threat environment presents a major challenge to inflexible capabilities, especially those with very long development cycles. The capabilities that will be of most utility will be those that are most agile either in terms of the way in which they are deployed, and/or their intrinsic ability to be rapidly adapted. The Treat and Transform courses of action should have adaptability and agility at their core. Many major platforms are less agile and adaptable, so these attributes will need to be delivered through exploitation of the electromagnetic spectrum, dynamic networks, tuneable effect weapons, hybrid sensors and special forces operations. The platforms will still be there, but as nodes in an adaptable, amorphous network, rather than as ends in themselves.
Conclusion

So a military force has no constant formation, water has no constant shape: the ability to gain victory by changing and adapting according to the opponent is called genius.

Sun Tzu, The Art of War

This paper has been set in the context of the US’s formative thinking under the banner of the TOS, but it is the underpinning recognition of a changed threat environment that has really driven the thinking. This thinking is explicitly focused on peer threats in contested A2/AD environments, as opposed to the operational environments that have characterised the past few decades. The relevance of this work has been established both in terms of the innate change in the UK-relevant threat environment and in terms of Britain’s role alongside its principal allies, particularly the US.

This paper has found that the vulnerabilities identified in the original TOS are clear and present. Most notable among these is the increased peer and near-peer threat from Chinese and Russian long-range precision missiles, which threaten large land, maritime and air platforms, as well as having the potential to make space-borne communications and navigation capabilities susceptible to denial. As a linked but important consideration, the cost-effect ratio has been skewed by recent capability development: it has become much cheaper to destroy major systems and platforms than to develop and build them, making large-scale attacks on a single target more likely. Note that the vulnerability of UK defence systems is not the only challenge and, indeed, it may be seen as secondary in the event of a peer-to-peer conflict, since it is likely that in such a conflict, an adversary would concentrate attacks on Britain’s crucial IT and satellite-dependent national infrastructure.

As in the US, the UK has begun to reinvigorate its defence innovation, but this is set against long-term reductions in defence S&T spending. To compensate, the new cash announced as part of the 2015 SDSR Innovation Fund needs to be explicitly geared to leverage the core S&T budget, the broader equipment plan and complementary commercial R&D spend. The last one is useful for exploiting existing matured technologies, but the constraints of such technologies are their equal availability to adversaries and the limited willingness of commercial organisations to subject their technology to export controls. With commercial technologies, key considerations regarding their adoption and adaptation for defence are the contract terms required by the MoD and the speed of the acquisition system involved. This latter issue is causing concern in the US, where the laws governing government procurement are much more extensive than in the UK.

TOS challenges previous thinking at the strategic and conceptual levels. Specifically, the Defence Capabilities Framework should look to promote Protect as the first among equals; this will require additional emphasis on defensive capabilities. This paper argues that protection capabilities should be made a central feature of all defence systems. In so doing, defence would be mirroring what experts have called for in the cyber domain: ‘cybersecurity needs to be accounted for as a central feature of all the products being developed and commercialized for tomorrow’. But defence also needs to go further, by asserting that the overall protection of defence systems needs to be a core consideration from the very beginning.

Within the British DII, the seven specified Defence Challenges align very well with the TOS, and the MoD’s core principles of innovation are well expressed. What is less convincing is the extent to which these have been inculcated into the culture, organisational structures and leadership focus of the relevant organisations.

A step change in the approach to innovation will require a readiness to acknowledge the risks inherent in true innovation and a change in risk appetite, both within government and among those holding it to account. A return to more experimentation and demonstration should feature strongly in the new approach, allowing early failure, discovery, and the ability to test relevance and applicability to military needs.

There is a need for a capability re-assessment in the context of the new peer threat environment; it is important to challenge the idea that the UK can seek a ‘full spectrum’ portfolio without maintaining contemporary and future relevance. This paper proposes a framework (Tolerate, Treat, Transform, Terminate: deliver the effect to meet the threat – T4ET) that assesses the ability of current capabilities to meet threats and designates courses of action as appropriate, including maintenance of the capability (Tolerate), adaptation for renewed effectiveness (Treat), introduction of transformational capability (Transform), or termination on the grounds of untreatable irrelevance, future ability to reconstitute, partner dependence, and/or reprioritisation (Terminate).

The messiness of today’s threat environment means that adaptability and agility will be the most prized characteristics for future capabilities. The Treat and Transform courses of action have these characteristics at their core. Although this paper has focused on threats from peer and near-peer entities, the challenges from non-state groups cannot be forgotten, requiring Western defence forces to be ready for a wide and uncertain range of contingencies. Agility, however, would require a process review within government that is aimed at speeding up decisions in acquisition processes, and accelerating overall capability development within the armed forces, as well as stressing dynamism and responsiveness in the technological and industrial sectors. As

---

the Defence Equipment and Support innovation strategy document observes, ‘innovation is an enterprise endeavour’.5

This refresh of critical thinking within government should also address the broader policy relating to deterrence. As we have witnessed in the discussion in this paper, deterrence is not simply a matter of keeping, maintaining and renewing nuclear capabilities, important though that might be. Rather, deterrence, in the modern epoch, is to be found in a range of flexible and adaptive capabilities that, if used, degrade and destroy a state adversaries will and capacity for aggression or conflict. The ability to deter will be based on a state’s ability to innovate, an agile use of its forces and private sector partners and supply chains, its commitment to investment in S&T and its policies relating to resilience and recovery. A public commitment to these themes should also be added to the list so the public discourse relating to their importance must emanate overtly from government as part of the policy narrative of defence and security.

Themes of adaptability, agility and change are as old as warfare itself. When an opponent changes his posture or capability a state has to adapt and respond. Should that change in posture relate to the erosion of technological advantage, it seems reasonable to frame a response (in part) around how the UK secures, develops and exploits known and emerging technologies. The UK also needs to embed a through-life culture and ways of working that value adaptability, adoption, agility and creative thinking. If the arguments in this paper are reasonable, to do so is a critical imperative, albeit one that is very difficult to achieve.6

The risks associated with a focus on innovation can be moderated by a range of techniques, including: a readiness to prioritise; to experiment in areas with diverse potential applications; to address balance in technologies at different points in the readiness spectrum and in the modernisation of existing assets, and the development of all new ones; and to ensure that decision-making processes are as agile and flexible as the speed of successful innovation requires.

The above suggests that partnerships – between governments, across the public and private sectors and within supply chains – should be at the heart of the search for innovation and agility. This suggests that the notion that some level of specialisation and dependency is necessary: the quest for each individual country to possess full-spectrum effects might be both unaffordable and anti-innovation.

Defence programmes have become increasingly rooted in complexity. As many who have been NATO staff officers are aware, allied forces in some areas – such as armoured vehicles – feature numerous types of national systems whose interoperability is often problematic. Different countries in Europe have duplicated their research and development efforts and it can be argued that they wasted resources re-inventing the wheel. Still, when a production run for a national market is limited and extensive development costs can be spread only over a small number of

6. For the authors, through-life is defined as the ability to plan, approve, deliver, refresh, support and integrate capabilities throughout the life of their utility, in an efficient and value-for-money manner.
produced units, the overall cost per item can make a national project unaffordable. If export prospects are poor, this consideration is even more prominent. The UK concluded in the mid-1960s that it could no longer afford national programmes for combat aircraft development. In these circumstances the options are buying a developed product from others or participating in a collaborative project to generate a nationally badged capability or relying on others’ armed forces for some elements. As systems become increasingly complex and expensive, the demand for specialisation, including in collaborative projects, will increase. Indeed, specialisation will be seen as a critical component of innovation.

As the MoD re-examines 2015 SDSR, and while the government looks at the protection of critical national infrastructure and seeks to address our societal vulnerabilities, the key principles of TOS thinking have to be applied. Using the Innovation Fund to leverage S&T budgets in order to reshape the form of the investment in the government’s equipment plan – thereby releasing commercial sector R&D budgets – is the route to the prize of innovative, adaptive, technologically rich and affordable future capabilities – capabilities that can survive to operate and keep the UK relevant to the needs of its allies and alliances. By adopting and actively adapting TOS thinking to the UK’s needs, the MoD should embrace innovation and seek to place it culturally at the heart of its defence enterprise. Not to do so would leave the country potentially vulnerable to its adversaries and dependent on the goodwill of its friends.
About the Authors

**Professor John Louth** is Director, Defence, Industries and Society at RUSI. He served in the RAF for sixteen years and has worked extensively across industry as a consultant and programme director. Professor Louth is an adviser to the Defence Select Committee in the House of Commons and is the UK representative of the Permanent Monitoring and Analysis Review Team of defence capabilities for the EU. He supervises PhD students at the University of Roehampton Business School.

**Professor Trevor Taylor** is Professorial Fellow in Defence Management at RUSI where he is based in the Defence, Industries and Society Programme. He is an Emeritus Professor of Cranfield University where he headed the Defence Management and Security Analysis Department at the Defence Academy of the UK for twelve years. He is a former head of the International Security programme at Chatham House and was for six years an elected council member of the Defence Manufacturers’ Association.

**Dr Andrew Tyler CBE** is an industrialist and former senior government servant. He worked in defence first as Managing Director of BMT Defence Services and from 2006 in the Ministry of Defence, becoming Chief Operating Officer of the Defence Equipment and Support organisation. Since 2013 he has been Chief Executive of Northrop Grumman Europe. He has a PhD in environmental science and is a Fellow of the Royal Academy of Engineering.

---

**About the Defence, Industries and Society programme at RUSI**

The Defence, Industries and Society (DIS) programme at RUSI is a multi-year research effort looking at the complexities and interdependencies of capability generation from across the public and private sectors. The programme constructs an understanding of defence as a broad and amorphous defence extended enterprise where the capillary nature of skills, technologies, values, behaviours and defence programmes of work come together to generate planned and unintended effects. The DIS programme seeks a greater understanding of the spaces where defence policy and practices intersect with commercial and societal intentions and what this means for national security, macroeconomic, fiscal and social policies and international relations.