Innovation and technological superiority in UK defence
Critically assessing risks to attaining and sustaining technological advantage in the context of contemporary military offset strategies.

Eur Ing Steve Nimmons FBCS CITP FIET CEng FRSA
London, February 2019
Abstract

This research provides a critical assessment of UK defence technology innovation strategy and its alignment with that of the US. It considers how the US and UK militaries are responding to the pace of technological change and seeking to attain and sustain technological superiority against rival state actors. This is framed in the context of the US 3rd offset strategy (3OS), the alignment of the UK’s own Defence Innovation Initiative (DII) and technology pacing threats from near-peer rivals such as China. The ability to attain and sustain technological superiority is examined thematically in four key areas:

1. The clarity and coherence of UK defence technology innovation strategy
2. Key challenges in delivering technology innovation strategy within the DII in a timely and cost-effective manner
3. Technology innovation challenges within the UK-US defence alliance
4. Technology innovation strategies, tactics and pacing threats of near-peer rivals (here limited to China)

Under each of the four thematic categories, key technology innovation risks are hypothesised through a substantive and multi-disciplinary literature review. The veracity of the hypothesised risks is then tested through desk research, structured interviews with UK defence innovation experts and supplemented by a modest online survey of technology supplier attitudes within the UK defence industrial base. Key findings include: a lack of publicly available technology weakness assessments of UK defence capabilities; indications of US defence market protectionism; highly nuanced UK-China trade and security relations; new risks in the protection of globalised technology supply chains and complexities in extending the defence industrial base to new suppliers. Through a series of concluding recommendations, this research contributes to the policy discourse, providing insight into risk priorities and opportunities for policy and practice intervention.
List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(US) 3OS</td>
<td>US Third Offset Strategy</td>
</tr>
<tr>
<td>A2/AD</td>
<td>Anti-Access / Area Denial</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>CBRN</td>
<td>Chemical Biological Radiological and Nuclear</td>
</tr>
<tr>
<td>DARE</td>
<td>Discovery, Assessment and Rapid Exploitation</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defence Advanced Research Projects Agency</td>
</tr>
<tr>
<td>DASA</td>
<td>Defence and Security Accelerator</td>
</tr>
<tr>
<td>DE&amp;S</td>
<td>Defence Equipment and Support</td>
</tr>
<tr>
<td>DIB</td>
<td>Defence Innovation Board</td>
</tr>
<tr>
<td>DIEAP</td>
<td>Defence Innovation External Advisory Panel</td>
</tr>
<tr>
<td>DIF</td>
<td>Defence Innovation Fund</td>
</tr>
<tr>
<td>DII</td>
<td>Defence Innovation Initiative</td>
</tr>
<tr>
<td>DIUX</td>
<td>Defence Innovation Unit Experimental</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
</tbody>
</table>

Innovation and Technological Superiority in UK Defence
Eur Ing Steve Nimmons FBCS CITP FIET CEng FRSA
Nimmons Consulting, London, February 2019
DSTL | Defence Science and Technology Laboratory
---|---
GDP | Gross Domestic Product
GDPR | General Data Protection Regulation
IRIS | Innovation and Research Insights Unit
ISS | Information Systems and Services
ITAR | International Traffic in Arms Regulations
JFC | Joint Forces Command
MDP | Modernising Defence Programme
NATO | North Atlantic Treaty Organisation
PII | Personally Identifiable Information
R&D | Research and Development
SDSR | Strategic Defence Spending Review
SME | Small and Medium Sized Enterprise(s)
Table of Contents

1  Introduction ........................................................................................................................................... 10
  1.1  Context of the Research..................................................................................................................... 12
  1.2  Central Questions and Debates in the Field ..................................................................................... 15
  1.3  Specific Problem under Study .......................................................................................................... 18
  1.4  Importance of the Study .................................................................................................................... 19
  1.5  Outline Research Approach ............................................................................................................. 19
  1.6  Risk Set Hypothesis .......................................................................................................................... 23
    1.6.1  Theme 1 - Qualities of Effective Defence Innovation Strategy .................................................. 23
    1.6.2  Theme 2 - Qualities of Effective Defence Innovation Strategy Execution ................................ 24
    1.6.3  Theme 3 - Qualities of Effective Defence Innovation Alliance ................................................ 25
    1.6.4  Theme 4 - Theorising China’s Strategic Defence Innovation Intent .......................................... 26
  1.7  Chapter Outlines .................................................................................................................................. 26

2  Literature Review ...................................................................................................................................... 29
  2.1  Introduction .......................................................................................................................................... 29
  2.2  Theme 1 - Qualities of Effective Defence Innovation Strategy .......................................................... 30
  2.3  Theme 2 - Qualities of Effective Defence Innovation Strategy Execution ...................................... 35
  2.4  Theme 3 - Qualities of Effective Defence Innovation Alliance .......................................................... 40
  2.5  Theme 4 - Theorising China’s Strategic Defence Innovation Intent ............................................... 46
  2.6  Literature Gaps ................................................................................................................................... 53
  2.7  Conclusion ........................................................................................................................................... 54

3  Methodology ........................................................................................................................................... 56
  3.1  Introduction .......................................................................................................................................... 56
3.2 Research Design........................................................................................................57
  3.2.1 Structured Interview Research Instrument .......................................................57
  3.2.2 Collection of Data..................................................................................................62
  3.2.3 Online Survey Research Instrument .................................................................63
3.3 Research Process .....................................................................................................65
3.4 Analysis of Data .......................................................................................................67
  3.4.1 Research Instrument 1 .............................................................................................67
  3.4.2 Research Instrument 2 .............................................................................................69
3.5 Ethical Considerations .............................................................................................71
3.6 Conclusion ...............................................................................................................73
4 Description of Findings ............................................................................................75
  4.1 Introduction .............................................................................................................75
  4.2 Terminology and Participant Coding .......................................................................75
  4.3 Theme 1 – Qualities of Effective Defence Innovation Strategy ....................................78
  4.4 Theme 2 – Qualities of Effective Defence Innovation Strategy Execution ...................80
    4.4.1 Structured Interview Findings .............................................................................80
    4.4.2 Online Survey Findings .....................................................................................83
  4.5 Theme 3 – Qualities of Effective Defence Innovation Alliance ....................................94
  4.6 Theme 4 – Theorising China’s Strategic Defence Innovation Intent .............................96
  4.7 Conclusion ..............................................................................................................98
5 Discussion of Findings ............................................................................................100
  5.1 Introduction ...........................................................................................................100
  5.2 Key Findings .........................................................................................................100
Innovation and Technological Superiority in UK Defence

Eur Ing Steve Nimmons FBCS CITP FIET CEng FRSA
Nimmons Consulting, London, February 2019
Figure 10 Online Survey Responses - Question 5.................................................................89
Figure 11 Online Survey Responses - Question 6.................................................................90
Figure 12 Online Survey Responses - Question 7.................................................................91
Figure 13 Online Survey Responses - Question 8.................................................................92
Figure 14 Online Survey Responses - Question 9.................................................................93
Figure 15 Online Survey Responses - Question 10...............................................................94

Tables

Table 1 Research Instrument 1 - Participant Coding............................................................77
Table 2 Summary Recommendations..................................................................................117
1 Introduction

Since the end of the Cold War, the US has enjoyed practically unrivalled global military dominance. The outsized spending power of US defence (McCarthy, 2018) has enabled development of highly sophisticated and effective military systems. Capability, coupled with geographic reach, has enabled the US to fight conventional wars, conduct expansive counterinsurgency and counter-terrorism operations across Afghanistan and Iraq and project power against traditional and emerging rivals including China, Russia and Iran.

From the early 1950s, the US has formalised offset strategy as part of its core military philosophy. An offset seeks to negate a rival’s strength advantage through cost-effective counterbalancing capabilities.

In US President Dwight D. Eisenhower’s New Look Strategy (regarded as the first US Offset Strategy), the counterbalance against superior Warsaw Pact troop numbers in Europe was tactical nuclear deterrents (Leighton, 2001; Waltz, 2008, pp. 260-275), with consequences of accelerating the nuclear arms race (Jackson, 2014).
In the 1970’s, the 2\textsuperscript{nd} offset strategy developed under US Defense Secretary Harold Brown (Keefer, 2017) focused on stealth and precision strike capabilities and intelligence, drones (Rich and Janos, 1995, pp. 284-293), reconnaissance and surveillance systems. During Operation Desert Storm, many of these capabilities showcased US superiority in deploying and co-ordinating electronic warfighting, stealth bombing and laser guided weapons at scale (Corrigan, 2017, pp. 55-62).

A third US offset strategy (hereafter referred to as 3OS or US 3OS) was announced by then US Defense Secretary Chuck Hagel (2014). 3OS focuses on technological superiority (Lange, 2016) and recognises the rapidity of capability gains by near-peer rivals such as Russia (Defense Intelligence Agency, 2017) and China (Cronk, 2018) and regional powers such as Iran (Uskowi, 2018, pp. 161-176). The fundamental premise of 3OS is that the US and its allies are under pressure from global rivals, and that defence technology overmatch could soon be reversed. The relevance of the strategy prevails, however there is recognition that the Trump administration may reframe the optics of what was an Obama-era policy (Fiott, 2018).
Chinese investment in quantum computing, artificial intelligence (AI) and cyber technologies has been argued to be a long-term play for global technological hegemony (Pillsbury, 2014). China’s ability to deploy sophisticated Anti-Access/Area Denial (A2/AD) capabilities is an increasing challenge to both US and UK. 3OS seeks to overturn or at least stifle the ability of rivals to leverage A2/AD and thus extend power projection options in areas such as the South China Seas (Martinage, 2014, p. 17).

Through the 2015 Strategic Defence Spending Review (HM Government, 2015a), the UK responded to several themes in 3OS, leading to the formation of the Defence Innovation Initiative (DII). This research assesses the UK’s response to and alignment with the major goals of 3OS (Fiott, 2016) through a risk-based assessment of UK defence innovation capability.

1.1 Context of the Research

The context of this research is therefore framed by the objectives of 3OS (Coletta, 2018) and the key risks that the UK faces in developing technology innovation.
capabilities that will attain and sustain technological superiority against near-peers such as China (United States Department of Defense, 2018b; Bitzinger, 2016) in partnership with the US as a strategic ally.

In elicitation of an initial risk model structure and risk hypotheses (section 1.6) four key areas of investigation were undertaken:

1. Key organisational elements of UK defence innovation capabilities were critically assessed. The scope was constrained to changes introduced since 2015 through the National Security and Strategic Defence Spending Review (HM Government, 2015b) and resultant DII (Ministry of Defence, 2016), which established new capabilities such as the Defence Innovation Fund (DIF), the Defence and Security Accelerator (DASA) and the Innovation and Research Insights Unit (IRIS).

2. The dynamics of the defence industrial base was examined through both US (United States Department of Defense, 2018a) and UK lenses, noting an aspiration by both governments to increase engagement and cost-effectiveness of the defence supplier base. Risk archetypes (Ibid, pp. 12-14)
and the US Defence Industrial Base Risk Framework (Ibid. p. 12) inspired methodological aspects of this research.

(3) Key technology supply chain risks (Conrad, 2016) were examined, including foreign ownership and investment, merger and acquisition risks, the transnational nature of global technology companies and the unwillingness of some suppliers to support what they perceive as the weaponization of their products and ideas (Wakabayashi and Shane, 2018).

(4) China’s strategies and tactics (Jacques, 2012, pp. 406-488) were considered in relation to differing legal and ethical frameworks. The premise that intellectual property theft (Mertha, 2007, pp. 1-34), cyberattacks (Hjortdal, 2011), industrial espionage and subterfuge on a grand scale present extensive threats to UK technological goals was examined.

This work thereby builds into a thematic risk framework that critically assesses the UK defence innovation capabilities established as part of the 2015 SDSR, and their alignment with US 3OS. Taking AI and cyber technologies as bellwethers, the ability to overmatch and thereby create sustainable offset against China is evaluated. Risk
hypotheses are principally examined through structured interviews with domain experts in UK defence. Mitigations against validated risk statements are proposed in section 5.3.

1.2 Central Questions and Debates in the Field

The substantive debates across the areas of investigation described in section 1.1 are drawn from several literatures (Figure 1). Security and strategic studies literature pose questions about great power politics and international relations. From these are derived a context and understanding of the potential strategic intents of US, UK and China (Hough and Malik, 2015). These inform key questions such as relative technological strengths and weaknesses, as well as threats and opportunities to overmatch rivals. The political economy of defence innovation is also germane (Sempere, 2017) giving rise to questions about affordability versus effectiveness of deterrents and offensive capabilities.
Innovation literature contains substantial discourse about the nature of incremental and disruptive innovation (C. M. Christensen, 2016; Christensen and Raynor, 2013) and delivery models such as Open Innovation (Chesbrough, 2006; Young et al., 2012). Open Innovation literature provides insight into ideation, co-innovation, intellectual property management and how best to leverage intellectual capacity from a diverse supply base.

**Figure 1 Intersections of Literature**

Innovation and Technological Superiority in UK Defence
Eur Ing Steve Nimmons FBCS CITP FIET CEng FRSA
Nimmons Consulting, London, February 2019
Organisational culture, structure, processes and leadership are important debates in terms of constructing organisations that foster and harness innovation for technological gain (Rogers, 1995, pp. 161-201). The ability to operationalise technologies into coherent military capabilities leads to questions of personnel numbers and skills, doctrine (Ministry of Defence, 2014), operating concepts and leadership (Rosenzweig, 2007, pp. 142-156).

Literature on entrepreneurism (Ries, 2017; Drucker, 2015) and start-up culture (Ries, 2011), scale-up and adoption (Moore, 2014) within private and public sector organisations (Mazzucato, 2018) provides a useful backdrop for further situating the research.

Literature across computer science is pertinent in deriving an understanding of the state of the art in technologies such as AI and cybersecurity (Taddeo and Floridi, 2018). This is considered alongside key UK defence publications including the Future Technology Trends in Security report (Defence and Security Accelerator, 2018b), Advantage Through Innovation (Ministry of Defence, 2016) and National Security Through Technology (Ministry of Defence, 2012).
Key ethical debates concerning the weaponization of AI (Knuckey, 2016), fully autonomous weapons systems (Tegmark, 2018, pp. 110-118) and the development of intrusive surveillance are important in deriving an understanding of supplier reluctance to support certain military capability developments and the future of warfare (Freedman, 2017, pp. 277-287). The literature on dual-use technologies and the cross-over between military and civilian applications is additionally pertinent.

Literature from the field of supply chain risk management (Manners-Bell, 2017, pp. 268-287) and procurement has relevance in understanding the capacity and health of the defence industrial base, supply chain security and resilience. This includes understanding national capability weaknesses, over-exposure to foreign ownership or influence and how best to align with and integrate allies into a cogent technology supply chain (Louth, Taylor and Tyler, 2017).

1.3 Specific Problem under Study

The specific problem under study is to better understand the key risks faced by UK defence in attaining and maintaining technological superiority and how these goals
are articulated within an offset strategy designed to achieve dominance over global powers such as China.

The success factor is articulating risk mitigations that provide insightful and critical assessment of existing approaches and their inherent weaknesses.

1.4 Importance of the Study

The overarching field is of critical importance to national and global security.

This research aims to make a modest contribution to the overall policy discourse. Some potential benefits may therefore include:

1. Provision of an opportunity for research participants to anonymously share feedback about UK defence innovation capabilities and help shape policy debate in an area of national strategic interest

2. To advance strategic policy debate, providing modest insight into achievement of cost-effective defence innovation outcomes in the UK

1.5 Outline Research Approach
The ability to attain and sustain technological superiority in UK defence is examined thematically in four key areas:

1. **Theme 1 - Qualities of Effective Defence Innovation Strategy** - the clarity and coherence of innovation strategy

2. **Theme 2 - Qualities of Effective Defence Innovation Strategy Execution** - key challenges in delivering technology innovation strategy within the DII in a timely and cost-effective manner

3. **Theme 3 – Qualities of Effective Defence Innovation Alliance** - technology innovation challenges within the UK-US defence alliance

4. **Theme 4 – Theorising China’s Strategic Defence Innovation Intent** - technology innovation strategies, tactics and pacing threats of near-peer rivals (here limited to China)

In each of the four areas, key technology innovation risks are hypothesised, and their veracity tested through desk research, structured interviews with UK defence experts and academics and an anonymous and modest online survey of suppliers from the UK defence industrial base.
Two research vehicles are used:

The primary research vehicle comprises structured interviews with UK defence specialists exploring key risks to delivery of effective technology innovation. The outcome is an enriched risk model and risk mitigations building on insight gained from subject matter expert interview. The model in Figure 2 illustrates the structure and scope boundary.

The secondary research vehicle is an anonymous online survey. This is to ascertain commercial perspectives on benefits and disbenefits that may impede the expansion of supplier engagement across the UK defence industrial base. The online survey is limited to Theme 2.
Figure 2 Thematic Approach to Structured Interviews and Online Survey

A set of risk hypotheses outlined in section 1.6 is assessed along with proposed risk mitigations.

This research suggests that there are opportunities for policy makers to refine the strategic coherence of UK defence innovation strategy, enhance delivery capability,
improve ways of working with US Defense and better understand and offset technology pacing threats from China.

1.6 Risk Set Hypothesis

An initial risk set was hypothesised through critical review of the literature described in outline in section 1.2 and in detail in Chapter 2. This has been limited for the purposes of brevity to three key risks per theme. Hypotheses H1 through H12 represent initial statements of the perceived risks derived from critical assessment of debates in the field. As described in section 1.5, these risks are discussed and explored through structured interview and anonymous online survey as part of the research process (described in section 3.2).

1.6.1 Theme 1 - Qualities of Effective Defence Innovation Strategy

Key risk hypotheses:

H1. There is a risk that UK defence technology strategy lacks specificity and clarity of focus, and technology development priorities could be misunderstood or miscommunicated.
H2. There is a risk that UK defence technology strategy is poorly communicated (Freeman et al., 2015, p. xii) leading to a general lack of awareness or engagement of key stakeholders across both public and private sector organisations.

H3. There is a risk that UK defence technology strategy is based on a set of false premises and is responding inappropriately to modern defence threats, including those set by US 3OS.

1.6.2 Theme 2 - Qualities of Effective Defence Innovation Strategy Execution

Key risk hypotheses:

H4. There is a seeming proliferation of innovation initiatives across UK defence organisations with questionable integration and co-ordination. There is a risk that an incoherent and divergent approach will be taken by defence stakeholders, and opportunities missed to secure efficient innovation outcomes.

H5. There is a risk of underinvestment stifling development potential in quantum computing, AI and cyber technologies in the UK defence sector.
H6. There are potential supply chain risks from companies objecting to their technologies and solutions being used in autonomous weapons systems. Private sector organisations may view defensive and offensive technologies differently, complicating supplier relations and technology delivery options. Ultimately there may be a developing overreliance on private sector technology suppliers, or suppliers from outside the UK market.

1.6.3 Theme 3 - Qualities of Effective Defence Innovation Alliance

Key risk hypotheses:

H7. There is a risk that US hegemony and protectionism will ‘crowd out’ technology innovation from the UK into US markets.

H8. There is a risk of misalignment of strategic technology goals, developing a mismatch in innovation priorities across the UK-US defence alliance.

H9. There is a risk that legislation and governance frameworks, such as International Traffic in Arms Regulations (ITAR) will stifle the free flow of innovation from US to UK and vice-versa (HM Government, 2007).
1.6.4 Theme 4 - Theorising China’s Strategic Defence Innovation Intent

Key risk hypotheses:

H10. There is a risk that intellectual property theft, cyberattacks and supply chain infiltration by Chinese protagonists present a significant (if not existential) threat to UK defence innovation objectives.

H11. There is a risk that China will attain comparative technological capabilities at significantly lower price points to the UK through exploitation and weaponization of dual-use technologies (Cheung, 2016).

H12. There is a risk that Chinese investment in quantum computing, AI (Lee, 2018, pp. 81-103) and cybersecurity will significantly outstrip and outpace that of the UK.

1.7 Chapter Outlines

The remainder of this work is structured as follows:
Chapter 2 presents a thematic and critical review of key literature. Structurally this is aligned to four themes described in section 1.5 which form the four quadrants of the risk model depicted in Figure 2.

Chapter 3 provides a detailed overview of the methodology used in addressing the research question. This includes rationale for designing a risk-based assessment, the means by which an initial risk framework was hypothesised, rationale for selection of structured interviewing (Bryman, 2016, pp. 197-219) and qualitative surveying over alternative approaches, design of interview questions (Gray, 2018, pp. 342-373) and selection of interviewees. Limitations in the research methodology are articulated and a description of steps taken to maximise utility and objectivity of the work described. Areas of sensitivity are highlighted alongside a description of steps taken to ensure research ethics were followed to the highest standard (O’Leary, 2017, pp. 53-77) and in accordance with the principles established in the Declaration of Helsinki (Israel, 2014, pp. 30-32).

Chapter 4 describes key findings from both research instruments.
Chapter 5 critically discusses key findings, situating them within debates in the literature and noting insights and modifications to the initial risk hypotheses described in section 1.6.

Chapter 6 concludes, summarising key findings, importance and novelty of the research.
2 Literature Review

2.1 Introduction

This chapter examines key literature, critically assessing substantive works in the field and highlighting key debates and controversies across the four themes introduced in section 1.5.

Under Theme 1, the literature review critically questions the priorities of UK defence technology policy makers and the overall coherence and independence of UK defence innovation strategy.

Under Theme 2, the literature review critically questions the ability of UK defence to deliver on its strategic vision. The debate centres around modernising defence, cultural, procedural and commercial challenges and the ability to leverage innovation into deployable and effective military capabilities. The reliance on private sector technology providers is examined alongside substantive debates such as the ethics of AI and fully autonomous weapons systems (Galliott, 2015).
Under Theme 3, the literature review critically questions potential fault lines between US and UK strategic technology objectives and approaches. This includes debates and controversies linked to ethical and doctrinal factors that may impede collaboration as well as cultural and commercial factors and protectionism.

Under Theme 4, the literature review critically questions assertions about Chinese strategic objectives and explores alternative interpretations and debates from varying theoretical juxtapositions. Controversial debates on cyberespionage, supply chain infiltration and intellectual property theft are explored.

2.2 Theme 1 - Qualities of Effective Defence Innovation Strategy

There are several important debates surrounding the efficacy of UK defence technology innovation strategy. These include: 1) the validity of the premises on which the strategy is founded; 2) technology capability priorities, or as termed in (Ministry of Defence, 2012, p. 14) “operational advantage”; and 3) independence of UK thought and action in meeting national security challenges (Zala, 2015), termed in (Ministry of Defence, 2012, p. 14) “freedom of action.”
Advantage through Innovation (Ministry of Defence, 2016, p. 8) contextualises a number of key strategic innovation objectives. These include providing technological capabilities that will help deter rival actors, enable UK power projection, provide agile and adaptive war-fighting capabilities and create sustainable information advantage. Desire to secure asymmetric advantage in these areas is unsurprising, but as noted in (Louth, Taylor and Tyler, 2017, p. 13), there is a reluctance for officialdom to acknowledge defence platform weakness or technology capability gaps. This gives rise to questions concerning the cogence and focus of innovation strategy and whether current instantiations are too broadly focused. Indeed, Advantage through Innovation (Ministry of Defence, 2016) provides at best tacit linkage to the three National Security Objectives outlined in the National Security Capability Review (HM Government, 2018, p. 9). Line of sight through key government strategies is somewhat problematic, risking potential confusion over priorities.

There is potential for further confusion in the transition from the National Security Strategy and Strategic Defence Spending Review (SDSR 2015) (HM Government, 2015b, p. 10) to uplifted priorities of the Modernising Defence Programme (MDP).
a statement to the UK Parliament, Defence Secretary Gavin Williamson (2018) précised the dynamic risk landscape and underscored the need for UK technological superiority in cybersecurity (Directorate of Force Development, 2012, pp. 7-9; Defence Cyber Protection Partnership, 2018; HM Government, 2016, p. 35) and space domains. With announcement of additional innovation funding and “spearhead innovation programmes”, Williamson (2018) is signalling the government’s view of the importance of technological innovation to future UK defence and national security. Roberts (2018) provides an alternative perspective, arguing for greater investment in personnel and skills.

Defence innovation objectives taken at the macro level of the SDSR 2015 or MDP however appear very high level. Without clear quantification of the relative strengths and weaknesses of UK defence technology capabilities, prioritisation of action and investment is challenging. An assessment of UK Defence Doctrine (Ministry of Defence, 2014) finds little mention of innovation, save at the conceptual level (Ibid, p. 32). Substantive Defence Committee reports (2017) are practically silent on
innovation. Cascading strategic innovation priorities through Joint Forces Command, Army, Navy and Air Force is therefore both non-trivial and potentially risk laden.

The National Security Strategy and Strategic Defence Spending Review (HM Government, 2015b, p. 10) additionally illustrates challenges. Taking UK-China relations as an example: on one hand, the UK seeks economic prosperity through trade relations, but at the same time must counterbalance risks from intellectual property theft, cyberattack or foreign ownership of critical national assets and supply chain links. This creates something of a dichotomy and raises questions about China’s role as military adversary or economic partner. Fusion Doctrine (HM Government, 2018, pp. 10-11) provides a potential balancing framework through which military and economic security tensions may be alleviated. Fusion Doctrine provides more transparent linkage to the UK’s National Security Objectives and is thereby a useful coupling point for other defence innovation strategies.

In the Future Technology Trends in Security report (Defence and Security Accelerator, 2018, p. 51), an important point is raised concerning policy debate and ethics of modern warfighting, including robotics, autonomous weapons systems and
AI. The report provides a credible synopsis of the trends in computer science, situating them with a broad defence context. The Defence and Security Accelerator (DASA) has co-ordinated substantial authoritative debate and numerous leading technology academics have contributed to the publication. Breadth of focus could however still be an Achilles heel and UK defence may not realistically be able to exert supremacy across a wide technology research landscape. A focus on AI, quantum computing and cybersecurity is noted and generally links with MDP goals expressed by the UK Defence Secretary throughout 2018.

Creating synergies with allies including the US, NATO and the European Defence Agency is a further important focus. This enables the UK to deliver against national security objectives of prosperity and security. Retaining independence from allies is however important in sustaining the UK’s global military and political influence and autonomy. Defence trade cooperation agreements such as (HM Government, 2007) between the UK and US government provide mechanisms for strategic cooperation, however US protectionism, hegemony and arms export regulations must be assessed as potential barriers.
In assessing key threats to attainment of technological offset against near-peer rivals, the literature surfaces key policy debates. The tension points include balancing strategic independence and the need to innovate effectively across alliances. There appear to be several potential coherence issues in extant policy and a lack of specificity in technology strategy that could lead to competing priorities and divergent delivery responsibilities.

2.3 Theme 2 - Qualities of Effective Defence Innovation Strategy Execution

There are several important debates surrounding the deliverability of UK defence technology innovation strategy. These include: 1) sponsorship and structure of UK defence innovation; 2) challenges relating to engagement and expansion of the defence industrial base and protection of the supply chain; and 3) the ability to scale processes, resources and capabilities to meet strategic technological aspirations. These qualities of effective strategy execution are examined, critically assessing UK capability strengths and weaknesses.
At ministerial level in the UK there is evidence to suggest significant levels of support for technology innovation in defence. Coming out of SDSR 2015, and arguably in alignment with aspects of US 3OS, several notable bodies including DASA and IRIS were established as part of the DII. The DII also ceded an £800m investment fund and established the Defence Innovation External Advisory Panel (DIEAP) (Fallon, 2016).

In addition to DASA and IRIS, Defence Science and Technology Laboratory (DSTL), Research Cloud (HM Government, 2015c), the Innovation Centre for UK Joint Forces Command (JHub), Information Systems & Services (ISS) Innovation, Defence Equipment & Support (DE&S) Innovation, Discovery, Assessment and Rapid Exploitation (DARE) teams (Advance, 2018) are driving the innovation agenda across Joint Forces Command, Army, Navy and Air Force (Wilkinson and Jewell, 2017, pp. 23-37). Elegant interfacing with the sprawling array of other pan-governmental innovation bodies (PA Consulting, 2018) could perhaps be described as optimistic. Portfolio management of defence innovation is therefore potentially somewhat haphazard. This could be mitigated through governance, tasking,
communications and holistic portfolio management and as announced by the UK Defence Secretary (Ministry of Defence, 2018) initiatives such as the AI laboratory sitting under DSTL.

According to Joy’s Law: “no matter who you are, most of the smartest people work for someone else” (Lakhani and Panetta, 2007, p. 97). The ability to use crowdsourcing and Open Innovation to drive scalable problem solving is an established pattern in private sector innovation. Pace of technological change has necessitated a shift in the private sector from closed vertical innovation systems to more porous and open horizontal systems that span multiple partners (Enkel, Gassman and Chesbrough, 2009). Exponential expansion of technology innovation in the private sector has long since reached the tipping point where private sector R&D spending outpaced that of the public sector. As significant technology R&D spending now sits within the private sector, there is a recognised need for defence to embrace Open Innovation as a model across established defence prime contractors (Freeman et al., 2015) as well as new potential suppliers and academia (100%Open,
Muzzucato (2013) further suggests that public sector investment has a significant role to play in developing technology innovation across economies.

Getting innovation right in private sector contexts has proven difficult. As (C. M. Christensen, 2016) highlights, the ability of organisations to successfully harness and navigate incremental innovation can be significantly different from their ability to secure opportunity from disruptive innovation. As the militarisation of technologies such as quantum computing, AI and cyber are likely to produce significant disruptive effects, it is important to question the ability of public sector defence organisations to navigate the inherent disruptive complexities.

US and UK defence policy talks of expanding the existing supply base and to provide greater openness and engagement potential for new entrants. This is logical in terms of expanding Open Innovation ecosystems, however there are risk factors to consider in terms of technology supply chains.

The US Defense Industrial Base Risk Framework (United States Department of Defense, 2018a, pp. 12-14) provides a set of useful risk archetypes. For example, it is important to consider factors such as single point of failure risks in the supply
chain, foreign ownership and investment in technology companies, potential transfer of innovation through dual-use technologies to foreign governments and nefarious statecraft such as subterfuge, infiltration and industrial espionage.

Multinational technology companies additionally need to balance complex geopolitical relations with corporate growth aspirations. This complexity is further compounded when employee leverage is considered. Employees may regard certain technology use as benign or defensive (such as in peacekeeping or cyber defence) but may reject offensive technology use (such as in fully autonomous weapons systems). Conscientious objection is hardly new, but the impact of ‘new manifestations’ in a widening innovation supply chain could have far-reaching consequences. For instance, Google’s refusal to renew contracts on Project Maven (Wakabayashi and Shane, 2018) following employee disquiet highlights key risk factors. Rival states may seek to undermine the technology supply chains through manipulation and amplification of employee unease. Policy makers must therefore consider how best to offset these risks through investment in government led R&D,
through established defence prime contractors and through the expanse of the technology marketplace.

Finally, the ability to execute strategy is influenced by factors such as sufficiency of funding, resourcing, flexibility of commercial frameworks, processes, organisational culture and leadership, ability to ideate, incubate and scale up innovation (Defence Innovation External Advisory Panel, 2018, p. 2). The OECD (2018, p. 41) cautions about the dangers of “innovation theatre” (Ibid.), a managerial anti-pattern, where commitment to genuine innovation is merely a pretence. Policy makers therefore need to demonstrate value for money and the ability to match pace and scale of technological rivals in a complex globalised environment.

2.4 Theme 3 - Qualities of Effective Defence Innovation Alliance

There are several important debates surrounding the effectiveness of UK-US defence technology co-operation. These debates can be viewed through three primary lenses, namely: (1) a strategy and policy lens; (2) a funding and commercial lens; and (3) a relationship and trust lens. The first lens considers the alignment of
UK-US strategic objectives, synergies and potential friction points in defence innovation goals. The second lens considers defence innovation funding and general points of tension between the spending power of the US and its smaller allies. Commercial tension points such as import and export controls, US protectionism and varying legal and commercial frameworks are considered in terms of barriers to innovation between the UK and US and vice-versa. The third lens considers the status of the UK-US ‘special relationship’ and potential trust issues or ethical barriers that may impede the free-flow of innovation particularly from the UK to US. This may arise for example, if UK sourced technologies were used in controversial military counter-terrorism operations with potential diplomatic or reputational difficulties for the UK government.

Defensive alliances, joint operations and coalition warfighting necessitate aligned strategic capabilities and postures. Countries have individual views of their own national interests, security threats and strategic priorities. Ideally, these align with limited friction with those of allies, enabling a coherent cross-alliance prioritisation of technology goals. The Trump administration has been somewhat silent on 3OS, and
some commentators question whether the US is focused on improving extant capabilities or developing advantage through disruptive technological offset (Fiott, 2018). The continued expansion of Defence Innovation Unit Experimental (DIUX) initiatives, the importance of the US Defense Innovation Board and organisations such as Defense Advanced Research Projects Agency (DARPA) indicate extensive continuing US interest in disruptive and incremental innovation.

The UK’s position could arguably be better clarified, in the transition from SDSR 2015 to MDP. Ideally, innovating through an alliance would provide increased “operational advantage” (Ministry of Defence, 2012, p. 14) to all parties as well as protect “freedom of action” (Ibid., p. 14) for individual nations. The UK must therefore seek to optimally leverage the relationship with the US as a co-innovator, customer and strategic partner. Ideally, UK defence innovation strategy would align UK strengths with US weaknesses and seek to mitigate risks across the ‘technological alliance’. The degree to which such finesse exists in current strategy and policy is highly questionable.
The joint meetings of the US and UK Defence Innovation Boards may help alleviate some of these challenges. However, the US in pursuing its own technology offset goals may seek to dominate alliance partners, with potentially injurious effect on co-innovation and trust.

The US has the world’s largest defence budget (base budget of circa $618bn in financial year 2019) (United States Department of Defense, 2018c, p. 3) with technology innovation spending at $13.7bn (Ibid, p. 11). The Trump administration has raised broad concerns about ally commitments to defence spending across NATO, with several nations criticised for falling below their 2% of GDP spending commitments.

The UK allocates circa 1.2% of core defence budget to science and technology, £800m to the DIF (Ministry of Defence, 2017, p. 19), with just under £2bn spend on R&D (Ibid, p. 2). Although the budget gap in UK and US defence innovation spending may not correlate directly with outcomes, there is an argument that the US is geared to significantly outpace the UK. This could further be magnified by the
strength of the US defence industrial base and the pre-eminence of Silicon Valley technology companies (Seligman, 2018b).

US defence has a disposition towards domestic sourcing, and President Trump has signalled protectionist policies across US industry. These factors risk adding friction to free trade, potentially impacting UK entry into US defence markets which already have complex rules and operating conditions such as International Traffic in Arms Regulations (ITAR).

A key policy requirement is therefore how best to manage an innovation portfolio spanning multiple nations, whilst: a) finding the optimal balance between national self-interest and cost effective and efficient purchase or transfer of technologies incubated by the US or other allies; b) minimising protectionist or hegemonic behaviour by a dominant party; and c) facilitating healthy competition to ensure the ‘best ideas win’.

Beyond commercial considerations, there are additional legal, moral and ethical debates. US foreign policy has at times drawn criticism from those within even close alliance. Criticism of US operations in Afghanistan and Iraq, over pre-emptive strikes
in Yemen, Syria and Pakistan, clandestine surveillance operations and alleged Stuxnet attack against the Iranian nuclear programme (Zetter, 2015, pp. 205-226) highlight the potential for technology to be weaponised and perhaps used in a manner contrary to the wishes of inventor or supplier.

Gillespie (2015) draws out legal challenges of AI and autonomous weapons systems. Differing views between the US and UK on the acceptability of use of technology could stifle both co-innovation and export of technology from the UK to US. Given the continuation of the ‘special relationship’ and the reliance of UK defence on US technology innovation this may seem unlikely. The field of AI and autonomous weapons however is relatively immature, and the expeditionary nature of certain US foreign policy may create interesting geopolitical and diplomatic challenges. In some regards this mirrors challenges of building Open Innovation ecosystems across private sector organisations with differing cultures, values and strategic objectives. Complexity is compounded greatly however when addressing co-innovation challenges at national level under conditions of national security.
These dimensions of Open Innovation seem under-researched and under-discussed, particularly in the context of military alliance.

2.5 Theme 4 - Theorising China’s Strategic Defence Innovation Intent

In understanding the utility of 3OS and offset strategy in general, it is next helpful to test its theoretical grounding against that of a near-peer ‘adversary’. China was selected from a shortlist including Russia and Iran, primarily because of Chinese technological pre-eminence (Rogers, 2019, p. 39), US assessments (United States Department of Defense, 2018b) about future Chinese threats (T. J. Christensen, 2016, pp. 95-114) and the size of Chinese defence spending (Lineberger and Hussain, 2018, p. 10). The literature is therefore examined to illuminate: a) China’s broad strategic technology objectives; b) Western perceptions of China as a significant threat to global world order (Hough and Malik, 2015); c) China’s dominant defence technology aims (Blasko, 2011); d) China’s relative technological strengths and weaknesses; and e) China’s observation (or otherwise) of intellectual property law (Kennedy, 2018, pp. 2-3). This leads to clearer understanding of the
technological pacing threats from China and the theoretical positions from which construction of these threats emerge.

China promulgates a domestic narrative of 100-years of humiliation (Easterly, 2013, pp. 47-79; Wang, 2012) and the need to develop into a strong and benevolent force that will foster civility, peace and sustainable world-order.

Western academics and policy makers debate the degree to which China is open or closed, repressive or reforming, peaceable or bellicose, predatory or benign (Mann, 2008, pp. 1-28) and it is therefore important to consider the varying theoretical perspectives, methodological approaches and substantiating evidence from which these views are constructed. At the same time, it is important to consider and question the degree to which ‘offset strategy’ is itself inherently Realist in ideology, and thereby a significant factor in framing conceptualisation of risk from near-peers.

Pillsbury (2014) argues that China is on a path to global hegemony and aims to achieve this by the middle of the 21st century. His thesis is based on primary sources in Chinese, interviews with former Chinese military leaders and narratives drawn from Chinese historical romanticism (Guanzhong, 2018). This interpretation leans
towards Realism, and some of Pillsbury’s Chinese military sources are noted as hawkish. However, as argued by (Elman and Jensen, 2013), within the various hues of Realist thought, from Offensive and Defensive Realism, to Rise and Fall Realism, and Neoclassical Realism, there are competing assessments as to the ultimate consequences of China’s rise, and counterbalancing actions that may be needed from Western policy makers.

The dawn of a new strategic era as proposed by Jakobsen (2016, pp. 288-290) suggests that as near-peers catch up militarily and technologically with the West, there will be a return to an era of symmetric struggle. This could be magnified if US President Donald Trump’s America First doctrine and defence policy (Seligman, 2018a) signals a renaissance of great power politics in US strategic thinking. US-China trade wars and diplomatic tensions reflect the rising friction between the two great powers. The Chinese narrative of humiliation and US as hegemon attempting to repress Chinese growth, may act as a catalyst for additional cyberattack and intellectual property theft.
In the Liberalism tradition, collaboration and mutual assistance is debated, highlighting complexities and nuances in international relations between China and the US (Kennedy, 2018; Kennedy and Lim, 2018) illustrating the dichotomy of economic and security collaboration and political and military competition. Urban (2015) highlights the potential for Chinese economic coercion through its vast ownership of US government debt.

Yip and McKern (2017, pp. 167-204) provide additional counterpoint suggesting successful Open Innovation is essential to Chinese economic development. This is particularly interesting, considering challenges inherent in developing Open Innovation ecosystems inside a ‘top-down’ state-controlled system. These challenges appear somewhat under-researched, particularly in the Chinese military context.

In balancing interpretations of Chinese strategic intent (Brown, 2017, pp. 185-208) within and between traditional theories, it is helpful to consider whether interpretative narratives are Orientalist in foundation (Said, 2003) or rooted in alternative frameworks such as the ‘clash of civilisations’. (Huntington, 2002, pp. 168-174).
Additionally, if ‘offset strategy’ is wedded to Realism, care must be taken not to simplify and reduce Chinese technology strategy to a narrow band of threat analysis. China is investing heavily in AI and machine learning, quantum computing research and cybersecurity (Central Committee of the Communist Party of China, 2016, pp. 70-78). In assessing defence ‘offset’ risks of these investments, it is important to consider the degree to which China is weaponizing technology and using hacking, espionage, infiltration and intellectual property theft as part of its programme of strategic capability development. Whilst US assessments (United States Department of Defense, 2018b) are comprehensive, it is important to consider where and if threats are being either omitted, over-stated, under-played or falsely attributed.

For example, questions are raised in the literature about coercive influence of the Chinese state across its citizenry at home and abroad. Alleged Chinese interference in Taiwanese elections (Rogin, 2018), hacking (Bing, 2018), cyberattack (Danks and Danks, 2016), and fall-out over the arrest of Huawei executive Meng Wanzhou (Kuo, 2018) highlight potential threat assessment and attribution controversies.
To reach appropriate levels of analytical sophistication, understanding the source and nature of threats is important. For instance, is the threat directly from the Chinese state, a state sponsored agent, a willing and patriotic citizen or a coerced executive? Alternatively, is the threat assessment based on misinformation, misunderstanding or outright Machiavellianism? These distinctions are important, as foreign ownership risks have been raised in the UK (Sengupta, 2018) and drive debates about Chinese influence in critical technology supply chains.

The protection of UK defence innovation ecosystems and supply chains from unwanted Chinese influence is critically important. There are specific challenges however, including the multinational nature of technology companies, the global proliferation of technological know-how and the potential for China and other nations to exploit dual-use technologies for military purposes.

This gives rise to interesting debate about the theorisation of innovation within Chinese governmental and military thinking. If China is attempting to attain technological hegemony ‘by any means’, then threats of infiltration, intellectual property theft, patent and copyright infringement, coercion, subterfuge and hacking
on a global scale appear reasonable concerns. Technology exchanges with North Korea, Iran and Russia multiply the competitive stakes. Dual-use technologies may provide opportunities for China to avoid arms embargoes (Stumbaum, 2009, pp. 12-14). However, this paints an incomplete picture and somewhat clumsily characterises Chinese technology strategy as primarily theft-oriented. As noted by Johnson (2017, p. 271) there is a risk of misinterpreting Chinese strategic intent, through bias and assumption.

Global-scale successes in the Chinese technology sector highlight the viability of domestic R&D (Chowdhury, 2018). Extensive collaboration between the UK and China and US and China emphasise the importance of Chinese economic power. Chinese defence innovation and capability development at low-price points demonstrates ingenuity at scale.

In assessing technology offset risks against China, opportunities for further research include determining the pace of Chinese military technology capability development and the relative importance of: self-directed R&D; collaboration with Russia (Gabuev,
2018), Iran (Brands, 2018) and North Korea; exploitation of dual-use technologies; and time and cost savings derived from intellectual property theft.

2.6 Literature Gaps

Several potential gaps in the literature are suggested. These include: 1) a systematic assessment of the impact of conscientious objection on the defence industrial base (this was observed in relation to the US but is thought to be generally applicable across Western democracies); 2) conceptual differences between offensive and defensive technologies and how some suppliers may resist dual-use technologies being deployed in weapons or surveillance systems; 3) the critical challenges of building and protecting Open Innovation supply chains within defence environments, spanning alliances and potential competitors (e.g. technological co-operation between UK and China and the US and China); 4) theorising China’s approach to defence technology innovation, particularly focusing on the challenges of implementing Open Innovation ecosystems within a top-down, state-controlled system and 5) developing a fuller understanding of the impact of globalisation on technology innovation and supply chain security.
2.7 Conclusion

Literature from a number of fields including security and strategic studies, innovation, supply chain management and risk management were thematically assessed to identify potential gaps in knowledge in relation to: 1) the coherence and clarity of UK defence innovation strategy; 2) key challenges in delivering UK defence strategy; 3) key challenges of innovating within an alliance; and 4) challenges of offsetting against the defence technology objectives of China. The key purpose of the review was to build a holistic perspective of the current state of understanding across each of the thematic axes. The review highlighted key works in each field drawn from government strategy and policy documents, think-tank reports, peer reviewed academic journals, international relations theories, scholarly books and newspaper articles.

The risk hypotheses outlined in section 1.6 were constructed from the literature review. These hypothesise by theme (and as a coherent set) critical risks that policy makers must address to ensure the technological offset objectives of 3OS and MDP are met and sustained. The findings from the literature review have been
summarised into a risk set as: 1) no similar model was found during the literature review; 2) the hypotheses allow for further validation and examination with an expert research audience; and 3) a ‘peer-reviewed’ risk model and set of proposed mitigations is a potentially useful contribution to defence innovation discourse. This underpins the research methodology described in Chapter 3.
3 Methodology

3.1 Introduction

Having examined the key literature (Chapter 2), qualified the research question, derived and situated it within current debates in the field (Graff and Birkenstein, 2018, pp. 91-98) and developed a set of hypotheses (section 1.6), this chapter describes the methodology used to examine the veracity of the hypotheses. This methodological description includes the rationale for selecting a risk-based assessment (Hopkin, 2018, pp. 142-150), the research design including the selection and construction of the research instruments (O'Leary, 2017, pp. 131-158), sample selection (Ibid, pp. 204-214), methods of data collection (Silverman, 2017, pp. 281-315), the research process (Bryman, 2016, pp. 39-72), how empirical data was analysed and key ethical considerations (Gray, 2018, pp. 70-95) that shaped the overall research approach. Limitations in respective elements of the research approach are highlighted along with steps taken to mitigate research risks and improve the quality and utility of the output.
3.2 Research Design

The research design is a hybrid approach (Dawson, 2015, pp. 16-23), combining two qualitative research instruments, the primary instrument being a structured interview (Bryman, 2016, pp. 465-499) and the secondary instrument being an online survey (Bell and Waters, 2014, pp. 156-176). These are classified as primary and secondary as the principal focus of the research is determining the veracity of the risk set hypothesised in section 1.6 through structured interview. The key objective of the secondary instrument is to develop an enriched understanding of key risks of the ability of UK defence to extend its technology ecosystems and supply chains to new market entrants. The research design is therefore primarily qualitative, although the secondary instrument does introduce some quantitative potential. The design rationale for each instrument is next presented, along with a discussion of limitations. Sample selection (Gray, 2018, pp. 173-175) for each instrument is also discussed and limitations of claimable research conclusions are highlighted.

3.2.1 Structured Interview Research Instrument
A uniform thematic structure has been used throughout this research, arising from the review of literature (Hart, 2009, pp. 44-78), through synthesis and testing of hypothesis, to conclusions and recommendations. This systematically coheres the research question around the categories outlined in section 1.5 into the risk model described in section 1.6.

The structured interview research instrument uses the risk model as its underpinning framework. The interview structure iterates through the 4 key themes, testing the risk hypotheses using a set of interview questions (Alvesson and Sandberg, 2013, pp. 10-23). To ensure a timely, balanced, orderly and repeatable process, the structured interview comprises 3 questions per theme, timeboxed to a 30-minute discussion.

As perception of risk can be highly subjective (Balzekiene, 2019), there are methodological challenges to ensuring meaningful insight is derived from the structured interview. To mitigate the risks of research participants being unduly influenced by the initial hypotheses, open interview questions were carefully chosen.

---

1 Participant is used as shorthand for Research Participant. These terms should therefore be considered synonymous.
to ensure sufficiency of debate and room for critique and disagreement. Questions were additionally written to illicit insight into potential risk mitigations.

3.2.1.1 Sample Selection

The inclusion criteria for participants in the structured interviews was possession of a substantive understanding and background in UK defence, particularly in technological research and development and innovation.

Structured face to face interviews with defence industry experts were limited to a population of 5 to 10 participants. This was capped primarily due to time considerations.

The research group was made up of policy advisors, defence experts, researchers (mostly from defence and international relations think tanks) and former members of the armed forces. In constructing the research group, the aim was to provide a range of different views and perspectives as well as build in a degree of meaningful participant diversity, thereby avoiding the cruder pitfalls of selection bias (Collier and Mahoney, 1996).
Recruitment of participants was facilitated both by direct approach from the lead researcher as well as through gatekeepers in various professional institutions.

3.2.1.2 Limitations

Although risk analysis typically assigns impact and likelihood scores to risks, this can add additional complexity and subjectivity to discussion (Turner, 2014, pp. 245-262). It was therefore decided to omit these dimensions from the structured interview. Focus was therefore directed towards: a) a discussion of the validity of the risk hypotheses presented by theme; b) examining potential risk mitigations that would be of especial interest to policy makers; c) identifying potentially missing risk hypotheses; and d) identifying areas where risk hypotheses required refinement or amendment.

A purest approach to risk assessment might further definitionally disentangle risks and issues, thereby delineating areas where risks are already manifest. This was considered, however the prospect of confusing participants with additional concepts necessitated that this remain implicit in the approach rather than be made explicit.
Care was taken to take account of the difference between risks and issues in the framing of both the risk hypotheses and the structured interview questions.

The risk hypotheses span several disciplines and it was recognised that participants may have varying levels of experience across each of the 4 themes. In analysis of the data it was therefore recognised that consideration must be given to the authoritativeness of opinion and the provenance of sources used to substantiate participant views. It was anticipated that in-depth knowledge of Chinese strategic intent may be limited. This led to the inclusion of a more general question about competitive threats to UK defence innovation from states such as Russia, Iran or North Korea.

In a more expansive study, it would be beneficial to include participants from outside the UK, particularly the US defence industry and to include counterpoint from Chinese sources. This has somewhat been mitigated by reviewing literature, however a study of Chinese primary sources was not feasible due to language barriers.
Every care was taken to select a representative sample of participants that would generate meaningful insight into the research question. It is acknowledged that this sample set (primarily due to time constraints) is relatively small. This limits the potential for triangulation of opinion as well as testing the degree to which more controversial opinions are held across the academy. Every effort was taken to minimise this limitation through expansive review of the literature. In a larger sample, there may be additional opportunity to expand levels of diversity.

The necessity to timebox structured interviews to 30 minutes was a key consideration in terms of the seniority of participants and competing demands for their time. It is recognised that time limits may somewhat impede complex exploration of a substantive topic. As a mitigation, participants were provided in advance with a research information sheet that set out the key objectives and outline questions.

3.2.2 Collection of Data

Data was collected in face-to-face interview. Data was coded to ensure confidentiality of source.
3.2.3 Online Survey Research Instrument

The online survey research instrument also used the risk model as its underpinning framework. However, it focused on Theme 2 – the Qualities of Effective Defence Innovation Strategy Execution. The purpose of the online survey was to elicit insight from Small Medium Enterprises (SMEs) supplying technology solutions into UK defence. This was to ascertain commercial perspectives on benefits and disbenefits that may impede the expansion of SME engagement across the UK’s defence industrial base.

The inclusion of this research instrument builds from a recognition in the literature review of reluctance by some suppliers to support the militarisation of dual-use technologies. The literature suggests a differentiation between support for defensive technologies and offensive or weaponised technologies and a difference between potential new suppliers (from outside defence) and established defence contractors. There may additionally be hints of an emerging trend in technological conscientious objection as evidenced by Google’s withdrawal from Project Maven. Ascertaining the
risk profiles of these trends is important in understanding the full spectrum of risks to achieving effective innovation strategy delivery.

As the online survey and structured interview research instruments share the same underpinning risk model, they naturally align into a hybrid, mutually reinforcing research design.

3.2.3.1 Sample Selection

The inclusion criteria for the online survey was SMEs that have engaged in technology supply into UK defence. SMEs were approached through specialist defence and innovation groups on Social Media, primarily LinkedIn.

3.2.3.2 Limitations

The online survey was limited to 10 questions. A more expansive survey may have yielded additional data points; however, this may have led to a lower completion rate.

There are opportunities to segment the sample SME population to enable richer quantitative analysis. Claiming definitive quantitative conclusions from a small online
survey would be insensible. Qualitative interpretation of data has therefore been the sole approach used.

The selection criteria for the sample is necessarily constraining. This applies clear limits on the number of potential participants. A more expansive survey, perhaps extending to the US defence industrial base would increase potential.

By the very nature of the sample selection criteria, SMEs that have never engaged with UK defence were excluded. Excluded from this study therefore is the potential to understand (empirically), broad attitudes of the technology industry to UK defence innovation participation. This provides scope for a follow-on study.

3.2.3.3 Collection of Data

A link to the survey was provided to participants as part of the research recruitment process. The online survey was completely anonymous.

3.3 Research Process
The high-level research process is depicted in Figure 3. A detailed literature review was undertaken from which was synthesised the thematic structure previously described and used throughout. A set of risk hypotheses was derived from the thematic analysis. This triggered further cycles of literature review, the synthesis and refinement of the initial risk hypotheses being an iterative process. The risk hypotheses then informed the design of the research instruments and their associated methodological elements. Review of literature on research methods additionally informed the design of the research instruments. Execution of the research plan led to refinements of the risk hypotheses and elicited insight into potentially valuable mitigating actions. These were critically synthesised into findings and conclusions.
### Figure 3 High-level Research Process

#### 3.4 Analysis of Data

Figure 2 depicts the scope boundaries of the two research instruments.

#### 3.4.1 Research Instrument 1

Data Analysis from Research Instrument 1 was performed as depicted in Figure 4.

The inputs to the structured interview were a set of questions aligned by theme and
the risk set hypotheses described in section 1.6. During the interview itself, agreement or disagreement with each risk was explored. Proposed amendments or refinement of risks or suggestions of mitigations were captured along with rationale (and where available supporting references to literature). All structured interviews were performed in the same way. Once all structured interviews were complete, post-interview analysis (Silverman, 2015, pp. 126-133) was conducted once, using all pseudonymised transcripts as input. A decision was made not to attempt to refine the risk set between each interview due to: a) the additional complexity; and b) the likelihood of a deleterious effect on repeatability and uniformity of process.

In assessing the data from the structured interview, the following decision logic was used and codified into a simple analytical tool in Microsoft Excel.

1. **Revision of risk set** – an assessment was made of the perceived authority of the participant, cogence of argument, supporting references in the literature and (where feasible) triangulation of opinion with other participants and with the academy in general.
2. **Revision of mitigations** – Mitigating actions proposed by participants were considered in terms of their perceived suitability, feasibility and acceptability to policy makers.

**Figure 4 Data Analysis from Structured Interview Research Instrument**

3.4.2 Research Instrument 2

Data Analysis from Research Instrument 2 was performed as depicted in Figure 5.

The input to the survey was an online questionnaire. The survey collected simple
company profiling data for selected defence suppliers. Key questions tested company attitudes towards the militarisation / weaponization of their technologies. Due to the very limited sample size, it was not deemed appropriate to quantitatively analyse the data. Rather, the sample was qualitatively assessed to determine if there are indicators of aversion in the supply chain to technology weaponization. This was felt to be a useful addition to the overall research methodology, providing additional insight into potential innovation supply chain risks.
3.5 Ethical Considerations

Key ethical considerations in the design of the research methodology included the privacy and confidentiality of participants and an open and transparent research process. Measures taken in the design included:

- Participants were provided with information sheets and informed of their rights to decline participation or leave the study at any point.
- It was made clear that providing answers to any questions in either research instrument was entirely voluntary.
- The limitations or processing and retention of data was outlined in both research instruments.
- Collection of personally identifiable information (PII) was strictly minimised. In line with General Data Protection Regulations (GDPR), pseudonymisation was used where feasible (Information Commissioner’s Office, 2018). No PII (including IP addresses) was collected as part of Research Instrument 2.
• Participants were not quoted or otherwise referred to by name in the study
• Participant details were not shared with other participants
• Where participants granted that structured interviews may be recorded, this was done using audio only on a password protected recording device. All audio files were stored on the device and not uploaded to cloud or other external storage. Once written transcripts had been made, the audio recordings were deleted. A separate coding system was maintained using an encrypted and password protected key file to ensure the confidentiality of participants
• All participants were informed that no commercially sensitive, restricted or otherwise protectively marked materials should be divulged or supplied. It was made clear to all participants that only unrestricted information should be shared in interview and survey. Careful reflection was made in terms of assessing transcripts and Chapters 4 and 5 written in such a way as to obfuscate any potentially sensitive material. There were no incidences during interviews that necessitated such action, however participants were informed
that obvious divulgence of restricted material was likely to result in the interview being both terminated and removed from research results

- The online survey was completed anonymously. No PII was collected or stored. Participants were instructed not to include project names or other details that could identify companies or their representatives directly or by inference
- No material thought to have potential to cause any party commercial embarrassment or harm was collected, processed or published
- Strict time keeping was observed to build confidence of the participants in the professionalism of the approach

3.6 Conclusion

A hybrid research design was selected using primary and secondary research instruments and qualitative analysis. Structured interviewing of UK defence innovation experts was the primary research method. The secondary method is an online survey of a small sample of UK defence technology suppliers. The overall
research methodology uses a hypothesised set of risks, presented thematically and derived from an in-depth review of defence innovation and related literature (Figure 1).

Meticulous care has been taken to ensure that the research methodology is open, transparent and ethical, in line with best practices and the Declaration of Helsinki. Inclusion criteria for both research instruments has been presented along with rationale. The sample sizes for the research population are limited, and key methodological limitations and mitigations have been discussed. The critical success factor for the research is to gain insight into the key risks and challenges in meeting technology offset objectives against near-peer rivals. The derivation of a holistic set of risks from an expansive review of the literature is a foundational aspect of the research method. In designing the methods as described, it has been possible to engage expert opinion in an efficient and highly structured examination of strategic defence technology objectives.
4 Description of Findings

4.1 Introduction

Over four weeks, structured interviews were held with subject matter experts in UK defence (Table 1). Due to the sensitivity of the research and participant affiliations, full anonymity and source protection has been applied to the description and analysis of findings. During the same period, the online survey was conducted. As described in section 3.2.3 this was an anonymous survey used to test (at a very high-level) technology supplier attitudes to UK defence. This chapter describes the key findings. The findings are presented thematically, therefore the insight gained from the online survey is presented under Theme 2 (Qualities of Effective Defence Innovation Strategy Execution). The implications of the findings are critically analysed in Chapter 5.

4.2 Terminology and Participant Coding
For the avoidance of doubt, those that *participated* in Research Instrument 1 (structured interviews) are referred to in this chapter as research participants or in shorthand participants. Those that *responded* to Research Instrument 2 (anonymous online survey) are termed respondents. There is no implied link whatsoever between participants and respondents.

Participants have been coded to protect identity and affiliation. Former members of UK Special Forces are not attributed in this chapter in any way. This opacity is deliberate. Respondents are anonymous by nature of the design of Research Instrument 2. In the following sections and where deemed ethically appropriate, findings are annotated with the corresponding participant codes, in square brackets. This provides traceability of finding to coded participant.
<table>
<thead>
<tr>
<th>Code</th>
<th>Participant Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>A former senior officer in the UK armed forces</td>
</tr>
<tr>
<td>P2</td>
<td>A senior policy advisor involved in several innovation and security panels</td>
</tr>
<tr>
<td>P3</td>
<td>A senior policy maker with extensive knowledge of UK defence strategy</td>
</tr>
<tr>
<td>P4</td>
<td>A cybersecurity industry expert with experience working for UK government agencies and with experience of Chinese and Russian cyber threats</td>
</tr>
<tr>
<td>P5</td>
<td>A cybersecurity industry expert with experience working for UK government agencies and with familiarity of US markets and regulations, particularly ITAR</td>
</tr>
<tr>
<td>P6</td>
<td>A legal expert with experience in UK defence, and expertise in collection and dissemination of Open Source intelligence</td>
</tr>
<tr>
<td>P7²</td>
<td>A former member of UK Special Forces with experience of joint UK-US operations</td>
</tr>
<tr>
<td>P8²</td>
<td>A former member of UK Special Forces with experience of electronic warfighting, cybersecurity and intelligence gathering</td>
</tr>
</tbody>
</table>

**Table 1 Research Instrument 1 - Participant Coding**

² Inputs from P7 and P8 have been obfuscated deliberately in the description of findings and neither are therefore cited.
4.3 Theme 1 – Qualities of Effective Defence Innovation Strategy

There was a degree of variability of expertise and interest among participants in terms of macro-level government strategy. Policy makers [P2, P3] and those in advisory roles within defence organisations [P1] had a more in-depth knowledge and familiarity with top-level strategy. Among these participants, there appeared to be consensus that policy change as part of new initiatives and changes in defence leadership (both political and military) were substantive but perennial challenges.

There was a strong sense that technology and innovation strategy could not be considered in isolation. Holistic thinking was essential to ensure defence capabilities were sufficiently robust and future proof to protect national security objectives [P1, P2, P3]. On several occasions, questions of government commitment to defence spending was raised [P1, P2, P4] as was recruitment and retention challenges into the armed forces [P1]. There was a sense that an over-reliance on European, NATO and US allies was creating long-term challenges for the UK’s ability to assert independence and “freedom of action” (Ministry of Defence, 2012, p. 14). Skills gaps,
training and attraction of talent into the armed forces was highlighted as strategically important by some [P1 et. al.] and perhaps lacking focus in extant policy.

There was both recognition of the importance of technology innovation and a sense of scepticism over its absolute utility. Strategy was here questioned in terms of overall geopolitical and domestic threats [P2, P3, P4]. There was a sense of frustration that technological superiority was being lionised and conflated with warfighting superiority and several examples given of the need to deploy well trained and well led soldiers into operational theatre.

In examining questions of strategic coherence, there was discussion with participant [P1] involved in capability portfolio management and long-term acquisition. This illuminated some of the key challenges in alignment of top-level strategic objectives through capability portfolios and tactical requirements. There was a sense that constrained thinking at the tactical level could impede disruptive innovation, leading to inefficient and potentially costly outcomes. Communication challenges were also highlighted as was a desire for greater clarity and engagement between private sector stakeholders and defence planners [P1, P2].
A recurring theme was the need for the UK to maintain independence and operational freedom. There were several vigorous contributions that particularly questioned UK defence strategy post-Brexit. Pacing threats were also raised [P4, P5], and a general concern expressed about ability to innovate cost-effectively, with independence and against highly fluid treats [P1, P6].

4.4 Theme 2 – Qualities of Effective Defence Innovation Strategy Execution

4.4.1 Structured Interview Findings

Participants [P1, P2, P3, P4 and P5] seemed to possess a good overall understanding of the key structures of UK defence innovation and there was familiarity with the work of DSTL, DASA and DE&S. Several [P1, P4 et. al.] mentioned areas in which they felt the UK had established world-class and innovative capabilities, including in Chemical Biological Radiological and Nuclear (CBRN) defence, intelligence, counter-terrorism, special forces and cybersecurity. The quality of UK academia and defence research was also exemplified [P2, P3].
The ingenuity of the intelligence services and foreign office was also mentioned in general terms, in relation to protection of agents working abroad.

The dangers of structural fiefdoms and underfunding was raised when discussing the risks of innovation sponsorship and delivery. There appeared to be general concerns that inter-service and inter-departmental rivalry, competition for budgets, resources and accolades may drive inefficient behaviours and stifle openness, sharing and knowledge transfer [P1 et. al.]. There was a further sense that at ‘lower-levels’ of the delivery model, pragmatism and a desire to achieve common aims were key drivers for collaboration. This may point to inherent (and enduring) cultural issues within hierarchical defence organisations.

There was recognition that processes, requirements definition and management, clarity of strategy and delivery ownership, complexity of governance in areas of commercial, legal, security, safety and compliance were all potential barriers to timely delivery and innovation [P1, P2, P3]. Notwithstanding the resonance of these themes with participants, there was a further sense that a ‘can do’ attitude among
suppliers and capability owners within defence helped alleviate some of the otherwise cumbersome requirements [P1 et. al.].

Interesting points were raised about the ability to scale innovation and the necessary symbiosis between UK public and private sector [P2]. Lowering entry barriers and cost of participation in defence innovation was mentioned and there was a sense that suppliers wanted more opportunity to contribute ideas and self-organise and direct innovation competitions and innovation themes within their own specialisms. Indeed, this was something of a Cri de Coeur from [P1] who saw potential in more openness, regular and simplified strategy communications and increased opportunity to engage earlier in requirements definition. Counterbalancing opinions were expressed however highlighting that suppliers are delivering to tight timescales and budgets and may then view innovation as at best a ‘nice to have’ and at worst a commercial distraction.

Participants [P1 to P6] were aware of emerging challenges from the globalisation of technology ownership and news stories about Google’s withdrawal from US defence contracts, particularly, Project Maven. In the research population sampled however,
there was only limited concern expressed [P6] about potential impact to the defence industrial base, which was considered robust. Participants [P1, P4, P5] agreed that considering whether potential defence suppliers might view offensive and defensive uses of technology differently was an interesting and valuable discussion point. Again, in the population sampled, this question did not appear to have been previously considered (at least in any meaningful depth).

Varying innovation postures were mentioned by one participant who felt that nations tended to be more innovative under conditions of war or existential threat and that as a cornerstone of the domestic economy, defence spending and expansion of the defence industrial base was an economic good.

4.4.2 Online Survey Findings

The online survey had 6 responses. The survey was extensively advertised on defence and innovation communities on social media, predominantly on LinkedIn. The very low uptake was considered primarily due to: a) reluctance to respond to surveys of any kind (i.e. lack of interest); b) reluctance and trust issues relating to responding to a survey of potentially sensitive commercial interests; c) the filtering
questions that would reduce potential respondents to low numbers; and d) a possible reluctance of otherwise qualified respondents to reply on behalf of their company (i.e. lack of authority or agency). Nevertheless, the research instrument has been retained in the methodology, not least due to important learning points which are further elucidated in Chapter 5.

This section presents snapshots of the responses from SurveyMonkey. The survey was designed to be completely anonymous and hence no personal or corporate information is retained or presented. In line with GDPR and handling of PII no IP addresses were collected.

4.4.2.1 Question 1

There were 6 total responses, 5 respondents had been engaged in the UK defence sector for more than 2 years and 1 respondent for less than 1 year.
How long has your company been supplying technology solutions into UK defence

Answered: 6  Skipped: 0

Figure 6 Online Survey Responses - Question 1

4.4.2.2 Question 2

There were 6 total responses. 4 of the 6 respondents were supplying into UK defence only, with 2 others supplying into external defence markets.
4.4.2.3 Question 3

There were 5 total responses, 1 respondent skipped this question. Answers ranged from 15% to 80% and the average of the 5 responses is shown in Figure 8.
What share of your overall corporate revenue comes from the UK defence sector

Answered: 5  Skipped: 1

Figure 8 Online Survey Responses - Question 3

4.4.2.4  Question 4

There were 6 total responses. 1 respondent replied Don’t Know, 2 replied yes and 3 replied no. Don’t Know was considered an interesting option across the survey indicating potential weaknesses in level of corporate familiarity and therefore overall insightfulness of the respondent’s answer set.
4.4.2.5 Question 5

There were 6 total responses to this question, all ‘no’. This was not considered surprising given the low-level of uptake of the survey and the limited number of suppliers who have engaged in innovation competitions through DASA since its (recent) inception.
Has your company participated in UK defence innovation competitions – e.g. those hosted by the Defence and Security Accelerator (DASA)

Answered: 6   Skipped: 0

4.4.2.6 Question 6

There were 6 total responses, 1 respondent answered yes and the remaining 5 answered no.
Does your company have commercial concerns about engaging in UK defence, such as potential loss of intellectual property, export restrictions, limitations of dual-use technologies in other markets

Answered: 6  Skipped: 0

![Bar chart showing survey responses: 4 respondents answered yes and 2 answered no.]

**Figure 11 Online Survey Responses - Question 6**

4.4.2.7 Question 7

There were 6 total responses. Four respondents answered yes and 2 answered no.
Would your company object to your technologies / solutions being used in specific contexts – e.g. on drones, surveillance systems, autonomous weapons systems

Answered: 6  Skipped: 0

<table>
<thead>
<tr>
<th></th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>60%</td>
</tr>
<tr>
<td>No</td>
<td>40%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Figure 12 Online Survey Responses - Question 7**

4.4.2.8 Question 8

There were 6 total responses. One respondent answered Don’t Know, 2 answered <10% and the remaining 3 answered 10 to 25%.
What percentage of your workforce comes from a military background (UK and others)

Answered: 6   Skipped: 0

![Bar chart showing survey responses](chart.png)

**Figure 13 Online Survey Responses - Question 8**

4.4.2.9 Question 9

There were 6 total responses. Two respondents answered Don’t Know, 2 answered yes and 2 answered no.
Do any of your company founders, owners or board members have a military background (i.e. have served in regular or reserve forces)

Answered: 6  Skipped: 0

![Survey Responses Chart]

**FIGURE 14 ONLINE SURVEY RESPONSES - QUESTION 9**

4.4.2.10 Question 10

There were 6 total responses. This question was a freeform text field. The 6 responses were:

- “Size, complexity and speciality of requirements”
- “Cultural fit for those outside of uniformed background”
- “Complexity of commercial frameworks and compliance”

Page 93 of 140
• “High level security requirements for personnel on some programmes”
• “Culture”
• “Legal and procurement requirements”

In your experience, what is the greatest challenge in engaging as a commercial supplier with UK defence - (for example: defence culture, process, commercials, security requirements, intellectual property protection, export restrictions). Please state:

Answered: 6  Skipped: 0

**Figure 15 Online Survey Responses - Question 10**

### 4.5 Theme 3 – Qualities of Effective Defence Innovation Alliance

Participants majored on the UK-US relationship and expressed serious (if at times light hearted) remarks about attitudes within US Defense. There was consensus [between P1, P2, P5] that the US Defense market was protectionist and hard to penetrate, although when pressed, several [P1, P5, P6] agreed that the US worked hard to protect national industries and domestic defence jobs.
There was certainly a sense that participants thought the US viewed the UK (primarily) as a defence customer and wanted to retain ownership of technologies and intellectual property. Examples were given such as intelligence sharing (the US wanting to see everything, but not necessarily disseminate), protection of restricted frequencies and limitation of access to US military satellites.

Examples of UK tactical ingenuity in adapting or repurposing equipment was contrasted with more regimented and tightly controlled US processes. Indeed, US doctrine may somewhat impede innovation at the tactical level, an area in which some participants felt the UK excelled. One participant noted that US doctrine majored on overwhelming force of action and suggested this mindset permeated US defence thinking.

There was some cynicism from participants that the US would only supply equipment which it could ‘defeat’. One suggested that possible weaknesses could therefore include (although this was not substantiated) backdoors, or supply of lower-grade equipment than was at the cutting edge of US technology superiority.
There was additional scepticism that some US defence companies were attempting to enter the UK defence industrial base using very small UK holdings. Points were raised about the sovereignty of companies, rights of access to UK defence opportunities and differences in attitudes and operational challenges in US and UK markets.

There was limited discussion about the UK’s role within both NATO and the EU. This was undoubtedly due to the framing of the structured interview questions (and the focus on US relations), however there appeared to be some cynicism and mistrust of the UK-EU relationship and what this could ultimately mean for the operational freedom of UK forces. This was an interesting twist and perhaps reflects that UK-US operations in Iraq, Afghanistan, Libya, Syria and others have forged levels of trust otherwise missing from other alliances.

4.6 Theme 4 – Theorising China’s Strategic Defence Innovation Intent

There was substantial discussion under this theme about China’s cyber aggression [P1, P2, P4, P5, P6] and suspected attacks on critical infrastructure (globally) as well
as intellectual property theft. Some uneasiness was expressed in terms of relations between China and governments in Russia, Iran and North Korea as well as China’s ambitions in Africa. Belligerence in the South China Seas was cited by several participants [P2 et. al.] as exemplifying Chinese expansionist ambitions.

Participant [P1] raised an interesting point regarding the potential advantage of Chinese autocracy and the ability to control domestic and foreign technology companies operating in China. There was a discussion about the organising models of defence innovation in China versus Western democracies and their relative advantages and disadvantages. The participant put across an argument that the Chinese state can mobilise and control significant resources (including an expanding defence budget) and is not squeamish about its choice of methods or suppliers.

Two cybersecurity experts [P4, P5] were interviewed and believed offensive Chinese cyber capabilities to be extremely effective and threatening. Continuous probing of governmental, defence, banking and other economic targets was cited as ‘the norm’. On delving deeper into the ability of China to exploit breaches and intellectual property theft at scale, there was limited understanding (inside the wider research
participant group) of the alleged mechanisms. Participant [P4] suggested that over-focus on cyber-security was itself a risk and was becoming a technological panacea.

China’s use of cyberattack against UK critical information infrastructure was noted by participant [P2]. They linked the presence of a UK naval vessel in the South China Seas with an alleged retaliatory cyberattack by China on a UK national public service. Whether there is a causative or correlative link may be questioned, however this raised interesting discussion about power projection models and the use of cyber offence against soft or civilian targets.

A recurrent theme in the interviews was broad participant concern for regional security in Asia, particularly in relation to Taiwan as well as the propensity for China to exploit new technologies for control and indoctrination of its citizenry [P6].

4.7 Conclusion

There was a high degree of interest and engagement with the research. A gatekeeper and participant from one institution went so far as to suggest that the structured interview questions be adopted into a ‘formalised’ internal study. Although
this is outside of the scope of this dissertation, it provides a degree of assurance of the resonance of questioning and approach with some. Areas of consensus emerging from the structured interviews included: a) a feeling that the US defence market is inherently protectionist; b) the UK risks sacrificing operational freedom through cost-cutting and defence restructuring; c) Chinese strategic intent appears expansionist and offensive cyber actions against UK interests are a significant threat; d) China has potential advantage through scale of defence spending and top-down control of suppliers; and e) Chinese investment in cutting edge technologies and strategic collaboration with Russia, Iran and others could amplify pacing threats.
5 Discussion of Findings

5.1 Introduction

This chapter presents a critical thematic assessment of key findings from both research instruments. In so doing, the veracity of the risk hypotheses outlined in section 1.6 is discussed and related back to debates in the literature. For brevity, the risk hypotheses in section 5.2 are referred to by label only, followed by a discussion of findings pertinent to each. Key recommendations for policy makers are discussed in section 5.3, and build on observations and risk mitigation opportunities discovered throughout the research process. A critical assessment of the research follows in section 5.4, outlining knowledge claims, their importance and limitations. Recommendations for extension of the research are then presented in section 5.5.

5.2 Key Findings
5.2.1 Theme 1 – Qualities of Effective Defence Innovation Strategy

5.2.1.1 Hypothesis H1

The significance of policy and leadership changes across government and defence were borne out as was the fluidity of risks to which technology strategy is responding. A perceived lack of commitment to defence spending and defence industrial policy highlighted degrees of scepticism of the utility of theoretical innovation strategy seemingly decoupled from warfighting capability. Aligned with findings of (Louth, Taylor and Tyler, 2017, p. 7) no systematic assessment of UK defence technology weaknesses was found in the public domain. Awareness of key technology trends in AI, autonomous systems and related ethical considerations (Defence and Security Accelerator, 2018, p. 51) varied and the cogence of UK strategy questioned in terms of its focus, clarity and urgency. Using Fusion Doctrine as the framework for coherence and deconfliction, there appear to be opportunities for better alignment of (HM Government, 2018; Ministry of Defence, 2016; Williamson, 2018; HM Government, 2016). In agreement with (Roberts, 2018) a
focus on capability must go beyond sole focus on technological superiority. Recommendations R4 and R6 (Table 2) are proposed in partial mitigation.

5.2.1.2 Hypothesis H2

This risk seemed less manifest and there were good examples of strategy awareness and communication from top levels of defence through capability owners and extant suppliers. Examples of new supplier engagement in innovation competitions within UK defence is encouraging and publication of case studies and key successes may help attract further engagement. The intimacy between defence customers and their suppliers could perhaps be improved, and the quality of communications critically assessed. This aim could be furthered through a framework of capability development strategies and amendments to UK Defence Doctrine (Ministry of Defence, 2014) to ensure rigour of both strategic and tactical focus. Recommendations R2 and R7 (Table 2) are proposed in partial mitigation.

5.2.1.3 Hypothesis H3
There are risks of making false assumptions in offset strategy and misinterpreting threats from rival states. Indeed, the dichotomous relationship between the US and China and UK and China highlight challenges of balancing defensive security and economic and scientific collaboration (Kennedy and Lim, 2018). Cyber threats and intellectual property theft directed by China were confirmed as concerns, and align with assertions in the UK’s National Cyber Security Strategy (HM Government, 2016). In mitigating H3, the use of retaliatory cyberattack by China against UK critical national information infrastructure merits further investigation. This highlights the need for aligned technology strategies across all aspects of global defence and homeland security (HM Government, 2018). Conversely, a potential aggravation of H3 could be over-focusing on technology and ignoring risks such as Russia gaining advantage by bending (if not breaking) missile defence treaties. Testing the efficacy and coherence of technology strategy through red teaming exercises using scenario-based risk models would be a prudent mitigation. UK policy makers should continue to evaluate Trump Administration policy in relation to the future of US 3OS as noted by Fiott (2018).
5.2.2 Theme 2 – Qualities of Effective Defence Innovation Strategy Execution

5.2.2.1 Hypothesis H4

Although this risk resonated, it could be argued that the proliferation of innovation simply mirrors the complexity of UK defence and public sector structures (PA Consulting, 2018). There was a general sense that cross-government innovation was somewhat haphazard and that innovation could potentially be ‘used as convenient cover’ to attract otherwise limited funding. Innovation competitions and challenges sponsored by capability owners provides a level of focus. Although still somewhat in infancy, the effectiveness of structures established under the DII should be further tested (Defence Innovation External Advisory Panel, 2018). Recommendations R4 and R6 (Table 2) are proposed in partial mitigation of the underlying structural risks. Conduits such as Government Digital Services (GDS) and the Open Innovation team in Cabinet Office could be used to help cross-fertilise initiatives.

5.2.2.2 Hypothesis H5
Underfunding risks were mentioned throughout structured interviews in relation to technology, equipment, training and general armed forces development. Examples where technology underfunding had a measurable impact were predominantly in homeland security, cyber defence and protection of critical national infrastructure. H5 raises important questions about sources of funding and the balance of R&D spending from government and private sector investors. Innovative commercial models such as co-innovation, joint funding initiatives, risk/reward frameworks, guaranteed revenue streams and others (Enkel, Gassman and Chesbrough, 2009) may attract additional funding into defence technology development. This observation is codified in recommendation R5 in (Table 2). Personnel development and creation of ‘in-house’ capabilities in AI, cybersecurity, quantum computing and other technologies would help ensure the defence customer was in a position of thought and market leadership. In agreement with Muzzucato (2013) public sector investment has a significant role to play in developing technology innovation and this is reflected in R3, R5 and R7 (Table 2). Plans for the Ministry of Defence to publish a Defence Innovation Index from 2019 onwards is welcomed. Developing a clearer picture of what is understood by underfunding is also critical. For example, what
specific aspects of the innovation value chain are underfunded and is government or industry best placed to rectify? Economic measures such as ‘return on innovation investment’ should be considered in relation to the Defence Innovation Index, key performance indicators (Sempere, 2017) across DII and the sufficiency of DASA’s annual reports (Defence and Security Accelerator, 2018a) and corresponding scrutiny from the Defence Innovation External Advisory Panel (2018).

5.2.2.3 Hypothesis H6

There is a critical challenge in ensuring supply of cutting-edge technologies into defence and protection of intellectual property and supply chains that deliver strategic advantage (United States Department of Defense, 2018a). There was recognition that supply chain risks could be counterbalanced through greater investment and ownership of technologies within defence (as per R3 and R5 in Table 2). However, the pace and scale of technological change demands ever expanding the industrial base and use of ‘open’ engagement models between new suppliers and existing defence primes (Chesbrough, 2006; Enkel, Gassman and Chesbrough, 2009). There was some anecdotal evidence to suggest that suppliers have concerns
about weaponization of their technologies and the impact this may have on other markets, partners and employees (Wakabayashi and Shane, 2018). There is a degree of novelty in the suggestion that technological conscientious objection may birth new forms of supply chain risk. In mitigating H6 it would therefore be fruitful to revisit (United States Department of Defense, 2018a) and consider the inclusion of an additional supply chain risk archetype which recognises this as a risk of supply withdrawal. This could then be cascaded into UK strategy through the MDP and Fusion Doctrine (HM Government, 2018).

5.2.3 Theme 3 – Qualities of Effective Defence Innovation Alliance

5.2.3.1 Hypothesis H7

This risk resonated with research participants and there was a strong sense that US defence was protectionist and biased towards domestic supply. The degree to which this impacts UK defence capability is of course debatable and nuanced. If the UK has access to cutting edge US technologies through inter-governmental agreements (HM Government, 2007), and multinational defence primes, then capability
degradation may be quite minimal. That said, there are considerable economic concerns for UK technology suppliers, if they are effectively barred from entry into the US defence market. An interesting follow on assessment would be to analyse partnering relationships between US and UK suppliers to determine where and how protectionist barriers are best overcome. While it is not surprising that both the UK and US will seek to maximise national self-interest (Ministry of Defence, 2012), the impact on trust and ability to use Open Innovation across an alliance seems weakened. The size of US defence spending (United States Department of Defense, 2018c) and links with Silicon Valley (Seligman, 2018b) may on one hand enable protectionist behaviour, while on the other create unnecessary supply chain risks and inefficiencies. Recommendation R1 (Table 2) proposes a bold ‘co-funding’ solution.

5.2.3.2 Hypothesis H8

There is evidence of strategic co-operation through the UK-US innovation board meetings. However, differing extant strengths and weaknesses, perceptions of threats and availability of funds are likely to make strategic technology alignment a
complex objective. Formalising innovation portfolio management across the alliance with co-ownership, funding and joint governance would be an interesting challenge. Recommendation R1 (Table 2) could be tested through the establishment of joint UK-US experimental units. There are additional challenges in the strategic clarity of the UK’s MDP (Williamson, 2018) as well as President Trump’s America First doctrine and the potential impact on US 3OS (Fiott, 2018). This raises key questions about where and how alignment could best be achieved. The answer may lie in the intersections of shared national security objectives, however differing foreign policy and ethical positions may impact full collaboration. The complexity and proliferation of US defence innovation structures must also be considered, including how and where UK and US bodies would engage. Tasking the UK and US Defence Innovation Boards to assess and formalise co-innovation opportunities would appear to have potential.

5.2.3.3 Hypothesis H9

ITAR was cited as a particularly complex and onerous US government restriction that could be injurious to commercial interests of UK suppliers. Additional hurdles
such as governance, procurement, security, safety and compliance were potential barriers to access to both US and UK defence markets. Governments may choose to increase investment in internal capabilities (recommendation R3 in Table 2), reduce friction of unwieldy regulation and maximise points of alignment through common standards. As part of the Ministry of Defence plans to publish an annual Innovation Index, it would be interesting to include cross-alliance measures and assessments of points of synergy and friction. Including co-innovation funding targets in the MDP could help open debate about defence spending in general and potential synergies across US, NATO and EU alliances. This could further link to economic measures such as of the ‘return on innovation investment’ suggested in H5 (section 5.2.2.2).

5.2.4 Theme 4 – Theorising China’s Strategic Defence Innovation Intent

5.2.4.1 Hypothesis H10

There are recognised risks of foreign ownership (Sengupta, 2018) and measures in place in both UK and US to manage Chinese ownership and influence in critical industries (Cheung, 2016; Bitzinger, 2016; United States Department of Defense, 2016).
2018b). The UK’s attitude appears somewhat laisse faire and economic drivers such as maximising foreign investment may impact aspects of technology supply chain security. China’s reputation for cyberattack and intellectual property theft may be well earned (HM Government, 2016; Pillsbury, 2014), however China’s ability to exploit ‘the take’ from breached data is less clear. Hypothesis H10 therefore gave rise to additional questions about the utility of cyberattack and whether risks posed were minimal nuisance or existential threat. China’s alleged use of retaliatory cyberattack against civilian targets raised greatest concern. Understanding Chinese, Russian and Iranian perspectives on R&D exchange (Gabuev, 2018) and the degree to which these accelerate pacing threats would make for interesting study.

5.2.4.2 Hypothesis H11

In exploring this hypothesis, the question of comparative defence innovation costs between China and UK-US arose. With a sizeable defence budget, lower labour cost, potential benefits gained from intellectual property theft and advantages of autocratic directiveness there are numerous dimensions on which China could exploit cost advantage (Lineberger and Hussain, 2018). Exploitation of dual-use
technology is therefore simply one dimension of a broader question on innovation economics. Hypotheses H11 presupposed that UK-US sectors were somewhat more traditional and less inclined to utilise dual-use technology. This hypothesis is therefore unproven and would benefit from a comparative study of the economics of defence innovation in China, the US and UK with focus on successes and failures of dual-use technology exploitation.

5.2.4.3 Hypothesis H12

Aligned with findings on hypothesis H11, the question of comparative defence innovation costs between China and UK-US arose. Although size of investment is something of an indicator of strategic priority, it does not necessarily correlate with uplift in strategic defence capability. Efficiency and tangible delivery of outcomes is paramount. In expanding H12 into a more sophisticated proposition therefore it would be prudent to consider the overall effectiveness of Chinese technology investments. In balancing UK and US investments against offset objectives this would open opportunities to develop sophisticated pacing threat models. This study
limited the scope to China, but H12 would benefit from expansion to consider threats from Russia, Iran and North Korea.

5.2.5 Risks missing from initial hypotheses

Concerns over levels of UK defence spending was a recurrent theme in the structured interviews. There is a potential risk that over-funding technology innovation at the cost of personnel development or exploitation of extant capabilities could be profligate and detrimental (Roberts, 2018).

This research assessed technology from a somewhat militaristic perspective. From the perspective of Kantian Liberal Peace Thesis, it could be argued that a lack of cooperation with near-peers risks impeding trade and international development, regarded in Liberal theories as cornerstones of stability of the international system.

This research suggests that models for assessing technology pacing threats from near-peers are somewhat scant. Constructing a framework for evaluating pacing threats appears to have merit and may assist in maximising innovation effort across national alliances.
No specific concerns were raised by participants about US foreign policy. This may reflect a lack of salient questioning, or perhaps a lack of diversity in the research group.

5.3 Key Recommendations

The recommendations presented in Table 2 are synthesised from analysis of the risk model and risk mitigations emerging from the research and are primarily aimed at policy makers.
### Innovation and Technological Superiority in UK Defence

Eur Ing Steve Nimmons FBCS CITP FIET CEng FRSA
Nimmons Consulting, London, February 2019

<table>
<thead>
<tr>
<th>Ref</th>
<th>Recommendation</th>
<th>Rationale</th>
<th>Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Establish joint UK-US innovation fund, administered by joint defence innovation board</td>
<td>There are established links between the Defence Innovation Boards in UK and US Defence. A joint portfolio, funding pot and aligned delivery objectives would increase opportunities for formalised cross-alliance innovation</td>
<td>This would require funding agreements between the US and UK, prioritisation of initiatives and clear ownership, governance and success measures. Opportunities to second UK staff into US defence innovation initiatives (and vice versa) would likely enhance outcomes</td>
</tr>
<tr>
<td>R2</td>
<td>Increase quality and frequency of communications with key suppliers</td>
<td>Not all suppliers are well sighted on defence strategy and technological needs. There are opportunities for suppliers at all levels to contribute to requirements shaping and capability prototyping</td>
<td>Scale the level of engagement between defence capability owners and the technology supply chain and provide timely and consumable strategic technology briefings as part of the MDP and any subsequent Strategic Defence Spending Reviews</td>
</tr>
<tr>
<td>R3</td>
<td>Invest in the development of strategic in-house defence technology capabilities to mitigate supply-side risks from industry</td>
<td>Skills in AI, cybersecurity, Quantum Computing and other critical technology capabilities are needed in-house under the control and direction of the UK military</td>
<td>Funding is required to ensure these skills are acquired, developed and retained within UK armed forces. Seek opportunities to incentivise and attract experienced talent into reserve forces</td>
</tr>
<tr>
<td>R4</td>
<td>Cohere and deconflict innovation initiatives across defence and wider public sector</td>
<td>There are numerous innovation bodies and initiatives across government and enhanced coherence and deconfliction of effort may help drive efficiencies including reduced capability development cost</td>
<td>The innovation portfolio and strategic technology needs across government should be systematically assessed to find synergies and opportunities for re-use and re-purposing</td>
</tr>
<tr>
<td>R5</td>
<td>Innovate with commercial models including co-innovation and risk/reward frameworks</td>
<td>Greater flexibility in commercial frameworks and sourcing may drive increased innovation in the supply chain, leading to increased supplier proactivity and engagement</td>
<td>Commercial frameworks and funding models should be reviewed and impediments to frictionless innovation removed or reduced</td>
</tr>
</tbody>
</table>
**R6** Establish a formal review of the Defence Innovation Initiative and progress since SDSR 2015

The newer structures of UK defence innovation (such as DASA) should be assessed to ensure sufficiency of funding and resources to meet requisite maturity development and scaling

A fundamental question must be asked as to whether the ‘accelerator could itself be accelerated’. This may require additional headcount, funding and sponsorship and perhaps a degree of consolidation across the various defence innovation structures

---

**R7** Ensure basic innovation and entrepreneurial theories are taught as part of officer cadre training

A sound awareness of innovation strategy will assist capability owners in avoiding mousetraps such as poorly specified or overly constraining requirements

Personnel development should include at least a basic awareness of innovation challenges and solutions in public and private sectors. A useful exemplar is the US Marine Corps Commandant’s reading list (US Marine Corps, 2018)

---

**Table 2 Summary Recommendations**
5.4 Critical Assessment of the Study

5.4.1 Importance

Technological superiority in defence is recognised by the UK and US governments as critical to national security and global national interests. Examining potential weaknesses in policy, strategy, delivery, cooperation and pacing challenges from rivals is a high value endeavour. Indeed, as recommended in section 5.3 [R6], policy makers should consider formalising and adopting such a review method as part of a regular innovation assurance lifecycle.

5.4.2 Limitations

Methodologically, the structured interview research instrument was a successful technique, and gatekeepers provided helpful access and referral to suitable participants. It would have also been both interesting and fruitful to interview representatives from both US and China (for additional counterpoint), however due to time constraints this was not feasible. Due to language barriers, source material on China was limited to that available in English. Care was taken during the literature
review to assess diverse perspectives on China, although this is still conceivably somewhat Western influenced.

The online survey research instrument was less engaging. An improvement would have been to operate a kiosk-style survey at a trade conference or to engage through a trade association such as the ADS Group³. Nonetheless, there are some marginal data points from the online survey that suggest that varying attitudes to offensive and defensive use of technology may impact some suppliers within the sector. This could be further assessed using an extended study and scaled quantitative analysis.

The risk model hypothesised from the literature review (Chapter 2) proved to be efficient and engaging, simple to understand, debate and critique. Limiting risks to the top 3 per theme is somewhat arbitrary and it is important to consider whether the risk model itself introduced anchoring bias. Emphasising that the model was simply a

---

³ ADS – Trade Association for UK Aerospace, Defence, Security and Space sectors - https://www.adsgroup.org.uk
‘strawman’ helped assure participants that they could (and indeed must) be fully critical of material presented.

As the research progressed, several opportunities to engage further institutions and research participants emerged. Due to time limits, not all these opportunities could be taken up. This may have impacted the full potential richness of findings.

Finally, the scope of the research was ambitious. A potential improvement in the methodology may have been the segmentation of the research participant community by specialism of each Theme. Thereby, the structured interviews would have been more focused on sub-sets of the risk model.

5.5 Further Research

Building on this research and fusing the observations from the literature gaps postulated in section 2.6, there appears to be significant opportunity to expand into a fuller assessment of Open Innovation challenges within global defence sectors. A particularly interesting line of enquiry would be to comparatively assess Open Innovation models in US, UK, Chinese and other defence industries such as in
Israel. Inclusion of Israel would be particularly interesting due to military service requirements for citizens and the intertwining of defence and private sector start-ups. Here, the question could be posed as to whether mandatory military service impacted the defence industrial base and created advantageous relationships and understanding between defence customers and technology innovators.

5.6 Conclusion

This chapter critically assessed the research question through interrogation of each hypothesis constructed from the literature review (Chapter 2) and tested using the research instruments described in Chapter 3. Key findings from the research were discussed in relation to debates in the literature. Areas of divergence from anticipated results were highlighted. In critically analysing research findings, a set of key recommendations for policy makers was proposed. These are abridgements but provide useful perspectives on areas of focus for future defence innovation research. Limitations of this work have additionally been outlined for transparency and to help the reader with their own critical assessment of recommendations and assertions.
Opportunities to expand this research into broader investigations of comparative approaches to Open Innovation in global defence have been proposed.
6 Conclusion

The importance of this research is to assist policy makers in understanding key technology innovation risks in UK defence. The approach taken was to construct a set of risk hypotheses, situated within a thematic framework in which the goals of attaining and sustaining technological superiority against near-peer rivals were assessed. The risk model, hypothesised from a substantive review of defence innovation literature, provides a useful architecture for further research. Actionable mitigations have been proposed that further the policy debate. Originality of this approach includes the testable hypotheses of the risk model, the methodology (which is readily extendable to threat assessment of Russia, Iran and North Korea) and key observations of emerging technology supply chain risks (such as globalisation of technology and new forms of conscientious objection). Several proposals for further research have been outlined including comparative studies of Open Innovation models used in UK, US, Chinese and Israeli defence sectors.

The substantive conclusions from this research span each of the 4 themes:
Theme 1 - The Qualities of Effective Defence Innovation Strategy - there are limited publicly available analyses of UK defence technology capability weaknesses, and changes in policy focus under MDP and 3OS risks the creation of incoherent and conflicting views of strategic innovation priorities.

Theme 2 - The Qualities of Effective Defence Innovation Strategy Execution - the DII has established key innovation structures including DASA, IRIS and the UK Defence Innovation Advisory Panel however aspects of scalability and maturity have yet to be fully proven. There are additionally new supply chain risks arising from globalisation of technology supply. Defence culture is a variable and heterogeneous concept when assessed through Army, Navy, Air Force, Special Forces, Reserves, political and supply-side lenses. Cultural change and adoption of innovation best practices is therefore complex, in what is effectively an ecosystem of organisations and organisational cultures.

Theme 3 - The Qualities of Effective Defence Innovation Alliance - there are apparent difficulties in the relationship between US and UK defence, impacting true co-innovation and technological exchange. There are opportunities for boldness in
UK-US relations and potential for co-innovation using joint experimental units. Additionally, there appears to be a level of mistrust at some levels of UK defence with the EU, including perceived challenges to UK operational freedom.

**Theme 4 - Theorising China’s Strategic Defence Innovation Intent** - the dichotomous nature of relations with China, in balancing defence competition and economic cooperation, is intriguing. Further enquiry is recommended to better understand the true nature of technology pacing threats from China and the extent to which risks are magnified by collaboration and technology exchange. Allegations of China’s use of retaliatory cyberattack against civilian targets are alarming. New forms of cyber coercion and cyber power projection must therefore be considered as key risks.

Finally, the UK military plays an important role in delivering national security objectives and ensuring geopolitical security with other nations as part of NATO, the EU, the 5-eyes community and directly with the US. Ensuring that service personnel have access to world-class capabilities and training is vital in ensuring the effectiveness of UK defence. The UK military has a long tradition of technological ingenuity and prides itself in strategic and tactical warfighting capability. Innovators
within UK defence play a leading global role in technology advancement and have unique perspectives to offer innovation practitioners and theorists. Development and publication of best practices in defence innovation would make substantive contribution to the wider innovation research community and help promote the UK as a global innovation thought leader. DASA is well placed to lead, and through the DII and MDP, innovation policy and practice developed that would benefit national security, international development and domestic economic wellbeing.
7 Bibliography


management-handbook-9780749478827.


Defense Intelligence Agency (2017) *Russia Military Power - Building a Military to Support
Strategic Thinking in a Complex World

Web: https://www.nimmonsconsulting.com


Innovation and Technological Superiority in UK Defence

Eur Ing Steve Nimmons  FBCS CITP FIET CEng FRSA
Nimmons Consulting, London, February 2019

2018).


Innovation and Technological Superiority in UK Defence

Eur Ing Steve Nimmons FBCS CITP FIET CEng FRSA

Nimmons Consulting, London, February 2019


POWER-REPORT.PDF.


About the Author

Steve Nimmons is an independent technology consultant and writer.

He is a
- Member of UKNDA
- Chartered Fellow of the British Computer Society (FBCS CITP)
- Fellow of the Institution of Engineering and Technology (FIET)
- Certified European Engineer (Eur Ing)
- Chartered Engineer (CEng)
- Fellow of the Royal Society of Arts (FRSA)

His interests include:
- Innovation and Digital Transformation in Defence, Policing and Security
- Smart Cities and the Internet of Things
- Counter-terrorism
- Cyber Security