serco INSTITUTE

The Whole Force by Design: Optimising Defence to Meet Future Challenges

Professor John Gearson (Study Lead)
Dr Philip Berry (Senior Researcher)
Dr Joe Devanny
Dr Nina Musgrave

October 2020

In partnership with

KING'S College LONDON

Centre for Defence Studies

Contents

Executive Summary

The Whole Force by Design (hereafter the Whole Force) was developed to ensure that Defence was able to **harness an integrated mix of Regular, Reserve, civilian and contractor personnel to deliver military effects in a resilient, efficient and cost-effective way**. Central to this concept was the notion that industry was becoming an increasingly important component of the military's operational capability.

This study aims to provide a timely contribution to the on-going debate on the Whole Force: identifying what progress has been made; what obstacles remain to deliver a fully integrated Whole Force model in the UK and, progressing the Whole Force debate by the generation of a list of practical recommendations designed to improve the Defence public-private partnership model. **The study's key conclusion is that decisive changes are required to advance the Whole Force and that any risks in embracing it are significantly outweighed by potential benefits.**

As Defence confronts a number of operational, equipment, budgetary and manpower issues, Ministry of Defence (MoD) leaders have seemingly embraced the Whole Force to meet current and future challenges. Whilst there has been movement in operationalising the Whole Force in areas such as training, facility management, support and operational capabilities, **progress has fallen short of a seamless integration of industry into the Whole Force** that many had hoped would develop.

Despite senior MoD leaders having accepted the Whole Force as a critical element of operational capability, **the MoD has not articulated a compelling narrative of the need for, and benefits of, industry support to Defence. Perhaps in consequence, the reforms necessary to move forward have not been made.** The process **lacks clear lines of accountability for delivery.** This has resulted in confusion at best, and suspicion at worst, about what the Whole Force means and how it should be implemented. This is partly the result of insufficient focus on developing a guiding framework and generating momentum for the Whole Force's implementation.

If the potential of the Whole Force is to be realised, **the Defence-industry relationship needs to evolve into a partnership model**, where industry is considered a vital component of a broader Defence Enterprise. To achieve this, a number of barriers must be overcome. One of the key 'frictions' standing in the way of achieving a fully integrated Whole Force remains **cultural barriers between the military and industry, underpinned by misperceptions of industry motives and the perceived risk to the military's capability**. There are several steps that may reduce 'Clausewitzian friction', such as the communication of a narrative explaining the benefits of the Whole Force; the inclusion in existing UK Military Staff Courses modules of the benefits of working with industry; and the establishment of joint military-industry training exercises.

Another key barrier to progress the Whole Force and move to a partnership approach is **sub-optimal commercial processes and contracting frameworks**. Notwithstanding the MoD's current procurement improvement initiatives and broader engagement with industry, such barriers sometimes include: Defence's lack of relevant and Whole Force specific engagement with industry; poor requirement setting within capability teams; complicated and inflexible contracts; and limited coordination between Defence's decision-makers, which can be underpinned by an adversarial approach to the procurement process.

Several public and private sector respondents indicated to the study team that **industry, for its part, must also improve its commercial processes, particularly around accepting additional risks and adopting more flexible solutions during the contracting process**. Other private sector representatives contended that the MoD's terms and conditions generate inappropriate transfer of risks to industry, and that the more industry is embedded in the Whole Force, the more risks that they may have to accept. Other respondents noted that industry should be more flexible when circumstances change, and not seek to increase the cost of contracts unnecessarily. **The key to improving the relationship is the development of trust and incentives to work collaboratively**.

The growing importance of the Whole Force has been underlined during the government's response to the coronavirus pandemic. Of note, there have been examples of successful public and private sector collaboration, particularly as some defence companies have

responded flexibly to the coronavirus challenge. That said, whilst these signs bode well for the future operationalisation of the Whole Force, there is limited publishable evidence to draw definitive conclusions about how these recent experiences will impact the Whole Force.

Whilst **industry can provide Defence with capacity and resilience in some cases, overreliance on industry can mean that Defence loses the in-house expertise to perform key functions**, and/or the ability to design and manage contracts effectively. This links into the broader question of assured delivery and another common argument against embracing the Whole Force - if industry fails to honour what has been agreed, the delivery of Defence outputs will be undermined.

Defence companies must decide if they are willing to accept the risks involved in participating in the Whole Force, such as putting employees in harm's way. These decisions must be made in advance of operations in order to facilitate the deployment of the employees at short notice; and to assure delivery. **The use of Sponsored Reserves (SR) may increase assured delivery as contractors deployed on operation could be activated as SRs, as the threat and risk level increases**.

In the coming years, it is likely that the Whole Force debate will be shaped by decisions about the size of the military and levels of Defence spending. An informed debate regarding what the United Kingdom's (UK) strategic ambitions are should be the starting point to decide and develop the correct force mix. Another trend likely to inform the future Whole Force debate is how the military, in partnership with industry, meets the technological challenges of tomorrow. As such, the **MoD must be willing to accept more failed projects as the price of being at the cutting edge**. Moreover, given that high-end **cyber operations require significant technical specialism, skill and experience, there is considerable scope to progress the Whole Force in this area**.

As the character of warfare changes, the **MoD should think creatively about the ways in which it can tap into a pool of expertise that is not traditionally associated with Defence, including through alternative routes of entry**, and how to incorporate this into a future force.

Industry may also need to be more willing to develop and provide a wider range of new skills and equipment than previously has been on offer.

Consideration of Whole Force (or similar) models from around the world reveals that there is an **increasing engagement with the private sector across a range of countries that is relevant to the UK Whole Force**. Particularly in the areas of cyber security and technology more generally, there has been a wide realisation that an efficient way of improving the quality of national capabilities is through leveraging expertise from the private sector.

Whilst the UK and United States (US) context varies, there are strong and instructive similarities between both countries respective approaches to combining Regular and Reservist, civilian, and contractor personnel in the cyber force. The **US's cyber approach offers lessons for the future application of the UK Whole Force; for instance, the US has highlighted the importance of recruiting cyber Reserves, and has developed an integrated force mix**, which emphasises the need to recruit and contract the right balance of skills and experience to meet its cyber challenges.

While **private sector engagement is a dominant theme internationally, it is evident that conceptions of Whole Force and Total Defence models vary**. The extent of civil society engagement and how this is articulated is important as it varies from context to context. Similarly, in considering Psychological Defence as a component of Total Defence, this has been fully embraced by some countries but rejected by others.

The model of integrating SRs alongside military personnel is an important part of the Whole Force, and has been considered internationally, including in the US and Australia. Generally, around the world there are calls for more fluidity and flexibility of movement between the military and the private sector.

The Whole Force, if planned strategically and implemented consistently and efficiently, provides Defence with a means of increasing its capacity and resilience. **The drivers to adopt a fully integrated Whole Force model are just as, if not more, pressing today than when Lord Levene introduced his reforms in 2011**.

The study's overriding conclusion is that while there are risks involved in further private sector integration into the UK's Defence system - surrounding issues of assured delivery and Defence losing the in-house expertise to perform key functions, and/or the ability to design and manage contracts effectively - **the benefits of maximising a fully integrated Whole Force considerably outweigh any disadvantages**.

Select Key Recommendations

1. *The Whole Force should be defined as: Effective, agile and resilient capability delivered by an integrated, pre-planned and affordable military force comprised of a mix of Regular, Reserve, civil servant and industry supported by appropriate technology to meet Defence outputs. It should be circulated among all component parts of the Whole Force as the first step in formalising and standardising a shared understanding of the Whole Force (see section 3.4).*

2. *The Development, Concept and Doctrine Centre should resume its work on the development of a Concept Note that has been informed by industry contributions. Once this work has been finalised it should be circulated for approval and endorsement in both the MoD and Frontline Commands (FLC) at two-star level and above. The resultant Concept Note should then be used as part of the MoD and FLCs core planning in response to the Integrated Review. (see section 3.5).*

3. *The Chief of Defence People (CDP) should be appointed Senior Responsible Owner to plan, oversee and ultimately execute the Whole Force's delivery. The CDP should be supported by Financial and Military Capability personnel to ensure a coordinated process across the three Services. It may also be useful for cadre of dedicated senior supporting staff working on the Whole Force to remain in post for longer than the typical two-year postings (see section 3.7).*

4. *Military education courses that highlight the role of contractors in the Whole Force should be embedded into the curriculum of existing UK Staff Courses. Such education should start as soon as officers (and non-commissioned officers) enter service and should continue throughout the entirety of their careers (see section 3.9.2).*

5. *To fully operationalise a true Whole Force model, there needs to be a comprehensive approach to the integration of contractors with their military partners before, as well as on operations. Joint training and exercise programmes not only would improve operational performance and integrated working practices but would also help to*

break down cultural barriers and help to foster a 'team Defence' mentality on both sides (see section 3.9.3).

6. *Defence officials should establish and regularly convene a Defence-industry working group including relevant senior officials from the MoD, officers from across the three Services, and industry representatives to identify a coherent plan to operationalise the Whole Force. Such forums could enable Defence to engage with industry as early as possible before framing contracts. Strategic engagement could improve outcomes; whilst also helping both sides progress towards a genuine partnership, with a greater sharing of both risks and rewards (see section 3.9.4).*

7. *All FLC officials responsible for managing and overseeing existing contracts should be given the opportunity to attend the foundation level of the civil service contract management training course if they are not already offered this, with consideration given to which staff would benefit from the advanced levels of this course (see section 3.9.4).*

8. *If companies decide they want to play an active part in the delivery of the Whole Force, they must facilitate open discussion about the nature of the risks involved. This may mean acceptance that the risk associated with potentially placing their employees in harm's way involves recruiting employees with the appropriate terms and conditions (see section 3.9.5).*

9. *The Integrated Review should include a Defence cyber workforce strategic audit, identifying the skills and force structure required for the defensive and offensive cyber missions through to 2030. This audit should assess the required size and scope of civilian, military (Regular and Reservist), and private sector contributions to Defence cyber (see section 3.12).*

10. *Alternative routes to entry, including lateral entry schemes, which open opportunities in Defence to suitably qualified applicants from outside the military, could offer Defence an untapped pool of human resource, especially in highly skilled areas. Whilst*

these routes to entry should not be considered a panacea to Defence's recruitment and skills challenges, such programmes should be encouraged and developed (see section 3.13).

The full list of recommendations is reproduced in section 7.1. of the Appendix.

1. Introduction

The Serco Institute, a think tank helping governments to develop the next generation of public service solutions for citizens, commissioned the Centre for Defence Studies (CDS), King's College London to produce an independent report on progress in delivering the Whole Force by Design (hereafter the Whole Force) in the United Kingdom (UK). The study, which was undertaken between late 2019 and spring 2020, and the resultant report contributes to the ongoing Whole Force debate, while also discussing several issues that are relevant to the forthcoming Integrated Review of Security, Defence, Development and Foreign Policy (hereafter Integrated Review).

Formally articulated by Lord Levene as the Whole Force Concept in his Defence Reform report in 2011, the policy offered to improve Defence by ensuring that it was '…supported by the most cost-effective balance of Regular military personnel, Reservists, MoD [Ministry of Defence] civilians and contractors'.[1] Central to this concept was the notion that the delivery of military capability should not be the sole responsibility of Regular personnel, but instead should rest with whatever element of the Whole Force that was most suited to deliver it.[2] Lord Levene's recommendation tacitly acknowledged that the military was becoming increasingly unable to deliver certain capabilities without industry and civilian support.[3]

The current coronavirus pandemic has dramatically re-ordered the government's short-term policy agenda and associated spending priorities. Whilst the long-term financial implications of the pandemic remain unclear, it is likely that the country will face a challenging economic situation at least in the short term, which in turn, could place significant pressure on many departmental budgets, including the MoD's. If such a scenario does materialise, the MoD may

[1] Lord Levene of Portsoken, *Defence Reform: An independent report into the structure and management of the Ministry of Defence* (London: Ministry of Defence, June 2011), 57, accessed 27 November 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27408/defence_reform_report_struct_mgt_mod_27june2011.pdf.
[2] John Louth and Pete Quentin, *Making the Whole Force Concept a Reality*, Royal United Services Institute (RUSI) Briefing Paper, (London: RUSI, November 2014), 1-2, accessed 10 May 2020, https://rusi.org/system/files/RUSI-BP-WholeForceConcept-Nov14.pdf.
[3] Defence is also reliant on public sector support, such as the NHS working with Defence Medical Services (DMS). Although Defence remains short of skilled medical personnel, the collaborative nature of DMS's work with the NHS is of critical importance to Defence's ability to deliver medical services.

have to adapt existing plans to respond to an altered operating environment, just as it goes through a policy review process, in the Integrated Review which is restarting after a pause from April 2020. In this context, the need for and benefits of the Whole Force may take on increased importance, as the MoD is forced to re-orientate its already stretched resources to meet future demands.

In the years since 2011, as the MoD has confronted a number of long-standing operational, equipment, budgetary and manpower challenges, senior officers and politicians appeared to embrace such an approach, in effect accepting that, 'the [Whole Force] is not an unfortunate necessity, but an indispensable requirement of our future operational capability'.[4] As such, there have been several attempts to translate this ambition into reality; not least, transitioning the language of the Whole Force from 'concept' to 'approach' and then to 'design' – all with the clear intent and purpose of forcing progress. Whilst some progress has been made in operationalising the Whole Force, it has been seen by many as limited and uneven, and ultimately has fallen short of a seamless integration of industry and the private sector more widely into the Whole Force.

While the reasons for this are manifold, most are in fact largely understood on both sides of the public-private divide. On the one hand, many elements of Defence (the combination of MoD civilian and military personnel) have embraced the Whole Force, leading one former MoD official to observe that the case for adopting the Whole Force, 'at the intellectual level…is [not] challenged'.[5] Consequently, several innovative Whole Force solutions have been implemented by Front Line Commands, however, there is still a degree of confusion at best, and suspicion at worst, about what the Whole Force means and how it should be implemented across FLCs.[6] This is partly the result of little conceptual work having been devoted to developing a framework by which to guide Whole Force decision-making and implementation. This limitation has been compounded by the fact that the MoD has not, as yet, articulated a compelling narrative of the need for, and benefits of, greater industry

[4] David Galbreath, 'Investigating the Whole Force Approach: Whitehall, the Army, and the private sector: working towards a genuine partnership,' *The occasional papers of the Centre for Historical Analysis and Conflict Research: ARES & ATHENA* 2, (Winter 2015/16): 1-36, 6.
[5] Interview with former Ministry of Defence official, London, 20 November 2019.
[6] Louth and Quentin, *Making the Whole Force Concept a Reality*, 2.

support to Defence. In short, there has been a disconnect between high-level political rhetoric in support of achieving a Whole Force and the absence of a deliberate strategy to guide (and ultimately force) its implementation.

Taking as its starting point the articulated high-level acceptance of the value that an integrated Whole Force can offer Defence, this report concentrates on how it can be successfully implemented, deepening and improving the Defence-industry relationship. To achieve this objective, the study has four key objectives:

1. assess what progress has been made in delivering the Whole Force;
2. identify the challenges that are preventing the full operationalising of an integrated Whole Force;
3. draw out lessons from the wider international community on the Whole Force; and,
4. generate practical recommendations and solutions to inform and shape the on-going Whole Force debate.

The research project has progressed through several distinct, but complementary, stages. The first included the production of a policy-relevant discussion paper, which situated the Whole Force within current trends related to the broader Defence sector. The discussion paper was used to inform a CDS-facilitated stakeholder roundtable, held at King's College London, in December 2019. The event, which was held under the Chatham House Rule, brought together current and former MoD and military officials, industry representatives and academics and commentators to generate further insights in support of the research effort, testing emerging themes and conclusions before the second stage of the project.

The second stage of the project was launched at two CDS-facilitated stakeholder roundtables, which were held at the MoD in February 2020. The events produced lively and stimulating discussions on how to further progress the Whole Force project, and how to optimise the Defence-industry relationship. As before, both roundtables were held under the Chatham House Rule, allowing senior MoD, military, industry and academic representatives to express their views candidly, which added depth to the discussions. In parallel to the three roundtable events, the CDS research team conducted a range of primary research interviews with policy

practitioners and recognised industry experts to support the study, along with secondary research across a range of sources.

1.1 Structure of the Report

The report provides contextual analysis of the current and future trends in the Whole Force debate. It does so by drawing out key themes, both from the UK and around the world, which are relevant to operationalizing a Whole Force. The report generates policy-focused recommendations, across a range of sub-themes, designed to offer practical steps to improve industry integration into the Whole Force. The recommendations are designed to be relevant to both sides of the public-private divide.

The report commences with an overview of the wider defence and security issues that are pertinent to the Whole Force debate. It assesses the strategic shift in the international and domestic security environments and the changing character of warfare, and the impact that these will have on the UK. The section then highlights several internal challenges that are impacting Defence's ability to consistently deliver outputs; namely, budgetary pressures; a recruitment and retention crisis; and a skills shortage. The section also briefly considers the impact that the coronavirus pandemic may have on the Whole Force.

The following section begins with a brief contemporary history of industry's involvement in the delivery of Defence outputs, before outlining the evolution and operationalising of the Whole Force since 2011. The section then examines three case studies that provide examples of Whole Force successes. The analysis then evaluates the key obstacles and barriers that have so far held-back the full operationalization of the Whole Force, including military/Defence culture; inadequate military education; a lack of joint military-industry training exercises; commercial processes and contracting frameworks unfit for purpose; technological challenges; and existing employment models. Throughout this analysis, the section offers a set of recommendations designed to break down these barriers and generate an improved Defence-industry partnership.

The next section situates the Whole Force debate within the broader context of international comparisons, drawing upon global Total Defence doctrines, which span a variety of Nordic and Asian countries. The section highlights several relevant international themes, which offer lessons for the Whole Force, including contractor support in the United States (US), the use of Reserves in countries such as Australia and US, Defence cyber, and lateral entry models.

The final section collates the various recommendations and conclusions presented throughout the entirety of this report. The recommendations are designed to be relevant for both government and industry, and, if adopted, should help to foster the deeper level of public-private engagement necessary to implement and enhance the Whole Force.

2. The Current and Future Defence Environment

2.1 Introduction

To properly understand the need for and benefits of the Whole Force, it is important to contextualise the complex strategic and operational challenges, both at home and abroad, that Defence now faces. Over the past several years, the military has responded to numerous domestic emergencies, including major terrorist attacks, widespread flooding and the recent coronavirus pandemic, as well as continuing contingent operations and overseas deployments, which while not on the scale of the decade after 2001, have proven demanding, especially in the context of the period of austerity following the financial crisis of 2007-09. The backdrop of continued funding pressures across most aspects of the Defence budget also saw:

- the UK's 2016 vote to leave the European Union (EU);
- a devaluation of sterling in the years following the referendum, resulting in the price of foreign equipment increasing;
- a recruitment and retention crisis; and,
- significant skills shortages.

Internationally, the security environment continues to become less stable, with a resurgence of state-based threats; a continuation of overseas terrorist activity; the West's shrinking technological edge; and, increased instability on several continents. It is worth noting, however, that the above-mentioned challenges do not pose equal levels of risk for the UK and, to some degree, how these challenges effect the UK is determined by the government's policy choices.

As these trends develop, Defence will be required to respond and adapt to meet current and future challenges. To do so, it will have to utilise all aspects of the UK's national security apparatus, including perhaps fully embracing a Whole Force, to increase resilience and capacity, as well as taking the best from the private sector. Much of this strategic planning should be determined by the on-going Integrated Review. This section will first outline the

rapidly evolving domestic and international security environment; before proceeding to assess Defence's budgetary pressures. The chapter will then evaluate the current recruitment and retention crisis, and the national skills shortage.

2.2 The Strategic Security Context

With the proliferation of multiple state and non-state threats, the global security context is now more hazardous and unstable than at any point in the last three decades.[7] So much so that the four threats identified as security priorities in the 2015 UK National Security Strategy and Strategic Defence and Security Review (NSS/SDSR) - increased terrorism, the recurrence of state-based threats, increased cyber threats, and the erosion of the rules based international order – have all intensified since its publication.[8] In the Middle East, while the situation in Syria and Iraq has improved, both countries still remain unstable; tensions have flared in the Gulf region, the civil war in Yemen still drags on; Libya remains on a knife edge; several conflicts across Africa remain unresolved; and despite recent agreement between the Taliban and US, violence still engulfs Afghanistan. Terrorism remains endemic in most of these conflicts.

Furthermore, some of the UK's traditional alliance relationships are now showing considerable strain. The 'special relationship' with the US, which has been on a downward trajectory for several years, has been further weakened under President Donald J. Trump, and even if Joe Biden was to be elected in the forthcoming presidential election, the relationship could still atrophy through US 'benign neglect'.[9] Central to US calculations of the relationship is the perception of the UK's utility as a defence and security partner, which may further be affected by the outcome of the forthcoming Integrated Review. The UK's decision to leave the EU has created uncertainty with many of its continental neighbours. Moreover, the international structures that the UK has historically prospered under, are now being tested

[7] House of Commons Defence Committee, *Re-thinking defence to meet new threats*, Session 2014-15 HC 512 (London: Stationery Office, 2015), 3.
[8] Ministry of Defence, *Mobilising, Modernising & Transforming Defence: A report on the Modernising Defence Programme* (London: Ministry of Defence: 2018), 12, accessed 10 May 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/765879/ModernisingDefenceProgramme_report_2018_FINAL.pdf.
[9] Alan Dobson and Steve Marsh, 'Benign Neglect: America's Threat to the Anglo-American Alliance,' *Orbis 58*, no. 2 (2014): 266-81.

by regimes seeking to challenge and weaken Western influence,[10] leading to 'a period of persistent and intense state competition.'[11]

As part of this competition, the UK's adversaries are attempting to destabilise its homeland and other areas of strategic importance through 'grey-zone' activities, which lie between traditional notions of peace and war, such as 'cyber-attacks, assassination, disinformation, theft of intellectual property, espionage and military intimidation.'[12] In recent years, Russia has launched a variety of attacks on the UK, including the nerve agent attack in Salisbury, major cyber-attacks and large scale disinformation campaigns.[13] The combination of kinetic attacks (such as in Salisbury) and non-kinetic aggression seeks to disrupt the UK's critical national infrastructure and political and social fabric by diminishing resilience and public confidence.[14] This has been coupled with intensified probing of the UK's defences – at sea and in the air; and destabilising activities in Eastern and Central Europe.

Core to the UK's defence posture is still the ability to project capabilities around the globe, and at short notice. This means balancing regional commitments, including dealing with an adversarial Russia, with the UK's broader global ambitions in the Middle East, Mediterranean, South Atlantic, and East Asia.[15] Consequently, in 2019, the UK military were involved in '36 operations and 36 per cent of trained strength being committed either to operations or at very high readiness'.[16] As the situation has evolved and become less stable, the UK has been forced to reassess its military's capabilities and capacity to meet these emergent challenges. The 2018 Modernising Defence Programme increased spending on improving readiness, enhancing weapon platforms and stocks, modernising capabilities, including through new

[10] Nick Carter, 'Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019,' *RUSI*, 5 December 2019, accessed 10 May 2020, https://rusi.org/event/annual-chief-defence-staff-lecture-and-rusi-christmas-party-2019.
[11] Ministry of Defence, *Mobilising, Modernising & Transforming Defence*, 12.
[12] Ibid.
[13] Ibid.
[14] Rod Thornton, 'Covid-19 and why state resilience in the United Kingdom needs to be strengthened: The link to the changing character of war and lessons from Russia,' *Defence-In-Depth Blog*, 8 April 2020, accessed 10 May 2020, https://defenceindepth.co/2020/04/08/covid-19-and-why-state-resilience-in-the-united-kingdom-needs-to-be-strengthened-the-link-to-the-changing-character-of-war-and-lessons-from-russia/.
[15] David Blagden, 'How Britain's Ministry of Defence is playing for time (and money) in a dangerous world,' *The Conversation*, 18 January 2019, accessed 10 May 2020, https://theconversation.com/how-britains-ministry-of-defence-is-playing-for-time-and-money-in-a-dangerous-world-109155.
[16] Carter, 'Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019.'

technology, and refining how Defence operates as a business.[17] Nevertheless, if the UK remains politically committed to active global engagement, it requires a commensurate investment in Defence capabilities, otherwise there could grow a consequential gap between rhetoric and reality.

Part of the on-going re-evaluation of capabilities is driven by a recognition that the nature of warfare is evolving at pace. Information and communication technology present the UK with opportunities and potential threats; the cyber and space domains are increasing in importance and continue to be contested by multiple actors. As the UK's rivals (and allies) are developing cutting edge technologies, such as artificial intelligence, processing power, automation, autonomous weapons systems and hypersonic weapons, it too must respond by ensuring it has the correct technologies to compete in the new defence and security landscape and be able to operate in future coalitions.[18] As is discussed below, Defence may have to accept more risk if it is to succeed in the information and communication technology age.[19]

In the context of continuing terrorist threats and events such as the nerve agent attack in Salisbury, flooding in the North of England and most recently the Covid-19 pandemic, homeland defence and security has progressively become a more important part of Defence's planning tasks. As adversaries have sought to manipulate hitherto unexploited vulnerabilities at home and abroad at times of heightened tension, a more integrated response from the Defence and security sector has been required. Previously – officially at least – articulated as a 'last resort', the military has become a vital component in the UK's on-going efforts to strengthen domestic security and resilience, including for example being at the forefront of the UK's counterterrorism response. Under Operation Temperer in 2017, the military were twice deployed to high-value sites to provide (public) reinforcement in the wake of terrorist incidents.

---

[17] Gavin Williamson, 'Modernising Defence Programme Oral statement to Parliament,' GOV.uk, 18 December 2018, accessed 10 May 2020, https://www.gov.uk/government/speeches/modernising-defence-programme-update.

[18] Ministry of Defence, *Mobilising, Modernising & Transforming Defence*, 13; Carter, 'Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019.'

[19] Carter, 'Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019.'

Most recently, the military has played an important role in the government's efforts to combat the coronavirus pandemic; providing logistical support to the NHS; assisting in the setting up of several Nightingale Hospitals; staffing mobile testing centres; and helping to repatriate UK citizens stranded abroad, while standing ready to support the Overseas Territories in responding to the crisis. The growing importance of the Whole Force was underlined by General Sir Nick Carter, Chief of the Defence Staff, who noted that the military had drawn on all components of the Whole Force in delivering the Covid-19 response:

> it has involved Defence civilians…contractors, scientists from Porton Down and…the Engineer and Logistics Staff Corps, where we bring in people from industry who work inside the military in times of crisis and provide expert support for how we might link into the civilian community to bring forward skills and indeed industrial support.[20]

As Defence's homeland responsibilities continue and probably increase, it is likely that industry will be further integrated into such responses, offering more opportunities to progress the Whole Force, especially since there appears to have been instances of successful collaboration between the public and private sector during the coronavirus pandemic (discussed below). That said, whilst these signs are early positive indicators for the future operationalisation of the Whole Force, there is limited publishable evidence to draw definitive conclusions about how these recent experiences will impact the Whole Force.

2.3 The Defence Budget

Although the true economic impact of the coronavirus pandemic is yet to be understood, it is likely to push the UK, along with other global economies, into recession at least temporarily. Whilst it is beyond the scope of this report to examine the impact of this projected economic downturn on Defence spending, it is worth highlighting in one 'pessimistic' forecast, the MoD

[20] *Army Technology*, 'UK Chief of Defence Staff participates in daily coronavirus briefing,' *Army Technology*, 23 April 2020, accessed 10 May 2020, https://www.army-technology.com/news/uk-chief-of-defence-staff-participates-in-daily-coronavirus-briefing/.

may have to 'shave another 5 to 10 per cent off the Defence budget by 2024'.[21] In such a scenario, some planned investments in equipment may have to be reviewed again and elements of the equipment programme and manning levels may have to be reduced. Defence may still benefit from a planned prioritisation of public spending projects, but few commentators believe it will be first in line.

Even before the outbreak of the coronavirus pandemic, Defence was facing significant budgetary challenges; the National Audit Office (NAO) had predicted that over the next three decades the MoD would face a £8.5bn shortfall on its estate budget.[22] Moreover, for the third consecutive year, the NAO judged the MoD's ten-year equipment and support plan, which covers the period 2019 to 2029, as 'unaffordable'.[23] This is partly a result of the commitments made in the 2015 NSS/SDSR, which increased Defence spending; invested in capabilities and outlined the creation of the Joint Force 2025. Whilst these investments were widely welcomed by the Defence community, these commitments, along with to date limited efficiency savings and the devaluation of sterling following the 2016 Brexit vote, have left Defence facing significant budgetary pressures.[24]

The MoD's equipment plan supports the delivery of major procurement projects, such as nuclear-deterrent submarines (Dreadnought-class SSBNs), Type 31 and 26 frigates, new and upgraded armoured vehicles (Ajax and Warrior) and new aviation platforms (F-35 Lightning, P-8A Poseidon, AH-64E Apache and Protector drones.[25] The MoD has forecast that the plan, which also funds the maintenance of existing equipment, will likely exceed its £181bn budget by £2.9bn; however, if all the risks identified emerge, the MoD has estimated that the funding shortfall could be £13.0bn (or 7 per cent of its budget).[26]

---

[21] Lucy Fisher, *The Times*, Twitter thread, 18 May 2020, accessed 19 May 2020, https://twitter.com/LOS_Fisher/status/1262371993976025088.
[22] Comptroller and Auditor General, *Ministry of Defence: The Equipment Plan 2019 to 2029*, Session 2019-20 HC 111 (London: National Audit Office, 2020), 36.
[23] Ibid., 6.
[24] House of Lords and House of Commons Joint Committee on the National Security Strategy, *National Security Capability Review: A changing security environment*, Session 2017-19, HL Paper 104 HC 756 (London: Stationery Office, 2018), 16-7.
[25] Comptroller and Auditor General, *Ministry of Defence: The Equipment Plan 2019 to 2029*, 13.
[26] Ibid., 6-7.

Constrained by immediate funding challenges, the MoD has opted to control its yearly expenditure to ensure its annual budget targets are met; however, this year-to-year approach is not sustainable in the long term. Moreover, this form of budget management also exacerbates other funding problems, such as complicating long-term planning across the FLCs, Defence Equipment & Support (DE&S) and the defence industry. It is projected that the funding gap over the next five years will be £6.0bn.[27] In order to remain within their annual expenditure limits, Top Line Budgets have postponed project costs into future years (increasing overall costs and driving inefficiencies) and halted less importance activities. This has resulted in the loss of capabilities; an inability to maintain current capabilities; and reduced spending on support work. As a result, some capabilities are being downscaled or withdrawn before the end of their service; for example, the Royal Air Force (RAF) is scrapping its E-3 Sentry aircraft, nine months before the replacement aircraft are projected to arrive on stream. The Army has also responded to these pressures by abandoning several projects.[28]

Given the current funding shortfall in the equipment plan, wider budgetary pressures, and the expected economic downturn as a result of the coronavirus pandemic, the Defence budget will probably be placed under significant pressure in the coming years. If the current funding gap increases, the Integrated Review may be forced to reassess Defence's priorities and make difficult spending decisions – potentially impacting on equipment and manpower calculations.

2.4 Recruitment and Retention

For several years, the military has faced, what is often characterised by outside observers as, a recruitment and retention crisis – in 2020, the size of the military contracted for the tenth consecutive year. While all three Services have faced significant shortfalls, the Army in particular, has struggled to meet its recruitment targets; not least because of what the Public Accounts Committee (PAC) described as its poorly implemented and managed partnership with Capita (although having now addressed some of the underlying technical issues, the

[27] Ibid., 7.
[28] Ibid., 37.

project with Capita has recently increased recruitment).[29] Mark Francois, a Conservative backbench MP, concluded in a report to the Prime Minister in 2017, that a variety of demographic and social changes have resulted in a '"perfect storm" against which military recruiters have had to battle', including near record employment, an ageing population, the conclusion of the Afghanistan campaign, a decreasing military footprint around the country, an increase in obesity in the last twenty years, and an increase in young people attending higher and further education.[30]

Against the backdrop of this 'perfect storm', Army manning stood at 73,670 in January 2020 - 2,210 down on the previous year and 8,330 below the manpower target set in the 2015 NSS/SDSR. In the same period, the RAF numbered 29,800 – a shortfall of 1,950 against the 2015 target. While the Royal Navy and Royal Marines stood at 28,890 – 1,510 below the MoD's 2015 goal.[31] As is discussed below, the overall deficit in military manpower actually disguises a more significant shortfall of Service personnel with critical skills.[32] Furthermore, manning pressures in the RAF and Royal Navy will be exacerbated as new advanced platforms arrive on stream, such as P-8A Poseidon aircrafts.[33] In an attempt to mitigate these shortfalls, existing personnel have had additional demands placed on them;[34] with retention rates in the military already sub-optimal, this added burden on existing personnel is likely to increase discontent with Service life.

Notwithstanding these trends, the military has made some limited progress with its recruitment campaigns in recent months. For the first time since 2010, intake surpassed outflow; in 2019, 15,830 people joined the military, whilst 15,230 people left, a net gain of

[29] House of Commons Committee of Public Accounts, *Capita's contracts with the Ministry of Defence*, Session 2017-19 HC 1736 (London: Stationery Office, 2019), 6.
[30] Mark Francois, *Filling the Ranks: A Report for the Prime Minister on the State of Recruiting into the United Kingdom Armed Forces* (July 2017), 2.
[31] Ministry of Defence, UK Armed Forces Quarterly Service Personnel Statistics - 1 January 2020, 20 February 2020, 5, accessed 10 May 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866842/1_Jan_2020_-_SPS.pdf.
[32] Comptroller and Auditor General, *Ministry of Defence: Ensuring sufficient skilled military personnel*, Session 2017-19 HC 947 (London: National Audit Office, 2018), 5.
[33] Francois, *Filling the Ranks,* 14.
[34] Comptroller and Auditor General, *Ministry of Defence: Ensuring sufficient skilled military personnel*, 8.

600. [35] After a successful, albeit controversial, advertising campaign and improved recruitment processes, the Army increased its intake by 68.6 per cent between December 2018 and December 2019.[36] Nevertheless, with a current workforce requirement deficit of 8.4 per cent and a 'perfect storm' of recruitment issues, it is unlikely that the military will reach its required strength in the immediate future.[37] It is possible that the consequences of the Covid-19 pandemic in terms of employment may result in a spike in recruitment and increased retention in 2020-22, but the underlying trends seem clear.

2.5 Mapping the Skills Gap

Compounding the recruitment challenges discussed above, Defence has also faced a growing skills gap in several key areas and in particular has consistently failed to acquire the specialist skills needed to ensure the delivery of outputs and operation of increasingly complex equipment and systems. Part of the problem is that the military operates on a base-fed-workforce model, meaning that the Services recruit at entry level and develop Service personnel's skills over the course of careers. However, given long-standing recruitment and retention issues, coupled with the time-consuming nature of developing in-house skills, the military has been unable to rapidly address capability gaps using this model.[38]

In April 2017, the three Commands (the Royal Navy, the Army and the RAF) highlighted shortfalls in 102 pinch-point trades - up from 88 in 2006 - that were required to perform operational duties. This figure equates to a shortfall of 7,700 personnel or 18 per cent below the requirement in those areas.[39] The Army was most affected with a shortfall of 4,485 troops; the RAF had a deficit of 2,032 personnel; and the Royal Navy was down 1,226 personnel. During this period, the six most common pinch-points trades were:

1. engineering (32);

[35] *BBC News*, 'Strength of British military falls for ninth year,' *BBC News*, 16 August 2019, accessed 10 May 2020, https://www.bbc.co.uk/news/uk-49365599.
[36] Ministry of Defence, UK Armed Forces Quarterly Service Personnel Statistics - 1 January 2020, 7.
[37] Ibid., 5.
[38] Comptroller and Auditor General, *Ministry of Defence: Ensuring sufficient skilled military personnel*, 9.
[39] Ibid., 7; 18; 21.

2. intelligence (11);
3. logistics (11);
4. pilots (7);
5. communications (7);
6. and medical (6).

Tellingly, the MoD predicted that it would be unable to address shortfalls in 96 of 102 pinch-point trades by 2023. Moreover, while it anticipated it could reduce the impact of shortfalls in 35 pinch-point trades, this would be offset by the fact the impact would increase in 23 other trades. In an attempt to combat these shortfalls, the MoD has implemented a series of financially unsustainable measures, such as paying £664m in recruitment and retention inducements in the five years to 2018.[40]

The dynamic nature of warfare and the rapidly evolving security environment means that Defence will be required to grow or access new skills, such as cyber and electronic warfare, artificial intelligence and missile defence in the immediate future.[41] Having identified accessing specialist skills as a priority, the 2018 Modernising Defence Programme outlined an ambition to forge a closer relationship with industry to acquire skills such as artificial intelligence, data analytics, cyberspace, space and other emerging technological areas.[42]

Complicating the challenge facing Defence is a national skills shortage in many of the key areas in which Defence is seeking to recruit personnel, increasing the competition between Defence and industry for access to these skills. It has been estimated that the broader employment marketplace will require an additional 700,000 science, technology, engineering and mathematics employees by 2024.[43]

Defence faces complex strategic and operational challenges, all of which are likely to intensify in the future and which are already placing significant strain on its ability to deliver military

[40] Ibid., 9.
[41] Ibid., 21.
[42] Ministry of Defence, *Mobilising, Modernising & Transforming Defence*, 23.
[43] Comptroller and Auditor General, *Ministry of Defence: Ensuring sufficient skilled military personnel*, 22.

capabilities. In meeting these future challenges, the full adoption of the Whole Force would, it is argued by proponents, help to increase MoD's resilience and capacity in doing so. The following section discusses how this might be achieved after assessing why it has not happened yet.

3. The Whole Force: Moving from 'Accident' to 'Design'

'WFA [Whole Force Approach] is not an unfortunate necessity, but an indispensable requirement of our future operational capability.' [44]

General Sir Nick Carter, October 2015

3.1 Introduction

As General Sir Nick Carter, then Chief of the General Staff (CGS), made clear in 2015: the adoption of the Whole Force Approach (as it was termed then) is not a luxury – it is a crucial component of the UK's future operational capability. In the same speech, he was also clear that:

> the drivers to exploit a WFA [Whole Force Approach] are profound… we want to maximise our front-end capability at a time when the cost of full-time military manpower is ever growing. We want to have niche and cutting-edge talent and skills, but the cost and effectiveness of growing such capability within the institution means we must draw these from the widest possible market. To thrive we need to seek investment, ingenuity and best practice, because these will be force multipliers to the effectiveness of our organisation, and we need to contribute to national prosperity.[45]

Today, proponents argue that the need to adopt the Whole Force is just as, if not more, pressing than when General Carter delivered his speech in 2015. Despite the well-reasoned and forceful arguments by CGS, little practical steps have been taken to progress the full adoption of the Whole Force since 2015. Part of the problem, implicit in CGS's 2015 speech, is that in some corners of Defence there is still a sense of antipathy, or at least reluctance, to embrace industry as 'trusted allies'. [46] If the UK is to optimise the delivery of current and future capabilities, more work is required to translate General Carter's ambition into reality. According to many respondents, this often-innate reluctance to accept the private sector as trusted partners is the key obstacle to be overcome.

---

[44] Galbreath, 'Investigating the Whole Force Approach,' 6.
[45] Ibid.
[46] Ibid.

This section provides contemporary analysis of industry contributions to the Whole Force in the UK. It begins by charting the evolution of private sector support to UK military operations, before defining the scope of industry contributions to the Whole Force since 2011. The chapter contextualises the Whole Force by examining its conceptual underpinnings; it then outlines examples of where the Whole Force has been successful. Drawing on these examples, as well as interviews and workshops conducted for this study, the chapter then articulates a set of barriers – some well-trodden, others emerging – which represent the main factors hindering industry's full integration into the UK Defence system, and thereby limiting the realisation of the Whole Force. Throughout, this section offers a set of recommendations, relevant for both Defence and industry, which, if adopted, will help to foster a deeper level of public-private engagement necessary to operationalise a true Whole Force.

3.2 A Brief Historical Overview of Industry Support to Military Operations

Although the formalisation of the Whole Force Concept arose out of the challenging economic environment that followed the 2007-09 global financial crisis, the contribution of the private sector to military operations has an established history in the UK, dating back centuries. For example, the Corps of Engineers was formally established in 1716 and historically relied heavily on contracted civilian workers.[47] Broadly speaking, however, for the next two-hundred-and-eighty-five years, the contribution of contractors to British military operations, as opposed to equipment programmes, remained relatively small. While the current trend of industry involvement in delivering Defence outputs can be traced to the 1980s, even as late as 1991, the number of contractors present in the Gulf War (providing equipment, logistic and infrastructure services) was said to have 'fill[ed] two mini-buses'.[48] Moreover, industry support to military operations during this period did not move past a basic form of contractorisation ('defined as the provision of a service by an external contractor that was

[47] National Army Museum, 'Corps of Royal Engineers,' accessed 10 May 2020, https://www.nam.ac.uk/explore/corps-royal-engineers.
[48] Louth and Quentin, *Making the Whole Force Concept a Reality*, 3.

previously provided by military or civil service personnel'[49]). As detailed below, the Whole Force seeks to move beyond this static relationship to a partnership model where industry is considered a genuine partner in the delivery of military outputs.

Since the end of the Cold War, successive governments have committed the UK to maintaining a global military footprint - including the ability to project capabilities overseas at high readiness - whilst at the same time, decreasing Defence spending and reducing the size of the military. In the space of a decade, the size of the Armed Forces decreased by more than 100,000, from 308,500 in 1990 to 205,600 in 2001.[50] Moreover, the UK, like the US, has placed a premium on the development of sophisticated defence platforms as a means of maintaining its competitive military edge; thereby, placing increased pressure on personnel to sustain and/or develop the appropriate skillsets to enable them to use increasingly complex equipment. This embracing of cutting-edge technology has also increased the need for wide ranging support services.[51]

It was during the expeditionary operations of the 21st century – particularly in Afghanistan and Iraq - that a sharp increase in the use of contractors as means of compensating for a shortage of personnel, support skills and resources was seen.[52] In Afghanistan, it was estimated that the number of MoD contactors totalled 6,500 - approximately 40 per cent of British personnel in Afghanistan (British troop numbers peaked at 9,500). This may be an underestimate, given the lack of accurate data, with some observers concluding that the actual number of deployed contractors could have been be closer to 10,000.[53] When military manpower is capped, as was the case in Afghanistan, contractors can act as force multiplier, adding capacity and resilience to an otherwise limited force structure. Given budget and

[49] Jay Edwards, *Contractorisation of UK Defence: Developing a Defence-Wide Contractorisation Strategy and Improving Implementation*, RUSI Occasional Paper, (London: RUSI, June 2018), 1, accessed 10 May 2020, https://rusi.org/sites/default/files/201806_rusi_contractorisationofukdefence_edwards_web.pdf
[50] Statista, Number of personnel in UK Armed Forces 1900-2019, accessed 4 December 2019, https://www.statista.com/statistics/579773/number-of-personnel-in-uk-armed-forces/.
[51] Mark Erbel, 'The underlying causes of military outsourcing in the USA and UK: bridging the persistent gap between ends, ways and means since the beginning of the Cold War,' *Defence Studies* 17, no. 2 (2017): 135-155, 141-2.
[52] Galbreath, 'Investigating the Whole Force Approach,' 18.
[53] Eugenio Cusumano, 'Bridging the Gap: Mobilising Constraints and Contractor Support to US and UK Military Operations', *Journal of Strategic Studies* 39, no. 1 (2016): 94-199, 108.

personnel constraints, the trend to use contractors, both at home and overseas, may well accelerate. Commenting on projections of possible future deployments, one analyst has noted that a medium-sized deployment of 8,000 would need to be supported by at least 1,000 contractors. Based on the experience of the Afghanistan campaign, this figure may be an underestimate.[54] This trend was politically and doctrinally confirmed in the 2015 NSS/SDSR which stated that the MoD would continue to rely on industry support where the private sector can add value to the delivery of Defence outputs.[55]

As the reliance on industry, at home and abroad, has increased, contractors have become an essential component of force structure planning, performing several non-military support functions at the 'tail-end'. Proponents argue that by incorporating this support, the Defence sector has been able to enhance delivery capabilities, whilst also improving efficiency.[56] It is estimated that contractorisation of public services in the UK could reduce costs by between 10 and 30 per cent.[57] If duplicated in the Defence sector, such efficiency savings should enable the MoD to maintain a well-equipped and combat-ready force during peacetime according to one academic.[58] Moreover, given the increasingly complex and sophisticated military technology in service, contractors can offer a variety of specialist skills that the military no longer possesses, in part because these skills are difficult and costly to develop in-house.[59] As Frank Camm notes:

> The military often uses a contractor source to maintain sophisticated equipment because, as the result of acquisition program decisions and personnel policies,

[54] Galbreath, 'Investigating the Whole Force Approach,' 18.
[55] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161 (London: Stationery Office, 2015), 33, accessed 10 May 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.
[56] David Shouesmith, 'Industry and Support to UK Contemporary Military Operations: A Practitioner's Strategic Military Perspective,' in *The Routledge Research Companion to Security Outsourcing in the Twenty-First Century*, eds. Joakim Berndtsson and Christopher Kinsey (Abingdon: Routledge, 2016), 225.
[57] DeAnne Julius, *Understanding the Public Services Industry: How big, how good, where next?* Public Services Industry Review (Department for Business, Enterprise & Regulatory Reform, July 2008), ii.
[58] Christopher Kinsey, 'Outsourcing Military Logistics and Security Services: The Case of the United Kingdom,' in *The Routledge Research Companion to Security Outsourcing in the Twenty-First Century*, eds. Berndtsson and Kinsey, 25.
[59] Ibid., 26.

> contractors often have better qualified personnel and more advanced methods to do this than military sources do, particularly when the equipment is newly fielded.[60]

To fully understand the role that industry has played, and continues to play, in the delivery of military outputs, Louth and Quentin note that contractors have provided two distinct, but complementary, roles:

> The first is the role played by businesses in preparing the military equipment, the servicing of equipment already in use by the military and the provision of training for military personnel in the use of materials and machines provided by the industrialist. The second function is the myriad of activities undertaken by industry within the theatre of operations itself at the sharp-end of military endeavours.[61]

The functions that this could encompass include: 'truck driving, warehousing and inventory management, depth repair of equipment, infrastructure engineering, non-military communications, and administration'[62] and strategic air and sea lift.[63]

Whilst recent decades have demonstrated the vital role that industry has played in the delivery of military output, during this period, the Defence-industry relationship has in many respects struggled to advance beyond that of a traditional client-supplier relationship. As is discussed below, if the full potential of the Whole Force is to be realised, the Defence-industry relationship will have to evolve into a partnership model, where industry is an essential pillar of a broader Defence Enterprise. In the words of one Army official, the Whole Force should be 'a seamless approach, which includes us having industry more deeply embedded and taking some decisions and control'.[64]

---

[60] Frank Camm, 'How to Decide When a Contractor Source is Better to Use Than a Government Source,' in *Contractors and War: the Transformation of US Expeditionary Operations*, eds. Christopher Kinsey and Malcolm Patterson (Stanford, CA: Stanford University Press), 239.
[61] Louth and Quentin, *Making the Whole Force Concept a Reality*, 3-4.
[62] Shouesmith, 'Industry and Support to UK Contemporary Military Operations,' 225.
[63] Kinsey, 'Outsourcing Military Logistics and Security Services,' 25.
[64] Interview with Army official, Telephone, 13 May 2020.

3.3 The Politics of the Whole Force

The origins of the Whole Force Concept (WFC) cannot be separated from the wider economic and political context that drove the 2010 SDSR which followed the financial crisis of 2007-09. The 2010 review, the first to link defence to a national security approach, was, as Cornish and Dorman have noted, also a 'politics-led' review, which was conditioned by the Conservative Party's view of economic management, as opposed to a truly strategic review.[65] As such, the 2010 SDSR cut the Defence budget by 7.5 per cent over four years; downsized the Armed Forces by 17,000 and the MoD's civilian workforce by 25,000 over five years; and abandoned several defence systems, such as the Nimrod MRA4.[66] The SDSR's findings, and the Coalition Government's broader austerity agenda, forced the MoD to launch a comprehensive reform programme, in which both civilian and military personnel would be restructured and cost-effectiveness was the driving principle. As one former MoD official noted, these 'politics-led' reviews had a 'distorting effect…on determining numbers' and prevented any discussion of workforce requirements, 'even though it would have made good sense to do so' as the numbers 'had no substantive underpinning'.[67]

The Levene report on Defence Reform in 2011 formalised the WFC, which sought to: '…ensure that Defence is supported by the most cost-effective balance of Regular military personnel, Reservists, MoD civilians and contractors'.[68] Despite broad acceptance of Lord Levene's recommendation, limited progress was made in turning the Whole Force into reality. Four years later, the then Defence Secretary, Michael Fallon, attempted to kick-start the process by shifting the language of the WFC into the Whole Force Approach (WFA) – in other words, moving from 'talking to walking a WFA'.[69] This political aspiration and indeed commitment was reflected in the 2015 NSS/SDSR, which re-affirmed the MoD's ambition to deliver a WFA.

[65] Paul Cornish and Andrew M. Dorman, 'Dr Fox and the Philosopher's Stone: the alchemy of national defence in the age of austerity,' *International Affairs* 87, no. 2 (2011): 335-353, 346.
[66] HM Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, Cm 7948 (London: Stationery Office, 2010), 32, accessed 27 November 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf; Louth and Quentin, *Making the Whole Force Concept a Reality*, 5.
[67] Communication with former Ministry of Defence official, 9 December 2019.
[68] Lord Levene of Portsoken, *Defence Reform*, 57.
[69] Galbreath, 'Investigating the Whole Force Approach,' 18.

The 2015 NSS/SDSR also sought to readdress some of the capability cuts of the 2010 SDSR by increasing spending on new equipment and increasing the size of the Royal Navy by 400 (to 30,450) and the RAF by 300 (to 31,750).[70]

Nevertheless, during this period, the high-level political direction failed to have the desired outcome and for many observers, the WFA stalled once again. As staff work got underway on the Modernising Defence Programme in 2017, MoD Capability personnel attempted to reinvigorate the process by renaming the WFA, the Whole Force by Design. In so doing, officials sought to move the WFA from being done by 'accident' to the deliberate approach of by 'design'.[71] Echoing these sentiments, the 2018 Modernising Defence Programme articulated that 'we now plan to strengthen the performance of the Whole Force'.[72] Reflecting on a decade of initiatives and some examples of genuine effort, supported by periodic political commitment, the Whole Force has almost been left to 'free-wheel',[73] as other priorities have emerged and then overtaken the Whole Force in importance.[74]

3.4 A Problem with Definition

In seeking to understand why the concept has continued to make only modest progress, many have returned to questions of definition and identity. Despite the Whole Force having been in existence for the best part of a decade, and its acceptance increasing across the Defence sector, including importantly amongst the FLCs, the MoD has not articulated a convincing Whole Force vision beyond an imprecise reference to a combination of Regular and Reserve military personnel, MoD civilians and contractors to deliver military effects. Consequently, as one senior Reservist noted, it 'means different things to different people…To me as a Reservist it is about Regular and Reservist…In another context it is military staff and civilian staff'.[75] This lack of clarity and resultant vision, is in many ways a direct consequence of the fact that the MoD has yet to fully develop and agree a concept that underpins the Whole

[70] Comptroller and Auditor General, *Ministry of Defence: Ensuring sufficient skilled military personnel*, 5-6.
[71] Interview with defence industry representatives, Skype, 7 April 2020.
[72] Ministry of Defence, *Mobilising, Modernising & Transforming*, 23.
[73] Louth and Quentin, *Making the Whole Force Concept a Reality*, 1.
[74] Interview with former Ministry of Defence official, London, 20 November 2019.
[75] Email communication with Royal Air Force Reserve officer, 20 November 2019.

Force. As recently as 2015, an MoD Defence Operational Capability Assessment on the Whole Force, concluded that: 'The WFA is neither formally defined within the Defence lexicon, nor commonly understood across Defence and the wider community; this has contributed to…only partial exploitation of potential benefits.'[76]

Drawing on evidence from several respondents, on both sides of the public-private divide, and evaluation of various existing characterisations, this study considers that the definition proposed by a joint MoD-ADS (the Aerospace and Defence sector trade body) working group (yet to be agreed throughout the MoD), is fit for purpose and should be adopted more widely:

> Effective, agile and resilient capability delivered by an integrated, pre-planned and affordable military capability comprised of a mix of Regular, Reserve, civil servant and industry supported by appropriate technology to meet Defence outputs.[77]

An agreed definition is important, but it is also important to emphasise that the Whole Force is not a fixed arrangement. It is context-specific and needs to consider who or what is best able to deliver outputs based on capability, skills, readiness and value for money.[78] Similarly, it is a mistake to simply view the Whole Force through the prism of replacing an expensive resource (Regular forces) with a less expensive resource (contractors). Rather, it needs to be understood as a capability-driven process.[79] Nor should the Whole Force be considered as solely people-centric, since it places capability at its heart. For advocates, it is primarily centred on blending different people, skills, infrastructure, equipment and resources together to deliver Defence outcomes.[80]

Recommendation: The Whole Force should be defined as: 'Effective, agile and resilient capability delivered by an integrated, pre-planned and affordable military capability

[76] Emma Parry et al., *Integration of the Whole Force: Understanding Barriers and Enablers to Task and Team Performance (O-DHCSTC_12_P_T2_083/005)*, Defence Human Capability Science and Technology Centre, (2016), 32.
[77] ADS Whole Force Working Group, Written Contribution to the Centre for Defence Studies (CDS), King's College London Whole Force study for The Serco Institute, 6 February 2020, 2.
[78] Interview with Royal Air Force Reserve officer, London, 2 December 2019.
[79] Parry et al., *Integration of the Whole Force*, 33.
[80] ADS Whole Force Working Group, Written Contribution to the CDS Whole Force study, 2.

comprised of a mix of Regular, Reserve, civil servant and industry supported by appropriate technology to meet Defence outputs.'[81] It should be circulated among all component parts of the Whole Force as the first step in formalising and standardising a shared understanding of the Whole Force.

3.5 Developing a Whole Force Framework

One of the key frictions associated with operationalising the Whole Force has been that decisions related to its implementation have not been placed within an overarching framework. As things stand all three Services - and arguably a number of individual units within each Service – have interpreted the Whole Force differently, leading to an inconsistent application across the Defence sector.[82] As one industry contractor noted, the way the Whole Force is implemented has been ad hoc and depends on 'what [a specific] unit is prepared to accept, either in how forward those people go or what roles they have. This var[ies] enormously'.[83] While there are significant examples of innovative working relationships between the FLCs and industry (discussed below), these have largely been developed in isolation and without a clear framework or doctrine to guide decision-making and broader implementation.

For the Whole Force to be properly understood and then consistently applied, it needs to be grounded in some form of conceptual framework, the development of which would allow projects to be assessed using clear and consistent metrics to determine if a Whole Force approach has been adopted.

Doctrine is one tool that could support this outcome which under the North Atlantic Treaty Organisation's definition is: 'Fundamental principles by which…military forces guide their actions in support of objectives. It is authoritative but requires judgement in application.'[84] This definition illustrates how doctrine is the link between principle and practice and, as a

[81] Ibid.
[82] Interview with former Ministry of Defence official, London, 20 November 2019.
[83] Interview with defence industry representative, Telephone, 26 November 2019.
[84] NATO Standardization Agency (NSA), *Allied Joint Doctrine for Host Nation Support AJP-4.5*, Edition B Version 1, (Brussels, NSA, May 2013), v.

former MoD official notes, 'allows you to challenge the Services and say, you have made choices in this area to [use an industry solution] and you are now getting the same output for less or better output but you haven't done it in this area, why haven't you done that?'[85]

There has also been limited conceptual debate in policy circles regarding what is and what is not an inherently governmental function; i.e., what functions can and what functions cannot be contractorised (although the Whole Force is clearly a wider issue than contractorisation).[86] According to the US Federal Activities Inventory Reform Act of 1998, an inherently governmental function is defined as 'a function so intimately related to the public interest as to require performance by…government employees'.[87] Unlike the US, where this discussion is well developed, in the UK little effort has been devoted to defining what are inherently governmental functions. The consequence has been confusion as to what is an appropriate role for industry, or how each constituent part of the Whole Force might combine in harmony to produce military outcomes.[88] This conceptual challenge has been complicated by the growing involvement of the private sector in more and more aspects of frontline operational delivery. For example, contractors were responsible, under military control, for operating the Hermes 450 Unmanned Aerial Vehicle in Iraq and Afghanistan.[89] As General Sir Nick Carter, as CGS, highlighted in 2015: 'WFA [Whole Force Approach] should probably be exploited in most areas of our endeavour – less combat perhaps, although I acknowledge that during the campaigns in Iraq and Afghanistan commercial expertise played a role in the "kill chain"'.[90]

Recognising the need to define the parameters of the Whole Force, there have been several attempts within the MoD to codify the Whole Force into doctrine. Approximately 18 months ago, MoD officials successfully lobbied the Vice Chief of the Defence Staff and the Deputy Chief of the Defence Staff (Financial and Military Capability) (DCDS (Fin Mil Cap)) to

[85] Interview with former Ministry of Defence official, London, 20 November 2019.
[86] Edwards, *Contractorisation of UK Defence*, 12.
[87] Kate M. Manuel, *Definitions of 'Inherently Governmental Function' in Federal Procurement Law and Guidance*, Congressional Research Service (CRS) R42325 (Washington, DC: CRS, December 2014), summary, accessed 29 July 2020, https://fas.org/sgp/crs/misc/R42325.pdf.
[88] Galbreath, 'Investigating the Whole Force Approach,' 20.
[89] Henrik Heidenkamp, *Sustaining the UK's Defence Effort: Contractor Support to Operations Market Dynamics*, RUSI Whitehall Report 2-12, (London: RUSI, April 2012), 5, accessed 10 May 2020, https://rusi.org/sites/default/files/201504_whr_contractor_support_to_operations_0.pdf.
[90] Galbreath, 'Investigating the Whole Force Approach', 6.

commission the Development, Concepts and Doctrine Centre (DCDC) to develop a Concept Note outlining the key principles of the Whole Force.[91] In consultation with and informed by the industry ADS Special Working Group on the Whole Force, DCDC produced a draft Concept Note that was (at least in part) circulated throughout the MoD – although the work was not shared with the FLCs. The Concept Note, once ready, should clearly articulate what the MoD wants the Whole Force to achieve and how it should operate.

Subsequently, this on-going work on the Whole Force was paused as DCDC shifted its focus to contributing to the Modernising Defence Programme and more recently the Integrated Review. Prior to the outbreak of the coronavirus pandemic, DCDC reportedly had intended to reinvigorate its work on the Concept Note in early 2020.[92] The Covid-19 pandemic and associated postponement of the Integrated Review again halted this work, further delaying this contribution to progressing the Whole Force. A clearly defined Whole Force framework could support the work of the Integrating Review by identifying *how* Defence will re-orientate its resources to address future strategic challenges.

Although the Concept Paper has yet to be finalised, there has been progress on defining a set of principles that determine what roles are suited to all component parts of the Whole Force. These principles, which will form part of the MoD's Defence People Strategy Part Two (due for publication in late 2020), outline the kinds of roles that can be performed by Regular or Reserve military, civil service personnel or external partners.[93] This codification is in our judgement an important element in advancing progress on the Whole Force and should be progressed as a matter of urgency.

Recommendation: DCDC should resume its work on the development of a Concept Note that has been informed by industry contributions. Once this work has been finalised it should be circulated for approval and endorsement in both the MoD and FLCs at two-star level and

[91] Interview with former Ministry of Defence official, Telephone, 16 April 2020.
[92] Interview with defence industry representatives, Skype, 7 April 2020.
[93] The MoD has transitioned its language from 'contractor' to 'external partner' to move away from an 'us and them' mentality to a partnership approach with industry. It also reflects the realisation that Defence may be reliant on 'external partners' from across the private sector, academia or individuals that are part of a Defence gig-economy. Interview with former Ministry of Defence official, Telephone, 16 April 2020.

above. The resultant Concept Note should then be used as part of the MoD and FLCs core planning in response to the Integrated Review.

3.6 Communicating a Whole Force Narrative

For the development of a detailed framework underpinning the Whole Force to succeed, it must be accompanied by a robust, top-down communication campaign to encourage greater acceptance. This requires the articulation of a strong and consistent narrative from MoD senior leadership to the FLCs, explaining the need for and potential benefits of the Whole Force.[94] Proponents believe that in adopting such an approach, the MoD will be able to increase its capacity and resilience, as it moves uniformed personnel 'from tail to teeth' and will gain the ability to access more critical skills.[95] In short, it is argued, the Whole Force can be a force multiplier.[96] Equally important in many ways, we heard that to ensure its acceptance across Defence, it is also important to communicate where it is not appropriate to use the Whole Force;[97] examples might include: where it is a combat role; where it is important for the MoD to retain in-house capabilities; and where industry cannot deliver an output more effectively or efficiently. Bounding the concept in this way would serve to reduce mistrust and 'friction' amongst sceptical elements across the Defence sector. As argued at a 2015 Centre for Historical Analysis and Conflict Research Whole Force workshop (which focused solely on the Army), the Whole Force's strapline could be 'civilian where possible, military where necessary'. The workshop also suggested that a possible Whole Force narrative should include:

1. *'Sharpening the bayonet not replacing it'.* Whilst industry will be integrated throughout much of the British Army's capability, it will not be employed in core direct combat roles.
2. *'Industry as a force multiplier'.* WFA is not about redundancies or necessarily reducing military manpower. It is about exploiting the talent civilians and contractors can bring

[94] Galbreath, 'Investigating the Whole Force Approach,' 18.
[95] Ibid., 16.
[96] ADS Whole Force Working Group, Written Contribution to the CDS Whole Force study, 8.
[97] Parry et al., *Integration of the Whole Force*, 32.

to many areas of our business and so allowing our soldiers to concentrate on their core business; soldiering.

3. *'Non-deployable, firm-base first'.* WFA efforts should be focused and proven in the firm-base first, before expanding into the deployed space – you simply cannot surge trust on operations.
4. *'Pan-Defence Lines of Development, pan-capability'.* WFA is more than logistic enablers and it is more than just a force mix of people types. Opportunities will be developed across all capabilities, functions and lines of development whilst recognising that the supporting functions are likely to provide the greatest opportunities.
5. *'Commanders' business'.* Industry must be a fully integrated part of the force both in barracks, on operations and on contingency. Commanders must engage with industry; they are part of the solution not a contractual minefield.[98]

Given that the Whole Force affects several diverse – public and private sector – organisations, the articulation of a clear and consistent narrative would allow each constituent part of the Whole Force to gain a better understanding of its respective role and responsibility and associated risk. It would also help to generate a deeper understanding across the sector that the success of the Whole Force rests upon the notion of a genuine partnership between the military and industry – in other words a Defence Enterprise approach. The need for such top-down direction was highlighted in a 2014 MoD concept paper setting out the challenge facing Defence:

> (CSO) [contractor support to operations] …provides capability that has been selected as more cost-effective than other sources and is delivered through choice or necessity. It is more than a 'bolt on' and must be integrated as a seamless part of the Whole Force… Success will require cultural and organisational change. Defence will need to move away from viewing CSO as something provided by 'outsiders' to Defence.[99]

[98] Galbreath, 'Investigating the Whole Force Approach,' 18-9.
[99] Parry et al., *Integration of the Whole Force*, 32.

The dissemination of a strong narrative would also help to reassure elements in the FLCs that the Whole Force is not an exercise in hiding manpower cuts or outsourcing by another name – a familiar refrain in certain circles we were told. There is no escaping the fact that the Whole Force was closely connected in the minds of some with, and resulted from, cuts to the size of the Armed Forces during the 2010 SDSR. It is also true that the use of contractors in the UK dates back centuries and in the words of one former MoD official, 'the intellectual [case for the Whole Force] is as sound now, as it was 200 years ago in Crimea – it is to make Defence better.' [100] It has been acknowledged by those across the Defence sector that, unless it is emphasised that the Whole Force is considered a means to increase capacity and resilience, it may be difficult to change the existing narrative in some sectors surrounding the Whole Force when the size of the military is being reduced[101] – as was the case in 2010.

Recommendation: Accompanying the communication of the proposed Whole Force definition, a persuasive, top-down narrative explaining the need for and benefits of the Whole Force should be communicated across the FLCs.

3.7 Who Owns the Whole Force?

It is apparent from this research project that a key part of the challenge of operationalising the Whole Force is a tension at the top of the MoD over who owns the process: is it the Chief of Defence People (CDP) or the DCDS (Fin Mil Cap), or both? According to a former MoD official, the ownership of the Whole Force seems '*de facto*' to rest with both teams; however, '*de jure*' responsibility for the Whole Force is unclear. At times, it has sat with the CDP, at other times with DCDS (Fin Mil Cap), whilst there has also been individual ownership by the heads of the Services. Concerned by the resource implications of taking full ownership of the Whole Force, both MoD Head Office teams 'have tried to push the responsibility to the other' to avoid being 'saddled with this rather ill-defined idea'.[102] This is despite the fact that during the 2015 NSS/SDSR and 2018 Modernising Defence Programme, senior MoD officials argued

[100] Interview with former Ministry of Defence official, London, 20 November 2019.
[101] CDS, The Whole Force by Design Roundtable: Summary of Discussions, King's College London, 11 December 2019.
[102] Interview with former Ministry of Defence official, Telephone, 16 April 2020.

that the ownership of the Whole Force needed to be established, with CDP taking full responsibility.[103] This confusion as to who owns the Whole Force has, inevitably, resulted in progress stalling and is an area where decisive change could yield positive results.

After consulting current and former MoD officials, we are persuaded that the CDP should be appointed Senior Responsible Owner (SRO) to plan, oversee and ultimately execute the Whole Force's delivery. As the Whole Force cuts across both CDP's and DCDS (Fin Mil Cap)'s portfolios, and both teams are essential in delivering the Whole Force, Fin Mil Cap personnel should support the CDP; thus, ensuring a coordinated process across all three Services. Having a clearly defined, accountable SRO would give operational momentum to the existing top-level intent to deliver the Whole Force. It has been indicated to the study team that these views chime with current thinking in the MoD.[104]

Connected to the issue of ownership, is the typical two-year rotation of many military and MoD staff which prevents institutional knowledge developing within Defence. [105] Consequently, officials sometimes have (understandably) limited knowledge of the intricacies of the Whole Force. Whilst the MoD has updated its employment policy to enable some staff to stay in post longer than two-years, reportedly this is seldom applied.[106] The creation of a cadre of dedicated MoD senior supporting staff, who remain in post for longer than two-years, would enable them to bring enhanced experience and expertise to the relationship with industry.

Recommendation: The CDP should be appointed SRO to plan, oversee and ultimately execute the Whole Force's delivery. The CDP should be supported by Fin Mil Cap personnel to ensure a coordinated process across the three Services. It may also be useful for cadre of dedicated senior supporting staff working on the Whole Force to remain in post for longer than the typical two-year postings.

[103] Email communication with former Ministry of Defence official, 7 July 2020.
[104] Interview with Ministry of Defence official, Skype, 19 June 2020.
[105] CDS, The Whole Force by Design Roundtable: Summary of Discussions, King's College London.
[106] Ibid.

3.8 Where the Whole Force Works

Currently, throughout most aspects of the military chain, elements of the Whole Force are evident, such as in training (the Royal School of Military Engineering-Holdfast), recruitment (Capita), facility management (Aspire), support capabilities (Babcock DSG) and operational capabilities (Heavy Equipment Transport with KBR/Fastrax).[107] However, as noted above, all three Services have implemented the Whole Force differently. For instance, the Royal Navy and RAF have reportedly adopted a more integrated and comprehensive approach, relying heavily on logistic and training support from contractors.[108] Reasons for this may be that both the Royal Navy and RAF do not have enough Regular manpower to be able to fulfil their core tasks without the help of Reserves, civil servants and contractors, and that more of the roles can be separated from direct combat.[109] A point that was reinforced by the then Chief of the Defence Staff, Air Marshall Sir Stuart Peach, in 2017, '…the navy can't operate…without the Royal Fleet Auxiliary'.[110] In examining realistic options for deeper, more effective private sector integration into Defence, it is helpful to outline three brief case studies to illustrate the breadth of industry contributions that have already been made in support of the Whole Force: KBR's provision of transporters to the Army; Serco's operation and maintenance support to the UK/US Ballistic Missile Early Warning Solid State Phased Array Radar (SSPAR) at RAF Fylingdales; and, the Command Support Air Transport contract for the BAe 146 aircraft of 32 (The Royal) Squadron.

KBR's provision of Heavy Equipment Transporters (HETs) to the Army, which included operational deployment during the Afghanistan and Iraq campaigns, is often cited as a Whole Force exemplar. Signed in 2001, KBR was awarded a 20-year contract for the provision of 92 HETs to transport the 72-ton Challenger II battle tank in a variety of peacetime and conflict

[107] Galbreath, 'Investigating the Whole Force Approach,' 18.
[108] Denis James, 'Strengthening the Private Sector's Role in UK Defence Engagement,' *Chatham House Research Paper*, (August 2017), 4, accessed 27 November 2019, https://www.chathamhouse.org/sites/default/files/publications/2017-08-25-defenceengagement1.pdf.
[109] Interview with former Ministry of Defence official, London, 20 November 2019.
[110] Stuart Peach, 'Valedictory Address as Chief of the Defence Staff: A Speech by Air Chief Marshall Sir Stuart Peach for Policy Exchange,' 5 June 2018, 5, accessed 27 November 2019, https://policyexchange.org.uk/wp-content/uploads/2018/06/CDS-transcript.pdf.

scenarios.[111] The HET capability has been integrated into Army Headquarters task planning functions. The scheme also pioneered the use of Sponsored Reserves (SR) - civilian contractors with special call-out liabilities who can be mobilised when the operational need arises. They comprised one third of HET drivers deployed on Operations Telic (Iraq) and Herrick (Afghanistan). Under this arrangement, the SR were held at high readiness, and served under military command when the risk level rose. Attached to a Tank Transporter Squadron during peacetime, the personnel receive basic military training and must achieve identical training standards as their Regular counterparts. Since 2003, over 150 SR have served in Iraq and Afghanistan, many of whom came under enemy fire; for example, one HET was destroyed in a rocket attack and a SR was awarded a General Officer's Commendation for his conduct during enemy contact. As is discussed below, a key risk that Defence faces when engaging industry is assured delivery; however, the use of SRs in Afghanistan and Iraq provides evidence that assured delivery is possible even in operational contexts.[112]

Serco's operation and maintenance support to the UK/US Ballistic Missile Early Warning Solid State Phased Array Radar (SSPAR), at RAF Fylingdales, is also cited as an example of the Whole Force in practice. The SSPAR, which replaced previous early warning radar in 1995, provides 360-degree cover over a nominal range of 3,000 nautical miles, day-and-night for 365 days per year. Other than 5 minutes of planned stoppage during the transition to SSPAR in 1995, Serco have provided uninterrupted around-the-clock assured delivery of the ballistic missile warning system. The maintenance of such a critical component of the UK's homeland defence requires a well-refined maintenance schedule and a fully integrated workforce. RAF Fylingdales has approximately 340 personnel, with roughly two-thirds drawn from the military and civil service and the remaining third made up of contractor personnel, who are on base 24 hours a day and are seamlessly integrated within the RAF's operational teams. Given military personnel only spend two-years in post at RAF Fylingdales, Serco operatives have lower training and evaluation costs as a result of lower staff turnover rates.[113]

---

[111] *KBR*, 'Replacing the Army's existing fleet of tank transporters and pioneering the use of Sponsored Reserves,' *KBR*, accessed 9 December 2019, https://www.kbr.com/en/experience/heavy-equipment-transporter-het.
[112] ADS Whole Force Working Group, Written Contribution to the CDS Whole Force study, 11-2.
[113] Ibid., 13-4.

Another example of the successful integration of industry in the delivery of military outputs, and the deployment of SRs, is the BAE/Serco Command Support Air Transport contract for engineering services on the BAe 146 aircraft of 32 (The Royal) Squadron. For most of their time, the engineering team work on the base at RAF Northolt, but when required, deploy with the aircraft on operations performing their primary role - but in uniform and under a different threat level.[114] Since 2003, there have been approximately 40,000 SR days on operations.[115] Moreover, SRs were used to operate port facilities in Iraq where there was no specialist capability in the Armed Forces to do so, highlighting the fact that SRs can provide capabilities that the military does not have access to. Whilst this model has proven successful, broadly speaking, the number of SRs that have been embraced by Defence remains limited – in 2015, it was estimated that only between 60-120 SRs per company had been deployed.[116]

These examples show some of the range of activities under the Whole Force. The research team repeatedly was told that there was patchy understanding of the scope and range of the Whole Force across the Defence sector and that a comprehensive compendium of existing and even planned Whole Force projects would be a valuable resource in promoting the concept. The study team understands that such work is being undertaken by the joint MoD-ADS Whole Force working group.

Recommendation: To generate understanding of where and how the Whole Force works, the MoD should compile a comprehensive compendium, regularly updated, that details all Whole Force projects, which can then be shared across the Services, and Defence more generally, to provide lessons learned.

3.9 Barriers to Optimising the Whole Force

As indicated above, there have been several innovative Whole Force solutions, but as an MoD official noted, such successes are 'probably an exception rather than the rule'.[117] To move the

[114] Galbreath, 'Investigating the Whole Force Approach,' 26.
[115] Email communication with defence industry representative, 9 December 2019.
[116] Galbreath, 'Investigating the Whole Force Approach,' 27.
[117] Interview with Ministry of Defence official, Telephone, 13 May 2020.

Whole Force debate forward, the challenge is to translate these isolated successes into a scalable and formalised approach;[118] however, before this can be achieved, several other challenges and barriers need to be overcome.

3.9.1 Cultural Frictions

As previous studies have highlighted,[119] one of the key 'frictions' standing in the way of the realisation of the Whole Force remains identity, or more broadly, the cultural barrier between the military and industry; much of this friction is of course the result of a lack of familiarity with the 'other', despite existing movement between these worlds already. The military is a tightly bounded institution and, as such, guards military culture and identity from dilution by internal (government) and external partners. As a result, such a dogmatic position can lead to an 'us and them' mentality, discouraging true partnerships from emerging.[120] Notwithstanding some progress in breaking down such 'frictions' over the past ten years, it is evident to many working in this area that a great deal more work needs to be done to ensure that industry is seen as a genuine partner, as opposed to 'just' a supplier of goods and services, or deliverer of output. The military's (and Defence more generally) limited understanding of industry, or an appreciation of the benefits that it can bring, has held back a genuine partnership between the military and external deliverers of service – a crucial step if the Whole Force is to be achieved.[121]

This lack of understanding has, at times, resulted in a degree of suspicion and mistrust towards industry, notwithstanding a different approach from those in the military who have embraced the Whole Force. At one end of this spectrum, a defence contractor claimed that, '[some military personnel] talk about partnership, but when it really comes down to it…you are just…a contractor. [The view is:] you are just there to steal as much money off the government as possible'.[122] While an extreme perspective, this view is, in part, conditioned

[118] Galbreath, 'Investigating the Whole Force Approach,', 18.
[119] Ibid.; Peter D. Antill and Jeremy C. Smith, 'The British Army in Transition: From Army 2020 to the Strike Brigades and the Logistics of Future Operations,' *The RUSI Journal* 162, no. 3 (2017): 50-58.
[120] CDS, The Whole Force by Design Roundtable: Summary of Discussions, King's College London.
[121] Galbreath, 'Investigating the Whole Force Approach,' 4.
[122] Interview with defence industry representative, Telephone, 26 November 2019.

by the misperception that contractors are *only* motivated by financial reward and do not share similar notions of serving the national interest as those in Service, civilian or uniformed. The study team was told that this was not the case, since contractors – some of whom are ex-Service personnel – are often as 'wedded to the [military's] desired outcomes as the people dressed in green'.[123] It is interesting to contrast this with the US, where the private and public partnership for the national good is a less contentious concept within the Service community.

There is also a common misperception that the Whole Force is outsourcing by another name (this study has found that a number of industry representatives consider the term outsourcing as generating negative connotations within government)[124] and, consequently, poses a threat to military capability. Whilst these views are not universally held, they do still exist in some areas of Defence. As one contractor recalled, an OF5 level officer responsible for a major capability programme betrayed such fears by remarking that 'I am not going to be the person responsible for emptying out the capability of my cap badge'.[125]

Another area of 'friction' relates to the perceived levels of exposure to risk and difference in pay, especially in high-threat environments, between contractors and Regular military personnel. A military officer argued that when on operations, a contract chef, who is perceived to be paid more than his Service counterpart, can refuse to 'go on patrol'; whereas a Service chef must obey this order, as he/she 'has no control over their life'.[126] This ignores the total contract cost and realised savings which are rarely appreciated by those not familiar with the detail, but this simplistic view also does not account for the fact that contractors also face significant risk on operation - between 2003 and 2010, 500 contractors lost their lives in support of Operations Telic and Herrick.[127] In comparison, during the same period, the number of casualties among military personnel in Iraq and Afghanistan totalled 354 and 179 respectively.[128] Unlike Service personnel, contractors are not entitled to the same state

[123] Ibid.
[124] Email communication with defence industry representative, 9 December 2019.
[125] Interview with defence industry representatives, Skype, 7 April 2020.
[126] CDS, The Whole Force by Design Roundtable, Ministry of Defence, 24 February 2020.
[127] David M. Moore and Peter D. Antill, 'The Use of Contractors on Deployed Operations (CONDO) in the Age of Austerity,' *RUSI Defence Systems* 14, no. 2 (2011), 4, accessed 27 November 2019, https://core.ac.uk/download/pdf/9637522.pdf.
[128] Cusumano, 'Bridging the Gap,' 108.

backed pension benefits or other associated assistance should they become injured.[129] More broadly, it is problematic to draw direct comparisons between military pay and civilian salaries, as the former is supplemented with indirect forms of compensation (e.g., subsidised accommodation, travel and other allowances, non-contributory pension, etc.) and generally, the civilian does not receive similar compensation. Added to this, it is also more likely that a contractor will be older than his Regular counterpart and correspondingly have more career experience and higher levels of pay.[130]

Significantly, in the above illustrations, perceptions, or rather misperceptions, of industry motives, supposed levels of threat to the military's culture and capability, exposure to risk on operations and perceived levels of pay, represent significant 'frictions' standing in the way of the Whole Force being fully embraced cross Defence. As Parry et al. suggest, 'perceptions may not be predicated on actual facts but may often rely on commonly held myths about the other…This underlines the importance of tackling workplace myths quickly and to produce a viable counter narrative.' [131]

As much of the cultural 'friction' between the military and industry is due to a lack of familiarity with the 'other', one solution to breaking down these barriers is for all component parts of the Whole Force to attend social events together.[132] Effective team and trust building, in many cases, is underpinned by informal contact. Socialising together offers a way of generating trust and breaking down cultural barriers.

Recommendation: Cultural barriers and misunderstanding about the nature of the Whole Force are critical 'frictions' holding back implementation of agenda. The MoD should develop and communicate a strong Whole Force narrative across the FLCs, explaining the critical role that contractors play within the Whole Force.

[129] CDS, The Whole Force by Design Roundtable, Ministry of Defence.
[130] Parry et al., *Integration of the Whole Force*, 55.
[131] Ibid.
[132] Ibid., 58.

3.9.2 Military Education

Another potentially important tool in breaking down the cultural barriers discussed above is through educating military personnel about the realities and possible benefits of working with other components of the Whole Force. During the Iraq campaign, US military personnel complained that they were unprepared to work alongside or manage contractors due to a lack of formal training prior to deployment. In particular, it was highlighted that most course syllabuses in staff training colleges did not include relevant information on the role of contractors. [133] It was noted, however, that shared experience on operations emphasised the importance of contractors to the delivery of military output, meaning that some of the barriers to understanding may be less than in the past.[134] The key, however, is to ensure that in the context of possibly fewer operational deployments this understanding is embedded in military education. British troops also reported that during the Afghanistan campaign there were several *ad hoc* instances where contractors were successfully integrated into the force structure; pointing to the fact that experience and familiarity of working together can help to break down cultural barriers. [135] Nevertheless, breaking down cultural barriers through experience on operations can be time-consuming, context specific and inconsistent.

The US has tried to address this and in 2009, the US Army established a tactical level Operational Contract Support course, which provides personnel with an introduction to the conceptual and practical aspects of operational contract support planning, requirements development, and contract management. In 2012, this was complemented by an Operational Contract Support Curriculum Guide, which outlines lessons learned from working with contractors and is used to inform Joint Professional Military Education. [136]

It is unclear to what extent comparable courses are offered at any level of officer or non-commissioned officer (NCO) training in the UK. As experience in Afghanistan and Iraq

[133] Moshe Schwartz and Jennifer Church, *Department of Defence's Use of Contractors to Support Military Operations: Background, Analysis, and Issues for Congress*, CRS R43074 (Washington, DC: CRS, May 2013), 4, accessed 29 July 2020, https://fas.org/sgp/crs/natsec/R43074.pdf.
[134] Ibid., 4; 11.
[135] CDS, The Whole Force by Design Roundtable: Summary of Discussions, King's College London.
[136] Schwartz and Church, *Department of Defence's Use of Contractors to Support Military Operations*, 12.

demonstrates, the trust and respect developed between Regular troops and contractors often fails to generate lasting cultural change, as Defence reverts to the status quo when the operation is concluded. Military education courses could provide a useful way of increasing awareness of the role of contractors in the Whole Force. If embedded into the curriculum of existing UK Military Staff Courses, such an option offers a long-term and sustainable way of breaking down some of the cultural barriers holding back the Whole Force and would help codify and imbue the notion of the Defence Enterprise as a joint endeavour. Such education should start as soon as officers (and NCOs) enter service, and it should continue throughout the entirety of their career. Moreover, the curriculum of existing UK Military Staff Courses could also be expanded to include specific modules on the contracting process and capability acquisition.

Recommendation: Military education courses that highlight the role of contractors in the Whole Force should be embedded into the curriculum of existing UK Staff Courses. Such education should start as soon as officers (and NCOs) enter service and should continue throughout the entirety of their careers.

3.9.3 Joint Defence-Industry Training Exercises

As previously mentioned, an important element in progressing the Whole Force is the development of trust between the military and industry. One method to build trust is to increase participation in joint training exercises. At present, contractors do not generally train with their military counterparts, except for SRs, however, even then the training is often designed to suit the military's schedule and/or is organised at short notice. It is self-evident that such an approach is sub-optimal.[137] As one military officer notes, 'by training together you engender that respect rather than master and subservient contractor.'[138] The Operation Herrick Campaign Study highlighted the importance of having 'routine contractor

[137] Interview with defence industry representative, Telephone, 26 November 2019.
[138] Interview with military officer, Telephone, 27 November 2019.

engagement in collective training'; a recommendation further identified in several other MoD reports.[139]

On the other side of the Atlantic, this lesson was echoed in a blunt Congressional Research Service report warning, 'conducting exercises without contractors could be akin to training without half of the force present.' Acknowledging the importance of training as a team, numerous US Government agencies and academics have petitioned for greater inclusion of contractors in military exercises. In response, the US has conducted training exercises that incorporate contractors; thereby helping to simulate the experience of cooperation on overseas deployment.[140] Another benefit of these joint exercises was noted:

> During a recent US Army 'UNIFIED QUEST' force development exercise, the extent of incremental 'contractorisation' of support and combat service support came as a sharp surprise to most operations-focused US Army leaders. They were unaware of the cumulative impact of an informal WFA on core US warfighting capability.[141]

Such exercises could offer the UK with potential examples of how to incorporate contractors into military training programmes. Not only would joint training exercises improve operational performance and integrated working practices, they would also help to break down cultural barriers between the military and industry and help to foster a 'team Defence' mentality on both sides.

Recommendation: To fully operationalise a true Whole Force model, there needs to be a comprehensive approach to the integration of contractors with their military partners before, as well as on operations. Joint training and exercise programmes not only would improve operational performance and integrated working practices but would also help to break down cultural barriers and help to foster a 'team Defence' mentality on both sides.

[139] Ministry of Defence, *Operation Herrick Campaign Study Report* (London: Ministry of Defence, 2015) in *Integration of the Whole Force*, Parry et al., 57.
[140] Schwartz and Church, *Department of Defence's Use of Contractors to Support Military Operations*, 18.
[141] Galbreath, 'Investigating the Whole Force Approach,' 20.

3.9.4 Commercial Structures and Contracting Frameworks

Discussions with numerous Defence stakeholders, on both sides of the public-private divide, indicated to the study team that another key barrier to progressing the Whole Force and moving to a partnership approach was existing sub-optimal commercial processes and contracting frameworks.[142] Notwithstanding the MoD's current procurement improvement initiatives and broader engagement with industry, one such barrier, it was contended, is Defence's lack of relevant and Whole Force specific engagement with industry. Generally, industry only tends to be invited into the chain at the end of an internal decision-making process when Defence puts a contract out to tender. This is especially true regarding conceptual development, the formulation of doctrine and training scenarios.[143] According to one MoD official, there are several reasons why industry is not always engaged early. First, the development and approval of business cases in the MoD is a slow process, meaning when projects are eventually approved there is often not enough time to conduct wide-ranging market engagement.[144] Second, whilst sections of the military do welcome early engagement with industry in the hope of developing innovative solutions, DE&S discourages FLCs from this, as it is feared that it could undermine the competition process.[145] This has had an unintended consequence of keeping the private sector unnecessarily at arms lengths in some cases, when a closer partnership would benefit MoD.

The problem is that across government, competition regulations stipulate that departments cannot favour one supplier over another; therefore, if a particular supplier is engaged before the contract goes out to tender, some believe that this could constitute one supplier gaining an advantage – such as influencing how the key requirements are written - in securing the contract. Consequently, if a supplier is perceived to gain an unfair advantage, some in Defence fear that they may be open to legal challenge. This anxiety, according to one Army official, 'makes us follow process doggedly… it would be a joy to have more discretion about how you

[142] CDS, The Whole Force by Design Roundtable, Ministry of Defence; Interview with defence industry representatives, Skype, 7 April 2020; Email communication with defence industry representative, 9 December 2019.
[143] Galbreath, 'Investigating the Whole Force Approach,' 4.
[144] Interview with Ministry of Defence official, Telephone, 13 May 2020.
[145] Interview with Army official, Telephone, 13 May 2020.

engage, and at what points you engage…[but] if we don't get the process right…[we are open to] challenge'.[146] While not unique to Defence, this does appear to be problematic in this sector and is worthy of further examination. An MoD official did note, however, that the informal engagement of industry was 'not impossible' but it 'takes a mature approach to do it well'.[147]

By not always engaging industry before the key requirements are written, Defence is constrained by incomplete knowledge of what the market can supply; leading to the lack of novel contractual frameworks, and ultimately, sub-optimal outcomes. This is especially problematic as the military sometimes has difficulty in framing key requirements accurately or keeping to those stated requirements as the contract proceeds. Part of the problem, according to an Army official, is that 'the right skills and experience do not exist in the people setting the requirements…particularly in the capability development directorate', which is responsible for horizon scanning and defining capability to meet future challenges.[148]

Even when industry is engaged before the start of the formal procurement process, there is sometimes limited coordination between Defence's capability, commercial, and DE&S teams. Contractors have noted that Defence commercial teams are often not part of these informal conversations with industry and as a result, this can lead to situations where the end-user's requirements are poorly communicated to industry, due to a lack of familiarity with commercial language/processes[149] Or, in other cases, 'results in unaffordable "gold-plated" solutions being offered by suppliers that are then "hollowed" out [by the commercial teams] to achieve an affordable contract'.[150] Instead, Defence commercial teams should ideally be involved in the process as early as possible to develop a joint approach with the FLCs that can then be communicated to industry, helping to ensure that the correct capability is attained, whilst also ensuring at value for money.[151] In response to some of these challenges, the Army has recently invested in three senior commercial officers who are embedded within the

[146] Ibid.
[147] Interview with Ministry of Defence official, Telephone, 13 May 2020.
[148] Interview with Army official, Telephone, 13 May 2020.
[149] Interview with defence industry representatives, Skype, 7 April 2020.
[150] Email communication with defence industry representative, 13 May 2020.
[151] Interview with defence industry representatives, Skype, 7 April 2020.

capability unit to help with the requirement setting process and to increase early market engagement.[152]

The requirement to ensure fair competition in tenders was not designed to prevent engagement with the private sector, rather it was designed to avoid companies from gaining an 'unfair advantage'. The unintended outcome of MoD caution in this area is clearly not the intention of the existing competition processes. To enable early and better communication between the MoD and industry, joint working groups could be convened, or other innovative methods should be identified to allow appropriate MoD-private sector engagement to support better outcomes.

Several industry representatives also reported that the contracting process with Defence can often be quite 'adversarial'.[153] The point was echoed by an Army official, who noted that there is 'an adversarial approach within pockets of DE&S'. This, it was argued, was a consequence of DE&S being heavily constrained by performance measures and targets, which though designed to aid delivery, in fact hinder the contract process. Given the number of projects that are not delivered as per the agreement or overrun, both in terms of cost and time, it was reported that DE&S are under severe ministerial pressure to demonstrate that they are working hard to ensure suppliers deliver on time and to budget.[154] If correct, this not only erodes trust between Defence and industry, but also hinders the progression of the Whole Force. Over the course of the study, it was frequently noted that positive behavioural models are critical to generating trust between Defence and industry that underpins the Whole Force. In the words of one contractor: 'Trust is the key ingredient in the Whole Force'.[155] A solution proposed by a number of respondents was to facilitate more joint Defence-industry dialogue, moving away from the existing transactional contracting model, to one based on a partnership approach.

[152] Interview with Army official, Telephone, 13 May 2020.
[153] Interview with defence industry representatives, Skype, 7 April 2020.
[154] Interview with Army official, Telephone, 13 May 2020.
[155] Personal communication with defence industry representative, 17 June 2020.

Recommendation: Defence officials should establish and regularly convene a Defence-industry working group including relevant senior officials from the MoD, officers from across the three Services, and industry representatives to identify a coherent plan to operationalise the Whole Force. Such forums could enable Defence to engage with industry as early as possible before framing contracts. Strategic engagement could improve outcomes; whilst also helping both sides progress towards a genuine partnership, with a greater sharing of both risks and rewards.

Another issue cited during this research that has reportedly hampered the progression of a partnership model is Defence's often inaccessible, complicated, and inflexible contracts according to those familiar with the process. As circumstances often change in Defence, even accurately drafted key requirements can quickly become out-dated. Therefore, existing contracting models were noted to better suit static or predictable situations that can be quantified as opposed to fluid situations; for example, in the context of surging or withdrawing, contracts are often ineffective at managing unpredictable or expensive situations.[156] As an MoD official observed, 'we are bound by our contracts…[because] we spend a lot of time writing contracts that are very tight and very rigid because we want to protect ourselves'. As a result, when the situation changes 'We find it hard to make those shifts within our contracts'. [157] The problem, in part, is again perhaps an unintended consequence of competition regulations; if Defence runs a procurement competition based on a set of key requirements, then significantly alters the requirements during lifecycle of the contract, it may have to test the market again. Moreover, since Defence finds it difficult to unpick tightly bound contracts, often the view is that it is easier to wait until the next competition.[158]

This was reinforced by a Royal Navy officer, who reported that Defence's internal commercial processes, and especially the complicated language used in many contracts, made it difficult to amend existing agreements. This was noted to be a problem given that military officers do

[156] Interview with former Ministry of Defence official, London, 20 November 2019.
[157] Interview with Ministry of Defence official, Telephone, 13 May 2020.
[158] Ibid.

not generally receive formal training in overseeing contracts.[159] Consequently, in the words of General Sir Nick Carter, 'the average quartermaster is not necessarily that well gifted in holding an industry contractor to account.'[160] An MoD official noted that Defence had 'written a library worth of commercial documents, but they are not easy for people to understand', even amongst commercial officers. In the wake of the collapse of the large construction and facilities management services company, Carillion, the government introduced a civil service-wide contract management training course. An MoD official suggested that the course, which offers three levels: foundation, practitioner and expert, could be beneficial for FLCs, so that they could better understand the process of contract management.[161] This appears to the study team to be a sensible suggestion and one that MoD should consider for all FLC officials who manage or oversee contracts.

Recommendation: All FLC officials responsible for managing and overseeing existing contracts should be given the opportunity to attend the foundation level of the civil service contract management training course if they are not already offered this, with consideration given to which staff would benefit from the advanced levels of this course.

Several respondents indicated to the study team that industry, for its part, must also improve their commercial processes by accepting more risk and adopting more flexible solutions during the contracting process. Other private sector representatives contended that the MoD's terms and conditions generate inappropriate transfer of risks to industry, and that the more industry is embedded in the Whole Force, the more risks that they may have to accept. An official noted that, from the Army's perspective, some defence companies are 'very risk averse' and that they can be very 'bureaucratic' in developing contracts.[162] This, it was suggested, resulted from industry's desire 'to ensure that the contract does not have loopholes and…what is to be delivered is…understood and "pinned-down" with appropriate penalties…in place'.[163] An industry representative further noted that:

[159] CDS, The Whole Force by Design Roundtable, Ministry of Defence.
[160] House of Commons Defence Committee, *Oral Evidence: Work of the Chief of Defence Staff,* Session 2019-21 HC 295 (2020), Q56.
[161] CDS, The Whole Force by Design Roundtable, Ministry of Defence.
[162] Interview with Army official, Telephone, 13 May 2020.
[163] Email communication with defence industry representative, 9 June 2020.

> In the same way that MoD commercial [teams] need to 'upskill', then industry needs to change approach to accept more calculated risk, to share the burden and move to being better 'partners'. [Industry] commercial staff tend to want to go for the jugular at…every opportunity. This needs to stop and…more fruitful dialogue [is required] with a better understanding of the customer's…needs and 'end game'. [164]

To achieve such a partnership, industry, it was suggested, may also have to consider adapting and liberalising its current operating frameworks. In terms of creating flexible contracts, the challenge as set out by an earlier study also 'is to enable the partnership to have the necessary flexibility to respond to changing circumstances without sacrificing VFM [value for money] as the industrial partner builds the cost of flexibility into the pricing'.[165] A contractor noted that industry needs to respond better to changing circumstances and provide more flexibility, by saying: 'you [Defence] are not using that pile of people or pile of equipment anymore because your requirements have changed, so why don't we transfer the resources into [something else]… That way, the [cost of the] contract doesn't need to increase over time, but it can evolve'.[166]

Early examples of this approach can be gleaned from how some defence companies have flexibly responded to the coronavirus challenge. For instance, the RAF's BAe 146 transport aircraft were rapidly repurposed to accommodate Medevac requirements and ventilators. This process would typically take at least a year, but it was achieved in eight weeks, and crucially, at no cost to the MoD.[167] Moreover, other Whole Force approaches have been evident in the creation of extensive hospital capacity (the Nightingale Hospitals) and the implementation of large-scale track and trace services in short periods. A contractor noted: 'Apart from operational necessity, the key to this has been that key suppliers have been trusted both to deliver at pace and to do so without abusing the resulting limited

[164] Ibid.
[165] Galbreath, 'Investigating the Whole Force Approach,' 22.
[166] Interview with defence industry representative, London, 29 November 2019.
[167] Royal Air Force, 'RAF Aircraft Adapted for Medical Use in Record Time,' Royal Air Force, 17 June 2020, accessed 30 June, https://www.raf.mod.uk/news/articles/raf-aircraft-adapted-for-medical-use-in-record-time/.

governance'. [168] Whilst these examples augur well for the future Defence-industry relationship, another contractor struck a more cautious note commenting, 'I think that you have to be careful about using the Covid-19 response as an exemplar for the Whole Force'. The contractor further stated that there are a variety of scenarios in which the Whole Force can be used and 'today we are in an extreme [scenario]…it is a national effort…a crisis that is essentially a threat to the whole nation. [Therefore, this scenario] invokes different behaviours.'[169] The study team believes that the Covid-19 crisis has changed the context of discussion around resilience and public-private co-operation and in this sense may prove to be an important stage in the adoption of Whole Force thinking.

3.9.5 Assured Delivery

Whilst the Whole Force offers Defence an avenue to increase resilience and capacity, there are a number of risks that the MoD need to assess and mitigate to enable further private sector integration. A commonly raised concern amongst Defence officials is that overreliance on industry in certain areas, can mean that Defence loses the in-house expertise to perform key functions, and/or the ability to design and manage contracts effectively.[170] Rebuilding in-house capability is often expensive and time-consuming, especially in, what has been, traditionally a base-fed organisation. As one Army official put it, there needs to be a clear strategy to determine 'where [Defence's] red lines are' in terms of what areas Defence could rely upon an industry solution. [171]

This links into the broader question of assured delivery, which is sometimes cited as an argument against embracing the Whole Force. The argument goes that if the contractual partner fails to deliver what has been agreed, as sometimes has been the case, Defence is exposed to risk. In other words, the contractor does not share the operational risk; rather, it is 'soldiers [who] do not have bullets to shoot at the enemy'.[172] Using an example from the recent 'unforeseen' coronavirus outbreak, an Army official noted that while there have been

[168] Email communication with defence industry representative, 29 June 2020.
[169] Interview with defence industry representatives, Skype, 7 April 2020.
[170] Shouesmith, 'Industry and Support to UK Contemporary Military Operations,' 225-6.
[171] Interview with Army official, Telephone, 13 May 2020.
[172] Interview with former Ministry of Defence official, London, 20 November 2019.

'some fantastic responses [from suppliers]', the situation has also been a 'great eye-opener in terms of the vulnerability of our supply chain' as some suppliers have 'refused to put their staff in harm's way'.[173] As the above example illustrates, in some cases, it is difficult to contract for unforeseen events, which involve high levels of risk; thus, undermining the delivery of military output. However, Defence needs to be also aware that both sides are accepting risk in Whole Force relationships and state-owned supply chains are not necessarily more reliable and efficient.

From an industry perspective, companies need to agree, from board level to shareholders, about the risks involved in participating in the Whole Force. For example, potentially putting employees in harm's way during operations, or having segments of their workforce deploy on operations with little warning and for prolonged periods.[174] Companies, for example in the extractive industries, have for many years on occasion put their employees into non-permissive environments, sometimes with acute forms of insecurity and have grappled with duties of care not commonly faced by the private sector. Agreed forms of good practice have been difficult to agree on, revealing the challenge for the private sector in embracing the Whole Force where it may involve deployment of staff alongside the Armed Forces in operations.[175] Aside from unforeseen circumstances, this is particularly important as the security environment becomes increasingly complex and peer-to-peer competition has returned. The possibility, albeit unlikely, of a high-intensity conflict or perhaps more likely 'grey-zone' conflicts with occasional spikes in ferocity, poses serious questions about the resilience of a Whole Force that relies heavily on contractors. This is especially so as the existence of the safer 'rear area' has been brought into question by recent operations. With Russian doctrine promoting the destruction of critical infrastructure early in a military campaign, it seems that the 'rear area' may no longer be an applicable term.[176] Of course 'rear areas' can now encompass the industrial base and the critical infrastructure of nations and already fundamentally involve the private sector. As such, decisions on whether

[173] Ibid.
[174] Galbreath, 'Investigating the Whole Force Approach,' 27.
[175] Trade associations and others have for many years attempted to get agreement for codes of conduct in various sectors but have faced issues in getting agreement across diverse private sectors entities, Private Study by CDS for industry association, 2010.
[176] Galbreath, 'Investigating the Whole Force Approach,' 21.

companies are willing to accept these risks must be made in advance, in order to facilitate the deployment of their employees at short notice, along with a better understanding of risk on both sides.

Connected to industry accepting the risks involved in participating in the Whole Force, companies also need to recruit employees with the appropriate skills and motivation and on the correct terms and conditions, i.e. this may mean specifically for SR positions, as opposed to transferring existing employees to SR roles.[177] The use of SRs may increase the provision of assured delivery as contractors deployed on operation could be activated as SRs, as the threat and risk level increases. Companies must also have the correct risk management structures, training, insurance, and family support systems in place.[178] By doing so, it is calculated, SR contracts have a greater chance of being fulfilled.[179]

Recommendation: If companies decide they want to play an active part in the delivery of the Whole Force, they must facilitate open discussion about the nature of the risks involved. This may mean acceptance that the risk associated with potentially placing their employees in harm's way involves recruiting employees with the appropriate terms and conditions.

Recommendation: When designing a blended workforce, the SR model should be considered having been proven through various overseas deployments (including the Afghanistan and Iraq campaigns), to be capable of ensuring assured delivery through highly capable and skilled individuals on deployments.

3.10 A Numbers Game

In the coming years, it is likely that the Whole Force debate will, to a large extent, be informed and shaped by decisions about the size of the military and levels of Defence spending not yet taken. Questions about the size of the military pose decision-makers with the conundrum, as one industry representative noted: it 'is a double-edged sword…the 2015 NSS/SDSR bought

[177] Interview with defence industry representatives, Skype, 7 April 2020.
[178] Galbreath, 'Investigating the Whole Force Approach,' 27.
[179] CDS, The Whole Force by Design Roundtable: Summary of Discussions, King's College London.

lots of new equipment… [but], if you have capped manpower how do you [operate] it?' On the other hand, capping manpower, 'actually ties one hand behind your back…the problem is that you can't go down on some numbers and up on others'.[180] This point was reiterated by several commentators, who noted that by maintaining force levels at arbitrary levels, commanders are restricted in their ability to 'balance their spending on people in uniform, those drawn from the contractor community, and the equipment and support bought'.[181] Consequently, Regular personnel often perform jobs that may be better suited – in terms of skillset and cost-efficiency - to contractors.[182] Moreover, as one former MoD official put it, the political commitments to maintain numbers at a pre-determined level, 'misses the point'; rather, 'the objective way of doing [it] would be to ask what is the best force mix to deliver the Defence tasks…re-defined…in the 2018 Modernising Defence Programme'.[183]

There are also practical obstacles that have prevented the realisation of a flexible, context specific workforce. One is rigid employment barriers within the MoD that prohibit civil servants or contractors from being temporarily appointed to Regular military posts to cover capability gaps. For example, once a Regular military post has been changed to allow a civil servant to take up position, financial barriers can make it virtually impossible to reassign the post to Regular military personnel when the in-house capability has been grown. As one former MoD official noted: 'we don't have the ability to say: for now, we have a temporary challenge how do we get short-term reinforcements... [until we have] time to grow the capacity internally'.[184]

Further consideration could also be given to the medium-to-long term impact of automation on the size of force structure; that said, some functions will be improved by developments in this area. There is also a broader – perhaps more fundamental – question that will impact the Whole Force debate, and one that should be answered in any forthcoming Integrated Review: What role the UK and its Armed Forces will play on the international stage in the coming

[180] Interview with defence industry representatives, Skype, 7 April 2020.
[181] John Louth and Trevor Taylor, *British Defence in the 21st Century* (Routledge: London and New York, 2019), 78.
[182] Interview with former Ministry of Defence official, London, 20 November 2019.
[183] Communication with former Ministry of Defence official, 9 December 2019.
[184] Interview with former Ministry of Defence official, London, 20 November 2019.

decades? Whilst this question falls beyond the scope of this paper, the nature of the UK's future international role is likely to be one of the most important shaping factors to determine the effectiveness of the Whole Force, especially if those pushing for the UK to transition from having an 'ambient' to a leading global role are successful.[185]

3.11 The Importance of Technology and Innovation

Another trend likely to inform the future Whole Force debate is how the military responds, in partnership with industry, to meet the technological challenges of today and tomorrow. In 2018, the sixth edition of the MoD's flagship public-facing horizon-scanning publication, *Global Strategic Trends*, highlighted the importance of the government-industry partnership: 'States that can form successful partnerships with private industry, especially with technology firms, are likely to derive a crucial advantage in future conflicts.' [186] More recently, the government indicated, in launching a new cross-government review into the UK's Defence and Security Industrial Strategy, the need for the development of a strong partnership with industry; the Defence Secretary stated that the Government's '…relationship with industry is crucial to maintaining the UK's position as a Tier 1 military power'.[187]

A critical element of this agenda is Defence's adoption of innovation, particularly new technologies, to defend the UK and its critical national infrastructure:

> The…challenge for…Defence…is profound…On the one hand…equipment is expensive to design, test, and manufacture, can be in service for decades, can be costly to operate, and must form part of an effective…force that can defeat Britain's enemies. On the other hand, technological development is so rapid and new technologies potentially so

[185] Lucy Fisher, 'Defence review in turmoil, say insiders,' *The Times*, 22 February 2020, accessed 10 May 2020, https://www.thetimes.co.uk/article/boris-johnson-s-foreign-policy-defence-and-security-review-in-turmoil-say-insiders-2fq9mz7gf.
[186] Ministry of Defence, *Global Strategic Trends: The Future Starts Today*, Sixth Edition, (London: Ministry of Defence, 2018), 137, accessed 6 April 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf.
[187] Ministry of Defence, 'MOD leads cross-government review into the UK's defence and security industrial strategy,' News story, 5 March 2020, accessed 7 April 2020, https://www.gov.uk/government/news/mod-leads-cross-government-review-into-the-uks-defence-and-security-industrial-strategy.

> disruptive to our existing forces and equipment that, what might be relevant and world-leading today, might become highly irrelevant…tomorrow.[188]

The development of new technologies is time-consuming and costly – and with no guarantee of success. As the UK's adversaries, particularly Russia, modernise and update their doctrines to exploit advantages such as in the sub-threshold space,[189] Defence needs to be agile in its response. It is often noted, however, that the MoD procurement process is cumbersome in reacting to technological change at pace and its decision-making processes are constrained by an inherent aversion to risk.[190] This reluctance is centred on the MoD's - and more broadly government's - desire to deliver capabilities whilst securing the greatest value for the public purse.[191] As such, the MoD's willingness to accept failed projects is considerably lower than it is in industry. Given the level of public and media scrutiny over how taxpayers' money is spent, in the words of a former MoD official, Defence expenditure must pass 'the *Daily Mail* test'. Therefore, guiding many of Defence's decisions is a desire to protect taxpayers' money and the MoD's reputation for financial probity. This approach, whilst understandable, can often lead to sub-optimal outcomes.[192]

In a 2018 report to the Defence Secretary, former Defence minister Philip Dunne MP argued that acceptance of failure needed to be adopted:

> A certain amount of failure should be acceptable when developing new ideas, especially during the early stages. In encouraging experimentation of different technologies and solutions, the key will be to identify failure quickly and as early and cheaply as possible.'[193]

---

[188] Louth and Taylor, *British Defence in the 21st Century*, 70.
[189] Stuart Peach, 'Annual Chief of the Defence Staff Lecture 2017, Air Chief Marshall Sir Stuart Peach, Chief of the Defence Staff,' *RUSI*, 14 December 2017, 2, accessed 27 November 2019, https://rusi.org/sites/default/files/20171214-rusi-cds_annual_lecture-acm_peach.pdf.
[190] Philip Dunne, *Growing the Contribution of Defence to UK Prosperity: A report for the Secretary of State for Defence* (July 2018), 44, accessed 10 May 2020, https://www.philipdunne.com/sites/www.philipdunne.com/files/attachments/Philip_Dunne_Defence.pdf.
[191] Irfan Ansari, 'Efficient and Effective Financial Management of Defence Resources,' in *The Political Economy of Defence*, ed. Ron Matthews (Cambridge: Cambridge University Press, 2019), 62-3.
[192] Interview with former Ministry of Defence official, Telephone, 16 April 2020.
[193] Dunne, *Growing the Contribution of Defence to UK Prosperity*, 44.

An MoD official echoed this view, noting that Defence could learn from the approach of start-up companies that abandon projects when it becomes evident they will fail, as opposed to the MoD which continues with projects even when failure is apparent.[194] This revised approach to risk strikes the authors of this report as crucial to the delivery of the Whole Force.

Recommendation: The MoD should accept more risk (including the possibility of early failure of some projects) when developing new technologies to ensure that it can respond in a timely manner to a rapidly evolving technological environment.

The evidence obtained in this research suggests that there is considerable scope for technological innovation to be a catalyst for the formation of a partnership approach between Defence and industry. The beginnings of such an approach are already underway, as General Sir Nick Carter noted citing the RAF's Tempest project, 'Team Tempest… [is] much more a technology partnership than an acquisition programme'.[195] The programme combines BAE Systems, MBDA, Leonardo and Rolls-Royce, RAF and MoD representatives working to develop the next generation of combat aircraft. To achieve this partnership model, General Carter emphasised that a new approach to risk would follow, since it '…will likely involve the adoption of a new outcome-focused approach to procurement that shares risk and opportunity with our suppliers, enabling collaborative development and incentivising innovation'.[196] To ensure trust forms the basis of such partnerships, there also needs to be robust communication channels between all members of the public-private consortium, we were told.

3.12 Defence Cyber and the Whole Force

Just as the development of new equipment is crucial, so too is the development of a highly trained workforce that has the capability of competing in the sub-threshold environment,

[194] CDS, The Whole Force by Design Roundtable, Ministry of Defence.
[195] Carter, 'Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019.'
[196] Ibid.

such as in the Defence cyber field.[197] General Mark Carleton-Smith, CGS, acknowledged recently that 'the threats posed by misinformation campaigns and cyber warfare', are more threatening than 'missiles and tanks'.[198] According to the MoD's Permanent Secretary, Sir Stephen Lovegrove, this is where 'the Whole Force is absolutely real, it is how our cyber capabilities will develop over the next few years'.[199]

Since 2010, the UK government has established cyber threats as a top-tier priority in successive national security strategies. It has developed a series of national cyber security strategies, currently coming to the end of its third iteration. These strategies have aimed to coordinate government activities and provide funding and strategic direction to grow digital skills and the cyber security sector as part of the national economy. There is a clear link between the success of governmental cyber activities, including Defence cyber, and the continuing growth of national digital skills and the vitality of cyber in the private sector.

The UK has a rapidly growing cyber security sector. A 2020 report for the UK government estimated that in 2019 there were 1,221 companies active in the cyber security industry, with the equivalent of a new cyber-security company being registered every week over the last two years. The report estimated that there were approximately 43,000 full-time equivalents working in the field, an increase of 37 per cent in the last two years. Annual revenue in the sector was estimated at £8.3bn, a 46 per cent increase since 2017.[200]

In the context of wider post-global financial crisis austerity and public expenditure reductions under the Coalition Government, cyber was prioritised for increased investment. For example, the 2010 SDSR invested £650m in a new national cyber security programme. Reportedly, the UK signals intelligence and information assurance agency, Government Communications Headquarters (GCHQ), secured 60 per cent of this investment, aimed at improving national

[197] Space and satellite operations, like cyber, offer examples of where Defence has turned to the private sector to deliver certain capabilities.
[198] David Bond, 'UK must rethink military strategy, warns army head,' *Financial Times*, 4 June 2019, accessed 4 May 2020, https://www.ft.com/content/094ad520-86d6-11e9-a028-86cea8523dc2.
[199] House of Commons Public Accounts Committee, *Skills Shortages in the Armed Forces*, Session 2017-19 HC 1027 (London: Stationery Office, 2018), Q. 61.
[200] Sam Donaldson et al., *UK Cyber Security Sectoral Analysis 2020: Research report for the Department for Digital, Culture, Media and Sport*, (London: Department for Digital, Culture, Media and Sport (DCMS), 2020), 2, accessed 29 July 2020, https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020.

cyber resilience and response to cyber-crime.[201] Significant investment was also directed to improving cyber security education, both at secondary and tertiary levels.

Robert Hannigan, former GCHQ Director, identified five core challenges facing governments as they reform their respective approaches to cyber: 'identifying and capitalising on scarce technical skills; access to data and advanced analytics; harnessing the talent and resources of the private sector; and achieving wider behavioural change.'[202] Whilst Hannigan was referring to broader national cyber security strategy, these categories are readily applicable to Defence cyber.

After a decade of broader national cyber strategy and investment, the progress of Defence cyber has been relatively incremental, particularly in the development of the joint GCHQ-MoD national cyber force. The slow pace of institutional evolution in offensive cyber has been offset, to some extent, by progress in military cyber operations – about which the government has become increasingly willing to speak publicly.[203] To build on this emerging capability, the government pledged £250m in 2018 to increase the national cyber force from its initial operating capacity of 500 to 2000 personnel.[204]

The Defence cyber mission is essentially two-fold. First, it involves the protection of defence networks and platforms from cyber-attacks. Second, it requires the development of an offensive component of the overall UK cyber force structure. Whether defensive or offensive in nature, high-end cyber operations require significant technical specialism, skill and experience. Defence cyber is, therefore, a particularly good example of the need for the Whole Force to be implemented effectively.

---

[201] Robert Hannigan, *Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre*, RUSI Occasional Paper (London: RUSI, February 2019), 8, accessed 29 July 2020: https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf.
[202] Ibid., 1.
[203] David J. Lonsdale, 'Britain's Emerging Cyber-Strategy,' *The RUSI Journal* 161, no. 4 (2016): 52-62, 54.
[204] Deborah Haynes, 'Britain to create 2,000-strong cyber force to tackle Russia threat,' *Sky News*, 21 September 2018, accessed 29 July 2020, https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653.

A multiplicity of actors currently operate in the domestic cyber security field, raising the question of how to determine the optimal relationship between Defence cyber and broader domestic cyber security initiatives in the public and private sectors.[205] There is a need, for example, to clarify the future Defence cyber role in homeland cyber defence, including the cyber security of critical national infrastructure. The MoD already cooperates closely with the national cyber security centre, but it is important to define the requirements for the future domestic cyber defence mission during the delayed Integrated Review. This determination will have direct implications for the future workforce strategy and force structure required for Defence cyber.

Reflecting on cooperation between GCHQ and the Armed Services on offensive cyber, Robert Hannigan has observed that, despite some progress in the last 10 years, the Armed Forces still need to address structural barriers to developing its cyber workforce: 'The UK Single Services have made great strides in cyber, but have much further to go. Unlike in the US, it is difficult to spend a whole career in cyber in the UK Armed Forces, for example; all involved know this will need to change. But career structures and incentives take time to modify and they lag behind the agility needed for personnel who are trained in the constantly advancing technologies applicable in cyber conflict.'[206]

In addition to the challenge of de-conflicting domestic roles and responsibilities between Defence and other institutional actors in cyber, and to addressing internal, structural barriers to progress, Defence also faces the challenge of being only one recruiter amongst many competing for the same talent. As compared with the private sector, for example, Defence (and other parts of government) starts at a disadvantage in the remuneration it can offer to attract top cyber talent. To succeed in these market conditions, Defence needs a clear understanding of its cyber skills requirement and an integrated cyber workforce strategy that incorporates both its defensive and offensive cyber missions. It must also continue to work closely with industry: Defence relies on a broad range of contractors[207] and coordinates with

[205] Noel K. Hannan, 'Use of Reserve Forces in Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches,' *The RUSI Journal* 160, no. 5 (2015): 46-51, 49.
[206] Hannigan, *Organising a Government for Cyber*, 31.
[207] DCMS, 'Guidance: Cyber security supplier to government scheme: list of participating companies,' GOV.uk, 17 September 2018, accessed 29 July 2020, https://www.gov.uk/government/publications/cyber-security-

industry, for example through the Defence cyber Protection Partnership to improve the cyber-security of the Defence supply-chain.

According to General Sir Nick Carter, the Defence cyber workforce is a leading part of Defence modernisation as it addresses the challenges of recruitment and retention of cyber talent:

> We are establishing integrated career structures where appropriate that are blended between the Services and our civilians – we are calling this 'unified career management' and the first of these blended career fields based on cyber will be initiated next year. It will be based on clearly understood skills frameworks and, on that, we will increasingly encourage lateral movement and entry on an enterprise basis with the private sector to provide greater opportunity for talent to be maximised for collective benefit. We will pilot this imminently, looking to establish a common human resource management model with some of our key industry suppliers.[208]

The use of Reservists has also played an increasing role in UK Defence cyber strategy,[209] as part of the broader shift towards developing the role of Reservists since 2010.[210] A joint cyber Reserve force was established in 2013. The respective Armed Services use different criteria for recruiting cyber Reservists, so the creation of a joint cyber Reserve was a positive step.[211] A recent example of the cyber Reserve in action was its contribution to Project OASIS, part of the development of national 'test and trace' applications during the COVID-19 pandemic emergency.[212]

Effective use of the Whole Force can provide significant benefits to Defence cyber. It is important, therefore, that Defence cyber proceeds on the basis of clear strategic objectives

---

supplier-to-government-scheme/cyber-security-supplier-to-government-scheme-list-of-participating-companies.

[208] Carter, 'Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019.'

[209] Lucy Fisher, 'Britain's parallel army of cyberwarriors,' *The Times*, 17 August 2019, accessed 29 July 2020, https://www.thetimes.co.uk/article/britains-parallel-army-of-cyberwarriors-gzkzzdnvh.

[210] Timothy Edmunds et al., 'Reserve forces and the transformation of British military organisation: soldiers, citizens and society,' *Defence Studies* 16, no. 2 (2016): 118–136.

[211] Hannan, 'Use of Reserve Forces in Support of Cyber-Resilience for Critical National Infrastructure,' 50.

[212] Sam Connell, 'Saluting our Cyber Reservists,' *Defence Digital*, 24 June 2020, accessed 29 July 2020, https://defencedigital.blog.gov.uk/2020/06/24/saluting-our-cyber-reservists/.

and a systematic determination of the division of effort: between Services; civilian and military contributors; Defence and other parts of government; and the private sector. Holistic strategy is required, integrating defensive and offensive dimensions of the cyber mission and based on rigorous analysis of the national Defence cyber capabilities and workforce that should be developed. With so many consequential participants in the cyber landscape, this process must be inclusive, but it must also be actively managed and driven by decisive leadership. Just as the Whole Force itself would benefit from greater clarity of ownership, so too would its Defence cyber component.

Recommendation: The Integrated Review should include a Defence cyber workforce strategic audit, identifying the skills and force structure required for the defensive and offensive cyber missions through to 2030. This audit should assess the required size and scope of civilian, military (Regular and Reservist), and private sector contributions to Defence cyber.

3.13 The Defence Enterprise Approach and Skills Framework

With a challenging recruitment and retention scenario, the MoD faces a number of obstacles in modernising its workforce and capabilities. A common refrain the study heard was that the MoD needed to think creatively about the ways in which it could tap into a pool of expertise that is not traditionally associated with Defence and how to incorporate it into a future force.

To be fair, in order to realise the benefits of the Whole Force, the MoD has tried to adopt some novel and flexible working models.[213] One example, reportedly under consideration, is a plan to create new military cyber-ranks to attract specialists from the private sector. Under the proposals, civilian experts could be encouraged to enlist on a part-time basis – perhaps, working in the evenings – through the establishment of a parallel career structure.[214] Such an approach forms part of a broader shift in thinking within the MoD, as previously, the MoD favoured addressing skills gaps by growing inhouse capability - as opposed to accessing skills

[213] Ministry of Defence, *Defence People Strategy Part One*, (London: Ministry of Defence, March 2020), 5.
[214] Fisher, 'Britain's parallel army of cyberwarriors.'

from the private sector (either contractually or on an ad hoc basis). The latter option, whilst traditionally considered sub-optimal, is now seen as advantageous, as one former MoD official elaborated: 'If I want a world class cameraman, I could recruit a *BBC* cameraman, who within two years would no longer be world class because Defence can't maintain the skills necessary for the communication of the message the way that the *BBC* could'. In this fluid recruitment environment, continual work is required to determine whether the advantages of growing specialist skills in-house outweighs the disadvantages of accessing them from the private sector.[215]

For its part, industry may also need to adopt different methods to help the MoD and military to address skills gaps. As the nature of warfare changes and drives the need to acquire new skills, industry will have to be willing to develop and provide a wider range of skills and equipment than previously has been on offer.[216]

Recommendation: As the character of conflict changes, industry must be willing to develop and provide new skills that Defence will increasingly need. This may involve both sides collaborating on identifying an effective long-term manpower strategy.

It should be remembered that to some extent, Defence and industry are facing similar recruitment and retention issues, especially that of accessing staff with critical skills. Given that these challenges are a result of wider societal shifts, Defence and industry will need to develop innovative solutions to enable both parties to continue to operate effectively and to ensure that they can access the required skillsets. Historically though, Defence and industry have often competed against each other in the recruitment marketplace.[217] As shortages in critical sectors become more acute, the development of a genuine partnership under the Whole Force could offer both sides a range of mutual benefits. For example, industry contains many skills, such as portfolio management, risk management and project delivery,[218] that could be highly desirable in Defence, but which are rarely core competences within the Armed

[215] Interview with former Ministry of Defence official, London, 20 November 2019.
[216] Galbreath, 'Investigating the Whole Force Approach,' 5.
[217] Ibid., 10.
[218] Louth and Quentin, *Making the Whole Force Concept a Reality*, 10.

Services and, as discussed above, are not elements that are currently taught at most levels of staff training. Moreover, not only can external partners bring a fresh perspective and innovative thinking to Defence problems, many of those working in the industrial sector already have years of subject matter expertise, making them potentially valuable and reliable partners. Similarly, Defence contains a variety of skills that are in demand in the private sector, such as 'command, leadership and management training and experience' raising the prospect of flexible career planning, beyond that currently offered. [219]

An important way in which Defence has sought to foster a genuine partnership with industry is through the adoption of a Defence Enterprise approach, which establishes a long-term, collaborative relationship to pool resources where they are most needed. [220] A pilot scheme, which is expected to be rolled out in 2020, involves Royal Logistic Corps (RLC) drivers being seconded to industry for an extended period.[221] This innovative programme, which is due to last for 12 weeks, is designed to offset an industrial sector recruitment and retention crisis for heavy good vehicle drivers, especially among younger drivers.[222] In turn, RLC drivers will enhance their skill levels and access opportunities to gain qualifications before their return to their military issues.[223] By working together in such ways, both sides could potentially manage skill shortages in the future, fostering a greater Defence Enterprise ethos.[224] There are, of course, risks with such an approach. From a Defence perspective, military personnel will be exposed to alternative, and perhaps more attractive, working conditions, such as working closer to home and more regular working patterns. [225] The private sector also expressed concerns about Defence poaching their best people, revealing that both sides of this debate are still struggling to accept the perhaps inevitable future of revised and more flexible employment models.

[219] Galbreath, 'Investigating the Whole Force Approach,' 10.
[220] Ministry of Defence, *Army People Strategy*, (London: Ministry of Defence, 2020), 7, accessed 10 May 2020, https://aff.org.uk/wp-content/uploads/2019/11/pers_sub_strat_booklet_final_screen.pdf.
[221] Ibid.
[222] Marie McBeth, 'Multimodal 2019 – The HGV Driver Skills Shortage Continues – What's The Solution,' Ten Live Group, 2 July 2019, accessed 10 May 2020, https://tenlivegroucom/multimodal-2019-hgv-driver-skills-shortage-whats-the-solution/.
[223] CDS, The Whole Force by Design Roundtable, Ministry of Defence.
[224] Galbreath, 'Investigating the Whole Force Approach,' 10.
[225] Parry et al., *Integration of the Whole Force*, 42.

Recommendation: Pilots projects such as the current RLC driver project, which focuses on low-skilled roles, could act as a pathfinder for the development of schemes that focus on higher-skilled roles and should be assessed with this in mind.

Recommendation: For an effective partnership model to develop, Defence and industry must move beyond the initial step of only sharing human resources to also sharing information and knowledge. This may involve companies sharing commercially sensitive information, such as Human Resources practices.

There are other opportunities to expand the Defence Enterprise approach. One ambitious proposal suggested by a Royal Navy officer involves a joint Defence-industry recruitment campaign. This, it was argued, could include a joint recruitment website for all component parts of the Whole Force, which would allow recruits to assess all options available to them in one place and choose which part of the 'Defence team' suited them most.[226] Whilst it was noted this was 'the utopia' outcome, realistically a wide-ranging joint recruitment campaign appears some way off. Nevertheless, there have been some isolated examples of a Defence Enterprise approach in this regard. Serco Group, for example, have made the Royal Navy aware of unsuccessful, but high scoring, applicants from their recruitment campaigns in the hope that they would gain employment in the broader Defence Enterprise.[227]

Defence has also considered other, complementary, recruitment approaches. One such model is lateral entry, which allows industry or private sector representatives to join the military in mid-level positions as opposed to entering at the base-level. One RAF officer noted that previously the military 'conflated qualified and experienced' but just because someone does not have the relevant military experience, does not mean that they cannot bring qualifications and expertise to Defence.[228] The scheme could allow personnel with relevant experience and, in particular, niche skills (such as cyber) to move back and forth between civilian and military roles gaining experience and seniority in appropriate places. Whilst the

[226] CDS, The Whole Force by Design Roundtable, Ministry of Defence.
[227] Of the 45 applicants in the 2019 assessment day, four were selected for apprenticeships with Serco and three subsequently applied to join the Royal Navy. Interview with Royal Air Force officer and defence industry representative, 19 February 2020.
[228] Ibid.

lateral entry option has been available for several years, it has been seldom used. For instance, as of 2018, only 50 people had been recruited through lateral entry schemes.[229] Notwithstanding this limited take-up, the Defence People Strategy is advocating the expansion of alternative routes to entry, including lateral entry schemes.[230] These schemes potentially offer an untapped pool of human resource for the military, especially in highly specialised areas.

Since 2010, the Reserves have become an increasingly important component of Defence's ability to deliver military outputs. So much so, the role of the Reserves has moved 'from supplementary forces to be called on at times of national emergency, to an integrated and indispensable part of the force structure as a whole.'[231] The Reserves also offer Defence the ability to access specialist or niche skills as demonstrated by their involvement in helping to build the Nightingale Hospitals during the coronavirus pandemic.[232] This study welcomes the Reserve Forces 2030 review which is developing a variety of innovative options to ensure that the talents of Reserves are maximised.

Recommendation: Alternative routes to entry, including lateral entry schemes, which open opportunities in Defence to suitably qualified applicants from outside the military, could offer Defence an untapped pool of human resource, especially in highly skilled areas. Whilst these routes to entry should not be considered a panacea to Defence's recruitment and skills challenges, such programmes should be encouraged and developed.

[229] House of Commons Committee of Public Accounts, *Skill shortages in the Armed Forces*, 14-5.
[230] Interview with former Ministry of Defence official, Telephone, 16 April 2020.
[231] Timothy Edmunds et al., 'Reserve forces and the transformation of British military organisation: soldiers,' 121.
[232] Ministry of Defence, 'Ministry of Defence seeks to maximise Reserves contribution through new review,' 3 June 2020, News story, accessed 30 June 2020, https://www.gov.uk/government/news/ministry-of-defence-seeks-to-maximise-reserves-contribution-through-new-review#:~:text=The%20Reserve%20Forces%202030%20review,wider%20government%2C%20business%20and%20society.

4. The Whole Force: International Examples

4.1 Introduction

Considering the Whole Force from a global perspective, the UK appears to be the most explicit in its articulation of its Whole Force intentions. However, this is not to argue – at this stage - that the UK has necessarily developed its Whole Force approach more than other countries. The US provides the most comparable example of where the Whole Force has, in some respects, been practiced. For example, in the area of public-private partnerships, the US has relied heavily on industry support.

The increasing discussion of the movement of employees between the private sector and the military is due to the realisation that expertise can be leveraged from the private sector that does not exist in the military. This approach addresses many of the issues militaries face in retaining talent. Conversely, as the case of Israel shows, the quality of military training, particularly in the area of cyber security, can be advantageous to the growth of small businesses and to the economy more broadly.

There are various small states which also adopt Whole Force (or similar) models. For the Nordic states, there are geopolitical reasons as to why they have traditionally adopted Total Defence postures – the integration of military and civilian activities within a holistic approach to security.[233] In other small states, such as Israel, Total Defence postures are both geopolitical and cultural. The concept of the Whole Force (or similar) addresses the question of civil society engagement and how this is articulated and enacted.

Internationally, the Whole Force is most advanced in the area of contractual relationships between the military and industry. While these relationships are firmly established in the UK and the US, the practice of contract management is consistently under review. The processes

[233] Björn von Sydow, 'Resilience: Planning for Sweden's "Total Defence",' *NATO Review*, 4 April 2018, accessed 29 July 2020, https://www.nato.int/docu/review/articles/2018/04/04/resilience-planning-for-swedens-total-defence/index.html.

through which governments and the military manage contractual relationships with industry is possibly one of the most important aspects of any attempt to enact any iteration of a Whole Force approach.

The Whole Force has developed during a decade of geopolitical and strategic transition. The era of the 'global war on terror' after the 11 September 2001 terrorist attacks was characterised by a focus on counterterrorism and counterinsurgency. This has gradually shifted towards the increasing prioritisation of state actor threats, most notably in the 2017 US National Security Strategy's statement that: 'after being dismissed as a phenomenon of an earlier century, great power competition [has] returned.'[234]

In the same period, UK national strategy has also responded to these developments, for example in its turn towards 'modern deterrence' and countering 'grey-zone' threats in the years after the Russian invasion of Ukraine in 2014.[235] The same imperatives have led other states to re-focus their respective national security strategies on the principle of Total Defence. The UK Fusion Doctrine, most closely associated with the 2018 National Security Capability Review, is motivated by a similar concern to pursue a 'whole of system' approach to national security.[236]

Whilst Total Defence, the Fusion Doctrine, and the Whole Force are conceptually distinct and separate activities, they represent national responses to a series of challenges faced by states in a shared strategic environment. Whatever the original motivation of the Whole Force, the principles and policies it encompasses are integral to effective delivery of the national defence strand of a Fusion Doctrine or Total Defence strategy. As such, understanding of the

[234] White House, *National Security Strategy of the United States of America* (Washington D.C: White House, December 2017), 27, accessed 29 July 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.
[235] Joe Devanny, 'UK National Security Decision-Making in Context: The Ukraine Crisis and NATO's Warsaw Summit Meeting,' *Sasakawa Peace Foundation*, 2018, accessed 29 July 2020, https://www.spf.org/projects/upload/UK%20National%20Security%20Decision-Making%20in%20Context%20%28Devanny%29.pdf
[236] HM Government, *National Security Capability Review* (London: Stationery Office, 2018), 10-11, accessed 29 July 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.

Whole Force can be improved by assessment of international comparators, analysing the similarities and differences between Total Force and Whole Force approaches. This assessment complements a parallel analysis of the potential lessons for the Whole Force from the broader US Defence context, especially in the area of public-private partnerships and the use of contractors. However, there remain calls for a more integrated Whole Force approach and increased coordination of a whole-of-government and industry mobilization, as outlined in the *Inspired to Serve* commission.

Moreover, a specific case of US Defence cyber offers a series of relevant lessons to the UK Whole Force. Cyber security is increasingly cited as one of the largest national security challenges, a fact that CGS General Mark Carleton-Smith recently acknowledged as noted in the previous section.[237] As such, cyber security may in time form a large component of the Whole Force, particularly in terms of private sector engagement. However, the integration of cyber security capability brings various challenges that relate to civil-military relations and will arguably continue to be one of the most challenging aspects within the Whole Force. The question of cyber security addresses questions of jurisdiction; whether cyber security should be under the authority of the military or government and how government and the military engage with the private sector. The complexity of the relationship with the private sector is outlined below and varies across countries.

This section starts by examining the Defence public-private partnership in the US and the specific case study of US Defence cyber. It then draws out other relevant Defence cyber examples from around the world, such as Israel and Estonia. The section then contextualises and explores the concept of Total Defence doctrines in Asia and Europe, highlighting lessons for the UK. It then briefly discusses the adoption of various Reserve models, before analysing employment models internationally. By considering international examples, the section draws out specific insights for the UK's Whole Force.

4.2 The Public-Private Defence Relationship in the United States

[237] Bond, 'UK must rethink military strategy, warns army head.'

The US is the world's most capable military power. It outspends all other countries, accounting for 39 per cent of global defence expenditure in 2019. In context, the world's second-highest spender, China, accounted for just 10 per cent.[238] This vast expenditure makes the US government the world's largest customer for the defence industry. As the 'special relationship' with the US has been the cornerstone of British defence policy for the past 75 years, a deep web of ties, centred on interoperability and mutual utility, have developed and continues to inform and shape UK policies. Moreover, many of the UK's national security structures have been directly influenced by the US, including the National Security Council and National Security Advisor role. It is, therefore, unsurprising that the US's embracing of industry offers valuable lessons for UK policymakers.

The US Department of Defense (DoD) has a long history of incorporating contractor support to military operations across a wide range of operations. Private sector contracts accounted for over half of the DoD budget in 2019, US$370bn out of US$676bn. This represented a 164 per cent increase in the department's contractor spending as compared with 2001.[239] As such, it has been calculated that contractors frequently accounted for 50 per cent or more of the total DoD presence in any given country.[240] Military contractors can be categorised into three groups: Military Provider Firms, Military Consultant Firms, and Military Support Firms.[241]

In the US, the benefits of industry support are widely acknowledged. Industry can provide expertise in a variety of areas such as training, supply chain management and equipment maintenance, with many proponents arguing that it is more efficient for industry to deliver these (and other) support tasks; [242] thus, allowing soldiers to move from 'tail to teeth'.

[238] International Institute for Strategic Studies, 'Chapter Two: Comparative defence statistics,' *The Military Balance* 120, no. 1 (2020): 21-27, 21.
[239] Heidi Peltier, *The Growth of the 'Camo Economy' and the Commercialization of the Post-9/11 Wars*, Watson Institute Brown University/Pardee Center Boston University (June 2020), 1, accessed 29 July 2020, https://watson.brown.edu/costsofwar/files/cow/imce/papers/2020/Peltier%202020%20-%20Growth%20of%20Camo%20Economy%20-%20June%2030%202020%20-%20FINAL.pdf.
[240] Heidi M. Peters, *Defense Primer: Department of Defence Contractors*, CRS IF10600, (Washington, DC: CRS, January 2020), 1, accessed 12 June 2020, https://fas.org/sgp/crs/natsec/IF10600.pdf.
[241] Alane Kochems, *When Should the Government Use Contractors to Support Military Operations?* (Washington, DC: The Heritage Foundation, May 2006), 2, accessed 20 June 2020, https://www.heritage.org/defense/report/when-should-the-government-use-contractors-support-military-operations.
[242] Ibid.

Another benefit is that industry can provide 'surge capability' when required, but this support can be withdrawn when there is no longer the need - a practice that is seen by some as more cost-effective in the longer term. However, just as in the UK, questions around assured delivery and the maintenance of inefficient spending and poor implementation have been raised. [243]

The 2019 DoD Office of Inspector General (OIG) report into DoD's acquisition and contract management performance identified many similar concerns that reportedly hamper the MoD's interaction with UK industry. In its report, for instance, the OIG reported that the DoD had identified a number of acquisitions without adequately defining the capability requirements, which meant that programmes did not meet the required performance parameters and planned procurement quantities were not justified. Moreover, it was also critical that the DoD had failed to provide effective oversight to ensure contracts were delivered on time and on budget. [244] Further noting that contracting officers were not obtaining the requisite commercial sales data for the acquisition of parts, with one example of the Air Force buying spare parts at inflated prices (valued at $58.8m). [245] Many of the reported failings of the DoD reflect similar problems reported in the MoD-industry relationship in the UK. The OIG was also critical of industry, for example, questioning its pricing structures, highlighting that industry and the military tended to agree on 'optimistic' cost and schedule estimates but, these were seldom met.[246]

A reflection of an increasing emphasis in the US government on improving its articulation of its Whole Force approach, including a considerable portion of analysis on cyber defence, was the March 2020 National Commission on Military, National, and Public Service in the United States *Inspired to Serve* report. The Commission was tasked by Congress to conduct a review of the military selective service process and 'consider methods to increase participation in military, national, and public service to address national security and other public service

[243] Peters, *Defense Primer: Department of Defence Contractors*, 1.
[244] Inspector General Department of Defense, *Fiscal Year 2019: Top DOD Management Challenges* (Washington DC: Inspector General Department of Defense, 2018), 87, accessed 20 June 2020, https://media.defense.gov/2018/Dec/12/2002071981/-1/-1/1/TOP%20DOD%20MANAGEMENT%20CHALLENGES%20FISCAL%20YEAR%202019.PDF
[245] Ibid., 86.
[246] Ibid., 88.

needs of the Nation'.[247] The report emphasised the role of the private sector, with a recommendation that the President designates a lead national mobilization official (within the National Security Council) to coordinate a whole-of-government and industry mobilization for a potential national mobilization effort.

4.3 Defence Cyber and the Whole Force: United States

As a case study to inform understanding of international comparators of the Whole Force, the US's defence and military cyber provides appropriate and valuable lessons. The DoD budget for cyber was US$9.6bn in FY2020, with US$9.8bn requested for FY2021. This cyber budget is split across a wide range of military commands and DoD entities. The US approach to Defence cyber follows the logic of a Whole Force, with military (Regular and Reservist), civilian and contractor participation.

US Cyber Command was created in 2009 at the National Security Agency (NSA), but was elevated to unified command status separate from NSA in 2018. According to recent congressional testimony by the current commander of Cyber Command (USCYBERCOM): 'USCYBERCOM performs three main missions: it defends the military's networks, it supports the broader joint force with cyber operations, and it defends the nation from significant cyber attacks. It executes an FY20 budget of $596m and has requested a budget of $638m for FY21. Its full-time personnel total 1,778 military and civilians, plus contractors. In January 2020, we rostered 5,094 active duty Service members and civilians in the Cyber Mission Force.'[248]

The statement indicates the breadth and depth of US military cyber activities. Furthermore, in addition to Cyber Command's headquarters, military personnel, Defence civilians and

[247] National Commission on Military, National, and Public Service, *Inspired to Serve The Final Report of the National Commission on Military, National, and Public Service* (Washington DC: National Commission on Military, National, and Public Service, 2020), accessed 20 April 2020, https://inspire2serve.gov/reports/final-report.

[248] Paul Nakasone, 'Statement of General Paul M. Nakasone, Commander, United States Cyberspace Command,' before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, US Congress, (March 2020), 2, accessed 29 2020, https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf.

contractors participate in cyber activities under the separate Armed Services. For example, the US Army Cyber Command comprises 'approximately 16,500 Soldiers, civilian employees and contractors worldwide.'[249] One example of Whole Force thinking is that Army Cyber Command has an established recruitment scheme for military and civilian cyber careers and is also piloting a programme to directly commission civilians as cyber operations officers.[250] The US Air Force contribution to the cyber mission force is 1,700, also comprising military, civilian and contractors. The Air Force contingent also includes Reservists from 15 Air National Guard squadrons and one Air Force Reserve squadron.[251] One recent estimate suggested that there were in total over 1,400 Reservists and National Guard serving in the cyber mission force.[252]

The composition of the US cyber force reflects the need to recruit, retain and, where necessary, contract in the right balance of skills and experience to fulfil the national cyber mission. This requires a series of aligned activities: investment in training; exploration of the division of effort between military and civilians; review of pay, conditions and promotion pathways with the defence and military cyber career pathways; improved integration of Reservists; and effective procurement of private sector services and integration of contractors into the cyber force. The US Senate Armed Services Committee noted in June 2020 that the FY2021 national defense authorization act would contain provisions for: 'Improving the training and retention of highly qualified cyber personnel, including providing Cyber Command with the same hiring authority for technical talent as exists at DARPA, the Strategic Capabilities Office, and the Joint Artificial Intelligence Center, and by allowing for pay that is more competitive with commercial industry.'[253] This initiative highlights the fact that, even with its significant budget, Defence cyber has struggled with competition from the

[249] US Army Cyber Command, 'About Us,' https://www.arcyber.army.mil/Organization/About-Army-Cyber/.
[250] Ibid.
[251] R.J. Biermann, 'Air Force Cyber Mission Force teams reach 'full operational capability,' *US Air Force*, 16 May 2018, accessed 29 July 2020, https://www.af.mil/News/Article-Display/Article/1523543/air-force-cyber-mission-force-teams-reach-full-operational-capability/.
[252] Marie Baezner, *Study on the use of reserve forces in military cybersecurity: A comparative study of selected countries*, Center for Security Studies (Zürich: ETH Zürich, April 2020), 23, accessed 29 July 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-03-military-cybersecurity.pdf.
[253] US Senate Armed Services Committee, *FY2021 National Defense Authorization Act (NDAA) Summary* (June 2020), 12, accessed 29 July 2020, https://www.armed-services.senate.gov/imo/media/doc/FY%2021%20NDAA%20Summary.pdf.

private sector, both in recruitment and retention of (both junior and more experienced) staff.[254]

To fulfil their missions, the three Armed Services and Cyber Command all work closely with the private sector to develop capabilities, sometimes leading to competing programmes and congressional intervention to re-direct resources from one project to another.[255] One example of significant cyber contracts is the recently announced request for proposals for a major cyber training contract, including delivery of the Persistent Cyber Training Environment. This contract is worth up to US$1bn and competitive team bids are likely from companies including Raytheon and General Dynamics.[256]

In addition to training contracts, operational support and analytics, private companies are also involved in the development of zero-day vulnerabilities for procurement by government clients.[257] There is also an international market for digital surveillance services, which has generated controversy regarding the private sector activities of former government officials, including former US intelligence agency analysts.[258] As cyber researcher Martin Libicki has observed regarding the division of effort between government and private sector participants in the life-cycle of offensive cyber operations: 'The laws of war dictate that the person who starts the process and ultimately pushes the button needs to be a lawful combatant, but the person who develops the tool doesn't.'[259]

---

[254] Ellen Nakashima and Aaron Gregg, 'NSA's top talent is leaving because of low pay, slumping morale and unpopular reorganization,' *Washington Post*, 3 January 2018, accessed 29 July 2020, https://www.washingtonpost.com/world/national-security/the-nsas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html.

[255] Mark Pomerleau, 'Senators seek to cut Army cyber program for greater joint investment,' *Fifth Domain*, 30 June 2020, accessed 29 July 2020, https://www.c4isrnet.com/cyber/2020/06/30/senators-seek-to-cut-army-cyber-program-for-greater-joint-investment/.

[256] Mark Pomerleau, 'Army releases $1B cyber training request,' *Fifth Domain*, 12 June 2020, accessed 29 July 2020, https://www.fifthdomain.com/dod/cybercom/2020/06/12/army-releases-1b-cyber-training-request/.

[257] Joseph Menn, 'U.S. aims to limit exports of undisclosed software flaws,' *Reuters*, 21 May 2015, accessed 29 July 2020, https://uk.reuters.com/article/us-software-exports/u-s-aims-to-limit-exports-of-undisclosed-software-flaws-idUKM1KBN0O604R20150521.

[258] Christopher Bing and Joel Schectman, 'PROJECT RAVEN: Inside the UAE's Secret Hacking Team of American Mercenaries,' *Reuters*, 30 January 2019, accessed 29 July 2020, https://www.reuters.com/investigates/special-report/usa-spying-raven/.

[259] Jeff Stone, 'Meet The Cyber-Industrial Complex: Private Contractors May Get $7B Windfall From Pentagon's Cyberwar On ISIS,' *International Business Times*, 7 March 2016, accessed 29 July 2020, https://www.ibtimes.com/meet-cyber-industrial-complex-private-contractors-may-get-7b-windfall-pentagons-2329652.

Defence cyber operates on a much larger scale in the US than in the UK. For example, the estimated number of Reservists in the cyber mission force exceeds the total size of the UK national cyber force. Whilst the size and resources are of a different magnitude, the approach to combining military (Regular and Reservist), civilian, and contractor components in the cyber force is similar. As the US is at a more advanced stage of maturity in developing its Defence cyber force, there is potential benefit to the UK studying the US approach and adapting lessons for future application of the Whole Force approach to Defence cyber in the UK. Similarly, as a significant investment has already been made by DoD and the Armed Services in developing a broad range of technical, training and operational capabilities to support the cyber mission, the UK government should consider, where appropriate and possible, the potential to purchase proven US products as a cost-efficient approach to UK Defence cyber procurement.

Recommendation: The Integrated Review should conduct a force structure assessment of UK Defence cyber, including analysis of the role of Reservists and contractors. It should also consider the US case as a comparator, and, where appropriate, explore the merits of procuring capabilities developed for US Defence cyber as a cost-efficient approach to UK Defence cyber procurement. This should be balanced against the competing strategic requirement for a domestic cyber defence industrial base.

4.4 Defence Cyber and the Whole Force: Israel and Estonia

4.4.1 Israel

Israel is widely acknowledged as being at the forefront of technology and cyber security,[260] with cyber security becoming a central activity for the Israeli Defence Forces. The 2015 Israel Defence Doctrine cited its four main domains of defence and protection: land, sea, air, and

[260] Dan Senor and Saul Singer, *Start-up nation: The story of Israel's economic miracle* (New York: Random House Digital, Inc., 2011), 1-2.

cyber.[261] The UK has pursued the development of a cyber Reserve in recent years, but the Israeli experience is more advanced and embedded. One former commander of Unit 8200, Israel's signals intelligence organisation, made the point that 'In the past, military Service was perceived as a waste of time, while it's different now. We didn't plan it that way. No one thought about how to make the IDF into a catalyst for the Israeli economy, but that's what happened.'[262] Unit 8200 is the largest unit – with the most competitive selection process for national service - in the Israeli Defence Forces and is considered to be one of the most advanced units of its kind in the world. While one of the core components of Israel's Defence Doctrine is deterrence, it should be noted that Unit 8200 is also utilised for offensive purposes. In May 2017, for example, the Lebanese government accused Israel of launching a cyber-attack on its state telecommunications company, Ogero. The following year, Unit 8200 was reported as having successfully thwarted an ISIS terrorist attack on a civilian airliner, which was flying between Australia and the UAE.[263]

The Israeli government is also a leader in harnessing international cooperation in the field of cyber security. It has established a cyber park (the Advanced Technology Park) to coordinate academic, private and public sectors, and, importantly, to also host international technology and defence companies.[264] Speaking in 2015, Prime Minister Benjamin Netanyahu explained that Israel had crafted a deliberate policy to be leaders in cyber security, and in the space of one year, it increased global investments in cyber security from 10 to 20 per cent.[265]

[261] Belfer Centre, Harvard Kennedy School, *Deterring Terror: How Israel Confronts the Next Generation of Threats* (Cambridge, MA: Belfer Centre, Harvard Kennedy School, August 2016), 12, accessed 11 March 2020, https://www.belfercenter.org/israel-defense-forces-strategy-document#!introduction

[262] Gil Press, '6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry,' *Forbes,* 18 July 2017, accessed 11 March 2020, https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#31f53f08420a.

[263] *Israel Defense,* 'IDF Unit 8200 Thwarted ISIS Terror Attack on Australian Flight**,'** *Israel Defense*, 22 February 2018, accessed 20 March 2020, https://www.israeldefense.co.il/en/node/33176.

[264] Sean Cordey, *Trend Analysis: The Israeli Unit 8200: An OSINT-based study*, Center for Security Studies (Zürich: ETH Zürich, December 2019), 12, accessed 10 June 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf.

[265] Danielle Pletka, 'A conversation with Benjamin Netanyahu,' *AEI*, 9 November 2015, accessed 10 June 2020, https://www.aei.org/research-products/speech/a-conversation-with-benjamin-netanyahu/.

4.4.2 Estonia

Estonia has also developed robust cyber defence capabilities through a Whole Force approach. Estonia's methodology, however, differs from Israel's due to dissimilar Defence structures and political-military relations. In Israel's case, there is a symbiotic relationship between the political elite and the military, a characteristic that has been called a 'political-military partnership'.[266] Technically and constitutionally, policy decisions are made by political leaders, however, it is generally acknowledged that the process is informal, allowing the professional officer class to be influential in policy decisions.[267] By contrast, the Estonian constitution stipulates that military servicemen cannot be members of political parties or be elected to representative bodies.[268]

In cyber defence, Estonia has been cited as a pioneering state – and is arguably, one of the most competent members of NATO in this field. This is largely due to Estonia's decision to invest heavily in the protection of information infrastructure following its independence from the Soviet Union. Moreover, after experiencing a series of cyber-attacks in 2007, which were widely believed to have originated from Russia, Estonia placed an even greater priority on developing its cyber defence capabilities.[269] The attacks underscored Estonia's need for a comprehensive approach to cyber security, with an emphasis placed on coordination between the government and private sector, such as telecommunications companies and internet service providers.[270] Broadly, it has been suggested that Estonia's response to these attacks was successful and that its response illustrated the effectiveness of its public-private cooperation.[271]

---

[266] Yoram Peri, *The Israeli Military and Israel's Palestinian Policy: From Oslo to the Al Aqsa Intifada*, Peaceworks No. 47 (Washington, DC: United States Institute of Peace, November 2002), 5, accessed 11 March 2020, https://www.tau.ac.il/institutes/herzog/peaceworks.pdf
[267] Ibid.
[268] Leonid A. Karabeshkin, *Civil-military Relations in Estonia: Legal Background and Contemporary Discourse The Estonian Case*, Research Paper No1/4 2007 (Frankfurt: Peace Research Institute Frankfurt, 2007), 3-4, accessed 11 March 2020, https://www.hsfk.de/fileadmin/HSFK/hsfk_downloads/ESTONI_4.pdf.
[269] Damien McGuinness, 'How a cyber attack transformed Estonia,' *BBC News,* 27 April 2017, accessed 11 March 2020, https://www.bbc.co.uk/news/39655415.
[270] Pirret Pernik and Emmit Tuohy, 'Interagency Cooperation on Cyber Security: the Estonian Model' in *Effective Inter-Agency Interactions and Governance in Comprehensive Approaches to Operations*, eds. P. J. M. D. Essens, M. M. Thompson and S. M. Halpin (NATO STO Symposium Proceedings AC/323 (HFM-236) TP/597, 2014), 9-1.
[271] Ibid.

A defining feature of Estonia's Cyber Defence Unit is its composition of volunteers from outside government, with expertise in cyber security and non-cyber fields (such as lawyers and economists). The Cyber Defence Unit falls under the authority of the Estonian Defence League (EDL), which is a voluntary, non-political organisation. The EDL has been described as the equivalent of a cross between the US National Guard and a nationwide militia.[272] Importantly, it has been noted that the EDL has markedly increased in size since Russia's annexation of Ukraine.[273]

The Cyber Defence Unit's main role is to supplement government efforts in times of need; thus, ensuring the government can always access the skills it requires. There are two main areas where the unit focuses its training and general readiness: capability building and operations.[274] Capability building concentrates on securing the cyber security for the public with an emphasis on information sharing between the public and private sectors. A founding member of the unit stated that private sector employers tend to encourage their employees to volunteer for the unit, noting the benefits they would gain from the training and experience.[275]

Due to Estonia's effective coordination of its cyber defence capabilities, its successful public-private coordination, and its innovative use of Reserves, some have questioned the desirability of emulating the Estonian model. This question has been posed in relation to the lack of formalised cyber strategy education. Internationally, a report by the Centre for Cyber Safety and Information stated that by 2022, the projected shortage of cybersecurity professionals worldwide would reach 1.8m.[276]

[272] Sharon L. Cardash, Frank J. Cilluffo, and Rain Ottis, 'Estonia's cyber defence league: A model for the United States?' *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787, 779.
[273] Shape NATO, 'Estonian Defence League – The Kaitselit – Strong in Defence,' Shape NATO, 14 May 2019, accessed 11 March 2020, https://shape.nato.int/news-archive/2019/estonian-defence-league-the-kaitseliit-strong-in-defence-.
[274] Monica M. Ruiz, 'Is Estonia's approach to cyber defense feasible in the United States?' *War on the Rocks*, 9 January 2018, accessed 11 March 2020, https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/
[275] Ibid.
[276] Ibid.

4.5 Total Defence

The concept of Total Defence relates to the preparation of the whole of society for the prospect of conflict. It is this direct involvement of civil society that distinguishes Total Defence from more traditional military deterrence and defence. More specifically, Total Defence is predicated on two main considerations: resilience and territorial defence. Therefore, Total Defence is concerned not only with traditional physical defence considerations, but equally with psychological considerations.[277] An example of Psychological Defence can be seen in the Total Defence approach of Singapore, where it is listed as one of the 6 pillars of the city-state's approach. Similarly, Estonia advocates a Total Defence approach, placing emphasis on the importance of Psychological Defence, explaining that it increases trust between civil society and the state. More importantly, it is said to strengthen resilience and ultimately help to avert anti-Estonian subversive activity.[278] Sweden has a National Board for Psychological Defence where it stresses the importance of the 'will to defend' before a crisis emerges. [279] Finland also utilises Psychological Defence, but terms it 'psychological resilience' and explains it as the ability of society at large to withstand pressures from crisis situations and recover[280] from their impacts.

In Asia, Total Defence and the articulation of Psychological Defence is firmly established. Singapore is a leader in this regard and every year on 15 February, the state celebrates Total Defence Day as a reminder of Singapore's fall to the Japanese in 1942.[281] Singapore first released the Total Defence concept in 1984. Singapore has one of the most comprehensive models of Total Defence and as noted above, emphasised Psychological Defence. Taiwan has had Psychological Defence at the heart of its Total Defence strategy since 1996, as President

---

[277] James Kenneth Wither, 'Back to the future? Nordic total defence concepts,' *Defence Studies* 20, no. 1 (2020): 61-81, 62.
[278] ADA Europa, 'National Security Concept of Estonia,' ADA Europa, 12 May 2010, 20/21, accessed 10 May 2020, https://www.eda.europa.eu/docs/default-source/documents/estonia---national-security-concept-of-estonia-2010.pdf.
[279] Niklas H. Rossbach, *Psychological Defence: Vital for Sweden's Defence Capability*, FOI Memo 6207, Strategic Outlook 7 (Stockholm: Swedish Defence Research Agency, November 2017), 1.
[280] Wither, 'Back to the Future? Nordic total defence concepts,' 62.
[281] Dominic Teo, 'See how Total Defence Day has evolved through the years,' *The Straits Times,* 16 February 2016, accessed 10 May 2020, https://www.straitstimes.com/singapore/see-how-total-defence-day-has-evolved-through-the-years.

Lee Teng-hui believed that Psychological Defence should form the bedrock of Total Defence, and that civil-military cooperation would ultimately strengthen national security.[282] Malaysia introduced its Total Defence concept, known as HANRUH (the Malay acronym of Pertahanan Menyeluruh) in 1986, but there has been limited public knowledge or engagement with the concept to date.[283] While the Malaysian government has made efforts to engage the public, an analysis of its National Defence Policy, uploaded to the Prime Minister's office's website as recently as July 2019, revealed only two references to Total Defence. Strikingly, the document explicitly rejects the notion of Psychological Defence, arguing rather that while Total Defence is the responsibility of all sectors of society, 'national prosperity and peace override individual needs and political ideology.'[284]

In developing the Whole Force in the UK, engagement with society in advance of any crisis may have merit, with an effort to focus on strategic communications and consideration of how other states succeed or struggle in securing 'buy-in' from their societies. While the UK has addressed and outlined the importance of strategic communications, particularly in Defence, its use in regard to the Whole Force is underdeveloped. This may change as discussions about future strategy (particularly post-Covid 19) increasingly emphasise resilience, and the Whole Force concept begins to be accepted as an important element in delivery of national effort in the future.

Discussion of the Whole Force in the UK has seen little, if any, mention of the role of Psychological Defence. Nevertheless, the MoD's Defence Science Technology Laboratory (DSTL) has been engaging in psychological research to address 'real world' defence and security challenges for many years and this capability could be leveraged in the Whole Force by articulating a commitment to Psychological Defence.[285] In 2018, the British Psychological Society (BPS) formed a Defence and Security Section with the intention of bringing together

[282] Linda Chao, *Assessing the Lee Teng-hui legacy in Taiwan's politics: democratic consolidation and external relations* (New York: ME Sharpe, 2002), 19-20.
[283] Mohamad Faisol Keling et al., 'The Malaysian government's efforts in managing military and defence development,' *International Journal of Business and Social Science* 2, no. 12 (2011): 180-193.
[284] Prime Minister's Office of Malaysia, 'Malaysia's National Defence Policy,' Prime Minister's Office of Malaysia, July 2019, accessed 10 May 2020, https://www.pmo.gov.my/wp-content/uploads/2019/07/National-Defence-Policy.pdf.
[285] Fiona Butcher, 'Role of research psychology in defence and security,' *Journal of the Royal Army Medical Corps* 165, no. 2 (2019): 113-115, 114.

psychologists from academia, government and industry to address issues in the area. The BPS stressed the importance of applying best practice and sharing knowledge and expertise in the areas of defence and security.[286]

Reflecting the timeliness of Psychological Defence in the UK, in March 2019 DSTL launched The Human Social Science Research Capability (HSSRC) framework with BAE Systems as its prime contractor. BAE Systems stated that 'the future environment will present different physical and psychological demands which will need to be understood and managed'[287] and the research has been designed around the following 6 research themes: personnel; training and education; humans in systems; human performance; understanding and influencing human behaviour; and, health, wellbeing and enhancing medical systems and capabilities.[288]

Emphasising the value that the private sector can bring to this initiative, BAE Systems has stated that as of March 2020 48% of research tasks by value had been awarded to Small and Medium Enterprises (SME) and 17% awarded to micro enterprises (enterprises with fewer than 10 employees).[289] In May 2020, it was announced that DSTL had awarded a contract worth up to £350m to BAE Systems CORDA, (an analytical consultancy team in BAE Systems). This Analysis for Science and Technology Research in Defence contract is designed to operate across five areas: strategy, policy and enterprise; capability and investment for platform and system level capabilities within current and future force structures. Announcing the new contract, the Divisional Head of DSTL emphasised the organisation's aim to 'exceed the MOD target of awarding 25% of the work to SMEs including non-traditional defence suppliers'.[290]

---

[286] Guest, 'Defence, Security, Psychology,' *British Psychological Society*, 26 October 2018, accessed 10 May 2020, https://www.bps.org.uk/blogs/guest/defence-security-psychology.
[287] BAE Systems, 'Human and Social Science Research Capability (HSSRC),' BAE Systems, accessed 10 June 2020, https://www.baesystems.com/en-uk/product/human-and-social-science-research-capability--hssrc-
[288] Ibid.
[289] Sam Wyatt, 'Introducing the Human Social Science Research Capability Framework,' *Tech UK*, 03 March 2020, accessed 10 June 2020, https://www.techuk.org/insights/opportunities/item/16986-introducing-the-human-social-science-research-capability-framework.
[290] Defence, Science and Technology Laboratory, 'Dstl Awards £350 million ASTRID contract to BAE Systems CORDA,' GOV.uk, accessed 10 June 2020, https://www.gov.uk/government/news/dstl-awards-350-million-astrid-contract-to-bae-systems-corda.

The term 'non-traditional' in this context is important and has been widely emphasised in the US. For example, in the US the term has a specific legal definition in terms of Defence acquisition policy which means that suppliers can avoid certain regulations when supplying products from outside military channels. It has been noted that the challenge for policymakers is how to leverage the skills found in commercial enterprises 'without suffocating them under a blanket of bureaucratic requirements that contribute little to finding novel solutions.'[291] Wider challenges are faced by these non-traditional suppliers, including how defence companies can respond to the challenge of leveraging expertise from non-traditional suppliers, while also remaining in compliance with government standards. One such obstacle is partnering with enterprises which have little or no prior experience of working in a classified environment. Raytheon, for example, has carved out a role for itself 'as a translator between the fluid world of commercial innovation and the rule-based environment of military acquisition'.[292]

Whilst noting the different national context, the UK could learn from the findings of a 2014 US study which outlined barriers that non-traditional suppliers face when dealing with the DoD:

- the DoD's sometimes cumbersome bid and selection process;
- DoD's limited communication with potential or actual bidders;
- extra work and delays in payments due to contract administration processes; and,
- extensive time between the initial bid and initial funding that smaller enterprises find difficult to contend with due to lack of capital, thereby impeding their progress.[293]

[291] Loren Thompson, 'Raytheon And BAE Systems Are Drawing Nontraditional Suppliers Into Defense,' *Forbes,* 24 January 2020, accessed 10 June 2020, https://www.forbes.com/sites/lorenthompson/2020/01/24/how-top-military-contractors-raytheon-and-bae-systems-are-drawing-non-traditional-suppliers-into-defense/#3b1b111a6af2.
[292] Ibid.
[293] Amy G. Cox, Nancy Young Moore, and Clifford A. Grammich, *Identifying and Eliminating Barriers Faced by Nontraditional Department of Defense Suppliers* (Santa Monica, CA: RAND Corporation, 2014), ix-xi, accessed 10 June 2020: https://www.rand.org/pubs/research_reports/RR267.html.

Another report examining US military spending noted that the military's ability to deal with future challenges had been impeded due to 'Budgetary and strategic inertia'.[294] It also called for a revision of the DoD's approach to research funding, arguing that the Pentagon should be granted more authority to invest in public and private research start-ups. From a Whole Force perspective, it also called for an overall 'fundamental reconceptualization of how the United States will use its forces in the future.'[295]

Increasing calls for the utilisation of non-traditional suppliers means that such barriers to entry could be actively considered in the UK context. For example, the UK MOD's 2019 'Small and Medium-sized Enterprise Action Plan' for 2019-2022 discussed the importance of investigating barriers to entry for SMEs to enable more effective engagement and innovation, but there was no discussion about the relationship between defence companies and non-traditional suppliers and whether the MOD should cultivate these relationships.[296]

Recommendation: Given the value that non-traditional suppliers can add to the Whole Force, the MoD should continue to identify specific barriers to entry that prevent non-traditional suppliers from engaging more fully in the Whole Force process.

BAE Systems, through the development of 'FAST Labs', has developed a process for leveraging the technology of smaller commercial enterprises by helping finance their businesses.[297] In the US, this has reflected criticism that the DoD has been slow to integrate new ideas into its strategies. With FAST Labs, BAE Systems' approach is unique as rather than producing prototypes of new weapons or developing new defence systems, it instead supports roughly 850 scientists and engineers. These are dedicated to developing commercial innovations that would ultimately be applicable to security challenges, particularly in the areas of electronic

[294] Eric Gomez et al., *Building a Modern Military: The Force Meets Geopolitical Realities*, White Paper (Washington, DC: CATO Institute, May 2020), 2, accessed 10 June 2020, https://www.cato.org/publications/white-paper/building-modern-military-force-meets-geopolitical-realities
[295] Ibid., 25.
[296] Ministry of Defence, *Small and Medium-sized Enterprise Action Plan, 2019-2022* (London: Ministry of Defence, 2019), accessed 10 June 2020: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793101/20190405_SME_Action_Plan_2019.pdf
[297] Ibid.

and information technologies.[298] This initiative and approach undertaken by BAE Systems has been considered novel due to how it has formed its own system of leveraging technological capability. More traditionally, the model has been to buy a smaller company to gain its technology, however, BAE Systems has instead been serving as the 'middleman' by connecting start-ups with both the DoD and BAE's other units.[299]

Recommendation: UK defence companies should develop options to improve the working relationship between the defence industry, SMEs and non-traditional suppliers in order to bolster the efficiency of the Whole Force.

While the MOD and DSTL have engaged with BAE Systems and the private sector more broadly, there have been criticisms of aspects of this approach, particularly regarding any potential accusations of the government relying on the private sector to manipulate public opinion. One criticism, for example, has been that (using the case of Russian interference) 'Growing international tensions have given the military the opportunity to move directly into the business of forming opinion.'[300]

In the UK context, the Army has attempted to exploit the Whole Force through the 77th Brigade, a counter-hybrid warfare unit that focuses on non-lethal forms of psychological warfare, including through social media and disinformation.[301] Whilst the development of the Brigade is still a work in progress, it harnesses expertise from across the military and Whitehall, including the security-stabilisation group and the Department for International Development, the psychological operations group and the media operations group.[302] Such an approach highlights the complementary nature of the Whole Force and the National Security Fusion

[298] Loren Thompson, 'BAE Systems Invents A Radically Different Way of Speeding Defense Innovation,' *Forbes,* 15 April 2019, accessed 10 June 2020, https://www.forbes.com/sites/lorenthompson/2019/04/15/bae-systems-inc-invents-a-radically-different-way-of-speeding-defense-innovation/#20d48211f9d2.
[299] Theresa Hitchens, 'BAE Makes Big Bet on Small Companies: FAST Labs,' *Breaking Defense,* 21 May 2019, accessed 10 June 2020, https://breakingdefense.com/2019/05/bae-makes-big-bet-on-small-companies-fast-labs/
[300] Chris Nineham *The British State: A Warning* (London: John Hunt Publishing, 2019), 4.
[301] Antill and Smith, 'The British Army in Transition,' 54.
[302] Nicholas Carter and James de Waal, 'The Future of the British Army: How the Army Must Change to Serve Britain in a Volatile World,' Transcript, *Chatham House*, 4, accessed 27 November 2019: https://www.chathamhouse.org/sites/default/files/field/field_document/20150217QBritishArmy.pdf.

Doctrine, which seeks to ensure that '…in defending our national security we make better use of all of our capabilities: from economic levers; through cutting-edge military resources; to our wider diplomatic and cultural influence on the world's stage'.[303] In other words, the doctrine espouses a truly whole-of-government approach to national security. A core asset in the UK's Defence capabilities, which the Brigade is attempting to utilise, is a well-trained and active Reserve Force; Reservists outnumber Regular personnel by 270 to 200. Efforts are also underway by the Intelligence Surveillance and Reconnaissance Brigade to integrate Reservists into its force structure, which stands at approximately 2,800 Regulars and 2,100 Reservists.[304]

The concept of Total Defence is generally embraced in certain geographical locations. While Finland retained its Total Defence doctrine after the end of the Cold War, Norway has reconfigured its approach, while Sweden has re-introduced Total Defence. However, these Nordic states provide a compelling example of how states can benefit from partnerships and alliances in utilising Total Defence. In discussing the various approaches to Total Defence, this study does not propose that the UK follow the model of in effect the militarisation of society; not only would there be limited political will for such an approach, but the UK does not face the same threats as the Nordic states. However, in adopting an effective strategic communications approach, these Nordic governments could be positive examples in the context of their ability to obtain public engagement with Whole Force ideas.

4.6 Use of Reserves and Sponsored Reserves

As previously discussed, the US offers several lessons for the UK's Whole Force. Whilst the study's focus is on industry's contribution to the Whole Force, a brief examination of the US National Guard adds depth to the discussion. The National Guard is a Reserve force frequently used for defence assistance and its structure relates directly to the US's federal structure and the National Guard serves a dual state and federal mission. The National Guard remains under the authority of respective State governors and is the first military force to respond to disaster

[303] HL Written Question, 26 April 2018, HL7352, accessed 4 December 2019, https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2018-04-26/HL7352.
[304] Ibid.

relief or emergencies. There are two characteristics of the National Guard that make it unique from other components of the US Reserve and Reserve forces elsewhere more generally. The first is the fact that it must fulfil both federal and state roles and in the latter sense must also be prepared for overseas deployment.[305] The second is how it is used for law enforcement. Generally, the National Guard can be used for law enforcement support tasks within respective states, where federal troops cannot. However, this changes under what is termed 'Title 10 Duty', where the Constitution gives the federal government the authority to use the National Guard, this time under federal control, at federal expense and for federal purposes. More specifically, this is when the federal government would use the National Guard for combat operations both at home and internationally. When employed under 'Title 10 Duty', the National Guard is not operating under state control and is solely answerable to the federal government.[306] It should also be noted that while employed under 'Title 10 Duty', the National Guard, like other military entities, is not allowed to be used for law enforcement purposes, unlike when operating under state control when the National Guard has regularly been used to support civil order.[307] Once Title 10 is approved, it comes under the operational control of NORTHCOM.[308]

However, the duality of the National Guard's mission does bring about complications in terms of how and where it can be deployed. For example, while the National Guard was lauded for its response to Hurricane Katrina in 2005, it was also recommended that the National Guard be given a federal mission to conduct homeland security activities and be allowed to prepare itself for rapid response for emergencies in other states.[309] In investigating the role of Reserves in the context of the Whole Force, the National Guard provides important questions about how Reserve forces should be used; how it fulfils both military and law enforcement functions and how the authorities under which it operates do not remain constant and are subject to various competing legal structures.

---

[305] Mark Philips, *The Future of the UK's Reserve Forces*, RUSI Occasional Paper (London: RUSI, April 2012), 56, accessed 11 June 2020, https://rusi.org/sites/default/files/201204_op_future_of_the_uks_reserve_forces.pdf.
[306] Ibid.
[307] In the UK, this is termed Military Assistance to the Civil Authorities (MACA).
[308] Richard J. Hayes, 'DOD Response Under the Stafford Act: A Call to Action', *Joint Force Quarterly* 77, 1 April 2015.
[309] Lynn E. Davis et al., *Learning the Lessons of Hurricane Katrina for the U.S. Army*, Research Brief (Santa Monica, CA: RAND Corporation, 2007), 1, accessed 12 June 2020, https://www.rand.org/pubs/research_briefs/RB9255.html.

As previously discussed, the SR model has proven itself to work in the delivery of Defence outputs in the UK; notwithstanding the fact this model has yet to be fully adopted within the UK context. In particular, the SR model has so far provided evidence of assured delivery – a key concern among Defence officials in the UK.

Other countries have followed suit by adopting similar models. For example, in 2002, Australia announced its iteration of the Whole Force, called 'Force 2020', which emphasised the aim of a 'Seamless Force' in order to maximise collective warfighting capabilities. Importantly, it was clarified that this 'Seamless Force' was not intended to signify a merger of the three Services, but rather to enhance them by including Defence civilians, contractors, and the defence industry.[310] In 2009, the Australian Department of Defence released a White Paper which in turn, led to the Strategic Reform Program 2009 and articulated a plan for Force 2030 (with no mention of the previous plan for Force 2020). The document identified the importance of considering alternative methods of employing a part-time component, with emphasis on SRs.

More recently, in 2016, the Australian Department of Defence released a White Paper which announced that while increasing the permanent Australian Defence Force (ADF) workforce, a contemporary workforce management model would allow ADF members to move between the Permanent ADF and the Reserves.[311] Related to this, during the consultation phase of Australia's 2020 Cyber Security Strategy, (which is yet to be published) the issue of what is and what is not an inherently governmental function was raised. One report argued that while the Australian government should remain the ultimate overseer of cyber security, government certified organisations could perform the assurance tasks of government, particularly in the area of compliance with regulations.[312]

---

[310] Australian Government Department of Defence, *Force 2020* (Canberra: Australian Government Department of Defence, June 2002), 17, accessed 10 June 2020, https://www.defence.gov.au/Publications/f2020.pdf.
[311] Australian Government Department of Defence, *2016 Defence White* Paper (Canberra: Australian Government Department of Defence, 2016), 23, accessed 10 June 2020, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.
[312] Deloitte, 'Australia's 2020 Cyber Security Strategy: A call for views,' Deloitte, November 2019, accessed 29 June 2020, http://images.content.deloitte.com.au/Web/DELOITTEAUSTRALIA/%7B2ac328f6-1dfc-4c2b-ba45-1a278dc03c83%7D_20191210-ris-inb-australias-2020-cyber-security-strategy-report.pdf?elq_mid=3097&elq_cid=292819&utm_medium=email&utm_campaign=20191210-ris-2020-cyber-strategy&utm_content=cta&elqTrack=true.

4.7 Lateral Entry and Civil-Military Relations

In the context of the UK's Whole Force, lateral entry involves increasing movement between industry and military personnel allowing talent and resources to flow back-and-forth. As previously highlighted, General Sir Nick Carter argued that the move would improve readiness and resilience within the Armed Services. He explained that the MoD would establish integrated career structures that would link the Armed Services with civilians. This initiative has been termed 'unified career management' and will be piloted and then possibly reviewed in the Future Reserves 2030 review.[313]

The US has also embraced lateral entry, but its development there has shown the complexity of operationalising such a programme. In 2016, former Defense Secretary Ash Carter highlighted that lateral entry would boost the military's technological capability by moving civilians with expertise and qualifications in areas such a cyber security (as one example) into the military. This formed part of Carter's broader 'Force of the Future' initiative to modernise the DoD to combat what he considered to be the five most pressing global challenges facing the US: Russian aggression in Eastern Europe; Chinese aggression in the South China Sea; North Korean nuclear and missile provocations; Iranian aggression and influence in the Gulf; and, the threat from global terrorism.[314] The threats, which have been has been characterised as presenting a 'grey zone of conflict', represent a series of threats that the United States must defeat as it tackles opaque adversaries.[315]

In Carter's vision, civilians with technological expertise could remain civilians while supporting the Armed Forces and would not have to complete traditional military training. Implicit in Secretary Carter's suggestion lay a challenge to the centrality of combat readiness in defence planning; that the changing nature of warfare required a decreasing reliance on infantry and

[313] Carter, 'Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019.'
[314] Lisa Ferdinando, 'Carter Legacy: Force of the Future, modernizing DoD, confronting threats,' Air Force Reserve Command, 19 January 2017, accessed: 12 March 2020, https://www.afrc.af.mil/News/Article-Display/Article/1053713/carter-legacy-force-of-the-future-modernizing-dod-confronting-threats/.
[315] Leon Panetta et al., *Building a F.A.S.T. Force: A flexible Personnel System for a Modern Military* (Washington, DC: Bipartisan Policy Center), 11, March 2017, accessed 10 June 2020, https://bipartisanpolicy.org/wp-content/uploads/2019/03/BPC-Defense-Building-A-FAST-Force.pdf.

combat arms more generally. The suggestion of lateral entry was greeted with suspicion by elements within the US Armed Services, particularly in the Marine Corps. One former Marine argued that lateral entry would degrade the essential characteristics of the Marine Corps, saying it would 'lose something that has made the Marine Corps what it is'.[316] Such opposition reflects the view that the presence of civilians within Services such as the Marine Corps could negatively affect the internal culture of the units. Notwithstanding the motto of the Marine Corps which has been 'Every Marine is a rifleman', argued by some as an adage which has sustained the unit throughout its history, the Marine Corps is now actually considering increasing its use of the lateral entry mechanism. Particularly in the area of cyber operations, the argument is that if Services such as the Marine Corps do not increase lateral entry and bring cyber expertise in from the private sector, they will have to find other ways to grow their cyber capability.[317]

Where the Armed Services lacks expertise across a diverse range of capabilities - such as cyber security, medicine, and translation services - lateral entry programmes which focus on short-term placements in the military could do much to counteract this trend.[318] The Bipartisan Policy Center has argued that the US Armed Forces could improve their expertise and efficiency if they addressed the onerous personnel bureaucracy that had hampered the Armed Services' ability to retain talent. This point was also highlighted by former a US Air Force intelligence officer, who criticised the US military's inability to accommodate lateral entry.[319]

More generally, the question of civilian entry into the Armed Forces internationally reflects a broader question in civil-military relations about readiness, how this is defined and then

[316] Julianne Simpson, 'Urgent Need for Cybersecurity Professionals Grows,' *The Cyber Edge*, 1 May 2019, accessed 11 March 2020, https://www.afcea.org/content/urgent-need-cybersecurity-professionals-grows
[317] Jeff Schogol, 'Every Marine a rifleman no more?' *Marine Times,* 7 May 2017, accessed 22 April 2020, https://www.marinecorpstimes.com/news/your-marine-corps/2017/05/07/every-marine-a-rifleman-no-more/.
[318] Panetta et al., *Building a F.A.S.T. Force*, 61.
[319] Tim Kane, *Bleeding talent: How the US military mismanages great leaders and why it's time for a revolution* (New York: Springer, 2017), 50.

operationalised.[320] The term lateral entry also has different meanings in different contexts. For example, Australia has a lateral recruitment scheme, which refers to lateral recruits who are military personnel who gain entry to the Australian Defence Force based on prior experience in foreign Armed Forces.[321]

Another example of private sector involvement in Defence is a growing exercise in the US called 'Hack the Pentagon', which is known as a 'bug bounty' programme. Through this programme, the DoD has sought to leverage expertise from the collective hacking communities and, in doing so, has awarded contracts to three crowd-sourced security firms: Bugcrowd, HackerOne and Synack. Within DoD, Hack the Pentagon is managed by the Defense Digital Service whose remit is to identify and bring in private sector expertise, ostensibly using 'ethical hackers'. Hack the Pentagon then works through two pathways for bug bounty assessments where these ethical hackers access systems in order to assess how many bugs are present in certain systems. The first is concentrated on public-facing DoD websites and applications, while the second pathway focuses on internal DoD systems.[322] In mid-April 2020 it was announced that the Hack the Pentagon initiative had been emulated by the US Air Force in late 2019, when it completed its fourth iteration of 'Hack the Air Force 4.0'. This resulted in 60 hackers taking part who uncovered 460 vulnerabilities and earned $290,000 in bounties. Similarly, Hack the Army 2.0 took place between October 9 and November 15, 2019 and 52 hackers uncovered 146 security vulnerabilities and were rewarded with bounties totalling $275,000.[323] Overall, it was reported by DoD that since the launch of Hack the Pentagon, 12,000 security vulnerabilities have been identified by ethical hackers.[324]

---

[320] Phillip Carter et al., *The Future of the All-Volunteer Force*, Working Paper AVF 4.0 (Washington, DC: Centre for a New American Security, March 2017), 4, accessed 22 April 2020: https://www.jstor.org/stable/resrep06308?seq=1#metadata_info_tab_contents.

[321] Australian Government Department of Defence, 'Overseas recruits,' Australian Government Department of Defence, accessed 10 June 2020, https://www.defence.gov.au/DCO/Overseas-recruits/#:~:text=Overseas%20or%20'Lateral'%20recruits%20are,be%20filled%20using%20Australian%20personnel.

[322] *DOD News*, 'Department of Defense Expands "Hack the Pentagon" Crowdsourced Digital Defense Program,' *DOD News*, 24 October 2018, accessed 12 March 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/

[323] Davey Winder, 'U.S. Air Force Successfully Hacked By 'Battalion' Of 60 Hackers,' *Forbes*, 16 April 2020, accessed 20 April 2020, https://www.forbes.com/sites/daveywinder/2020/04/16/us-air-force-successfully-hacked-by-battalion-of-60-hackers/.

[324] *Bloomberg*, 'Over 460 Vulnerabilities Resolved in Tenth Bug Bounty Challenge with U.S. Department of Defense Thanks to Hackers on HackerOne,' *Bloomberg,* 15 April 2020, accessed 20 April 2020,

Even following the outbreak of COVID-19, the DoD's Defense Digital Service has continued recruiting candidates from the private sector, where the contract is for two years with the option to extend it before returning to the private sector.[325] Overall, the DoD has shown the benefit of engagement with the private sector through initiatives such as Hack the Pentagon and by utilising expertise from the private sector in the Digital Defense Service.

https://www.bloomberg.com/press-releases/2020-04-15/over-460-vulnerabilities-resolved-in-tenth-bug-bounty-challenge-with-u-s-department-of-defense-thanks-to-hackers-on-hackerone.

[325] David Vergun, 'Defense Digital Service Is Hiring Talent, Continuing Mission Despite COVID-19,' *DOD News*, 17 June 2020, accessed 18 June 2020, https://www.defense.gov/Explore/News/Article/Article/2223499/defense-digital-service-is-hiring-talent-continuing-mission-despite-covid-19/.

5. Conclusion

This study has aimed to provide a timely contribution to the on-going debate on the Whole Force by identifying what progress has been made and what obstacles remain to deliver a fully integrated Whole Force model in the UK. The report also sought to progress the Whole Force debate by generating a list of practical recommendations designed to improve the Defence public-private partnership model. The UK case study has been supplemented by an examination of Whole Force (or similar) models from around the world, drawing on examples of best practice.

The study has found that despite progress in operationalising the Whole Force over the last decade, efforts have stalled in achieving a seamless partnership between the military and industry. Paradoxically, while senior MoD leaders have accepted the Whole Force as 'an indispensable requirement of our future operational capability',[326] Defence has not yet articulated a convincing Whole Force vision. This has been compounded by a lack of consistent focus on enacting the necessary reforms to drive progress, and confusion over which MoD team - CDP or Fin Mil Cap - owns the process. Perhaps predictably, this lack of ownership has allowed the Whole Force to stall as other priorities have overtaken it. As outlined in the recommendations, it is our judgement that the CDP should be appointed SRO to plan, oversee and ultimately execute the Whole Force's delivery, with Fin Mil Cap personnel supporting CDP. Having a clearly defined, accountable SRO would give operational momentum to the existing top-level intent to deliver the Whole Force.

Connected to this, until very recently, there had been little conceptual work dedicated to defining the Whole Force or a framework by which to guide its implementation. The study welcomes the fact that the MoD has codified (in its People Strategy Part 2) the areas where it is appropriate (and inappropriate) for Defence to use an industry solution. This vital work should be supplemented with the development of a Concept Note (which has been supported by ADS, the Aerospace and Defence industry trade body) to guide the Whole Force's implementation.

[326] Galbreath, 'Investigating the Whole Force Approach,' 6.

If the full potential of the Whole Force is to be realised, the Defence-industry relationship needs to evolve into a partnership model, where industry is considered a vital component of a broader Defence Enterprise. To achieve this, a number of barriers – some long-entrenched, others emerging more recently – must be overcome. One of the key 'frictions' standing in the way of achieving the Whole Force, identified by most respondents the study team talked to, remains cultural barriers between the military and industry/private sector, underpinned by misperceptions of industry motives, perceived risk to the military's capability, exposure to risk on operations and levels of pay, many of which are essentially 'workplace myths'. Breaking down these barriers may prove difficult and time-consuming (but not impossible), particularly as the military jealously guards its unique culture. Nevertheless, there are several steps that may help to reduce 'friction', such the communication of a persuasive, top down narrative explaining the need for and benefits of the Whole Force; the inclusion in existing UK Military Staff Courses modules on the realities and possible benefits of working with other components of the Whole Force; and the establishment of joint military-industry training exercises.

Discussions with stakeholders, on both sides of the public-private divide, indicated to the study team that another key barrier to progressing the Whole Force and moving to a partnership approach was sub-optimal commercial processes and contracting frameworks. Notwithstanding the MoD's current procurement improvement initiatives and broader engagement with industry, such barriers sometimes include: Defence's lack of relevant and Whole Force specific engagement with industry; poor requirement setting within capability teams, complicated and inflexible contracts, and limited coordination between Defence's internal decision-makers. Moreover, it was also indicated that an adversarial approach was often adopted by pockets of Defence during this process.

Similarly, it was noted that industry for its part, must also improve its commercial processes, particularly around accepting additional risk and flexibility when negotiating contracts. There were also suggestions that industry commercial teams must focus on being 'better partners'

and not 'go for the jugular' when the opportunity arose.[327] The key to improving the relationship is the development of trust and incentives to work collaboratively. This could involve industry showing greater flexibility when the situation changes and, as such, not seeking to increase the cost of contracts unnecessarily.

There were early signs of industry moving towards such an approach as some defence companies responded flexibly to the coronavirus challenge. For instance, the RAF's BAe 146 transport aircraft were rapidly repurposed to accommodate Medevac requirements and ventilators at no cost to the MoD. Whilst these examples could provide a framework by which to base future Defence-industry engagement on, recent cooperation may not transcend the current 'national effort' to combating coronavirus.[328] It is, of course, too early to judge if these examples will prove a successful basis on which to progress the Whole Force, but given the potential, this area is worthy of further research, encompassing an almost inevitable focus on national resilience in coming years.

Even if the Defence-industry relationship is positively reconfigured as a result of recent cooperation, defence companies must still decide if they are willing to accept the risks involved in participating in the Whole Force, such as putting employees in harm's way. These decisions must be made in advance of operations in order to facilitate the deployment of the employees at short notice; and to assure delivery. This early commitment to participate (or not) will help to bring a degree of certainty to the Whole Force agenda.

The growing importance of the Whole Force has been underlined during the government's response to the coronavirus pandemic. Of note, there have been examples of successful public and private sector collaboration, particularly as some defence companies have responded flexibly to the coronavirus challenge. That said, whilst these signs bode well for the future operationalisation of the Whole Force, there is limited publishable evidence to draw definitive conclusions about how these recent experiences will impact the Whole Force.

[327] Email communication with defence industry representative, 9 June 2020.
[328] Interview with defence industry representatives, Skype, 7 April 2020.

In the coming years, it is likely that the Whole Force debate will be informed and shaped by decisions about the size of the military and levels of Defence spending not yet taken, and to an extent, will be heavily shaped by political, not strategic, considerations. Notwithstanding this uncertainty, having a capped manpower target may prevent FLCs from developing the correct force mix. An informed debate regarding what the UK's strategic ambitions are should be the starting point to decide and develop the correct force mix. Another trend likely to inform the future Whole Force debate is how the military responds, in partnership with industry, to meet the technological challenges of tomorrow. Whilst the development of new technologies is time-consuming and costly, it is often noted that the MoD procurement process is cumbersome in reacting to the pace of technological change and its decision-making processes are constrained by an inherent aversion to risk. As such, the MoD must be willing to accept more failed projects as the price of being at the cutting edge of technological advancement. Moreover, given that high-end cyber operations require significant technical specialism, skill and experience, there is considerable scope to progress the Whole Force in this area.

A common refrain the study heard was that, as the character of warfare changes, the MoD may need to think creatively about the ways in which it can tap into a pool of expertise that is not traditionally associated with Defence and how to incorporate it into a future force. Industry may also need to be more willing to develop and provide a wider range of new skills and equipment than previously has been on offer.

Consideration of Whole Force (or similar) models internationally reveals that there is an increasing engagement with the private sector across a range of countries that is relevant to the Whole Force. Particularly in the areas of cyber security and technology more generally, there has been a realisation by some militaries and governments that an efficient way of improving the quality of their capabilities is through leveraging expertise from within the private sector. Conversely, it is also evident that in states with sophisticated military and technological training, the relationship between the military and industry becomes mutually beneficial and advantageous to that state's economy and technological expertise. While several governments and militaries have forged contractual relationships with their defence industries, in turn these defence industries have then proceeded to foster relationships with

other, generally smaller, suppliers of expertise - sometimes termed 'non-traditional suppliers'. The relationship with 'non-traditional suppliers' is often mutually beneficial, but also comes with challenges and barriers that governments and militaries should remain aware of and, if possible, endeavour to mitigate in order to sustain these relationships.

Whilst the UK and US context varies, the two countries pursue analogous approaches to combining Regular and Reservist, civilian, and contractor personnel in their respective cyber forces. As the US has made greater progress in developing its Defence cyber force, there is potential benefit to the UK studying the US approach and adapting lessons for future application of the Whole Force approach to Defence cyber in the UK. For instance, the US has highlighted the importance of effectively recruiting cyber Reserves, which adds significant depth to its cyber force. Connected to this, the US has developed an impressive force mix, which emphasises the need to recruit and contract the right balance of skills and experience to meet its cyber challenges. Moreover, the UK could conduct, as part of the Integrated Review, a force structure assessment of UK Defence cyber, including analysis of the role of Reservists and contractors.

While engagement with the private sector is a dominant theme across various states, it is evident that conceptions of what a Whole Force or Total Defence approach means varies. The extent of civil society engagement and how this is articulated is important. Some like the Nordic states have continually focused on civil society engagement, but this is not actually an overarching theme. Similarly, in considering Psychological Defence as a component of Total Defence, this has been fully embraced by some countries (such as Estonia) and rejected by others (such as Malaysia).

Finally, the model of integrating SRs alongside military personnel is an important part of the Whole Force, and has been considered internationally, including in the US. While explaining its aim for a 'Seamless Force', Australia also referred to the SR model, in addition to a contemporary workforce model that would allow movement between the Defence forces and the Reserves. Generally, around the world there are calls for more fluidity and flexibility of movement between the military and the private sector.

The study's overriding conclusion is that while there are risks involved in further private sector integration into the UK's Defence system (surrounding issues of assured delivery and Defence losing the in-house expertise to perform key functions, and/or the ability to design and manage contracts effectively) the benefits of maximising a fully integrated Whole Force considerably outweigh any disadvantages. The Whole Force, if planned strategically and implemented consistently and efficiently, provides Defence with a means of increasing its capacity and resilience. This is especially important given that Defence faces significant strategic and operational challenges, all of which are likely to intensify, and which are already placing strain on its ability to deliver military outputs. The study concludes that the drivers to adopt a fully integrated Whole Force model are just as, if not more, pressing today than when Lord Levene introduced his reforms in 2011.

6. Bibliography

ADA Europa. 'National Security Concept of Estonia.' ADA Europa, 12 May 2010. Accessed 10 May 2020, https://www.eda.europa.eu/docs/default-source/documents/estonia---national-security-concept-of-estonia-2010.pdf.

Aerospace, Defence, Security & Space Group Whole Force Working Group. Written Contribution to the Centre for Defence Studies (CDS), King's College London Whole Force study for The Serco Institute, 6 February 2020.

Ansari, Irfan. 'Efficient and Effective Financial Management of Defence Resources.' In *The Political Economy of Defence*, edited by Ron Matthews. Cambridge: Cambridge University Press, 2019.

Antill, Peter D. and Smith, Jeremy C. 'The British Army in Transition: From Army 2020 to the Strike Brigades and the Logistics of Future Operations.' *The RUSI Journal* 162, no. 3 (2017): 50-58.

Army Technology. 'UK Chief of Defence Staff participates in daily coronavirus briefing.' *Army Technology*, 23 April 2020. Accessed 10 May 2020, https://www.army-technology.com/news/uk-chief-of-defence-staff-participates-in-daily-coronavirus-briefing/.

Australian Government Department of Defence. 'Overseas recruits.' Australian Government Department of Defence. Accessed 10 June 2020, https://www.defence.gov.au/DCO/Overseas-recruits/#:~:text=Overseas%20or%20'Lateral'%20recruits%20are,be%20filled%20using%20Australian%20personnel.

Australian Government Department of Defence. *2016 Defence White Paper*. Canberra: Australian Government Department of Defence, 2016. Accessed 10 June 2020, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

Australian Government Department of Defence. *Force 2020*. Canberra: Australian Government Department of Defence, June 2002. Accessed 10 June 2020, https://www.defence.gov.au/Publications/f2020.pdf.

BAE Systems. 'Human and Social Science Research Capability (HSSRC).' BAE Systems. Accessed 10 June 2020, https://www.baesystems.com/en-uk/product/human-and-social-science-research-capability--hssrc-.

Baezner, Marie. *Study on the use of reserve forces in military cybersecurity: A comparative study of selected countries*. Center for Security Studies. Zürich: ETH Zürich, April 2020. Accessed 29 July 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-03-military-cybersecurity.pdf.

BBC News. 'Strength of British military falls for ninth year.' *BBC News*, 16 August 2019. Accessed 10 May 2020, https://www.bbc.co.uk/news/uk-49365599.

Belfer Centre, Harvard Kennedy School. *Deterring Terror: How Israel Confronts the Next Generation of Threats*. Cambridge, MA: Belfer Centre, Harvard Kennedy School, August 2016. Accessed 11 March 2020, https://www.belfercenter.org/israel-defense-forces-strategy-document#!introduction.

Biermann, R.J. 'Air Force Cyber Mission Force teams reach 'full operational capability.' US Air Force, 16 May 2018. Accessed 29 July 2020, https://www.af.mil/News/Article-Display/Article/1523543/air-force-cyber-mission-force-teams-reach-full-operational-capability/.

Bing, Christopher and Schectman, Joel. 'PROJECT RAVEN: Inside the UAE's Secret Hacking Team of American Mercenaries.' *Reuters*, 30 January 2019. Accessed 29 July 2020, https://www.reuters.com/investigates/special-report/usa-spying-raven/.

Blagden, David. 'How Britain's Ministry of Defence is playing for time (and money) in a dangerous world.' *The Conversation*, 18 January 2019. Accessed 10 May 2020, https://theconversation.com/how-britains-ministry-of-defence-is-playing-for-time-and-money-in-a-dangerous-world-109155.

Bloomberg. 'Over 460 Vulnerabilities Resolved in Tenth Bug Bounty Challenge with U.S. Department of Defense Thanks to Hackers on HackerOne.' *Bloomberg*, 15 April 2020. Accessed 20 April 2020, https://www.bloomberg.com/press-releases/2020-04-15/over-460-vulnerabilities-resolved-in-tenth-bug-bounty-challenge-with-u-s-department-of-defense-thanks-to-hackers-on-hackerone.

Bond, David. 'UK must rethink military strategy, warns army head.' *Financial Times*, 4 June 2019. Accessed 4 May 2020, https://www.ft.com/content/094ad520-86d6-11e9-a028-86cea8523dc2.

Butcher, Fiona. 'Role of research psychology in defence and security.' *Journal of the Royal Army Medical Corps* 165, no. 2 (2019): 113-115.

Camm, Frank. 'How to Decide When a Contractor Source is Better to Use Than a Government Source,' In *Contractors and War: the Transformation of US Expeditionary Operations*, edited by Christopher Kinsey and Malcolm Patterson. Stanford, CA: Stanford University Press.

Cardash, Sharon L., Cilluffo, Frank J., and Ottis, Rain. 'Estonia's cyber defence league: A model for the United States?' *Studies in Conflict & Terrorism* 36, no. 9 (2013): 777-787.

Carter, Nicholas and Waal, James de. 'The Future of the British Army: How the Army Must Change to Serve Britain in a Volatile World.' Transcript. *Chatham House*. Accessed 27 November 2019:

https://www.chathamhouse.org/sites/default/files/field/field_document/20150217QBritishArmy.pdf.

Carter, Nick. 'Annual Chief of the Defence Staff Lecture and RUSI Christmas Party 2019.' *RUSI*, 5 December 2019. Accessed 10 May 2020, https://rusi.org/event/annual-chief-defence-staff-lecture-and-rusi-christmas-party-2019.

Carter, Phillip, Kidder, Katherine, Schafer, Amy, Swick, Andrew. *The Future of the All-Volunteer Force*, Working Paper AVF 4.0. Washington, DC: Centre for a New American Security, March 2017. Accessed 22 April 2020: https://www.jstor.org/stable/resrep06308?seq=1#metadata_info_tab_contents.

Centre for Defence Studies. The Whole Force by Design Roundtable: Summary of Discussions, King's College London, 11 December 2019.

Chao, Linda. *Assessing the Lee Teng-hui legacy in Taiwan's politics: democratic consolidation and external relations*. New York: ME Sharpe, 2002.

Comptroller and Auditor General. *Ministry of Defence: Ensuring sufficient skilled military personnel*, Session 2017-19 HC 947. London: National Audit Office, 2018.

Comptroller and Auditor General. Ministry of Defence: The Equipment Plan 2019 to 2029, Session 2019-20 HC 111. London: National Audit Office, 2020.

Connell, Sam. 'Saluting our Cyber Reservists,' *Defence Digital*, 24 June 2020. Accessed 29 July 2020, https://defencedigital.blog.gov.uk/2020/06/24/saluting-our-cyber-reservists/.

Cordey, Sean. *Trend Analysis: The Israeli Unit 8200: An OSINT-based study*, Center for Security Studies. Zürich: ETH Zürich, December 2019. Accessed 10 June 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf.

Cornish, Paul and Dorman, Andrew M. 'Dr Fox and the Philosopher's Stone: the alchemy of national defence in the age of austerity.' *International Affairs* 87, no. 2 (2011): 335-353.

Cox, Amy G., Moore, Nancy Young, and Grammich, Clifford A. *Identifying and Eliminating Barriers Faced by Nontraditional Department of Defense Suppliers*. Santa Monica, CA: RAND Corporation, 2014. Accessed 10 June 2020: https://www.rand.org/pubs/research_reports/RR267.html.

Cusumano, Eugenio. 'Bridging the Gap: Mobilising Constraints and Contractor Support to US and UK Military Operations.' *Journal of Strategic Studies* 39, no. 1 (2016): 94-199.

Davis, Lynn E., Rough, Jill, Cecchine, Gary, Schaefer, Agnes Gereben and Rohn, Laurinda L. *Learning the Lessons of Hurricane Katrina for the U.S. Army,* Research Brief. Santa Monica, CA: RAND Corporation, 2007. Accessed 12 June 2020, https://www.rand.org/pubs/research_briefs/RB9255.html.

DCMS. ‘Guidance: Cyber security supplier to government scheme: list of participating companies.’ GOV.uk, 17 September 2018. Accessed 29 July 2020, https://www.gov.uk/government/publications/cyber-security-supplier-to-government-scheme/cyber-security-supplier-to-government-scheme-list-of-participating-companies.

Defence, Science and Technology Laboratory. ‘Dstl Awards £350 million ASTRID contract to BAE Systems CORDA.’ GOV.uk. Accessed 10 June 2020, https://www.gov.uk/government/news/dstl-awards-350-million-astrid-contract-to-bae-systems-corda.

Deloitte. ‘Australia’s 2020 Cyber Security Strategy: A call for views.’ Deloitte, November 2019. Accessed 29 June 2020, http://images.content.deloitte.com.au/Web/DELOITTEAUSTRALIA/%7B2ac328f6-1dfc-4c2b-ba45-1a278dc03c83%7D_20191210-ris-inb-australias-2020-cyber-security-strategy-report.pdf?elq_mid=3097&elq_cid=292819&utm_medium=email&utm_campaign=20191210-ris-2020-cyber-strategy&utm_content=cta&elqTrack=true.

Devanny, Joe. ‘UK National Security Decision-Making in Context: The Ukraine Crisis and NATO’s Warsaw Summit Meeting.’ *Sasakawa Peace Foundation*, 2018. Accessed 29 July 2020, https://www.spf.org/projects/upload/UK%20National%20Security%20Decision-Making%20in%20Context%20%28Devanny%29.pdf.

Dobson, Alan and Marsh, Steve. ‘Benign Neglect: America’s Threat to the Anglo-American Alliance.’ *Orbis* 58, no. 2 (2014): 266-81.

DOD News. ‘Department of Defense Expands “Hack the Pentagon” Crowdsourced Digital Defense Program.’ *DOD News*, 24 October 2018. Accessed 12 March 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/.

Donaldson, Sam, Shah, Jayesh Navin, Pedley, Daniel, Crozier, David and Furnell, Steven. *UK Cyber Security Sectoral Analysis 2020: Research report for the Department for Digital, Culture, Media and Sport*. London: Department for Digital, Culture, Media and Sport (DCMS), 2020. Accessed 29 July 2020, https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020.

Dunne, Philip. *Growing the Contribution of Defence to UK Prosperity: A report for the Secretary of State for Defence*. July 2018. Accessed 10 May 2020, https://www.philipdunne.com/sites/www.philipdunne.com/files/attachments/Philip_Dunne_Defence.pdf.

Edmunds, Timothy, Dawes, Antonia, Higate, Paul, Jenkings, K. Neil. and Woodward, Rachel. ‘Reserve forces and the transformation of British military organisation: soldiers, citizens and society.’ *Defence Studies* 16, no. 2 (2016): 118–136.

Edwards, Jay. *Contractorisation of UK Defence: Developing a Defence-Wide Contractorisation Strategy and Improving Implementation*. RUSI Occasional Paper. London: RUSI, June 2018. Accessed 10 May 2020, https://rusi.org/sites/default/files/201806_rusi_contractorisationofukdefence_edwards_web.pdf

Erbel, Mark. 'The underlying causes of military outsourcing in the USA and UK: bridging the persistent gap between ends, ways and means since the beginning of the Cold War.' *Defence Studies* 17, no. 2 (2017): 135-155.

Faisol Keling, Mohamad, Na'eim Ajis, Mohd, Shuib, Md Shukri, Muhammad, Fuad Othman, and Som, Hishamudin Md. 'The Malaysian government's efforts in managing military and defence development.' *International Journal of Business and Social Science* 2, no. 12 (2011): 180-193.

Ferdinando, Lisa. 'Carter Legacy: Force of the Future, modernizing DoD, confronting threats.' *Air Force Reserve Command*, 19 January 2017. Accessed: 12 March 2020, https://www.afrc.af.mil/News/Article-Display/Article/1053713/carter-legacy-force-of-the-future-modernizing-dod-confronting-threats/.

Fisher, Lucy. 'Britain's parallel army of cyberwarriors.' *The Times*, 17 August 2019. Accessed 29 July 2020, https://www.thetimes.co.uk/article/britains-parallel-army-of-cyberwarriors-gzkzzdnvh.

Fisher, Lucy. 'Defence review in turmoil, say insiders.' *The Times*, 22 February 2020. Accessed 10 May 2020, https://www.thetimes.co.uk/article/boris-johnson-s-foreign-policy-defence-and-security-review-in-turmoil-say-insiders-2fq9mz7gf.

Fisher, Lucy. *The Times*, Twitter thread. 18 May 2020. Accessed 19 May 2020, https://twitter.com/LOS_Fisher/status/1262371993976025088.

Francois, Mark. *Filling the Ranks: A Report for the Prime Minister on the State of Recruiting into the United Kingdom Armed Forces*. July 2017.

Galbreath, David. 'Investigating the Whole Force Approach: Whitehall, the Army, and the private sector: working towards a genuine partnership.' *The occasional papers of the Centre for Historical Analysis and Conflict Research: ARES & ATHENA* 2, (Winter 2015/16): 1-36.

Gomez, Eric, Preble, Christopher A., Sander, Lauren and Valeriano, Brandon. *Building a Modern Military: The Force Meets Geopolitical Realities*, White Paper. Washington, DC: CATO Institute, May 2020. Accessed 10 June 2020, https://www.cato.org/publications/white-paper/building-modern-military-force-meets-geopolitical-realities.

Guest. 'Defence, Security, Psychology.' *British Psychological Society*, 26 October 2018. Accessed 10 May 2020, https://www.bps.org.uk/blogs/guest/defence-security-psychology.

Hannan, Noel K. 'Use of Reserve Forces in Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches.' *The RUSI Journal* 160, no. 5 (2015): 46-51.

Hannigan, Robert. *Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre*. RUSI Occasional Paper. London: RUSI, February 2019. Accessed 29 July 2020, https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf.

Hayes, Richard J. 'DOD Response Under the Stafford Act: A Call to Action', *Joint Force Quarterly* 77, 1 April 2015.

Haynes, Deborah. 'Britain to create 2,000-strong cyber force to tackle Russia threat.' *Sky News*, 21 September 2018. Accessed 29 July 2020, https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653

Heidenkamp, Henrik. *Sustaining the UK's Defence Effort: Contractor Support to Operations Market Dynamics*. RUSI Whitehall Report 2-12. London: RUSI, April 2012. Accessed 10 May 2020, https://rusi.org/sites/default/files/201504_whr_contractor_support_to_operations_0.pdf.

Hitchens, Theresa. 'BAE Makes Big Bet on Small Companies: FAST Labs.' *Breaking Defense*, 21 May 2019. Accessed 10 June 2020, https://breakingdefense.com/2019/05/bae-makes-big-bet-on-small-companies-fast-labs/.

HL Written Question, 26 April 2018, HL7352. Accessed 4 December 2019, https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2018-04-26/HL7352.

HM Government. *National Security Capability Review*. London: Stationery Office, 2018. Accessed 29 July 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.

HM Government. *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161. London: Stationery Office, 2015. Accessed 10 May 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

HM Government. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, Cm 7948. London: Stationery Office, 2010. Accessed 27 November 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf.

House of Commons Committee of Public Accounts. *Capita's contracts with the Ministry of Defence*, Session 2017-19 HC 1736. London: Stationery Office, 2019.

House of Commons Defence Committee. *Oral Evidence: Work of the Chief of Defence Staff*, Session 2019-21 HC 295. 2020.

House of Commons Defence Committee. *Re-thinking defence to meet new threats, Session 2014-15 HC 512*. London: Stationery Office, 2015.

House of Commons Public Accounts Committee. *Skills Shortages in the Armed Forces*, Session 2017-19 HC 1027. London: Stationery Office, 2018.

House of Lords and House of Commons Joint Committee on the National Security Strategy. *National Security Capability Review: A changing security environment*, Session 2017-19, HL Paper 104 HC 756. London: Stationery Office, 2018.

Inspector General Department of Defense. *Fiscal Year 2019: Top DOD Management Challenges*. Washington DC: Inspector General Department of Defense, 2018. Accessed 20 June 2020, https://media.defense.gov/2018/Dec/12/2002071981/-1/-1/1/TOP%20DOD%20MANAGEMENT%20CHALLENGES%20FISCAL%20YEAR%202019.PDF.

International Institute for Strategic Studies. 'Chapter Two: Comparative defence statistics.' *The Military Balance* 120, no. 1 (2020): 21-27.

Israel Defense. 'IDF Unit 8200 Thwarted ISIS Terror Attack on Australian Flight.' *Israel Defense*, 22 February 2018. Accessed 20 March 2020, https://www.israeldefense.co.il/en/node/33176.

James, Denis. 'Strengthening the Private Sector's Role in UK Defence Engagement.' *Chatham House Research Paper* (August 2017). Accessed 27 November 2019, https://www.chathamhouse.org/sites/default/files/publications/2017-08-25-defenceengagement1.pdf.

Julius, DeAnne. *Understanding the Public Services Industry: How big, how good, where next?* Public Services Industry Review. Department for Business, Enterprise & Regulatory Reform, July 2008.

Kane, Tim. *Bleeding talent: How the US military mismanages great leaders and why it's time for a revolution*. New York: Springer, 2017.

Karabeshkin, Leonid A. *Civil-military Relations in Estonia: Legal Background and Contemporary Discourse The Estonian Case*, Research Paper No1/4 2007. Frankfurt: Peace Research Institute Frankfurt, 2007. Accessed 11 March 2020, https://www.hsfk.de/fileadmin/HSFK/hsfk_downloads/ESTONI_4.pdf.

KBR. 'Replacing the Army's existing fleet of tank transporters and pioneering the use of Sponsored Reserves,' KBR. Accessed 9 December 2019, https://www.kbr.com/en/experience/heavy-equipment-transporter-het.

Kinsey, Christopher. 'Outsourcing Military Logistics and Security Services: The Case of the United Kingdom.' In *The Routledge Research Companion to Security Outsourcing in the Twenty-First Century*, edited by Joakim Berndtsson and Christopher Kinsey. Abingdon: Routledge, 2016.

Kochems, Alane. *When Should the Government Use Contractors to Support Military Operations?* Washington, DC: The Heritage Foundation, May 2006. Accessed 20 June 2020, https://www.heritage.org/defense/report/when-should-the-government-use-contractors-support-military-operations.

Lonsdale, David J. 'Britain's Emerging Cyber-Strategy.' *The RUSI Journal* 161, no. 4 (2016): 52-62.

Louth, John and Quentin, Pete. *Making the Whole Force Concept a Reality*. Royal United Services Institute (RUSI) Briefing Paper. London: RUSI, November 2014. Accessed 10 May 2020, https://rusi.org/system/files/RUSI-BP-WholeForceConcept-Nov14.pdf.

Louth, John and Taylor, Trevor. *British Defence in the 21st Century*. Routledge: London and New York, 2019.

Manuel, Kate M. *Definitions of 'Inherently Governmental Function' in Federal Procurement Law and Guidance*. Congressional Research Service (CRS) R42325. Washington, DC: CRS, December 2014. Accessed 29 July 2020, https://fas.org/sgp/crs/misc/R42325.pdf

McBeth, Marie. 'Multimodal 2019 – The HGV Driver Skills Shortage Continues – What's The Solution.' Ten Live Group, 2 July 2019. Accessed 10 May 2020, https://tenlivegroucom/multimodal-2019-hgv-driver-skills-shortage-whats-the-solution/.

McGuinness, Damien. 'How a cyber attack transformed Estonia.' *BBC News*, 27 April 2017. Accessed 11 March 2020, https://www.bbc.co.uk/news/39655415.

Menn, Joseph. 'U.S. aims to limit exports of undisclosed software flaws.' *Reuters*, 21 May 2015. Accessed 29 July 2020, https://uk.reuters.com/article/us-software-exports/u-s-aims-to-limit-exports-of-undisclosed-software-flaws-idUKM1KBN0O604R20150521.

Ministry of Defence. 'Ministry of Defence seeks to maximise Reserves contribution through new review.' News story, 3 June 2020. Accessed 30 June 2020, https://www.gov.uk/government/news/ministry-of-defence-seeks-to-maximise-reserves-contribution-through-new-review#:~:text=The%20Reserve%20Forces%202030%20review,wider%20government%2C%20business%20and%20society

Ministry of Defence. 'MOD leads cross-government review into the UK's defence and security industrial strategy.' News story, 5 March 2020. Accessed 7 April 2020, https://www.gov.uk/government/news/mod-leads-cross-government-review-into-the-uks-defence-and-security-industrial-strategy

Ministry of Defence. *Army People Strategy*. London: Ministry of Defence, 2020. Accessed 10 May 2020, https://aff.org.uk/wp-content/uploads/2019/11/pers_sub_strat_booklet_final_screen.pdf.

Ministry of Defence. *Defence People Strategy Part One*. London: Ministry of Defence, March 2020.

Ministry of Defence. *Global Strategic Trends: The Future Starts Today*, Sixth Edition. London: Ministry of Defence, 2018. Accessed 6 April 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf.

Ministry of Defence. *Mobilising, Modernising & Transforming Defence: A report on the Modernising Defence Programme*. London: Ministry of Defence: 2018. Accessed 10 May 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/765879/ModernisingDefenceProgramme_report_2018_FINAL.pdf.

Ministry of Defence. *Small and Medium-sized Enterprise Action Plan, 2019-2022*. London: Ministry of Defence, 2019. Accessed 10 June 2020: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793101/20190405_SME_Action_Plan_2019.pdf

Ministry of Defence. UK Armed Forces Quarterly Service Personnel Statistics - 1 January 2020, 20 February 2020. Accessed 10 May 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866842/1_Jan_2020_-_SPS.pdf

Moore, David M. and Antill, Peter D. 'The Use of Contractors on Deployed Operations (CONDO) in the Age of Austerity.' *RUSI Defence Systems* 14, no. 2 (2011). Accessed 27 November 2019, https://core.ac.uk/download/pdf/9637522.pdf.

Nakashima, Ellen and Gregg, Aaron. 'NSA's top talent is leaving because of low pay, slumping morale and unpopular reorganization.' *Washington Post*, 3 January 2018. Accessed 29 July 2020, https://www.washingtonpost.com/world/national-security/the-nsas-top-talent-is-leaving-because-of-low-pay-and-battered-morale/2018/01/02/ff19f0c6-ec04-11e7-9f92-10a2203f6c8d_story.html.

Nakasone, Paul. 'Statement of General Paul M. Nakasone, Commander, United States Cyberspace Command.' House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, US Congress. March 2020. Accessed 29 2020, https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf.

National Army Museum. 'Corps of Royal Engineers.' Accessed 10 May 2020, https://www.nam.ac.uk/explore/corps-royal-engineers.

National Commission on Military, National, and Public Service. *Inspired to Serve The Final Report of the National Commission on Military, National, and Public Service*. Washington DC: National Commission on Military, National, and Public Service, 2020. Accessed 20 April 2020, https://inspire2serve.gov/reports/final-report.

NATO Standardization Agency (NSA). *Allied Joint Doctrine for Host Nation Support AJP-4.5*, Edition B Version 1 (Brussels, NSA, May 2013).

Nineham, Chris. *The British State: A Warning*. London: John Hunt Publishing, 2019.

Panetta, Leon, Talent, Jim, Jones, Jim, Roth-Douquet, Kathy. *Building a F.A.S.T. Force: A flexible Personnel System for a Modern Military*. Washington, DC: Bipartisan Policy Center, March 2017. Accessed 10 June 2020, https://bipartisanpolicy.org/wp-content/uploads/2019/03/BPC-Defense-Building-A-FAST-Force.pdf.

Parry, Emma, Connelly, Vincent, Robinson, Dilys, Robinson, Zoe and Taylor, Chris. *Integration of the Whole Force: Understanding Barriers and Enablers to Task and Team Performance (O-DHCSTC_12_P_T2_083/005),* Defence Human Capability Science and Technology Centre, 2016.

Peach, Stuart. 'Annual Chief of the Defence Staff Lecture 2017, Air Chief Marshall Sir Stuart Peach, Chief of the Defence Staff.' *RUSI*, 14 December 2017. Accessed 27 November 2019, https://rusi.org/sites/default/files/20171214-rusi-cds_annual_lecture-acm_peach.pdf.

Peach, Stuart. 'Valedictory Address as Chief of the Defence Staff: A Speech by Air Chief Marshall Sir Stuart Peach for Policy Exchange.' 5 June 2018. Accessed 27 November 2019, https://policyexchange.org.uk/wp-content/uploads/2018/06/CDS-transcript.pdf.

Peltier, Heidi. *The Growth of the 'Camo Economy' and the Commercialization of the Post-9/11 Wars*. Watson Institute Brown University/Pardee Center Boston University. June 2020. Accessed 29 July 2020, https://watson.brown.edu/costsofwar/files/cow/imce/papers/2020/Peltier%202020%20-%20Growth%20of%20Camo%20Economy%20-%20June%2030%202020%20-%20FINAL.pdf.

Peri, Yoram. *The Israeli Military and Israel's Palestinian Policy: From Oslo to the Al Aqsa Intifada*, Peaceworks No. 47. Washington, DC: United States Institute of Peace, November 2002. Accessed 11 March 2020, https://www.tau.ac.il/institutes/herzog/peaceworks.pdf.

Pernik, Pirret and Tuohy, Emmit. 'Interagency Cooperation on Cyber Security: the Estonian Model' In *Effective Inter-Agency Interactions and Governance in Comprehensive Approaches to Operations*, edited by P. J. M. D. Essens, M. M. Thompson and S. M. Halpin. NATO STO Symposium Proceedings AC/323 (HFM-236) TP/597, 2014.

Peters, Heidi M. *Defense Primer: Department of Defence Contractors*, CRS IF10600. Washington, DC: CRS, January 2020. Accessed 12 June 2020, https://fas.org/sgp/crs/natsec/IF10600.pdf.

Phillips, Mark. *The Future of the UK's Reserve Forces*. RUSI Occasional Paper. London: RUSI, April 2012. Accessed 11 June 2020, https://rusi.org/sites/default/files/201204_op_future_of_the_uks_reserve_forces.pdf.

Pletka, Danielle. 'A conversation with Benjamin Netanyahu.' *AEI*, 9 November 2015. Accessed 10 June 2020, https://www.aei.org/research-products/speech/a-conversation-with-benjamin-netanyahu/.

Pomerleau, Mark. 'Army releases $1B cyber training request.' *Fifth Domain*, 12 June 2020. Accessed 29 July 2020, https://www.fifthdomain.com/dod/cybercom/2020/06/12/army-releases-1b-cyber-training-request/.

Pomerleau, Mark. 'Senators seek to cut Army cyber program for greater joint investment.' *Fifth Domain*, 30 June 2020. Accessed 29 July 2020, https://www.c4isrnet.com/cyber/2020/06/30/senators-seek-to-cut-army-cyber-program-for-greater-joint-investment/.

Portsoken, Lord Levene of. *Defence Reform: An independent report into the structure and management of the Ministry of Defence*. London: Ministry of Defence, June 2011. Accessed 27 November 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27408/defence_reform_report_struct_mgt_mod_27june2011.pdf.

Press, Gil. '6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry.' *Forbes*, 18 July 2017. Accessed 11 March 2020, https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#31f53f08420a.

Prime Minister's Office of Malaysia. 'Malaysia's National Defence Policy.' Prime Minister's Office of Malaysia, July 2019. Accessed 10 May 2020, https://www.pmo.gov.my/wp-content/uploads/2019/07/National-Defence-Policy.pdf.

Rossbach, Niklas H. *Psychological Defence: Vital for Sweden's Defence Capability*, FOI Memo 6207, Strategic Outlook 7. Stockholm: Swedish Defence Research Agency, November 2017.
Royal Air Force. 'RAF Aircraft Adapted for Medical Use in Record Time.' Royal Air Force, 17 June 2020. Accessed 30 June, https://www.raf.mod.uk/news/articles/raf-aircraft-adapted-for-medical-use-in-record-time/.

Ruiz, Monica M. 'Is Estonia's approach to cyber defense feasible in the United States?' *War on the Rocks*, 9 January 2018. Accessed 11 March 2020, https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.

Schogol, Jeff. 'Every Marine a rifleman no more?' *Marine Times*, 7 May 2017. Accessed 22 April 2020, https://www.marinecorpstimes.com/news/your-marine-corps/2017/05/07/every-marine-a-rifleman-no-more/.

Schwartz, Moshe and Church, Jennifer. *Department of Defence's Use of Contractors to Support Military Operations: Background, Analysis, and Issues for Congress*, CRS R43074. Washington, DC: CRS, May 2013. Accessed 29 July 2020, https://fas.org/sgp/crs/natsec/R43074.pdf.

Senor, Dan and Singer, Saul. *Start-up nation: The story of Israel's economic miracle* (New York: Random House Digital, Inc., 2011).

Shape NATO. 'Estonian Defence League – The Kaitselit – Strong in Defence.' Shape NATO, 14 May 2019. Accessed 11 March 2020, https://shape.nato.int/news-archive/2019/estonian-defence-league-the-kaitseliit-strong-in-defence-.

Shouesmith, David. 'Industry and Support to UK Contemporary Military Operations: A Practitioner's Strategic Military Perspective.' In *The Routledge Research Companion to Security Outsourcing in the Twenty-First Century*, edited by Joakim Berndtsson and Christopher Kinsey. Abingdon: Routledge, 2016.

Simpson, Julianne. 'Urgent Need for Cybersecurity Professionals Grows.' *The Cyber Edge*, 1 May 2019. Accessed 11 March 2020, https://www.afcea.org/content/urgent-need-cybersecurity-professionals-grows.

Statista, Number of personnel in UK Armed Forces 1900-2019. Accessed 4 December 2019, https://www.statista.com/statistics/579773/number-of-personnel-in-uk-armed-forces/.

Stone, Jeff. 'Meet The Cyber-Industrial Complex: Private Contractors May Get $7B Windfall From Pentagon's Cyberwar On ISIS.' *International Business Times*, 7 March 2016. Accessed 29 July 2020, https://www.ibtimes.com/meet-cyber-industrial-complex-private-contractors-may-get-7b-windfall-pentagons-2329652.

Sydow, Björn Von. 'Resilience: Planning for Sweden's "Total Defence".' *NATO Review*, 4 April 2018. Accessed 29 July 2020, https://www.nato.int/docu/review/articles/2018/04/04/resilience-planning-for-swedens-total-defence/index.html.

Teo, Dominic. 'See how Total Defence Day has evolved through the years.' *The Straits Times*, 16 February 2016. Accessed 10 May 2020, https://www.straitstimes.com/singapore/see-how-total-defence-day-has-evolved-through-the-years.

Thompson, Loren. 'BAE Systems Invents A Radically Different Way of Speeding Defense Innovation.' *Forbes*, 15 April 2019. Accessed 10 June 2020, https://www.forbes.com/sites/lorenthompson/2019/04/15/bae-systems-inc-invents-a-radically-different-way-of-speeding-defense-innovation/#20d48211f9d2.

Thompson, Loren. 'Raytheon And BAE Systems Are Drawing Nontraditional Suppliers Into Defense.' *Forbes*, 24 January 2020. Accessed 10 June 2020, https://www.forbes.com/sites/lorenthompson/2020/01/24/how-top-military-contractors-

raytheon-and-bae-systems-are-drawing-non-traditional-suppliers-into-defense/#3b1b111a6af2.

Thornton, Rod. 'Covid-19 and why state resilience in the United Kingdom needs to be strengthened: The link to the changing character of war and lessons from Russia.' *Defence-In-Depth Blog*, 8 April 2020. Accessed 10 May 2020, https://defenceindepth.co/2020/04/08/covid-19-and-why-state-resilience-in-the-united-kingdom-needs-to-be-strengthened-the-link-to-the-changing-character-of-war-and-lessons-from-russia/.

US Army Cyber Command. 'About Us,' https://www.arcyber.army.mil/Organization/About-Army-Cyber/.

US Senate Armed Services Committee. 'FY2021 National Defense Authorization Act (NDAA) Summary.' June 2020. Accessed 29 July 2020, https://www.armed-services.senate.gov/imo/media/doc/FY%2021%20NDAA%20Summary.pdf.

Vergun, David. 'Defense Digital Service Is Hiring Talent, Continuing Mission Despite COVID-19.' *DOD News*, 17 June 2020. Accessed 18 June 2020, https://www.defense.gov/Explore/News/Article/Article/2223499/defense-digital-service-is-hiring-talent-continuing-mission-despite-covid-19/.

White House. *National Security Strategy of the United States of America*. Washington D.C: White House, December 2017. Accessed 29 July 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

Williamson, Gavin. 'Modernising Defence Programme Oral statement to Parliament.' GOV.uk, 18 December 2018. Accessed 10 May 2020, https://www.gov.uk/government/speeches/modernising-defence-programme-update.

Winder, Davey. 'U.S. Air Force Successfully Hacked By 'Battalion' Of 60 Hackers.' *Forbes*, 16 April 2020. Accessed 20 April 2020, https://www.forbes.com/sites/daveywinder/2020/04/16/us-air-force-successfully-hacked-by-battalion-of-60-hackers/.

Wither, James Kenneth. 'Back to the future? Nordic total defence concepts.' *Defence Studies* 20, no. 1 (2020): 61-81.

Wyatt, Sam. 'Introducing the Human Social Science Research Capability Framework.' *Tech UK*, 03 March 2020. Accessed 10 June 2020, https://www.techuk.org/insights/opportunities/item/16986-introducing-the-human-social-science-research-capability-framework.

7. Appendix

7.1 Comprehensive List of Recommendations

1. *The Whole Force should be defined as: Effective, agile and resilient capability delivered by an integrated, pre-planned and affordable military capability comprised of a mix of Regular, Reserve, civil servant and industry supported by appropriate technology to meet Defence outputs. It should be circulated among all component parts of the Whole Force as the first step in formalising and standardising a shared understanding of the Whole Force (see section 3.4).*

2. *The Development, Concept and Doctrine Centre should resume its work on the development of a Concept Note that has been informed by industry contributions. Once this work has been finalised it should be circulated for approval and endorsement in both the MoD and FLCs at two-star level and above. The resultant Concept Note should then be used as part of the MoD and FLCs core planning in response to the Integrated Review. (see section 3.5).*

3. *Accompanying the communication of the proposed Whole Force definition, a persuasive, top-down narrative explaining the need for and benefits of the Whole Force should be communicated across the FLCs (see section 3.6).*

4. *The Chief of Defence People (CDP) should be appointed Senior Responsible Owner to plan, oversee and ultimately execute the Whole Force's delivery. The CDP should be supported by Financial Military Capability personnel to ensure a coordinated process across the three Services. It may also be useful for cadre of dedicated senior supporting staff working on the Whole Force to remain in post for longer than the typical two-year postings (see section 3.7).*

5. *To generate understanding of where and how the Whole Force works, the MoD should compile a comprehensive compendium, regularly updated, that details all Whole Force*

projects, which can then be shared across the Services, and Defence more generally, to provide lessons learned (see section 3.8).

6. *Cultural barriers and misunderstanding about the nature of Whole Force are critical frictions holding back implementation of agenda. The MoD should develop and communicate a strong Whole Force narrative across the FLCs, explaining the critical role that contractors play within the Whole Force (see section 3.9.1).*

7. *Military education courses that highlight the role of contractors in the Whole Force should be embedded into the curriculum of existing UK Staff Courses. Such education should start as soon as officers (and non-commissioned officers) enter service and should continue throughout the entirety of their careers (see section 3.9.2).*

8. *To fully operationalise a true Whole Force model, there needs to be a comprehensive approach to the integration of contractors with their military partners before, as well as on operations. Joint training and exercise programmes not only would improve operational performance and integrated working practices but would also help to break down cultural barriers and help to foster a 'team Defence' mentality on both sides (see section 3.9.3).*

9. *Defence officials should establish and regularly convene a Defence-industry working group including relevant senior officials from the MoD, officers from across the three Services, and industry representatives to identify a coherent plan to operationalise the Whole Force. Such forums could enable Defence to engage with industry as early as possible before framing contracts. Strategic engagement could improve outcomes; whilst also helping both sides progress towards a genuine partnership, with a greater sharing of both risks and rewards (see section 3.9.4).*

10. *All FLC officials responsible for managing and overseeing existing contracts should be given the opportunity to attend the foundation level of the civil service contract management training course if they are not already offered this, with consideration*

given to which staff would benefit from the advanced levels of this course (see section 3.9.4).

11. *If companies decide they want to play an active part in the delivery of the Whole Force, they must facilitate open discussion about the nature of the risks involved. This may mean acceptance that the risk associated with potentially placing their employees in harm's way involves recruiting employees with the appropriate terms and conditions (see section 3.9.5).*

12. *When designing a blended workforce, the Sponsored Reserve model should be considered having been proven through various overseas deployments (including the Afghanistan and Iraq campaigns), to be capable of ensuring assured delivery through highly capable and skilled individuals on deployments (see section 3.9.5).*

13. *The MoD should accept more risk (including the possibility of early failure of some projects) when developing new technologies to ensure that it can respond in a timely manner to a rapidly evolving technological environment (see section 3.11).*

14. *The Integrated Review should include a Defence cyber workforce strategic audit, identifying the skills and force structure required for the defensive and offensive cyber missions through to 2030. This audit should assess the required size and scope of civilian, military (Regular and Reservist), and private sector contributions to Defence cyber (see section 3.12).*

15. *As the character of conflict changes, industry must be willing to develop and provide new skills that Defence will increasingly need. This may involve both sides collaborating on identifying an effective long-term manpower strategy (see section 3.13).*

16. *Pilots projects such as the current Royal Logistic Corps driver project, which focuses on low-skilled roles, could act as a pathfinder for the development of schemes that focus on higher-skilled roles and should be assessed with this in mind (see section 3.13).*

17. *For an effective partnership model to develop, Defence and industry must move beyond the initial step of only sharing human resources to also sharing information and knowledge. This may involve companies sharing commercially sensitive information, such as Human Resources practices (see section 3.13).*

18. *Alternative routes to entry, including lateral entry schemes, which open opportunities in Defence to suitably qualified applicants from outside the military, could offer Defence an untapped pool of human resource, especially in highly skilled areas. Whilst these routes to entry should not be considered a panacea to Defence's recruitment and skills challenges, such programmes should be encouraged and developed (see section 3.13).*

19. *The Integrated Review should conduct a force structure assessment of UK Defence cyber, including analysis of the role of Reservists and contractors. It should also consider the US case as a comparator, and, where appropriate, explore the merits of procuring capabilities developed for US Defence cyber as a cost-efficient approach to UK Defence cyber procurement. This should be balanced against the competing strategic requirement for a domestic cyber defence industrial base (see section 4.3).*

20. *Given the value that non-traditional suppliers can add to the Whole Force, the MoD should continue to identify specific barriers to entry that prevent non-traditional suppliers from engaging more fully in the Whole Force process (see section 4.5).*

21. *UK defence companies should develop options to improve the working relationship between the defence industry, SMEs and non-traditional suppliers in order to bolster the efficiency of the Whole Force. (see section 4.5).*

7.2 About the Centre for Defence Studies

The CDS team on the Whole Force by Design study included: Dr Philip Berry (Senior Researcher), Dr Joseph Devanny, Professor John Gearson (Principal Investigator & Study Lead), and Dr Nina Musgrave. The team would like to thank all those who generously offered their time and knowledge to informing the report, including all those who attended the cross-sector workshops and those who commented on emerging themes during the study.

The Centre for Defence Studies (CDS) is a world-leading think tank for defence and security research, thought-leadership, consultancy and executive development. Established in 1990, it promotes interdisciplinary approaches to international security and defence policy research. Working with governments, international organisations and the private sector, the CDS operates in three overlapping research areas: academic, public policy, and corporate consultancy.

The CDS conducts research and consultancy on national security, terrorism, counterterrorism, intelligence, defence policy, and public policy questions for domestic and international clients. Drawing upon the expertise within the CDS, as well as across King's College London and partner institutions, the Centre works closely with clients in identifying the most appropriate content and delivery style for its activities.

The CDS has extensive experience in providing bespoke professional development courses and executive education solutions in the fields of defence, security, and public policy. The Centre launched the first MA in National Security Studies in the UK at King's College in September 2017 which brings full time students together with practitioners from across government and the private sector to consider this growing area of public policy.

The CDS was voted the 4th Best University Affiliated Think Tank of 2019 in the Global Go To Think Tank Index Report by the University of Pennsylvania. For more information on the Centre for Defence Studies visit: https://www.kcl.ac.uk/research/centre-for-defence-studies

7.3 About the Serco Institute

The Serco Institute is a think tank originally established by Serco in 2002 to explore and develop thinking on mechanisms for delivering public services, and in particular around the benefits of contestability and competition; in 2012 the Institute became dormant. However, at a time when there has never been greater need for public services which deliver high-quality and resilience to service users, and which represent value-for-money for taxpayers, we decided to relaunch the Institute in December 2018.

While we of course look at what the private sector can bring to public service provision and we believe in the merits of diversity of provision, our thinking horizon is a much broader one and we look to examine how public services can be improved as a whole.

We seek to garner insight from experts from all sectors and from across the globe to help develop ideas which will underpin the next generation of public service solutions for citizens.

The more perspectives we gather, from academics, technologists, start-ups, outsourcers, procurers, policy makers, or charities, the more likely we are to capture insight that allows for the design and delivery of public services that make society work better.

7.4 The Centre for Defence Studies Contact Information

Professor John Gearson
Director, Centre for Defence Studies
Vice Dean – International, Faculty of Social Science & Public Policy
Professor of National Security Studies
Department of War Studies
Email: john.gearson@kcl.ac.uk
Tel: +44 (0)7713 088929