**Print:** ISSN 2634-0968
**Online:** ISSN 2634-0976

ROYAL AIR FORCE

# Air and Space Power Review

Volume 25 Number 1 Spring 2023

**Foreword**
Air Commodore Catherine Coton, Head Air Staff

**Introduction**
Wing Commander Amanda Scarth

**Articles**
> Doing 'All We Can To Help Mr Tizard' The Role of Sholto Douglas in Radar Development and Its Application
Dr Katharine Campbell

> JOINT SACEUR-SACLANT Air Defence Operations in North European Waters
Wing Commander Joan Hopkins

> How Does Russia Wage Contemporary Political Warfare, and Consequently Challenge International Order?
Wing Commander Jade Richards

> To What Extent Does China's Increasing Influence in the Black Sea Region Promote Stability?
Wing Commander Sarah McDonnell

> Female Radicalisation and ISIS: What are the Implications for UK Domestic Security?
Wing Commander Siân English

> Evaluate the Potential Effectiveness of Air Power in Sub-threshold and 'Grey Zone' Operations
Wing Commander Clare Mummery

> Artificial Intelligence Changing the Nature of War – Strategic Security Implications for the United Kingdom?
Wing Commander Alison Morton

> Strategic Competition to Security Dilemma – The Language and Narrative of Space and Why it Matters
Wing Commander Sas Duffin

**Viewpoint**
> The Seam between Chaos and Order
Group Captain Emma Keith

**Book Reviews**
> Human Compatible: AI and the Problem of Control
Author: Stuart Russell / Reviewed by Group Captain Emma Keith

> Why I'm No Longer Talking To White People About Race
Author: Reni Eddo-Lodge / Reviewed by Flight Lieutenant Sabrina Sheikh

> The Weaponisation of Everything
Author: Mark Galeotti / Reviewed by Squadron Leader Beth Lindley

> RAF WWII Operational and Flying Accident Casualty Files in the National Archives – Exploring their Contents
Author: Mary Hudson / Reviewed by Flight Lieutenant Lilie Weaver

> The Ledger: Accounting for Failure in Afghanistan
Author: David Kilcullen and Greg Mills / Reviewed by Squadron Leader Chloé Bridge

A Peer Reviewed Journal by the
**RAF Centre for Air and Space Power Studies**

**See The Royal Air Force Air and Space Power Review online**

https://www.raf.mod.uk/rafcasps

**Air and Space Power Review**
is the professional flagship publication of the Royal Air Force

# RAF Air and Space Power Review

The Royal Air Force *Air and Space Power Review* is produced by the Royal Air Force Centre for Air and Space Power Studies. The publication provides a forum for academically credible articles on air power, space power and cyber power, with the objective of stimulating debate and promoting the evolution of focussed thinking within the broader military and academic communities. Authors are encouraged to challenge accepted norms and offer novel conclusions. Consequently, the views expressed in this journal are those of the individual authors and do not necessarily represent those of the UK Ministry of Defence, or any other department of His Britannic Majesty's Government of the United Kingdom. Further, publication of those views should not be considered as constituting an official endorsement of factual accuracy, opinion, conclusion or recommendation by the UK Ministry of Defence, or any other department of His Britannic Majesty's Government of the United Kingdom.

Contributions from both Service and civilian authors are sought provided the submission is original and unpublished. Any topic will be considered by the *Air and Space Power Review* Editorial Board provided that it contributes to existing knowledge and understanding of air, space and cyber power. Articles should comply fully with the style guide published at the RAF Centre for Air and Space Power Studies website, https://www.raf.mod.uk/rafcasps; essentially they should be between 5,000 and 10,000 words in length, list bibliographical references as endnotes, and state a word count. Shorter articles and those which offer more of a personal opinion will also be considered for inclusion as a 'viewpoint'. A short biography and abstract should be submitted with each paper. A payment of £230 will be made for each full article published, or £100 for a published viewpoint and £50 for a book review. Additional constraints apply for payments to Service personnel for which details are available from the Editor.

Feedback from readers is encouraged and those wishing to comment on published articles or make suggestions for how *Air and Space Power Review* can better meet the needs of the broader air and space power community can do so by contacting the Editor at the address below. The Editor reserves the right to publish feedback in part or in full, where it contributes meaningfully to the debate.

All material for publication should be submitted in a Microsoft Word compatible format by e-mail. Digital pictures should be saved as TIFFs or JPEGs at 300dpi or greater. Final design format for article presentation on the printed page will be at the discretion of the Editor.

**Please send articles to:**
Director of Defence Studies (RAF)
Cormorant Building (Room 119)
Shrivenham, Swindon
Wiltshire, SN6 8LA

**E-mail:** CAS-ASDefenceStudies@mod.gov.uk

## Executive Board Members

**Gp Capt Paul Sanger-Davies**
Director of Defence Studies (RAF)

**Dr David Jordan**
King's College London (JSCSC)

**Mr Sebastian Cox**
Head of Air Historical Branch (RAF)

## Editorial Board Members

**Gp Capt (Retd) Clive Blount**

**Dr Bleddyn Bowen**
University of Leicester

**WO Sara Catterall RAF**

**Dr Jonathan Fennell**
King's College London

**Dr Ian Gooderson**
King's College London

**Dr Christina Goulter**
King's College London

**Air Cdre (Retd) Prof Peter Gray**
University of Wolverhampton

**Dr David Hall**
King's College London

**Dr Mark Hilborne**
King's College London

**Dr Frank Ledwidge**
University of Portsmouth

**Prof Peter Lee**
Portsmouth Business School

**Dr David Lonsdale**
University of Hull

**Cpl Lee Maddison RAF**

**FS Paul Marr RAF**

**AVM (Retd) Prof Tony Mason**

**Gp Capt (Retd) Clare Muir**

**Dr Steven Paget**
University of Lincoln

**Dr Matthew Powell**
Portsmouth Business School

**Dr Sebastian Ritchie**
Air Historical Branch (RAF)

**Flt Lt Sabrina Sheikh RAF**

**Gp Capt (Retd) Ian Shields**
University of Cambridge

**Dr Victoria Taylor**
University of Hull

## Editorial Staff

**Editor**
**Gp Capt Paul Sanger-Davies**
Director of Defence Studies RAF

**Assistant Editor**
**Wg Cdr Amanda Scarth**
Deputy Director of Defence Studies RAF

**Assistant Editor**
**Sqn Ldr Rob Kevan**
SO2 Directorate of Defence Studies RAF

**Researcher**
**Cpl Chris Hargreaves**
Portal Fellow in Residence,
Defence Studies RAF

**Office Manager**
**Miss Jane Curtis**
Directorate of Defence Studies RAF

**Production and Design**
**Mr Anthony Jones**
Air Media Centre, Air Command



General enquiries on Journal publication and distribution may be made to the following address:
Director of Defence Studies (RAF)
Cormorant Building (Room 119)
Shrivenham
Swindon
Wiltshire SN6 8LA

**E-mail:** CAS-ASDefenceStudies@mod.gov.uk
**Print:** ISSN 2634-0968
**Online:** ISSN 2634-0976

Alternate issues will be published on line. Those wishing to be placed on the distribution list to receive a printed version, when produced, should contact the Editor directly.



The views expressed are those of the authors concerned, not necessarily the MOD.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor. Unless by prior arrangement, articles and photographs will not normally be returned.



**Print:** CDS

# Air and Space Power Review

Volume 25 Number 1 Spring 2023

4
**Foreword**
Air Commodore Catherine Coton, Head Air Staff

5
**Introduction**
Wing Commander Amanda Scarth

8
**Article**
Doing 'All We Can To Help Mr Tizard' The Role of Sholto Douglas in Radar Development and Its Application
Dr Katharine Campbell

36
**Article**
JOINT SACEUR-SACLANT Air Defence Operations in North European Waters
Wing Commander Joan Hopkins

46
**Article**
How Does Russia Wage Contemporary Political Warfare, and Consequently Challenge International Order?
Wing Commander Jade Richards

80
**Article**
To What Extent Does China's Increasing Influence in the Black Sea Region Promote Stability?
Wing Commander Sarah McDonnell

104
**Article**
Female Radicalisation and ISIS: What are the Implications for UK Domestic Security?
Wing Commander Siân English

142
**Article**
Evaluate the Potential Effectiveness of Air Power in Sub-threshold and 'Grey Zone' Operations
Wing Commander Clare Mummery

164
**Article**
Artificial Intelligence Changing the Nature of War – Strategic Security Implications for the United Kingdom?
Wing Commander Alison Morton

190
**Article**
Strategic Competition to Security Dilemma – The Language and Narrative of Space and Why it Matters
Wing Commander Sas Duffin

222
**Viewpoint**
The Seam between Chaos and Order
Group Captain Emma Keith

230
**Book Review**
Human Compatible: AI and the Problem of Control
Author: Stuart Russell
Reviewed by Group Captain Emma Keith

232
**Book Review**
Why I'm No Longer Talking To White People About Race
Author: Reni Eddo-Lodge
Reviewed by Flight Lieutenant Sabrina Sheikh

236
**Book Review**
The Weaponisation of Everything
Author: Mark Galeotti
Reviewed by Squadron Leader Beth Lindley

240
**Book Review**
RAF WWII Operational and Flying Accident Casualty Files in the National Archives – Exploring their Contents
Author: Mary Hudson
Reviewed by Flight Lieutenant Lilie Weaver

244
**Book Review**
The Ledger: Accounting for Failure in Afghanistan
Author: David Kilcullen and Greg Mills
Reviewed by Squadron Leader Chloé Bridge

ROYAL AIR FORCE
Centre for Air and Space Power Studies

# Foreword

by Air Commodore Catherine Coton, Head Air Staff

It gives me enormous pleasure to introduce this unique edition of the *Air and Space Power Review (ASPR)*, which celebrates the contribution of women to military academia. Acknowledging International Women's Day, which was on 8 March 2023, all our contributors in this Review are women. International Women's Day was designed to celebrate women's achievements and reinforce a commitment to women's equality. The event has been marked for over a century, with the first gathering in 1911, so it feels apt to reflect this historic moment in the ASPR and as the first female incumbent of the Head of the Air Staff role.

Women have made significant contributions to the military debate for decades, often remaining below the horizon of their male counterparts. The purpose of this special edition is to highlight the incredible academic ability of women, linked to the RAF by either serving themselves, or having a strong connection to the Service. Following the amalgamation of the Women's Royal Air Force (WRAF) into the Royal Air Force in 1994, recognising transformation within wider society, more women have felt able to promote their views and provide erudite analysis. I trust you will enjoy this special edition of the Review, and the wide range of subjects covered by the articles.

ROYAL AIR FORCE
Centre for Air and Space Power Studies

# Introduction

by Wing Commander Amanda Scarth

**As Deputy Director for Defence Studies (RAF) I am delighted to have this opportunity to review the contributions to this edition of the ASPR. Several of the articles in this publication were written as Defence Research Papers (DRPs), while the authors attended the Advanced Staff Course in the last few years, all of them achieving the highest assessment grade. Additionally, one of the papers was written as a dissertation by a Henderson Fellow attending Exeter University. It should be appreciated that these papers were written either before, or in some cases just after, the Russian invasion of Ukraine. Consequently, aspects of the analysis and perceptions have since been tested, and in some cases changed, and will continue to do so as events unfold.**

The first article written by Wing Commander Joan Hopkins was originally published in The Hawk: The Independent Journal of The Royal Air Force Staff College in July 1977. Even at 47 years old, the paper provides an interesting analysis of the relationships between strategic commands within NATO and the need to introduce automated systems for improved interoperability and integration between air defence and naval forces.

Recognising emerging technologies and their utility was not lost on Sholto Douglas, who was involved in the development of radar. Later to become Marshal of the Royal Air Force Lord Douglas of Kirtleside, his daughter Dr Katharine Campbell, provides a fascinating insight into her father's contribution to the introduction and application of radar across the RAF.

The subsequent articles cover a wide range of topics and reflect the diversity in studies undertaken by our scholars. In the first of the Papers, Wing Commander Ali Morton examines how Artificial Intelligence is changing the nature of war and the implications to our nation's security. Wing Commander Siân English tackles the complex issue of female radicalisation and ISIS, and the obvious security implications for UK domestic security. Topically, Wing Commander Jade Richards discusses how Russia is challenging international world order through political warfare. Although written prior to the Ukraine conflict, it will provide a useful comparison to the contemporary thinking at the time and what has happened over the last year. With another potential adversary, Wing Commander Sarah McDonnell looks at China's geopolitical influence relationships in the Black Sea Region and the potential impact on stability. Wing Commander Clare Mummery addresses the effectiveness of air power in sub-threshold and 'grey zone' operations, using Iran and Japan as case studies. For the final academic article, Wing Commander Sas Duffin explores how the language and narrative of space has evolved over the decades, and what this might mean for the space domain.

The viewpoint is provided by Group Captain Emma Keith, Commandant of the Tedder Academy of Leadership. Group Captain Keith explains how leadership can be used to navigate

the line between chaos and order and how the RAF can retain a competitive edge now and in the future.

This special edition of the ASPR concludes with five book reviews. First, Group Captain Emma Keith reviews Human Compatible: AI and the Problem of Control by Stuart Russell Human, which considers the interface between humans and machines and asks the question of how we ensure that the AI we are creating is compatible with the world that humans want to live in. Flight Lieutenant Sabrina Sheikh reviews Why I'm No Longer Talk to White People About Race by Reni Eddo-Lodge, in which she discusses Britain's relationship with Race and Racism, at a time when sensitivity around language such as, 'white people' and 'privilege' exists. Squadron Leader Beth Lindley reviews The Weaponisation of Everything by Mark Galeotti, which considers hybrid warfare and aims to be a guide rather than advocacy to a way of war that is increasingly playing out on the global stage. RAF WWII Operational and Flying Accidents Casualty Files in the National Archive by Mary Hudson is reviewed by Flight Lieutenant Lilie Weaver. The author uses her research into those who lost their lives during WW2 serving with, or alongside, the RAF, and is able to weave together the stories collated from Archive files into a compelling read. Finally, Squadron Leader Chloe Bridge has reviewed The Ledger by David Kilcullen and Greg Miles. This book was based on years of experience advising senior leaders and academic research and the authors provide a detailed analysis of what went wrong during the twenty-year Western intervention in Afghanistan.

I hope you enjoy the articles and book reviews in this unique edition of the ASPR.

Article

# Doing 'All We Can To Help Mr Tizard' The Role of Sholto Douglas in Radar Development and Its Application

By Dr Katharine Campbell

**Biography:** Dr Katharine Campbell was a neuroscientist before becoming a writer, completing her PhD at University College London and staying on as a post-doctoral fellow. Her biography of her father Sholto (MRAF Lord Douglas of Kirtleside), *Behold the Dark Gray Man*, published in 2021, was selected for the 2022 CAS' Reading List. She collaborates with historians across Europe and with world experts on PTSD. She was invited to participate in the Australian Royal Commission into Defence and Veteran Suicide, in which she is still involved.

**Abstract:** The prevailing historical narrative has been that the creator of the 'Dowding System' of air defence, of which radar was a vital part, was the brainchild of Air Chief Marshal Sir Hugh Dowding, the contribution of other Air Force officers, including my father Sholto Douglas, having been largely ignored. However, Sholto was involved in radar development from its early days in 1936, when he coordinated the first aircraft interception experiments as Director of Staff Duties at the Air Ministry. From that point up to and into World War Two, he was at the forefront of radar evolution and its application, particularly to night fighting, pursuing this engagement for the remainder of WWII as AOC-in-C of Fighter Command especially, but also when he oversaw Middle East and Coastal Commands.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

Air Chief Marshal Sir Sholto Douglas, C-in-C Fighter Command, inspecting film in his office at Bentley Priory, December 1942. © Getty Images.

## Introduction

Until I began researching the life of my father, Marshal of the Royal Air Force Lord Douglas of Kirtleside (known always as 'Sholto', which he preferred), to write his biography,[1] I subscribed to the prevailing narrative, articulated by the historian Dr David Jordan, that success in the Battle of Britain 'was the result solely of the efforts of Air Chief Marshal Sir Hugh Dowding as Air Officer Commanding-in-Chief [AOC-in-C] of RAF Fighter Command.' But as Dr Jordan continues, this 'obscures the fact that success was built upon a long period of development,'[2] beginning in World War One. Following the 'Gotha raids' in 1917, in which, among other atrocities, twenty-three children aged between four and six years old were killed on one day alone, eighteen of whom died when a bomb demolished Upper North Street Council School in Poplar,[3] the London Air Defence Area was formed under the command of Major General E. B. Ashmore. He also oversaw the foundation of the Observer Corps in 1925, which was to become a vital part of what was, and is, known as the 'Dowding System.'

The Radar Chain was another essential element of this network of air defences, becoming, as Vincent Orange observed: '"the catalyst of defence science". In short, Watson-Watt gave it birth; Tizard supported it; and Dowding grasped it.'[4] However, in his biography of Dowding, Orange neglects to mention the other Air Force officers who championed radar from the

beginning, including Sholto, who was not only responsible for instigating the Biggin Hill radar experiments, but who also sanctioned the necessary funds to make those trials a reality.

In January 1936, Sholto, who had been promoted to the rank of Air Commodore, was appointed Director of Staff Duties (DSD) at the Air Ministry, a position that he took up officially in the same month.[5] The most important element of his work was to take care of the training programme for the entire RAF, including organising major exercises,[6] and it was in this post that his involvement with radar began.

## The Biggin Hill interception experiments

Following moderately successful demonstrations of the utility of radar in detecting aircraft under daylight conditions in 1935 and 1936, Watson-Watt made a prediction that the success of fair-weather radar detection meant that a potential enemy would be driven to night attack, or attack through cloud. This was presented to the Committee for the Scientific Survey of Air Defence (CSSAD), chaired by Henry Tizard and therefore known as the Tizard Committee, in February 1936, and thereafter Watson-Watt's team set to work on developing airborne radar equipment, which, because of the difficulties in its realisation, would not come to fruition until 1941, when Sholto was AOC-in-C Fighter Command. Along with its essential counterpart, Ground Control Interception radar (GCI),[7] Airborne Interception (AI)[8] would be instrumental in ending the Blitz.

Tizard had come to the same conclusion as Watson-Watt: that techniques would have to be developed that would direct fighter pilots to the point of interception with enemy bombers whatever the conditions. He had a meeting with the Deputy CAS (DCAS), Air Marshal Christopher Courtney, on 13 July 1936 to obtain approval for experiments. Tizard wanted to know how long it would take to intercept an enemy bomber following receipt of the bomber's approximate position ten minutes from the coast. Furthermore, Watson-Watt and his team of AI investigators needed to know the minimum distance that an aircraft required for effective interception.[9]

Sholto, as DSD, was given the task of implementing the proposed interception experiments. On 14 July, the day after Tizard and Courtney's meeting, Sholto wrote to the AOC No.11 (Fighter) Group, Air Marshal Philip Joubert de la Ferté, to inform him of the aircraft and ground facilities needed for the exercises. Sholto wrote: 'we are very anxious to do all we can to help Mr Tizard, as these experiments are, in our opinion, most important, particularly from the bearing that they have on the future employment of the RDF [radio direction finding] system.'[10] Together, Sholto and Joubert de la Ferté decided on the sector station at Biggin Hill in Kent as the optimum location, Sholto informing Courtney of this suggestion.[11] From this time on, they were known as the Biggin Hill Experiments. As soon as Sholto had established both the location and that the necessary aircraft could be supplied from both Bomber and Fighter Commands, on 27 July he wrote a preliminary letter to the AOCs-in-C of these Commands, and the AOC of No.22 Army Co-operation Group.

The following day Sholto received a reply from Dowding who had taken over as AOC-in-C Fighter Command in July. He was a little put out that little information concerning the exact nature of the experiments was contained in the letter, and that therefore the station commander at Biggin Hill, Wing Commander Grenfell, and Tizard, would be 'in complete control not only of the details but also of the experiments as a whole.'[12] Dowding wanted to be included in the loop, and particularly to be in personal touch with Tizard. Sholto replied within three days to Dowding with all the information that he required.

Dowding then arranged a conference between himself, Tizard, and the major players who would be involved in the exercises including Joubert and Grenfell, on 7 August without apparently inviting Sholto,[13] to whom he wrote a letter that was critical of the Air Ministry while at the same time appearing to exclude him. Dowding wrote that the Air Ministry needed to take more action, specifically to provide more specialist staff and to allow more time for the experiments, although the Air Ministry already had in hand the task of appointing a navigation officer, an essential member of the proposed team, and had made tentative suggestions regarding time scale to fit in with Tizard's schedule. The RAF Signals History notes that Sholto sanctioned the continuation of the experiments for as long as was necessary, into 1937 if need be.[14]

It is clear from Dowding's correspondence that there was a definite 'prickliness' to his communication, and that, as Sholto had observed many years before, he was suspicious of those in the Air Ministry. Sholto's initial letter was intended only as a preliminary approach, but Dowding thought immediately, without any foundation, that he was being sidelined. Perhaps, as he indicated, he did not like being told what to do by those who had until quite recently been his subordinates, even though Sholto was acting at Courtney's behest.[15] Or perhaps there was some truth to the assertion, made almost exactly four years later in a very controversial memo sent anonymously to influential people in the government, parliament, and the RAF during the summer of 1940, that 'HQ Fighter Command is substantially a one man show and is ruled by Air Chief Marshal Dowding who has definite personality…..He is also a classic example of a complete non-co-operator either with the Air Ministry or any other authority.'[16] Although Air Vice-Marshal Keith Park, AOC No.11 (Fighter) Group, praised Dowding for his ability to delegate tactical control of fighter operations to his group commanders, when it came to supervision of the elements of what has been called the Dowding system, he was certainly a micro-manager.[17]

The Biggin Hill interception experiments began on 5 August 1936, and the suggestion was quickly made that it would be most desirable for the two RAF navigation officers in the Operations Room to be provided with some form of automatic equipment for calculating the fighter course needed to intercept the bomber, as well as the estimated time of interception, taking into account the wind, relative positions, and the track and ground speed of the fighters and bombers. The RAF officers decided initially that the practised eye or 'dead reckoning' was the best method.

At first, bombers were instructed to fly on a pre-arranged straight course from a known starting point and at an agreed height, in which case interception was very successful (twenty-six out of twenty-eight runs). In the second series of experiments, they were allowed to alter their courses at will, necessitating frequent redirection of fighters with delays resulting from having to work out another course, and sometimes a failure of interception altogether. Nevertheless, the fighters became more expert as the tests continued, and the bombers were permitted to make changes to course, height and finally to speed.

In the important meeting on 7 August, the matter arose of the aircraft to be used for searchlight experiments, and Dowding said that these exercises were to be kept quite separate from those carried out in daylight under different weather conditions.[18] Even at this early stage, night fighting did not seem to be a priority for Dowding. Failure to deal with this expeditiously would later be one reason for his undoing.

Tizard noted in a memo on 3 September that the longer the time lapse to interception and the more frequent the changes of direction of the bombers, the more likely it was that the error in dead reckoning would increase, necessitating the need for direction finding (D/F) or other methods. He emphasised that the object was to effect interception of enemy aircraft in the shortest possible time, but certainly to intercept them before they crossed the coast on their return journey.[19]

Continuation of the Biggin Hill interception trials until April 1937 demonstrated that 85% of twenty experiments had 'advanced to a stage at which the fighters had been navigated to within three miles of a bomber even though it was changing height, speed and course'. The changes that were made due to the discovery of flaws in the D/F system during the Biggin Hill experiments illustrated that these exercises were foundational for the development of RDF as a vital part of air defence.[20]

Investigations on multiple interceptions continued in early 1937 but were hampered by the slow speed of the Westland Wallace aircraft being used as bombers, so Sholto wrote to the AOC-in-C of Bomber Command, Sir John Steel, requesting that he liaise with Dowding to ascertain which aircraft would be most suitable.[21] In a meeting on 21 April 1937, it was emphasised that up to this point, no RDF had been available for these experiments, but that it was hoped that one inland RDF station to assist with the Biggin Hill exercises would be operational from July 1937.[22]

Meanwhile, work on RDF at the Bawdsey Radar Research Establishment continued, if somewhat chaotically due to Watson-Watt's informal management style. The team there were becoming adept at plotting the incoming tracks and heights of civil airliners, especially Dutch KLM aircraft.[23] However, cooperation with Biggin Hill in any potential interceptions of the KLM aircraft would have been hampered by the limited coverage of the Bawdsey station and the lack of suitable RDF stations near the coast, although one was being constructed at Canewdon

in Essex and an advanced R/T station at Dunkirk in Kent. Tizard commented drily in the meeting that interception of incoming civil aircraft 'would afford valuable experience in conditions closely approximating to what might be expected in war but that regular interceptions of foreign Air Liners would be undesirable for political reasons and should be avoided.'[24]

To address the problem of coverage all along the coast, plans for a coastal radar chain had been under way since July 1936, and Squadron Leader Raymund Hart, an RAF Signals specialist, was attached to Bawdsey to assist in its development. He became very influential in the methodology of improving and integrating the use of radar into the increasingly sophisticated system of air defence and worked closely with Sholto when he took over from Dowding as C-in-C Fighter Command.[25]

The meeting on 21 April had shown that there was still a reluctance to conduct experiments in night interception due to the extra challenges involved, although Dowding suggested that a limited number of these should be made and could run concurrently with those examining the control of multiple formations.[26] The exercises continued through 1937, and began to address something that was on everyone's mind: how would our fighters differentiate between friendly and hostile bombers by day and also by night?[27] Bawdsey had the nucleus of a method but considerable time would elapse before it was established.

A further problem was the probability of deliberate radio jamming by an enemy, necessitating alternative R/T systems that would operate over a narrower frequency band. Deliberate jamming by German and French broadcasting stations was being experienced every time an exercise was held but could be mitigated to some extent by avoiding certain frequencies. It was proposed that an outside source such as the GPO or the Admiralty could provide organised jamming for the experiments.[28]

In November 1937, Dowding suggested that the Interception Experiments be transferred from Biggin Hill to the Air Fighting Development Establishment (AFDE) at Northolt,[29] but this idea was quickly countered by Sholto and Group Captain Robert Saundby, Deputy Director of Operations at the Air Ministry (and a significant figure later in the War as Deputy AOC-in-C Bomber Command), because of the installation of new equipment at Biggin Hill and its proposed use in conjunction with the Dunkirk RDF station. Nevertheless, they agreed that, in future, all experimental work of a similar nature should be centralised at AFDE.[30]

There was continuing tension between the Air Ministry and Dowding over these exercises, evident in a letter sent by Dowding to Sholto on 20 December 1937 in which Dowding said that he had received a copy of a programme for the next round of interception experiments that the Station Commander at Biggin Hill had been instructed to carry out, but which had come to Dowding's notice by chance. He said that he proposed to carry out his own series of experiments that would limit the use of *his* RDF stations for the Biggin Hill trials to times when they would not be required by his team, and that, in future, all instructions concerning

experimental programmes for Biggin Hill should be sent through his HQ.[31] Dowding received a reply not from Sholto but from Saundby stating that certain paragraphs in Dowding's letter 'suggest that some misunderstanding exists regarding the detailed arrangements for these experiments.' Saundby reminded Dowding that events had proceeded entirely in the manner agreed by Dowding himself at the meeting on 21 April 1937, and that close communication had been maintained between Bawdsey and Fighter Command HQ, between Tizard and Dowding himself, and between RAF Biggin Hill and the Directorate of Research at the Air Ministry. He stated further that the programme that had come to Dowding's notice had been devised by the CO of Biggin Hill, not by the Air Ministry, and that there had been no question of instructions being issued to Biggin Hill directly without reference to Fighter Command HQ.[32]

Despite these hiccups in communication, the Biggin Hill experiments continued and without them, 'it is doubtful whether Fighter Command could have been adequately prepared for the Battle of Britain. Apart from their value in developing new interception techniques, the exercises brought other advantages. The sector commander at Biggin Hill was emphatic that one of the benefits of the new system was the great confidence it gave to pilots in the air. They learnt the value of accurate flying. When a method was evolved, primitive at first, to ensure that pilots' positions were always roughly known to their commanders on the ground, they knew that they could always be brought home in difficult conditions. This was an essential part of the new tactics and had an immense moral effect. An important feature of the Biggin Hill experiments was their freedom from undue guidance from higher authority. The operational flying problems anticipated on account of the development of radar were allowed to work themselves out in the hands of competent men at squadron and sector level. In consequence the results of the experiments were essentially practical and well fitted for adoption by those on whom the task fell in war.'[33]

## The run-up to World War Two

At the beginning of 1938, only 18 months after Sholto's promotion to Air Commodore, he was promoted to Air Vice-Marshal, and with that he hoped that he would be posted to an operational command, having been a staff officer at the Air Ministry for the past five and a half years. However, instead of a command of his own, Sholto was appointed to a newly created post, that of Assistant Chief of the Air Staff (ACAS). In his new post, Sholto was to serve directly under the CAS, Cyril Newall, and to be responsible for the Directorate of Staff Duties, which he had headed for the past two years, and the Directorate of Operational Requirements. He was involved still with the Biggin Hill interception experiments and the development of AI for use at night. He also insisted on being kept abreast of developments in the technology to identify friendly from enemy aircraft, termed 'Identification Friend or Foe' (IFF).[34]

Just after Sholto had been promoted to Air Vice-Marshal, Tizard wrote a letter to him, saying that his promotion might mean a move away from the Air Ministry, which would be bad from some points of view.[35] It is clear from correspondence between them that Sholto was in

the vanguard of the Air Staff's communication with Tizard, seeking to 'ensure a closer liaison between the Air Staff and your Scientific Committees in the study of air tactics and equipment generally.'[36]

Tizard's valuable work with the Air Staff was too often disrupted by the clash between him and Churchill's scientific adviser, Professor Lindemann, who consistently pressed his own agenda for such outlandish ideas as 'aerial mines' and undermined the committee's valuable work on radar. Sholto wrote that Lindemann never really believed in radar, which was problematic when he had the ear of Churchill. No doubt ironically, Sholto even called Lindemann 'the evil genius of radar' and thought that he was not a very good scientist,[37] but he was a good statistician, and it was in this latter guise that he was useful to Churchill.[38]

Sholto regretted that the Air Staff had not made more use of Tizard's other Committee, for the Scientific Survey of Air *Offence*, which had been formed in 1936. In December 1938, Sholto became a member of both Tizard Committees and used the opportunity provided to keep his Air Tactics section fully up-to-date with all their developments.[39] On the Offence Committee, he also worked with Tizard to devise a realistic programme for the resolution of problems regarding a possible bomber offensive against Germany, especially difficulties with navigation and target identification and bombing by night.[40]

In July 1938, Watson-Watt had put forward to the Air Staff a proposal for the formation of an inter-Service committee on RDF to keep all three Services informed of progress in RDF research, development, application and production, to be chaired by a member of the Air Staff. Sholto was chosen to be its chairman.[41]

Six days after Chamberlain's 'Peace in our time' statement following the signing of the Munich agreement with Hitler on 30 September 1938, Sholto held a meeting to discuss emergency measures to increase war readiness. It was agreed that work on the Radar Chain should be stepped up to reach completion by 1 April 1939. A further meeting was arranged to thrash out how these measures would be implemented practically by the projected deadline. The day before the Munich Agreement was signed, the process had begun to move the Filter Room from Bawdsey to Bentley Priory, Fighter Command's HQ. The assembly of the Filter Room was carried out with amazing speed so that it was able to take control on 8 November staffed by experienced personnel from Bawdsey.[42]

In the year that was gained between Munich and the actual outbreak of WWII, the rate of RAF expansion began to outstrip that of the *Luftwaffe*, particularly in those vital areas of air defence - fighter aircraft and radar - so that by September 1939 there were at least enough modern fighters for the British to make a stand, supported by a radar screen that seemed largely effective, but which needed further development. Sholto wrote that those in the Air Ministry had been hardened to panic 'in the forge of fright'[43] over a long period of time, having observed the mass bombings carried out by the Germans and Italians in Spain.

Further progress in radar interceptions was made during 1939, causing the physicist A P Rowe, who had by then replaced Watson-Watt as Superintendent of the Bawdsey Research Station, to invite Dowding to a demonstration at Martlesham, near Woodbridge in Suffolk on 16 June. Unfortunately, this did not go well as the pilot of the Fairey Battle that was being used to monitor progress made a very bad landing, causing Dowding to remark: 'that the most important thing is to land the aircraft the right way up.' Barely two weeks later, Dowding attended a conference at the Air Ministry convened to consider problems with interception. Orange remarked that: 'Although Douglas was chairman, several scientists had been invited to attend and were able to give substance to the discussions.'[44] This implied criticism of Sholto was wholly unjustified. Dowding reported on the success of the Biggin Hill trials and said that radar detection from British coasts was now possible up to a range of 60 miles, but at that distance the radar operators could not distinguish between friendly and possibly hostile aircraft, something of which Tizard, also present at the meeting, was acutely aware.

However, progress was made on AI, a special preoccupation of Sholto's.[45] In early July, Dowding was given a flight demonstration, in a single-engined Fairey Battle fitted with an AI radar set, of a successful interception with a target aircraft. He wrote an enthusiastic report to the Air Ministry on 10 July, recommending that a twin-engined fighter with a two-man crew might be used for further tests and suggesting the Blenheim, used for both bomber and fighter operations, as a possible candidate. On 14 July, as a result of Dowding's report, Sholto initiated a scheme in which a Blenheim was fitted with AI radar in order that the tactical use of the equipment could be worked out. This was to be given top priority. Furthermore, he instructed that 21 AI sets should be made by hand, six to be given to Fighter Command, and the others to be kept for emergencies. Four Blenheims were to be equipped with the sets, which was achieved by 30 August, and these experimental aircraft were attached to a special flight of No.25 Squadron.[46] A day later, war was declared.

## World War Two

At a meeting of the Inter-Service RDF Committee on 19 September, Sholto brought up the matter of AI development yet again, and Watson-Watt told the Committee that arrangements were being made to equip a further 144 aircraft with AI, firstly more Blenheim fighters, and subsequently Bristol Beaufighters. At the next meeting on 23 October, Sholto enquired on progress with the production of AI sets and stressed that every first line Blenheim fighter would need to be equipped with one of these, necessitating the provision of 336 sets, and that the Beaufighter installation would commence the following year in May or June.[47]

The next few months saw further timely improvements in radar development. Although the series of radar stations around the coast, Chain Home (CH), were operational, the fact that they could not detect aircraft flying below 1,000 feet meant that another layer of protection, named Chain Home Low (CHL), had to be installed. The first of these low-looking radar stations was opened on 1 November 1939. Nevertheless, there were still gaps in the coastal coverage and inaccuracies in estimation both of altitude and numbers of aircraft above three.

United Kingdom radar coverage as of 3 September 1939. Reproduced from Michael Bragg, RDF1, Plate IX.
© Dr Philip Judkins. Reproduced with his kind permission.

Additionally, there was a 90-second time lag between sighting by a radar operator to the plot appearing on group and sector tables. As late as 8 March 1940, Dowding wrote that radar was 'very capricious and unreliable, but it is better than nothing, as being the best evidence we have of what is going on over the sea.'[48]

On 14 March 1940, at the instigation of Dowding and Tizard, a 'Night Interception Committee' was formed, to coordinate all the efforts being made to solve the problems of defence against night attack and to apply practically the research and development being done on night interception. The Committee comprised scientists including Tizard himself, Sir George Lee (Director of Communications Development at the Air Ministry) and Watson-Watt, and Service officers including Dowding, Sholto, who took the chair at the early meetings, and Raymund Hart, as well as Army representatives. The topics under discussion over the next few weeks were the development of radar equipment and techniques, aircraft detection using infrared apparatus, the use of aircraft-towed flares to provide illumination of the enemy and advances in anti-aircraft (AA) gunnery and searchlight capability. At the first meeting of the Committee, the Fighter Interception Unit (FIU) was formed and was thenceforth based at RAF Tangmere. This resulted in the first airborne radar intercepted 'kill' in history, achieved on the night of the 22/23 July 1940, when a Blenheim intercepted an enemy Dornier Do 17 aircraft and sent it plunging into the sea off the Sussex coast south of Bognor Regis. The German crew was rescued later.[49]

Progress was also being made on strengthening both CH and CHL. Unfortunately though, IFF was not yet operated at CHL frequencies. This was pointed out at a meeting of the Air Ministry RDF Panel in July 1940, when it was realised that it was essential that IFF should be extended to these aircraft to distinguish between enemy aircraft engaged in mine laying or other low altitude operations and low-flying friendly aircraft.[50]

Furthermore, there were shortcomings in the early warning CH radar stations. They were unable to indicate accurately the number of aircraft in a group and were inconsistent when reading aircraft altitude. Radar was being pressed into use before it was fully developed, and it became a race against time in which waiting for improved equipment inevitably meant delays.[51]

## Night Fighting

During the Battle of Britain, Sholto became dissatisfied with what he felt was Park's failure to deal with the new threat of enemy night raids that began on 7 September 1940, the Blitz. On 28 September Sholto sent a letter to the CAS and VCAS, with a copy sent to the Director of Operations (Home), Air Commodore Donald Stevenson, which stated that in Park's report of 12 September, he had dealt 'almost entirely with day fighting; night fighting is barely mentioned, save for a brief reference in the final paragraph.'[52] In fact, Fighter Command was making desperate attempts to develop a night-fighting capability. The problem was that the use at night of Hurricanes and Defiants not equipped with radar, known as Cat's Eye fighters, something that Sholto had championed as a stopgap,[53] greatly increased the Command's

accident rate. In the period 10 July to 11 August, out of 115 accidents, 28, fully one quarter of the total, occurred during night flying practice. Six of them were fatal. This high price was in no way compensated by success in night interceptions. All those involved knew that the Beaufighter equipped with AI manned by a skilled radar operator was the answer, but the first of these aircraft had not become available until 27 July.[54] It was mid-September before a squadron of them became operational,[55] and mid-October when the first successful interception was made and an enemy bomber shot down.[56]

Earlier, at a meeting on 11 September that was a precursor to the Salmond Night Air Defence Committee, at which both Sholto and Dowding were present, Sholto emphasised that the various methods of controlling interception referred to in the agenda for the meeting were nothing new, but that their application at night might be extended, specifically the control of AI night fighters by sub-controllers at selected forward positions, implying a decentralisation of operational control. Dowding reported that the adaptation of RDF to searchlights was promising, but as was confirmed later, these lights had only a limited range and pilots could not use searchlights to detect enemy aircraft flying at heights of over 10,000 feet.[57] Above 12,000 feet, they could not even see the searchlight beams, even on 'bright and clear nights.'[58] To address this problem, Sholto introduced an idea that he had received from the Ordnance Board for the use of naval star shells in AA guns. These were very powerful and could be used to light successive strips of cloud in the path of a raider flying above cloud and out of reach of searchlights. Fighter interception would be facilitated by the silhouette of the raider seen against the lighted cloud. He recommended that star shells be given a trial.

On 16 September, at the first meeting of the newly formed Salmond Committee, Sholto proposed that the control of operational aircraft at night should be vested in the sector commander instead of being under the control of Group HQ as it was at present, and when RDF stations became available for controlled interception work only, interception over the sea should be controlled by the RDF station itself. Sholto also took the opportunity to criticise Fighter Command's practice of filtering RDF information, suggesting that it should be given straight to Groups to speed up the process of night interception. This proposal received support from Air Vice-Marshal Arthur Tedder, who was working in the Ministry of Aircraft Production (MAP) and who was also present at the meeting. Sholto's third suggestion was for the immediate formation of a Night Fighter Training Unit combined with a Tactical Development Section and incorporating searchlights. The Committee understood that Fighter Command would need more staff specialised in night fighting both at Fighter Command HQ and at Group level to implement these changes.[59]

All these recommendations were reiterated at an Air Council meeting on 24 September, principally by Sholto, and it was decided that Dowding should be consulted on the location of the proposed Night Fighter Training Unit. The development of radar operation using searchlights, Searchlight Control Radar (SLC), nicknamed 'Elsie', was underway, the responsibility for which had been given to MAP, which was hastening its production. Despite pressures due

to the scale of daytime attacks, MAP was also attempting to expedite the development of everyone's preferred option, the AI-equipped Beaufighter.[60]

However, in his response on 27 September to the findings of the Salmond Committee, Dowding stated that the Committee had been under a misapprehension as night operations had normally been controlled by sector commanders for several years! Regarding decentralisation of filtering, in his reply Dowding dismissed this too, saying that it had been suggested earlier in the year when he thought that he had disposed of it. Dowding felt that the suggested Night Fighter Training Unit could be built up on the existing Fighter Interception Unit without any large increase in establishments, and the extra staff recommended by the Committee at HQ and Group level could be of lower rank and less numerous than the Committee members had proposed. Furthermore, he was anxious to keep a small portion of night-trained pilots in the day Squadrons, deploying them to take part in night operations only in certain locations when day activity was not intense. He felt that the withdrawal of existing experienced 8-gun fighter pilots for the benefit of a Night Fighter Training Unit would hamper his plans.[61]

Nevertheless, Dowding was making strenuous efforts to improve night interception, but considerable difficulties were encountered both with AI, and with the gun-laying (GL) RDF systems used by AA guns at night to track enemy aircraft, but by 21 September, encouraging results were achieved with GL sets in the Kenley sector, which proved to be more accurate than either the Observer Corps or even RDF stations on the South Coast. But success in tracking still did not mean effective interceptions of enemy aircraft.[62] General Frederick Pile, the C-in-C of AA Command, wrote in his memoir: 'The teething troubles with radar were enormous. By the beginning of October 1940 we had not succeeded in firing a single round at night. It was bitterly disappointing - we got the sets rigged up in wonderful time, but then we had the greatest difficulty in calibrating them. Every plan we made broke down and always from causes beyond our power to deal with. The whole GL technique was so empiric that many were the disappointments we had to endure before radar settled down into the killer it became.'[63]

As for Sholto's suggestion of using RDF over the sea for interception, Dowding observed that this would be possible, but it was a refinement that could not be allowed to interfere with existing trials to determine the accuracy of searchlight radio sets or Elsies. His experiments with this equipment were useful in that they showed that Elsie was incapable of being used as a short-term expedient until the problems with GL sets had been addressed, because it could not locate aircraft in cloudy weather or at heights above 10,000 feet. Additionally, it did not respond to IFF then fitted to Blenheims and Beaufighters and so could not distinguish friendly from enemy aircraft. So Elsie could only be used as a searchlight pointer, and Dowding postulated that the real solution to night interception, which was realised in 1941, would be the use of GCI, used in conjunction with AI in aircraft.[64] The advantages of GCI were that it had a longer range than the GL set, and it was possible to track both enemy bombers and British fighters by the same equipment instead of following one with GL and the other with

radiotelephone direction finding (R/T D/F), the accuracy of which was inadequate for night interceptions.[65] However, GCI also had its teething troubles, notably 'gaps' in its coverage at a range of 15 or 20 miles, but Dowding was optimistic that a height finding feature would be included in it that would enable better interception, and meanwhile, he hoped that Elsie's ability to gauge the altitude of aircraft would be improved also.[66]

Problems were also encountered with the Beaufighter and in his report of 30 September, Dowding wrote that not more than one of these aircraft had been in the air on any night, and that such flights as had been made were often terminated prematurely due to breakdowns in AI equipment, which was susceptible to damp, or technical difficulties with the Beaufighter itself. The Blenheims however had had greater success and had shot down one or possibly two enemy aircraft in the preceding week. Dowding's next report of 11 October emphasised the Blenheims' continuing success despite their earlier version of AI and inferior performance versus that of the Beaufighter, whose bullet-proof windscreens were more susceptible to icing when descending through cloud from altitude.

At the second meeting of the Salmond Committee on 1 October, Dowding said that transferring filtering directly to Groups would not improve the efficiency of night interception. Furthermore, it would be extravagant in his view, and then there was the difficulty of recognition and identification of aircraft. This would be largely solved when IFF was generally fitted and working.[67] Dowding opposed the Air Staff's belief that Group filtering would save time, which assumed that Operations and Filtering work could be done on the same table, thereby removing the need for 'telling' plots between the two functions. Unfortunately, calculations of the size of table that would be needed showed that it would be so large (50 x 60 feet) that manual plotting during intensive operations would be impossible, so separate tables using the existing arrangements continued.[68] Nevertheless, in the meeting the Air Staff, including Sholto, insisted that filtering should be devolved to Group level as soon as IFF had been installed more widely, which was due to be completed in November of that year, and as for Dowding's rather parsimonious concern about extravagance, the Air Staff was of the view that the damage being caused by day and night bombing was ample justification for the extra expenditure.[69]

Interestingly, by May 1941 when Sholto had replaced Dowding as C-in-C Fighter Command, he was having second thoughts about decentralisation of filtering. He wrote to Portal, now CAS: 'My predecessor was strongly opposed to decentralisation…I think the present centralised system works quite well from the point of view of efficiency, and I do not think there is much to be gained by the proposed change.'[70]

Although Dowding was being challenged at every opportunity, without his meticulous approach in tackling each obstacle to effective night interception, the system that evolved eventually would not have been possible. However, his careful plan was not solving the current problems. During the month of September, the *Luftwaffe* had flown an estimated 6,135 sorties at night, yet only four German bombers had been destroyed by fighters.

This small number had to be offset against 1,500 civilians killed in the week ending 26 September, 1,300 of whom lived in London. A further 1,700 were killed there during the following seven days, quite apart from the heavy damage sustained.

Perhaps the greatest blow to Dowding's handling of night air defence, which was instrumental in his removal from Fighter Command, was the devastating raid on Coventry, which took place on the night of 14 November 1940, when more than 4,300 homes were destroyed and around two-thirds of the city's buildings were damaged. An estimated 554 people were killed (the exact figure was never precisely confirmed), with another 865 badly injured,[71] and 393 sustaining lesser injuries. Fighter Command flew 125 night sorties but failed to shoot down a single *Luftwaffe* bomber, the blame for which was laid at Dowding's door.[72]

Four days after the Coventry bombing and a week before he replaced Dowding as C-in-C Fighter Command, Sholto wrote a paper precisely articulating what he thought needed to be done regarding night interception. His ambitious recommendations included the provision of 24 specialist night fighting squadrons instead of the current ten, which should be located in a semi-circle from Newcastle in the north round to Prawle Point in Devon, with a special squadron each for Coventry/Birmingham, Liverpool and Glasgow. Regarding methods of deployment, two or more Beaufighters should work over the sea in the forward part of each sector, controlled by CHL stations and later by GCI stations as these became available, augmented by AI. Further back, there should be a 'half-back' line of Defiants or Hurricanes working with Elsie controlled searchlights. Lastly, over the actual targets being attacked, there should be a 'full-back' or 'goal-keeper' line of Beaufighters, Hurricanes or Defiants operating with the RDF methods enumerated thus far, but with the aid of star shells should the experiments with these prove successful. More control facilities would be needed, and to this end, better trained controllers. A school for these had just been started at Uxbridge. Additionally, more and better aerodromes with 100% night flying facilities were required, including those for blind landing in zero visibility, homing beacons and AI. Sholto insisted on intensive specialist training for personnel involved in night flying and wrote that the recent formation of a night fighter Operational Training Unit (OTU), for which he had been pressing for a long time, was a step in the right direction. All pilots and gunners, before selection for night fighter duties, should be tested for night vision. Finally, Sholto observed that radar scientists were complaining that one of the reasons why better results were not being obtained was indifferent maintenance, so he proposed the allocation of engineers or scientific officers to each Night Fighter Wing, in the same way as scientific officers were being allocated to AA batteries.[73] Tizard fully supported Sholto's observations, stating in a note written at the end of December that the disappointing results from AI were due to 'lack of training, maintenance and good engineering, not to lack of science.'[74]

## Fighter Command

In the two years that Sholto spent as C-in-C of Fighter Command, by far his greatest difficulty was 'what happened under cover of darkness.'[75] He wrote in a report later: 'The burning

question…was how to stop the Hun's night bombing. I was sent for by Winston, who told me that I had to concentrate everything on stopping the bombers. Every facility would be placed at my disposal.'[76] By the end of 1940 there was still no answer to the German night bomber. Sholto wrote in a report on 8 December, two weeks after taking over Fighter Command: 'It cannot be said that, since my predecessor's last report on 17th November, any great success in night interception has been achieved…In nearly 500 sorties, only 31 enemy aircraft have been sighted.' Sholto had been visiting fighter squadrons in the South of England, and had identified problems with night interception, such as the inaccuracy both of tracking enemy aircraft inland from the coast and of assessing the height of enemy bombers. He welcomed a proposal by General Pile to install a 'carpet' of GL radar sets along a 60-mile belt from Kent to Bristol to address these problems and had even asked for Dowding's views on this plan. All the other devices that had been trialled had yet to prove their worth, including AI, although Sholto had visited stations where research was being carried out and was most impressed with its performance, 'even in its present immature state.'[77]

In the same report, Sholto reasserted that there should be more specialised night fighter squadrons. He only had 11 of these, but wanted at least 20 as soon as possible, including 12 comprised of twin-engined fighters fitted with AI. An adjunct to Sholto's report, which he wrote on 14 December, reiterated his suggestion of Fighter Regional Control Aerodromes specially equipped for night fighters. To improve radio control at these aerodromes, Sholto advised that specialised Control Officers be employed, including, as he also suggested for pilots, transferring professional Control Officers from Civil Aviation for war service.

AA Command was almost three times as successful as Fighter Command in shooting down bombers, claiming 102 enemy aircraft at night between June and December 1940 as against 35 shot down by fighters. German night raids on London did decrease in December, but there were more attacks on other cities. Civilian casualties were still high for that month: 3,793 killed and 5,044 injured.[78] The official historian Basil Collier criticised Sholto for his suggestion of using Cat's Eye fighters at night, especially in the poor weather conditions that prevailed in the winter of 1940/41. However, there were experienced pilots who supported Sholto in this endeavour, including Quintin Brand, the AOC of No.10 Group. In WWI he had succeeded in shooting down a number of enemy bombers at night flying a single-seater fighter. The prevailing opinion of the Salmond Inquiry was that the use of these aircraft at night should be tried until AI became effective.[79]

In his later response to Collier's draft of his Official History, *The Defence of the United Kingdom*, Sholto defended his advocacy of Cat's Eye fighters. Citing Collier's own Appendix 34 in the book, he wrote that several visual contacts were made by these aircraft, especially during the period January-May 1941, when they had made almost as many detections as twin-engine Beaufighters using AI. It is hard to see how Sholto arrived at this conclusion, since a glance at the figures shows that single-engine fighters made visual contact on 7.5% of sorties flown, whereas Beaufighters detected enemy aircraft by AI on 34% of sorties. However, the number of

combats made by these two types of fighters were closer in number: 39.6% for single-engine fighters and 30.2% for twin-engine aircraft. Sholto conceded that although that Cat's Eye fighters could only ever be a fair-weather weapon at night, and this is borne out by the figures, he asserted that this was being wise after the event, since at the time, it was necessary to try anything as Beaufighters were still in such short supply.[80]

In a letter to Portal on 9 December 1940, Sholto wrote: 'I do not think that Hurricanes, Spitfires or even Defiants will ever be anything but "fine weather" night fighters.' He ended his letter with an impassioned plea: 'I do feel most strongly about this. It is vital to defeat the enemy night bomber - we may even lose the war if we don't', adding: 'Actually I think my demand is really a modest one.'[81] Nevertheless, Sholto tried to make use of Cat's Eye fighters by instigating what he called 'Fighter Nights', when large numbers of these fighters were sent up in high concentrations on nights of good visibility.[82] But this form of patrol, even in ideal weather conditions, was profitable only in an area of concentrated enemy activity, such as over London on 10 May 1941.[83] Another priority was to have GCI sets installed at all Fighter Command Sector Stations, especially those near London, which was recognised as 'by far the most important development in the Command.'[84]

However, the solution was closer than Sholto realised. Soon after he had settled into Bentley Priory, he was pleased to receive Trenchard as one of his many visitors. They discussed the difficulties that Fighter Command was having with its radar-equipped night fighters, and Trenchard said: 'Never mind, Sholto, you take my word for it…a man will arise.'[85] In fact, on the night of the 20 November, three weeks before Trenchard's visit, an event had occurred that heralded the fulfilment of Trenchard's prophecy. The Germans staged the second of three nights of heavy raids on Birmingham. One of the night fighters in the skies that night was a Beaufighter of No. 604 Squadron, stationed at Middle Wallop in Hampshire. It was flown by Flight Lieutenant John Cunningham with Sergeant John Phillipson as his radio observer. They managed to intercept and shoot down a Junkers 88. One month later on 20 December, the same team shot down another raider, a Heinkel that was part of a heavy force of enemy bombers that attacked Liverpool and Birkenhead.

Nevertheless, problems with the radar chain continued into 1941, made worse by the latest enemy tactic: German bombers were flying at heights of 50 to 100 feet above sea level, attacking shipping travelling along the east coast of the UK. CHL was of little use in combatting this menace. The Telecommunications Research Establishment, as it was now known, relocated from Bawdsey to Worth Matravers near the Dorset coast, suggested altering the position of CHL aerials and increasing the power of CHL at shorter wavelengths.[86]

Over the next few months, the number of engagements with the enemy rose, as did the number of aircraft destroyed, from two in the whole of January to 65 in the first week of May alone.[87] By the end of January, when Sholto had been at Fighter Command just two months, the GL 'carpet' that Pile had suggested had been installed with the exception of wire mats that

were to be laid at GL sites to improve their accuracy.[88] Although this carpet was supposed to be a temporary expedient, the initial slowness both of progress in GCI and in the supply of AI/GCI night fighters meant that it continued to operate for many more months.[89] However, by the end of July, increased use of GCI and improvements in Elsie meant that Sholto could dispense with the GL carpet for the South of England.[90] In fact it was found impractical to keep GCI and searchlight areas apart, so arrangements were being made for these to work together.[91]

The end of January also saw the completion of another of Sholto's ideas, a new searchlight layout in clusters of three to improve detection of night raiders. However, he was still desperately concerned about the slow supply of night fighter aircraft to the Command, and the shortage of well-trained night fighter pilots he described as 'serious.' The total number of night fighter squadrons of all types had risen by only two to 13. He wrote that he had 'appealed to the Air Ministry for assistance' and had renewed his request for ex-night bomber pilots who had for the time being finished their allotted span of operational flying over Germany. He had been against this idea the previous year, but now the desperate reality of enemy night attacks that it was his responsibility, as C-in-C Fighter Command, to stop had caused him to change his mind completely.

In a letter to the Air Ministry written in March, Sholto wrote that on two nights in that month, six Beaufighter sorties destroyed ten enemy aircraft, whereas 431 Cat's Eye fighters only accounted for five 'in the most favourable conditions possible for them.'[92] Watson-Watt added his support to this conclusion, observing: 'GCI makes an AI aircraft about five times as effective in producing night combat, and about six to seven times in destruction or damage as is the AI aircraft with other forms of ground control or on patrol.'[93] Meanwhile, Sholto had the continuing problem of enemy attacks being mounted at lower altitudes, possibly to avoid detection by AI and GCI, since AI became ineffective when close to the ground and GCI could not see enemy aircraft at low altitudes. However, Sholto proposed illuminating these aircraft more effectively with searchlights so that they would be once again forced upwards.[94]

Another idea that Sholto had was to use plan position indicator (PPI) tubes[95] fitted in CHL stations that would work with AI and GCI to improve detection of these low flyers. He also proposed that the wavelength at which AI then operated be altered to attenuate the decrease in its effectiveness at low altitude due to reflections from the earth's surface or from the sea. He also thought that single-engine fighters aided by Elsie searchlights might be another solution to the problem.[96]

Sholto kept up his incessant pressure on the Air Ministry to provide more aircraft such as Beaufighters and Douglas Bostons/Havocs to form more twin-engined night fighter squadrons. Over the next two months, despite aircraft and pilot shortages, the success of AI coupled with GCI continued to accrue, night interceptions aided by such developments as the fitting of an improved version of IFF in aircraft, which responded to the GCI frequency and made the identity of the fighter plain.

7 May 1941, King George VI talking with C. F. (Jimmy) Rawnsley, John Cunningham's navigator (sixth from left), just before they went off on patrol and shot down a Heinkel, which the King observed. Sholto called this episode a 'Command Performance'. He is standing with his back to the camera. Cunningham is on the extreme left and Group Captain Elliott, Station Commander at Middle Wallop, is standing next to Sholto. Collection of Katharine Campbell.

Sholto was trying all sorts of other methods to increase the likelihood of successful night interceptions and the destruction of enemy night raiders. These included various ways of illuminating hostile aircraft, such as flash flares, 4.5-inch naval star shells and Helmore Searchlights carried in the nose of aircraft. Bad weather, particularly when there was a 'haze', hampered the effectiveness of both the flares and the shells, and the latter only really worked when there was perfect coordination of the firing of the shell with the appearance of the target aircraft.[97]

The airborne searchlights showed promise, but Sholto felt that more experiments were needed. Meanwhile the telephone communication network between ground searchlight stations was a top priority, in order that searchlight and fighter efforts could be properly coordinated. One of the greatest dangers in cooperation between fighters and radar-operated ground searchlights was of the searchlights illuminating the fighter itself rather than the raider that it was approaching. Sholto therefore found it a matter of grave concern that no means of responding to IFF signals from aircraft was incorporated into the Elsie equipment.[98]

In the next Night Air Defence Committee meeting on 12 May 1941, chaired by Churchill, Sholto continued to press for more Beaufighters equipped with AI and aided by GCI. The VCAS, Air Chief Marshal Wilfrid Freeman, suggested that Bostons/Havocs would do just as well, but Sholto was most insistent on Beaufighters. In this and in every other point that he made at the meeting, he was backed up by Churchill.[99] By the end of June, Beaufighters were being produced in sufficient numbers to convert to these aircraft squadrons operating older types, but Sholto was concerned by the shortage of AI operators and radio mechanics to service AI both in Beaufighters and in Defiants that were to be newly supplied with AI. However, he noted that enemy night attacks were decreasing, and tracings of the tracks of enemy aircraft over the UK revealed that on many occasions their paths were erratic, which, coupled with the fact that they were not flying high,[100] suggested that they had not been using their beam navigation system.[101]

A month later, Sholto wrote that experiments with searchlight clusters had shown them to be less effective than single searchlights spaced at intervals of 6,000 yards and equipped with Elsie.[102] By the end of October, just as Sholto had managed to get the twelve Beaufighter Squadrons on which he had insisted at the beginning of the year, he had to release the aircraft, pilots and AI operators for a complete night fighting squadron to the Middle East. Demands such as this would inevitably postpone further expansion of the night fighter force that he had fought so hard to build up.[103] He raised this issue in the next Night Air Defence Committee Meeting over which Churchill presided. Churchill said that the weakening of Fighter Command to strengthen the Middle East must be accepted to meet air attacks on the Suez Canal and the Nile Delta.[104] In this, Churchill was supported by Portal and Sinclair, although they were both concerned that, if attacks against the UK increased the following spring, there should be enough home defence squadrons to repel them.[105]

## Low altitude flying and enemy jamming

As winter turned into the spring of 1942, despite the opening up of the Eastern Front, it became clear that the Germans had maintained a force of some 200-250 bombers in the West, available for night operations against the UK. Their principal operations included minelaying, followed by attacks on shipping and lastly raids against land targets on the British mainland. German operations over the sea were conducted at low altitude, making interception difficult. So as well as decreasing his own losses, the enemy inflicted considerable damage on British shipping. Sholto considered that to counter this threat, the range of the GCI stations would have to be increased. Experiments using two CHL stations for interception purposes had also met with success, these having a range of 60-65 miles compared to the 35-40 miles of ordinary GCI stations. Sholto proposed that a further 18 CHL stations be adapted for the interception role.[106] Three months later, Sholto had discovered that the use of AI in conjunction with Elsie could lead to faster interceptions, and he wrote that he had restricted the use of GCI/AI fighters to operating over the sea while Elsie 'belts' provided the next line of defence inland, thus minimising complications arising from the simultaneous operation of GCI and searchlight-controlled fighters within the belts.[107]

A continuing problem with which Sholto had had to contend in the winter of 1941/42 was that of aircraft identification, both from the air and from the ground. The need for greater accuracy had become more urgent with the increasing number of raids conducted by Bomber Command over Europe, and it was essential that fighter aircraft should not be involved in useless chases of friendly aircraft while enemy bombers arrived and dropped their bombs before Fighter Command was aware of their true identity. Devices had been tried such as an infra-red air-to-air identification system, but Sholto's hope for identification from the ground lay in the latest Mark III IFF. However, this would not be produced until July, when Bomber Command aircraft would be the first to be fitted with it.[108] Six months later, much to his frustration, Sholto stated in his report to the Night Air Defence Committee that although the infra-red system showed promise, the new form of 10-centimetre (10 cm) AI did not respond to Mark IIG IFF and Mark III had still not been introduced.[109]

Sholto expected that the changes to the ground element of radar would be accompanied by the rapid introduction of newer marks of AI that operated on the 10 cm wavelength, which was designed to operate at lower altitudes, as opposed to the 1.5 metre (1.5 m) wavelength in general use up until that point. A few of these new AI sets had been used already with considerable success, and Sholto felt that 10 cm AI would prove to be a most valuable asset to the UK's night defence,[110] being much more resistant to enemy jamming.[111] GCI was also vulnerable to interference, but this would also be countered if mobile GCI stations were operated on variable frequencies using a shorter 50 cm wavelength than the 1.5 m wavelength currently in use.

In a memo for the Night Air Defence Committee, Tizard confirmed Sholto's observations, the Germans having effectively jammed the 1.5 m equipment in an area east of a line from Selsey to Gravesend from land jamming stations on the north coast of France. The supreme example of jamming came on 12 February 1942 when it enabled the Channel Dash: the escape of the battlecruisers *Scharnhorst* and *Gneisenau* and the heavy cruiser *Prinz Eugen* from the port of Brest up the English Channel to their home port in Kiel.[112] Use of the new form of AI still depended largely on skilled ground control from GCI stations fitted with 1.5 m equipment and on radio communication within the 2.5 m waveband, both of which were susceptible to enemy jamming. Therefore, Tizard reiterated Sholto's suggestions to provide mobile GCI stations working on variable frequencies and the use of Elsie in conjunction with AI but operating on a different band to the 1.5 m wavelength on which it operated at present. Tizard also suggested organised attacks on the enemy ground jamming stations at the right time and the interception of jamming aircraft by 'specialised machines.' In order to implement these changes, more staff would be needed.[113] Following Tizard's memo, Sholto was informed by the Air Ministry that his views on the need to insure against enemy interference had been fully accepted.[114] In a meeting a few days later at which Tizard, Sholto and Churchill were present, Sholto reiterated that every effort should be made to improve jamming countermeasures, particularly those involving ground to air communication.[115]

By September, although there was no evidence that enemy jamming aircraft were being used against the UK, their use was being reported in the Middle East and Malta. However, extensive jamming was being used primarily against CHL and GCI stations in the UK from the enemy ground stations along the French coast. Sholto reiterated his demands for equipment more resistant to jamming by radio or by the use of metallised leaflets,[116] including the use of high-powered VHF transmitters with directional aerials capable of flooding any attempt to jam from the ground or from the air.[117]

## Middle East and Coastal Commands

Although Sholto's most intense contribution to radar ended when he left Fighter Command, his involvement with it continued when he was AOC-in-C Middle East Command from January 1943. He instigated a large expansion programme involving armament, signals and navigation instruction.[118] As AOC-in-C Coastal Command from January 1944, he was keen to equip his squadrons with the latest marks of air-to-surface vessel radar to combat U-boat activity,[119] both during and after Operation Overlord, insisting on extended training to maximise the equipment's effectiveness and the confidence of his personnel.[120]

## Conclusion

It is interesting that when Watson-Watt considered in his memoir the RAF officers who were for him the greatest champions of radar, he wrote: 'Sholto Douglas, (Director of Staff Duties when we first met) was imaginative, enterprising, receptive and constructive. We owed him much of our education as amateur air staff officers, perhaps too ready to teach our teachers! He was decisive and vigorous in action, and as he progressed rapidly to Assistant Chief of Air Staff, Deputy Chief of Air Staff, and Air Officer Commanding-in-Chief of several of the Commands that we hoped to serve most directly, he carried many of our hopes and potentialities with him. If I were given the invidious task of naming the Royal Air Force officer, outside the little group of those engaged wholly on radar duties, who did most to ensure that radar became an effective weapon of war, effectively wielded, I think I should name Air Chief Marshal Sir W. Sholto Douglas, K.C.B., M.C., D.F.C., now Lord Douglas of Kirtleside…'[121]

## Acknowledgements

Special thanks are due to Squadron Leader Mike Dean (retired), keeper of the Historical Radar Archive, and Group Captain Jim Beldon for reading and commenting on the manuscript.

## Notes

[1] Katharine Campbell, *Behold the Dark Gray Man: Triumphs and Trauma, the Controversial Life of Sholto Douglas* (London, Biteback Publishing, 2021).

[2] David Jordan, *Invented and Predicted Futures: Britain and the Challenge of Air Defenc*e, Freeman Air and Space Institute, https://www.kcl.ac.uk/warstudies/assets/invented-and-predicted-futures.pdf.

[3] TNA, AIR 1/589/16/15/199, Air Raids on England, Part 1, 13 June 1917.

[4] Vincent Orange, *Dowding of Fighter Command: Victor of the Battle of Britain* (London,

Grub Street, 2008), p. 80.
[5] *The London Gazette*, https://www.thegazette.co.uk/London/issue/34242/page/311, accessed 20 February 2018.
[6] IWM Collections, Personal papers of Lord Douglas of Kirtleside, Box P31.
[7] GCI was a ground-based 360° radar that plotted the position of attacking and defending aircraft on a map-like display, allowing ground control of intercepting fighters fitted with AI.
[8] AI was an airborne aircraft-to-aircraft radar system.
[9] Michael Bragg, *RDF1: The location of aircraft by radio methods 1935-1945* (Paisley, Hawkhead Publishing, 2002), p. 57.
[10] TNA, AIR 2/2625 - Flying arrangements for Biggin Hill experiments, 1936 - 1938, Letter from Douglas to Joubert de la Ferté, 14 July 1936.
[11] Ibid.
[12] Ibid., Letter from Dowding to Douglas, 'Interception Experiments - August and September 1936', 28 July 1936.
[13] Ibid., Minutes of Conference held at Headquarters Fighter Command on Friday 7 August 1936 to discuss questions concerning special Interception Experiments at Biggin Hill during August and September 1936.
[14] Royal Air Force Signals, 1939 - 1945: *Official History by the Air Historical Branch of the Ministry of Defence*, Volume V: Fighter Control & Interception, Chapter 1: Biggin Hill Experiments, p. 12.
[15] Orange, *Dowding*, p. 96.
[16] TNA, PREM 4/3/6, Appointment of Chief of Air Staff, 1 August 1940 – 30 November 1940. Anonymous memorandum '*A Weak Link in the Nation's Defences*'. Also in list of papers used by Denis Richards housed in the Lord Portal Archive at Christ Church College, Oxford.
[17] Orange, *Dowding*, p. 118.
[18] TNA, AIR 2/2625, Minutes of Conference held at Headquarters Fighter Command on Friday 7 August 1936 to discuss questions concerning special Interception Experiments at Biggin Hill during August and September 1936.
[19] Ibid., 'Interception Experiments', memo by Henry Tizard, 3 September 1936.
[20] Bragg, *RDF1*., p. 59.
[21] TNA, AIR 2/2625, Letter Director of Staff Duties to AOC-in-C Bomber Command, 16 March 1937.
[22] Ibid., Minutes of a meeting held at the Air Ministry on 21 April 1937 to draw up a programme for the Biggin Hill Interception Experiments.
[23] Ibid., Interception of K.L.M. aircraft from Biggin Hill.
[24] Ibid., Minutes of a meeting held at the Air Ministry on 21 April 1937.
[25] Peter Flint, *Dowding and Headquarters Fighter Command* (Airlife Publishing Ltd, England, 1996), p. 13.
[26] TNA, AIR 2/2625, Minutes of a meeting held at the Air Ministry on 21 April 1937.
[27] TNA AIR 2/2615, RADAR AND RADIO COUNTERMEASURES (Code B, 61), Method of deciding whether bombers located by RDF are friendly or hostile, 1936 - 1938, memo from DCAS to AMRD, 4 November 1937.
[28] TNA, AIR 2/2625, Letter from E L Gossage, AOC No.11 (F) Group to HQ Fighter Command,

28 October 1937.
[29] TNA, AIR 16/180, *Special interception experiments at Biggin Hill, November 1937 – August 1938*, memo from Dowding to HQ No.11 (F) Group, 22 November 1937. Transfer of Biggin Hill interception experiments to Northolt.
[30] TNA, AIR 2/2625, Letter from Saundby to Dowding, 16 November 1937.
[31] Ibid., Letter from Dowding to Director of Staff Duties, 20 December 1937.
[32] Ibid., Letter from Saundby to Dowding, January 1938.
[33] RAF Signals History, Vol. V, Chapter 1, pp. 19-20.
[34] TNA, AIR 2/2615.
[35] IWM, Henry Tizard Archive, HTT38, Correspondence between Henry Tizard and Sholto Douglas, letter from Tizard to Sholto, 10 February 1938.
[36] IWM, HTT 38, Letter from Douglas to Tizard, 17 November 1938.
[37] IWM, Personal papers of Lord Douglas of Kirtleside, Box P31, Letter to Wing Commander R C Wright, 18 March 1960.
[38] https://etherwave.wordpress.com/2008/11/12/hump-day-history-the-tizard-committee/, accessed 13 April 2018.
[39] IWM, HTT 38, Letter from Douglas to Tizard, 17 November 1938.
[40] Ibid., Letter from Tizard to Douglas, 30 November 1938, and reply in December 1938.
[41] TNA, AIR 2/3103, Inter-service committee on RDF: final report of CHL Planning sub-committee, 1938-1941.
[42] TNA, AIR 2/2145, Radar & radio countermeasure (Code B, 61), Sites: constructional policy, 1937-1939, in Peter Flint, *Dowding*, pp. 18 & 19.
[43] Sholto Douglas with Robert Wright, *Combat & Command: The Story of an Airman in Two World Wars* (New York, Simon & Schuster, 1966), p. 356.
[44] Orange, *Dowding*, p. 127.
[45] TNA, AVIA 12/41, Inter-service committee on RDF: meetings 1-5, 1938-1939.
[46] TNA, AIR 10/5485, Signals - Fighter interception and control, 1939-1945, in Flint, *op. cit*., pp. 27 & 28.
[47] TNA, AVIA 12/41.
[48] Orange, *Dowding*, pp. 152-153.
[49] Flint, *Dowding*, pp. 59-61.
[50] TNA, AIR 2/3107, RADAR, Air Ministry RDF Panel: Minutes of Meetings, 1940.
[51] Flint, *Dowding*, pp. 91-92.
[52] TNA, AIR 2/7281, ROYAL AIR FORCE: Fighter Command (Code B, 67/12) Tactics against German mass formations, Operations by No.11 Group Units over France, May-June 1940.
[53] TNA, AIR 20/2062, Fighter Command: miscellaneous papers, 1940 July - Dec.
[54] Stephen Bungay, *The Most Dangerous Enemy: A History of the Battle of Britain*, (London, Aurum Press, 2000), p. 195.
[55] TNA, AIR 19/230, Night Air Defence, 1940-41, Minutes of a meeting held at the Air Ministry (Whitehall) on Wednesday, September 11th, 1940, to discuss methods of night interception.
[56] Ibid., Report by Dowding on Night Interception, 28 October 1940.
[57] Ibid., Report by Dowding on Night Interception, 30 September 1940.

[58] TNA, AIR 16/524, Night Air Defence Committee, Minutes of Meetings, Reports etc., Sept. 1940 - April 1942. Reports by Dowding on Night Interception, 30 September & 20 October 1940.
[59] TNA, AIR 19/230, Air Council, Night Air Defence.
[60] TNA, AIR 6/70, Air Council, Draft conclusions of the meeting (5/40) on Tuesday 24 September 1940.
[61] TNA, AIR 19/230, Letter from Dowding to Balfour (Under Secretary of State for Air), 27 September 1940.
[62] Ibid. & AIR 16/524.
[63] General Sir Frederick Pile, *Ack-Ack: Britain's Defence Against Air Attack During the Second World War* (London, George G. Harrap & Co. Ltd., 1949). In: *The Radio and Electronic Engineer*, Vol. 51, No.1, January 1981, pp. 10-11.
[64] TNA, AIR 16/524, Report by Dowding on Night Interception, 03 November 1940.
[65] TNA, CAB 106/1193, Dispatch on the Battle of Britain, 1940-1941, by Air Chief Marshal Sir Hugh C.T. Dowding, Air Officer Commanding-in-Chief, Fighter Command, Royal Air Force (Supplement to London Gazette 37719) (H.M. Stationery Office 1946).
[66] TNA, AIR 16/524, Report by Dowding on Night Interception, 17.11.1940.
[67] TNA, AIR 19/230, Night Air Defence, Note of a meeting held on 1st October 1940.
[68] TNA, AIR 41/18, The Air Defence of Great Britain, Vol IV: The Beginning of the Fighter Offensive, 1940-1941, 1947 & TNA, AIR 20/5192, Air Raid Warnings: decentralisation, 1940 Oct. - 1945 May.
[69] TNA, AIR 19/230, Air Council, draft conclusions of the meeting (6(40) held on Wednesday 2 October 1940.
[70] TNA, AIR 2/5230, ROYAL AIR FORCE: Groups (Code B, 67/31): Devolution of filtering and issue of air raid warnings to Fighter Groups, 1940 - 41.
[71] J. B. Collier, *Official History of World War II, The Defence of the United Kingdom*, (London, HMSO, 1957), p. 263.
[72] John Terraine, *The Right of the Line* (London, Hodder & Stoughton, 1985), pp. 220-221.
[73] TNA, AIR 19/230, Night Interception, a paper written by W.S. Douglas, 18 November 1940.
[74] TNA, AIR 16/524, Night Defence, Note by Sir Henry Tizard, 31 December 1940.
[75] Sholto Douglas with Robert Wright, *Years of Command* (London, Collins, 1966) p. 101.
[76] TNA, AIR 40/307, Observations by Sir Sholto Douglas on Fighter Command when he was C-in-C.
[77] TNA, AIR 16/524, Night Interception, Report by AOC-in-C Fighter Command, 08 December 1940.
[78] John Ray, *The Battle of Britain: New Perspectives - Behind the Scenes of the Great Air War, (London, Brockhampton Press, 2000 [1994])*, p. 172.
[79] Douglas, *Years of Command*, p. 103.
[80] IWM, Personal papers of Lord Douglas of Kirtleside, Letter to J. B. Collier Esq., 14 February, 1956.
[81] TNA, AIR 16/622, Sir W Sholto Douglas, C-in-C Fighter Command: correspondence with Sir C.F.A. Portal, Chief of Air Staff, 1940 Dec.- 1942 Nov., Letter from Douglas to Portal, 09 December 1940.

[82] TNA, AIR 16/524.
[83] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 10 May to 19 June 1941.
[84] TNA, AIR 41/17 in John Ray, *The Night Blitz: 1940-1941* (Edison NJ, Castle Books, 2004 [1996]), p. 191.
[85] Douglas, *Years of Command*, p. 109.
[86] Bragg, *RDF1*, p. 262.
[87] TNA, AIR 16/524.
[88] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 8 December 1940 to 31 January 1941.
[89] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 20 March to 16 April 1941.
[90] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 20 June to 31 July 1941.
[91] Ibid., Night Air Defence Committee Meeting, 11 August 1941.
[92] Ibid., Letter from Douglas to Air Ministry, 'Expansion and re-equipment of night fighter squadrons', 22 March 1941.
[93] TNA, AIR 19/231, Scientific equipment progress meetings, 1941 - 1944, Minute from Watson-Watt to Sinclair, 25 March 1941.
[94] TNA, AIR 16/524, Progress Report by the AOC-in-C. Report on Developments and the results obtained in Night Interception for the period 1 February to 19 March 1941.
[95] PPI is a type of radar display that represents the radar antenna in the centre of the display, with the distance from it and height above ground drawn as concentric circles. As the radar antenna rotates, a radial trace on the PPI sweeps in unison with it about the centre point. It is the most common type of radar display.
[96] TNA, AIR 16/524, Progress Report by the AOC-in-C Fighter Command on Developments and the results obtained in Night Interception for the period 1 August to 24 October 1941.
[97] Ibid., Progress Report by the AOC-in-C Fighter Command on Developments and the results obtained in Night Interception for the period 1 February to 19 March 1941.
[98] Ibid., Progress Report by the AOC-in-C Fighter Command on Developments and the results obtained in Night Interception for the period 20 March to 9 May 1941.
[99] Ibid., Night Air Defence Committee Meeting, 12 May 1941.
[100] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 10 May to 19 June 1941.
[101] The German beam navigation technique and equipment (X-Gerät and Knickebein) were based on the *Lorenz* blind-landing system developed in Berlin during the 1930s. The beams were transmitted from the other side of the Channel to guide enemy bombers to their targets for the night. Coupled with this was a special Squadron of trailblazers that marked with incendiaries the targets to be bombed.
[102] TNA, AIR 16/524, Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 20 June to 31 July 1941.
[103] Ibid., Progress Report by the AOC-in-C Fighter Command on Developments and the results

obtained in Night Interception for the period 1 August to 24 October 1941.
[104] TNA, AIR 16/525, Night Air Defence Committee: Minutes of meetings, Reports etc., November 1941 – August 1943. Night Air Defence Committee Meeting, 17 November 1941.
[105] TNA, AIR 8/316, Reinforcements for Middle East, 1940 Aug. - 1942 Jan., Minute from Portal to Sinclair, and reply from Sinclair to Portal, 5 September 1941.
[106] TNA, AIR 16/525, Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 16 November 1941 - 31 March 1942.
[107] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 1 April to 15 June 1942.
[108] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 16 November 1941 - 31 March 1942.
[109] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 1 July to 30 September 1942.
[110] Ibid., Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 16 November 1941 - 31 March 1942.
[111] Ibid., Memo from Douglas to Director General & Inspector of Signals (DGIS), 6 June 1942.
[112] Bragg, *RDF1*, p. 279.
[113] TNA, AIR 16/525, War Cabinet, Night Air Defence, Jamming of RDF, Memorandum by Sir Henry Tizard, Chairman of the Radio Policy Sub-Committee, 4 July 1942.
[114] Ibid., Letter from DGIS to Douglas, 10 July 1942.
[115] Ibid. Meeting to discuss Sir Henry Tizard's memorandum, 19 July 1942.
[116] Metallised leaflets were a radio countermeasure in which incoming aircraft spread a cloud of small, thin pieces of black paper backed with aluminium foil cut to half of the target radar's wavelength, which either appears as a cluster of primary targets on radar screens or swamps the screen with multiple returns. Originally named *Window* by the British and *Düppel* by the Germans (from the Berlin suburb where they were first developed).
[117] TNA, AIR 16/525, Progress report by the AOC-in-C Fighter Command on the Development and the Results obtained in Night Operations for the period 1 July to 30 September 1942.
[118] TNA, AIR 41/71, Flying training during World War II: volume 2 part 3; operational training, 1952, Chapter 21, training in Middle East Command, p. 940.
[119] Andrew Hendrie, *The Cinderella Service, RAF Coastal Command, 1939-1945*, (Barnsley, Pen & Sword Aviation, 2010 [2006]), p. 156.
[120] TNA, AIR 41/71, training in Coastal Command, p. 889.
[121] Sir Robert Watson-Watt, *Three Steps to Victory: A Personal Account by Radar's Greatest Pioneer* (London, Odhams Press Ltd, 1957), p. 163.

Article

# JOINT SACEUR-SACLANT Air Defence Operations in North European Waters

By Wing Commander Joan Hopkins

**Biography:** Wing Commander Joan Hopkins joined the Women's Royal Air Force in 1955, in the Fighter Control Branch. She served as a Fighter Controller in the United Kingdom, the Near East and the Far East, on such widely separated units as Bukit Gombak and Buchan. After a tour in CTTO, and a period on the Air Staff in MOD, she served as Master Controller and OC Ops at Buchan, taking up a similar appointment at Boulmer on completion of 67 Advanced Staff Course.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

This paper was originally published in *The Hawk: The Independent Journal of The Royal Air Force Staff College* No 38, 1976-77 Edition, July 1977. It was shortened and amended for publication in *The Hawk*.

## Introduction

NATO planning for the defence of continental Europe by SACEUR and for maritime operations by SACLANT and CINCHAN was kept separate for many years. 'Little attention was given to … the integration of maritime and continental strategies, and the NATO command structure developed into two completely separate operational commands, SACLANT … and SACEUR. These Commands developed their own staff organisation, alert states, rules of engagement and operational doctrine'.[1] The differences are relatively unimportant to forces which are allocated to either SACEUR or SACLANT on a functional or a geographical basis, but they are extremely important to forces which have a multi-role capability or are responsible to both commanders simultaneously.

The main area in which continental and maritime responsibility overlaps lies between Norway, Iceland, Brittany and the European coastline. The area covers the strategic Iceland-Faeroes-UK gap and the air and sea approaches to the UK and major European ports. Militarily, it includes SACEUR's air defence Early Warning Area 12, a major part of SACLANT's command and the whole of CINCHAN's command. This division of responsibility, combined with the increasing participation of land-based aircraft in maritime operations, has caused problems in tactical air defence.

SACEUR and SACLANT both operate fighter, tanker and airborne early warning (AEW) aircraft in Area 12. Although SACLANT's main air power is based on board the aircraft carriers of the Strike Fleet Atlantic (STRKFLTLANT), air support for other naval groups is now provided by land-based aircraft. Procedures have been developed for the request, provision and transit of land-based aircraft to a fleet and for a limited exchange of radar information between shore stations and ships, and although 'the progress towards achieving inter-service operational capability and efficiency has been remarkable',[2] much yet remains to be done. It is only natural that air and naval commanders still tend to fight their own battles and this can often lead to duplication of effort, disruption of each other's plans and interception of each other's aircraft.

In a NATO maritime exercise in 1974 'nearly half the 60 or so aircraft "shot down" were destroyed by their own side'.[3] The lack of co-ordination is due mainly to inadequate communications between commanders, but the situation is exacerbated by the inadequacies of the common data base, by different procedures and operational doctrines and by over-lapping responsibilities. Air defence operations in North European waters should be improved; better co-ordination is needed between land-based and naval air defence forces.

## Communications

Air and naval air defence (AD) commanders need to exchange three types of information to co-ordinate their operations:

Recognised Air Picture. Recognised air picture (RAP) data include the position and identification of all aircraft detected in an area. RAP data are required in real time and are exchanged continuously.

Air Transfer. Aircraft transfer information includes details of airborne times, armament, and joining and leaving instructions for land-based aircraft supporting a fleet. These messages occur frequently and require rapid transmission.

Battle Management. Battle management information is primarily concerned with deployment of aircraft and reaction to specific threats. Communications are required intermittently but immediately.

These types of information are exchanged on a variety of radio communication circuits. However, radio communication is not without its problems in northern latitudes. These include:

HF Circuit Quality. HF is notoriously unreliable in northern latitudes, and its quality varies with the time of day, the season, the weather and the location of the transmitting and receiving units. Unless special transmission techniques are used HF will normally be of poor quality and will sometimes be unusable in latitudes above about 60 degrees North. If this happens individual messages may have to be transmitted several times and the exchange of information on HF is slow and laborious.

Congestion. Ships' communications equipment is usually limited, and sometimes insufficient to meet all their tasks. The quantity of information carried, combined with the poor quality of some circuits, could result in serious congestion. Aircraft transfer information would normally be given priority, followed by RAP data. Conditions would rarely permit useful battle management discussion.

Security. HF transmissions can reveal the location of a fleet at long range, and the contents of the messages can also give away tactical information. A naval force can stop transmitting on HF to conceal its location, but this reduces any exchange of information to one-way traffic. Aircraft can be used to relay information passed on UHF, but this system has a limited range and is only effective when a relay aircraft is airborne. Messages can be coded to maintain security but unless sophisticated on-line cryptography is used this cannot be done quickly enough to cope with large quantities of information or extremely urgent messages.

Many shore sector operation centres (SOCs) and ships have automated or semi-automated RAP, and data are automatically exchanged between compatible systems. However, within NATO 'tactical communications equipment in many cases cannot directly communicate with corresponding equipment used by other nations'.[4] At sea '5 major navies use one and 3 navies use another'. As a result, 'there is no guarantee that ships can talk with each other or with a shore station'.[3] A manual system therefore has to be superimposed on the automatic system during joint operations with the consequent duplication of communications, manpower and training.

These problems of incompatible communications and data systems were foreseen.[5] It was planned to provide the NATO system with 'interface with surveillance radars of the US Sixth Fleet and possibly other NATO naval units under the Shore Buffer programme'.[6] The data were to have been transmitted on HF skywave, but this has been found to be too unreliable a medium in northern latitudes. Development of the buffer continues, and there remains an urgent need for such equipment. Alternative transmission systems either lack range or are more expensive than HF skywave, however. If a buffer system is introduced the congestion on voice circuits would be reduced and time made available for battle management discussions.

A switch from HF to satellite communications would, however, resolve most of the current problems. Satellite communications would have the range and capacity needed for automated RAP data to be exchanged, although a limited manual exchange would still be required for non-automated units. Most major ships, including STRKFLTLANT carriers and command ships, already use satellite communications for other purposes, and co-operational use of satellite communications already exists[7] between the US, UK and NATO.

A NATO airborne warning and control (AWACS) aircraft would introduce yet another communications and data handling system. However, as AWACS would also affect all the other matters discussed here, it is dealt with separately below.

## Common Data Base

The RAP is the common data base used for battle management ashore and afloat. It gives the position, heading, speed, height, identification and reference number of all friendly and hostile aircraft known to be flying in an area. Data used for compiling an RAP and identifying aircraft are obtained from a variety of sources including surface and airborne radars, flight plans, in-flight position reports, IFF/SIF, and track behaviour. RAP data are exchanged by all interested units to supplement their own sources of information.

Friendly aircraft are normally distinguished from hostile by a variety of criteria. Ships and SOCs both have flight plans of land-based aircraft operating in direct support of the ships. Identification details of other aircraft are exchanged in the RAP crosstell, or the aircraft can be identified by their IFF/SIF transmissions. However, naval forces may adopt HF silence and monitor the shore RAP but not transmit. Without access to the identification criteria it would be extremely difficult for SOCs to identify aircraft under naval control. Similarly, individual

ships which are not in contact with an SOC would have difficulty in identifying all aircraft. Unidentified aircraft are very vulnerable to interception, particularly when jamming is being experienced and especially when the defence forces feel themselves actively threatened.

At present AD forces use several different geographical reference systems and various combinations of aircraft reference numbers and letters. Each type of reference is a fundamental part of the data language of an automated weapon system and cannot be changed without difficulty. A neutral grid and the reference number of the originating unit are used in joint operations, and each customer then translates the information as required. This is a slow, laborious and inaccurate process which degrades the performance of all the automated systems involved. A co-ordinated re-equipment programme would be required for standardisation, but an automatic interface, such as the ship-shore buffer, would allow the rapid exchange of automated data.

## Procedural Differences

SACEUR and SACLANT 'at any time, may be holding their own alert states'.[8] This could cause two problems:

> Command and Control. Control of some squadrons is transferred from SACEUR to SACLANT at a specific alert state. However, unless the procedures for generation of alert states and transfer of control are absolutely clear, some confusion could result among the forces involved in the transfer. This could also affect those airfields and SOCs which support these aircraft.
>
> Rules of Engagement. With overlapping areas of responsibility, fighters from the same base responsible to different authorities could be using different rules of engagement (ROE) in the same area. One of SACEUR's fighters could be a considerable distance out to sea, restricted to shadowing a target. At the same time, a colleague, assigned to SACLANT and flying close to the mainland, could be cleared to engage a similar target. Enemy aircraft are unlikely to appreciate the subtle difference. If different ROE are necessary, it would be best to stipulate a clear geographical division between areas in which they each apply.

Plans exist for UK fighter, AEW and tanker aircraft to operate autonomously when their controlling SOCs are destroyed or severely hampered by jamming.[9] Communication difficulties are likely under these conditions, and co-ordination could be degraded. Heavy friendly aircraft losses could be expected unless plans for autonomous operations are standardised and well known to all participants.

## Operational Doctrine

The differences in operational doctrine between naval and air AD commanders are mainly caused by the range and scale of their operations. Naval operations are concentrated on the

point defence of the parent ships whereas shore operations provide defence for large land or sea areas. The differences reduce flexibility and may cause unnecessary waste of effort.

Naval forces establish AD zones of varying size around themselves. The zones range from approximately 20 miles radius around an isolated missile-equipped ship, through 150 miles around a land-supported force, to 200 miles around a carrier group. It is a common doctrine for aircraft operating in direct support of a fleet to remain in a zone under naval tactical control, although there are occasions when shore stations could provide more effective control of AD forces.

Area 12 covers nearly one million square miles, and AD aircraft are rapidly redeployed throughout the area to match specific threats. Interceptions frequently take place at ranges up to 700 miles from the coast[10] and it is not unusual for a fighter to be tactically controlled by a number of different agencies in a single sortie. Aircraft which pose a threat to a land or island target outside a fleet's AD zone could be intercepted on the far side of the fleet, and fighters frequently transit through the zone to get to their interception point. Under these circumstances the use of carrier AD aircraft might be preferable.

## Overlapping Responsibility

Some of the difficulties in co-ordination are caused by three conflicting maxims: air power should be centrally controlled; air defence is indivisible; and all forces involved in a battle at sea should be controlled by the naval tactical commander. In applying these maxims, both air and naval commanders will prefer to operate independently; indeed they are conditioned to do so by experience and training. At present, they can operate independently throughout the whole of Area 12 because both SACEUR and SACLANT have responsibilities throughout the area. This causes particular problems in the south of the area.

The airspace south of 62° North is very heavily congested with civil and military air traffic in peacetime, and the further south, the worse the congestion. In wartime, the UK fighter force would probably be concentrated in this region, and aircraft supporting the Central Front from UK will transit through it. Current communications appear inadequate for the degree of co-ordination required for peacetime flight safety requirements and for effective joint battle management in the war. The only practical alternative to effective close co-operation is the physical separation of forces under different tactical control, so far as this can be done. Separation would avoid duplication of effort, reduce friendly losses, minimise long exchanges of information and provide a clear chain of command.

To achieve separation, Area 12 could be divided approximately along the lines of 62° North and 9° West with SACEUR and SACLANT assuming responsibility to the south/east and north/west respectively. Each commander could then be given complete control over all AD forces operating within area and use his own ROE and procedures. This would require the transfer of certain radar facilities to SACLANT's control and the transfer of all carrier-borne AD aircraft in

the south/east to SACEUR's control. These, however, are radical proposals, and it is doubtful if commanders could be persuaded willingly to abdicate their sovereignty in this way.

An alternative solution would be for Area 12 to be divided along the same lines, but with commanders assuming primary responsibility only for the overall direction of forces within their sub-areas. The commanders with secondary responsibility could then exercise tactical control in mutually agreed and clearly defined and limited sectors, as follows:

North/West. Air and naval forces could operate independently in this area with little conflict. They could use SACLANT's ROE and be aware of each other's procedures. Limited battle management discussion would be required, and present communications might be adequate.

South/East. AD forces in this area could operate under SACEUR's overall direction. Naval AD commanders could exercise tactical control in sectors which could be avoided by aircraft not under their control. However, these sectors would have to be considerably smaller than the 20-200 mile radius zones currently claimed by different types of ships so that land-based aircraft could get around them. Unless there were a high probability of correct blind identification, it would be preferable for all fighters operating near a carrier to identify a target visually before firing. All forces in this area could use SACEUR's ROE. Some extra co-ordination might be possible as ships would be in range of an airborne UHF relay. A relay aircraft would be required continuously, but relatively short-range aircraft could be used.

## Future Developments

The introduction of the Nimrod AEW to UK service, and the Boeing E-3A AWACS aircraft into the US and, possibly, the NATO inventory will affect all issues raised above:

Communications. AWACS and, hopefully, Nimrod will use a time division multiple access (TDMA) system for transmitting automated data.[11] Information on the Nimrod fit is sparse, but it is assumed that it will be compatible with AWACS equipment and, therefore, the TDMA. AWACS will feed data to the TDMA for relay between similarly equipped surface units and aircraft.[12] The TDMA system is not compatible with other communications systems currently in use, but it will be made inter-operable by interfacing buffers located at surface units.[13]

Other Problems. AWACS and Nimrod will provide air and naval commanders with a greatly improved data base when airborne. However, they are likely to exacerbate other problems. These aircraft will introduce a third agency to the current air/naval mixture. AEW aircraft could be switched rapidly from one NATO flank to another or deployed to Europe from the US,[14] and alert states, ROE and procedures must be standardised if the crews are to cope. Although AWACS and Nimrod will improve communications

to a degree where co-ordinated battle management will be possible, air and naval commanders will probably still prefer to operate independently. Moreover, the range and performance of AWACS and Nimrod's facilities will give them increased ability to do so. Commanders are therefore likely to compete actively for their share of an AEW aircraft's facilities. Thus a clear division of responsibility between commanders will still be required.

Command and Control Systems. Great savings could be made if NATO adopted a single, standard command and control communications system. The US Department of Defence believes that NATO AWACS 'would force cohesion in the Alliance, particularly in the Command and Control Areas'.[15] All NATO nations wishing to use AWACS or Nimrod data will require access to a TDMA terminal, and interface units for their own systems. Increasingly sophisticated interfaces will be required in the long term as US forces intend eventually to change to TDMA systems. The AWACS communications unit 'is the forerunner of a family of compatible units projected for the US tri-service joint tactical information system (JTIDS).[16] The US 'is offering NATO participation in JTIDS's development and access to US technology'.[17]

## Conclusion

Lack of standardisation affects joint SACEUR/SACLANT AD operations in all fields. Incompatible communications and data handling systems currently require a superimposed manual system during joint operations. The automated systems could be made inter-operable by a series of interface buffers provided a suitable transmission medium could be provided. Satellite communications would provide such a medium and give reliable voice communication. AWACS equipment is incompatible with current surface systems. Its introduction into the NATO inventory would require widespread use of interface buffers and may eventually force nations to standardise their equipment.

SACEUR and SACLANT forces can be using different alert states and ROE in the same area at the same time. They also use different operational procedures. Standardisation in these fields would be invaluable, particularly for AWACS or Nimrod AEW aircraft which are likely to be deployed rapidly between different operational zones. However, the major operational limitation to effective AD co-ordination lies in conflicting maxims which state that both air and naval operations are indivisible. Air and naval AD commanders prefer to operate independently, and AWACS and Nimrod will increase their ability to do so. At present there are few constraints on independent AD action as Area 12 is claimed equally by SACEUR and SACLANT. A clear geographical division of responsibility for AD operations is required. This would not preclude overlapping operations but in such cases would define the senior partner. Without such a division, duplication of effort, mutual disruption and heavy friendly losses can be expected.

## Notes

[1] *International Defence Review* (IDR) 6/1974, page 733.
[2] IDR 6/1974, page 733.
[3] *The Guardian*, 11 Dec 1974. Statement to the NATO Military Committee.
[4] *Aviation Week and Space Technology* (AW&ST), 28 Jun 1976, page 22.
[5] L.W. Martin, *The Sea in Modern Strategy* (1967), page 129.
[6] IDR 3/1974, page 312.
[7] *AW & ST*, 28 Jun 1976, page 21.
[8] IDR 6/1974, page 734.
[9] *The Guardian*, 8 Feb 1974.
[10] *Jane's Weapons Systems*, 1976, page 246.
[11] *AW & ST*, 26 Apr 1976, page 48.
[12] *AW & ST*, 26 Apr 1976, page 49.
[13] *IDR* 5/1975, page 672.
[14] *Annual Defense Department Report*, FY 1976 and FY 1977, pages 111-117.
[15] *AW & ST*, 21 Jun 1976, page 15.
[16] *AW & ST*, 26 Apr 1976, page 48.
[17] *AW & ST*, 21 Jun 1976, page 14.

Article

# How Does Russia Wage Contemporary Political Warfare, and Consequently Challenge International Order?

By Wing Commander Jade Richards

**Biography:** Wing Commander Jade Richards is a People Operations Officer currently serving as Personal Staff Officer to Deputy Commander Capability and Air Member for Personnel & Capability. During her non-commissioned service she completed a PGDip in Strategic Human Resource Management before Initial Officer Training in 2008. A graduate of the Advanced Command and Staff Course, she holds an MA in Defence Studies with King's College London.

**Abstract:** In twenty-first century conflict Western states face a range of tactics conducted in the information space to coerce, influence and undermine their strategic interests. Malign actors operating in the grey zone capitalise on the ambiguity and deniability of contemporary political warfare where information has become weaponised. Political warfare waged by Russia employs propaganda and disinformation to undermine the US-led international order and the democratic values that underpin it. Free speech and freedom of information are the greatest strengths of democracy, but with the advent of the internet and social media, they may also be its biggest threat.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

> 'The character of politics and warfare is evolving rapidly, driven by the pervasiveness of information and the rate of technological change. Our competitors have become masters at exploiting the seams between peace and war… what constitutes a weapon in this 'grey zone', below the threshold of conventional war, no longer has to go bang'.[1]

## Introduction

Events over the last decade have led to an increase in debate about how revisionist states are challenging the world order. Using tactics below the threshold of war, 'the idea of political warfare has returned'.[2] The UK's Integrated Operating Concept (IOpC) 2025 identifies how adversaries seek to challenge the West's long-established strategic advantage by using political warfare tactics below the threshold of war.[3] The IOpC has identified ways to respond to contemporary political warfare waged in the information space, but fails to identify the challenges in formulating response options. Therefore, this research paper seeks to understand how political warfare has changed in twenty-first century conflict and how it is waged by malign actors, such as Russia, before identifying the challenges it poses to the international order. In analysing the research question of 'how does Russia wage political warfare waged in twenty-first century conflict', it is important to first define the character of warfare in the modern era and, whilst the nature of war is said to be fixed, the speed of technological developments in the twenty-first century have vastly changed its character and complexity. Not only do states need to be prepared to fight a traditional state-on-state conventional conflict, in the twenty-first century they will be increasingly engaged in non-conventional warfare.

Traditional conflict was limited in territory (the battlespace), limited in time (there was a beginning and an end), and you knew who you are fighting (the enemy).[4] In parallel, unconventional conflict can be transnational (you cannot define the battlespace), it may be difficult to know when you are at war and when you are not (there is no discernible start or end) and you may not know who is attacking you (your adversary). Arguably non-conventional tactics in some form or another have been used throughout history, but the 9/11 terror attacks, and subsequent wars in Iraq and Afghanistan, sparked debate about the changing character of conflict from a traditional notion of war as military competition between states. The 'War on Terror' involved both state and non-state actors, it was transnational in its nature, and used asymmetric warfare tactics and presented new threats, such as cyberattacks. Until relatively recently, domains of warfare focused on the physical (land, sea, air and space), but the introduction of cyber as the fifth domain recognised not just technological and fighting aspects of warfare, but the information space where the non-physical domain is one as crucial as the physical.[5] This started a modern era of unconventional conflict and warranted recognition of new concepts in international relations literature.

It is not just non-state actors that are employing non-traditional means of warfare to further their interests. Revisionist states that are unable to match the military power of the US are increasingly employing tactics below the threshold of armed conflict to exert influence around

the globe and to challenge the existing international order.[6] Within international relations literature there are many definitions used to define the global world order. A wide-held view is that it is multifaceted; the complex integration of military, diplomatic, political, and social constructs, underpinned by democratic institutions.[7] The US-led international rules-based order, established after the Cold War, is commonly considered to be enduring.[8] Revisionist states challenge the rules-based international system and the democratic institutions that underpin it, 'rather than follow the existing order, rising powers will seek to revise that order'.[9] As this paper will explore, the key difference in twenty-first century conflict is the interconnectedness of people.[10] The security environment of the future will be increasingly complex, ambiguous and uncertain, and Western states are facing a new challenge presented by rapid technological developments and conflicts conducted not on the battlefield, but online.[11]

Revisionist states, such as Russia, are exploiting this new environment to further their own political interests and to destabilise democracy, that it views as a threat to its own security. When viewing contemporary conflict, literary discourse has developed modern terminology to define these emerging threats and the space in which they occur. There is a theoretical labyrinth of definitions relating to activity conducted below the threshold of war and chapter one will critically examine literary discourse surrounding modern concepts that provide context on where contemporary political warfare is waged. The term grey zone best describes the operational space where contemporary political warfare is conducted as, alongside the operational and tactical, it also relates to the strategic level of warfare and is concerned with the revisionist ambitions of actors. There is little consensus on the term political warfare, but it commonly refers to the use of one or more of the instruments of power.[12] As twenty-first century conflict is increasingly waged in the information space, where victory is not simply military defeat of an adversary but determined by perceptions, this paper will only focus on that of information,[13] characterised by technological advancements and the introduction of the internet that has transformed the information battlespace. In twenty-first century conflict, states not only have to consider traditional military conflict conducted on a battlefield, but also the war of the narrative carried out online.

Second, it is important to understand what is said to be contemporary political warfare, its distinguishing features, and how tactics and techniques are employed in the twenty-first century, and chapter one will continue to explore key concepts and discourse amongst authors, including credible Russian analysts. The aim of this paper is not to provide a complete analysis of Russia's history, but an assessment of its strategic culture will be explored within chapter two, along with a brief overview of Russia's historical use of political warfare, to set the context for how Russia conceptualises it in the twenty-first century. The term political warfare is contested and has evolved over time, and in order to understand how political warfare is conducted in a contemporary context, case studies of recent Russian activity will be explored. Events from Ukraine in 2004 to the present day, highlight how Russia uses political warfare in an attempt to challenge the international order by undermining its principal value; that of democracy. Political systems that encompass high levels of competition amongst the

elite are susceptible to information operations. This tends to be a key feature of democratic states which are inherently vulnerable to political warfare campaigns aimed at sowing discord amongst the populous.[14] Finally, this paper does not seek to make recommendations for how to counter contemporary political warfare, but will assess what challenges it presents to the international order in chapter four.

### Methodology

As this paper seeks to explore a contemporary subject within the field of international relations, a pragmatic approach has been adopted where both positivist and constructivist views are considered, to enable greater objectivity in the research. As there is a wide range of sources and literature available, a deductive approach has been taken to develop the research question. A normative theory was taken to objectively analyse the observable phenomena available in relation to the research question. A conceptual analysis of the key scholars and commentators was undertaken to explore the key themes and arguments surrounding the research question. As the subject was very new to me as a researcher, this process was extremely time consuming, as reflected in the extensive bibliography. This paper has combined both empirical and case study reviews of political warfare to gain a wide perspective of the subject and how it is used in practice. Case studies on Russian historical and contemporary uses of political warfare were examined to establish contextual generalisations[15] and to verify the legitimacy of events.[16] A mixed-method of research (including both qualitative and quantitative data) was applied to incorporate existing empirical data, such as facts and figures, and personal descriptions such as newspaper articles and speeches.[17] A longitudinal lens was applied as sources accessed covered both historical and contemporary events related to Russian political warfare activity. A mono-method of data collection was utilised for this paper as sources accessed were secondary in nature as the research question relied on literature and reports that already exist and are easily accessible. The COVID-19 pandemic presented various challenges during the period of research, such as access to hardcopy data from libraries, and a sole reliance on internet sources and online texts. This necessitated the need to critically evaluate data and verify the credibility of sources from which it was obtained. As the subject chosen for this paper was new to myself as the researcher, there was little risk of personal bias affecting the outcome of my findings, and home working also meant that I was unlikely to be affected by the opinions of others.

## Section One:
## Conceptual Analysis

### The Operational Space

Discourse on twenty-first century conflict encompasses many terms – unconventional, asymmetric and, more recently, hybrid. The term hybrid warfare has been used extensively in literary discourse since Russia's annexation of Crime in 2014 and, as with many concepts, the term is amorphous and used in different ways by different scholars and actors to mean different things.[18] There is no agreed literary definition of what hybrid warfare is, and even

disagreement that it should be coined at all as arguably every war throughout history has been hybrid.[19] However, it can be useful to describe the complexity of the battlespace where conventional military force is often supported by tactics conducted in the cyber domain.[20] This type of 'new war' encompasses economic warfare, cyber-attacks, psychological operations and information warfare.[21] The term hybrid warfare first appeared in international relations discourse in 2006 following the conflict between Israel and Hezbollah.[22] Facing the might of the superior Israeli Defence Forces, Hezbollah simultaneously used conventional forces and weapons alongside other non-conventional tactics, such as terrorism, guerrilla warfare and psychological operations.[23] It was however the crisis in Ukraine in 2014, where Russia used coercive operations alongside kinetic force, that truly ignited the debate on the rise of hybrid warfare and demonstrated how technological advancements and the introduction of new modes of communication have altered the shape and character of conflict.[24] The power of these strategic communication platforms can amplify the reach of both state and non-state actors which blurs the notion of a battlespace, who is waging war, how and when.[25]

Some authors have described today as a stark resemblance to the prelude of war in the early twentieth century, characterised by shifts of global power in the international system and a rapid rise in technological advantage. In describing the complexity of twenty-first century conflict, hybrid warfare has become an increasingly popular term. However, Dan Puyvelde suggests that warfare, contemporary or not, is always complex and should not be 'subsumed into a single adjective', such as hybrid.[26] Hoffman highlights that definitions of hybrid warfare are too narrow and focus on tactics directly linked to war and violence and fail to address non-kinetic, non-lethal activity.[27] But as David Betz argues, 'if we had a mature understanding of [contemporary] war, then we would have no need for the concept of hybrid war', but as this is not yet the case, the concept provides some utility in understanding conflict in the twenty-first century.[28] As hybrid warfare can be used to describe any conflict that is not purely state-on-state war, it is arguably too broad to be of utility for the political warfare activity analysed within this paper.[29] Radin et al also highlight that hybrid warfare is not the way Russia conceptualises this type of warfare.[30] A more useful term to describe activity conducted in the information space is grey zone conflict.

The term 'grey zone' can easily be critiqued for being yet another buzzword to describe hybrid warfare, however, demarcating the term allows for a narrower focus on the conflicts conducted within it. Unlike hybrid warfare, which deals with conflict at the tactical and operational levels, grey zone conflict also incorporates activity conducted at the strategic level and is therefore concerned with the 'global and/or regional revisionist ambitions' of an actor.[31] Within hybrid warfare, non-conventional tactics may be employed alongside traditional military methods but are usually less dominant. In grey zone conflict, non-traditional methods can be stand-alone activity conducted over a protracted period.[32] These distinctions mean that the activity conducted by Russia, in the case studies presented, are best defined under grey zone activity. The widespread use of the term grey zone highlights that there is a void between war and peace and such a binary distinction does not reflect the reality of twenty-first century conflict.

Conflict can be considered a continuum along which a range of violence, from conventional state-on-state war to measures short of armed attack, are features.[33]

To establish the essential nature of activity conducted within this spectrum, literary discourse can be reviewed to explore the conflicts within definitions and the common characteristics throughout. The grey zone can be defined as the space between war and peace, where coercive actions are conducted below the threshold that would traditionally warrant a conventional military response, aimed at challenging the status quo and are where attribution is complex.[34] Elkus describes the term grey zone as an ill-defined analytically incoherent concept that is nothing new and that encompasses too many types of conflict, including state aggression from China and Russia, terrorism in Nigeria, and civil war in Syria.[35] Whilst his critique is valid to some degree, in that the concept is ambiguous and applied to a broad range of conflicts and behaviours, it does not make it meaningless, just rather slippery. The concept takes greater coherence when considered as a 'planned campaign in the space between traditional diplomacy and overt military aggression', typically employed by revisionist states with grand political ambitions.[36] Actors that conduct conflict within the grey zone seek political wins rather than overt clearly identifiable military actions which are easier to respond to.[37] Ambiguity is a defining characteristic of grey zone conflict; who is conducting it, what they seek to gain, and when activity crosses a threshold for military response.[38] It is these features that make it attractive to revisionist actors seeking to challenge the US-led international order.[39]

### Political Warfare

**'Winning modern wars is as much dependent on carrying domestic and international public opinion as it is on defeating the enemy on the battlefield'.[40]**

Political warfare is a term that relates to tools of statecraft, conducted within the grey zone, to achieve strategic goals.[41] In 1948, Kennan described the phenomenon of political warfare as 'the employment of all the means at a nation's command, short of war, to achieve its national objectives'.[42] There are scholars who argue that political warfare, as a concept, is inherently flawed as the term 'warfare' denotes the use of physical force and, as the methods deployed within the concept are non-kinetic, the term should not apply. Hoffman is critical of Kennan's definition of political warfare as 'all means' goes beyond the political component and, if these means are 'short of war', it is not warfare at all.[43] Political warfare is separate from other forms of conflict and sits within the grey zone between conventional war and peaceful diplomacy and its purpose is to avoid traditional warfare. However, political warfare does contain acts of violence, or the incitement of, and is therefore still warfare. The tactics employed in political warfare, that will be explored further in this paper, have either the ability to influence behaviours or the propensity to mislead, and therefore they have the potential to harm.

Political warfare refers to the range of measures an actor can use to coerce, undermine, influence, or intimidate their adversaries, whether politically, economically, militarily, or informationally.[44] Contemporary political warfare can be waged in various forms, such as

economic pressure, but increasingly important is the role the internet plays in international conflicts with the information arena commonly used as today's battlefield. Political warfare in the information space centres on indirect psychological operations, often conducted via social media, to manipulate information and therefore opinions, to shape political outcomes.[45] In an ever more connected world, where the opinion of the public can be as influential as the application of international law, 'the battle of words is as important as military capability'.[46] In contemporary conflicts, public perception is now the strategic centre of gravity.[47] Political warfare conducted in the grey zone is no longer a supplement to conflict but an alternative.[48] Actions carried out in the information space are not necessarily a precursor to armed conflict, it may be the only force used. Political warfare is a term that encompasses information warfare and subversive tactics, such as propaganda and disinformation, which will be explored further in this chapter.[49]

Information warfare, like political warfare, is not new and has been waged throughout history, but the technological advancements of the twenty-first century have enabled actors to practice it in novel ways.[50] The terms 'information operations' and 'information warfare' are used interchangeably amongst literature, the latter implying you need to be 'at war' for methods to be used against an adversary. However, as Giles states, 'information warfare is not an activity limited to wartime. It is not even limited to the initial phase of conflict before hostilities begin'. Instead, he argues that information warfare is conducted continually, regardless of the relationship between opponents, and therefore reinforces the notion that conflict is a spectrum.[51] The term information warfare is an amorphous concept covering a wide range of activity and definitions are used interchangeably and applied in numerous contexts.[52] It covers terms such as psychological operations, information operations, disinformation and propaganda to describe information-based conflict.[53] Information warfare can be defined as the use of narratives by hostile actors to influence the actions and shape the perceptions of populations and decision-makers,[54] and these non-military means of warfare have 'exceeded the power of force of weapons in their effectiveness'.[55] Information warfare relates to information activities that aim to influence the will of an adversary and to disrupt, degrade, deny or manipulate both the information available to an adversary, and also to their information infrastructure. The information space has become an area where cognitive dissonance is created on a daily basis, and where there is a tenuous distinction between truth and mendacity.[56] Narratives are spread on the internet and gain legitimacy without any merit, and conflict in the twenty-first century is often a battle over minds.[57]

One technique in support of this information warfare is the use of psychological operations; activities aimed to influence attitudes or perceptions of individuals or groups, and to affect their subsequent behaviours. By conveying certain information to target audiences, people can be manipulated to think in a certain way, or even to re-think what they believe.[58] NATO defines psychological operations as 'planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military

objectives'.[59] The aim of psychological operations is to use non-lethal means to convey a specific message in the cognitive battlespace. Whilst often thought of as a form of contemporary warfare, psychological warfare is of ancient origin. In the twenty-first century, the incredible speed of technological innovation and vast array of platforms in which to deliver psychological operations has changed the ways in which it can be conducted.[60] Although a broad term, the aim of psychological operations is to intimidate or persuade an individual or group and is therefore a tactic of manipulation. In the twenty-first century this is carried out, in the main, through tactics conducted in the information space, exercised through propaganda and disinformation campaigns. Again, definitions used to describe tactics employed in psychological operations often overlap (the terms disinformation, fake news and conspiracy theories are used interchangeably on a single page in one text),[61] and this paper will seek to define them as individual entities.

The degree to which the terms propaganda and disinformation overlap is open to debate, but they can be considered distinct concepts. One distinction of disinformation is that it specifically relates to *false* messaging that is politically driven to engender distrust and create uncertainty amongst a populous to bring about social or political change,[62] whereas literary discourse on propaganda falls short of calling activity conducted as dishonest.[63] Unlike misinformation, disinformation is disseminated with the intention to actively mislead. Floridi states that if the content is false, it is misinformation. If the person disseminating it knows it to be false it is disinformation.[64] But this definition is too broad as, for example, it could capture examples where the person disseminating the information did not intend to cause harm, such as a cartographer drawing maps that are knowingly not to scale.[65] A more robust definition is provided within a House of Commons report that defines disinformation as a tool used by malign actors to create influence by distorting the truth through the 'spread of false, misleading and persuasive content'.[66] Danesi also highlights that this activity can be conducted to distort or reinforce existing beliefs for ideological or political purposes, with the overall objective to destabilise.[67]

Contemporary political warfare encompasses disinformation campaigns that often use conspiracy theories and fake news to deliver a narrative that seeks to entertain an audience and, therefore, gain momentum of dissemination. Again, there are many definitions of what constitutes a conspiracy theory, but there is common consensus that they contain a narrative to unite people against 'the imagined other',[68] where political actors use fear as a tool for propaganda.[69] Conspiracy theorists work towards subverting our deep-held beliefs with the goal of destabilising the established international order.[70] The aim of a conspiracy theory is to 'mobilize passions' and, by repeating the narratives many times over, they gain incremental credibility.[71] Harnessing the power of an individual's cognitive bias, their conceptual roots filter out any contradictory narrative that is subsequently absorbed.[72] Although conspiracy theories are a traditional tool for subversion, the advent of the internet has established fake news as a contemporary tactic of political warfare. Dice describes fake news as a modern term for propaganda, disinformation and conspiracy theories,[73] and the advent of social media means

it can be spread at unprecedented speed. The term fake news has become widely-used since the US elections in 2016 and can describe false information designed to manipulate, mislead or distort the views of the target audience.[74] It can be conceptualised as a form of disinformation, deliberately spread via different media platforms.[75] A House of Commons report on fake news described how its use to effect outcomes of elections is threatening 'the very fabric of our democracy',[76] substantiated by a 2018 survey in which 83% of participants perceived fake news to be a problem for democracy.[77] In the case of twenty-first century conflict, the main enabler is social media, and the effects of fake news on entire societies can be devastating as 'falsehoods spread through a community like a virus'.[78]

Disinformation and propaganda have been tools of warfare for millennia, however the advent of the internet has made these tactics more ubiquitous and potent in twenty-first century conflict and with greater anonymity.[79] Political warfare is increasingly waged via social media[80] as it is fast becoming the preferred medium for people to find out what is happening in the world over more traditional communication outlets.[81] There are over three billion users (45% of the global population) of social media across the world,[82] with over 80% of people accessing news online.[83] Paynne argues that the media is now 'indisputably an instrument of war' as influencing the opinions of a population is as important as military defeat of an opponent.[84] In this way, social media is revolutionising the role of citizens and challenging the existing norms within our political systems,[85] and has emerged as a 'critical threat to public life' by manipulating opinion.[86] Facebook's creation in 2005 was deemed to be a revolution in free speech and a platform for the sharing of discourse.[87] However, the algorithms used by the platform can create echo chambers that cater to our cognitive bias where we receive more of the same content we choose to engage with.[88] The echo chambers created by social media platforms mean audiences self-select the information they view, which therefore confirm existing biases.[89] These platforms not only enable mass targeting of populations, but also the micro-targeting of individuals through personalised messaging.[90] Using social media to convey fake news and conspiracy theories has become the preferred channel for dissemination and an easy way to reinforce the narrative. Social media platforms enable influence on a global scale and, as a result, today's battlespace has become 'mediatised' where the use of social media platforms has become a weapon waged on a global scale.[91]

## Summary

The conceptual analysis of the operational space of twenty-first century conflict has explored the increasingly popular term of hybrid warfare but, as it is not concerned with the strategic level of war, a more useful definition would be that of grey zone conflict. This term accounts for the political ambitions of revisionist states and can be used to describe the space between war and peace, where coercive actions are carried out below the threshold that would traditionally trigger a military response. Political warfare is a term that relates to tools of statecraft, conducted within the grey zone to achieve strategic goals. In twenty-first century conflict, political warfare is not necessarily a supplement to traditional warfare, it is increasingly used as an alternative. Political warfare encompasses, propaganda and disinformation, utilising fake

news and conspiracy theories. Arguably many of these techniques are not new to twenty-first century conflict, but the internet and creation of social media platforms have changed the way tactics are deployed and information has been weaponised. It would be easy to say that political warfare is not war, but arguably these tactics typify conflict in the twenty-first century, as demonstrated by Russia.[92]

## Section Two:
## Russia

**'Like it or (probably) not, the West is at war, but not necessarily the kind of war it imagines or with which it is accustomed. It is at war with Russia for the simple reason that it takes only one side to make a war, and the Kremlin has already made the decision that the West has started it'.[93]**

When assessing how the character of conflict has changed, for Russia the most profound development has been its use of political warfare tactics conducted in the grey zone using information operations to create psychological effect. Valery Gerasimov, the Russian Chief of General Staff, highlights these changes in twenty-first century warfare, and how the information space can be used as a means in which to achieve political goals.[94] The wide media coverage of psychological operations undertaken in Ukraine has ensured that information warfare has taken centre stage globally and, since its annexation of Crimea in 2014, Russia has been characterised as the biggest threat to the liberal world order. Not in the traditional concept of military state threat, but one where its aggressive use of political warfare seeks to undermine democratic institutions and promote its efforts to gain recognition of its status as a great power.[95] As Putin himself declared, 'Russia is a country with a history that spans more than a thousand years and has practically always used the privilege to carry out an independent foreign policy. We are not going to change this tradition today'.[96]

Whilst clear that Russia has been employing methods to meddle in democratic institutions, the motivation for these actions may be somewhat confusing.[97] What could be a starting point is consideration of strategic culture, which can be defined as a framework for understanding the perceived threats of a state and how it protects its values and interests.[98] Russia's open geography and long adversarial history with the West has created a strategic culture that has a sense of paranoia and distrust at its core.[99] When viewed against the seemingly aggressive actions of Russia, this strategic culture may explain that these actions are arguably defensive as they see 'plots against Russia from every direction'.[100] Strategic culture can offer some utility in understanding why a state may act in a certain way, but the role played by the political elite of that state must also be considered.[101] Putin's extensive background working in the intelligence services, and experience of employing covert tactics, may go some way to understanding a preference for operations within the grey zone.[102] Political leaders can legitimise their decisions by deliberately manipulating facets of their strategic culture,[103] and Putin views the previously held great power status as Russia's 'geopolitical birth right'.[104] Strategic culture can be defined as 'a negotiated truth among elites who often conceptualise national identity to validate their

own strategic choices' and, since his re-election in 2012, Putin has created a narrative around Russia's vulnerability from the West.

Throughout history, Russia has used psychological operations extensively and successfully more than any other power, and has a long history of using disinformation and propaganda tactics.[105] In Soviet Russia, the 'Disinformation Office' was created in 1923,[106] followed by a KBG established 'Department for Active Measures' in 1958.[107] Active measures was the term used by the Soviet Union to describe the techniques used to influence the behaviours of citizens by undermining confidence in political institutions, and to discredit the government of an adversary.[108] In 1983, an article appeared in the Indian *Patriot* newspaper (created as a front for the KGB decades earlier)[109] that accused the US of creating the AIDS virus to deliberately target and kill homosexuals, drug takers and black African-Americans.[110] Whilst a seemingly preposterous accusation, empirical data shows that many years later, millions of Americans still believe the claims to be true.[111] This activity was in fact conducted by the Soviet Union, codenamed Denver[112] (also commonly termed 'Operation Infektion'),[113] carried out by the KGB to generate distrust of the American government and weaken strategic alliances.[114]

Since the fall of the Soviet Union at the end of the Cold War, Russia's loss of military might and extreme sense of paranoia has seen it increasingly look to new ways to exert power, both domestically and regionally, and to challenge Western unipolarity at the international level.[115] This paranoia and distrust of the West has led the Kremlin to employ political warfare tactics, such as the spreading of disinformation, utilising social media platforms. Propaganda and disinformation spread by state-owned media outlets is especially dangerous,[116] and these falsehoods are legitimised by state-owned news networks, such as RT, which specialises in promoting conspiracy theories.[117] The 'About Us' page of RT, boasts a wealth of international media awards, reputable key figures appearing on broadcasts, and a strap-line of 'Question More'. Along with ten billion views of its published content on YouTube in 2020, its online reach is vast,[118] but rather than fulfilling its objective of providing a perspective that is not seen in mainstream media, its main purpose is to create 'confusion, chaos and mistrust'.[119] By creating other state-owned media outlets, such as Sputnik and Baltica, the Kremlin can provide alternative media platforms to give credibility to the narrative, and this constellation of channels can drown out competition.[120]

Much of the literature explored points to Russia as aggressive, operating in ways that shock the international community. However, US interference in Russian politics in the 1990s, where US advisors reportedly aided Yeltsin's re-election, substantiated Putin's paranoia against the West and show that these tactics have not always been the preserve of authoritarian states.[121] This interference affirmed to Putin that a state was entitled to use every available means in international politics, including meddling in elections of other nations. Russia is using the information domain for propaganda tactics in twenty-first century conflict to undermine democracy and conduct political sabotage to influence the foreign policies of adversaries.[122] Jensen describes this change in the character of warfare as the 'new Cold War'

and, although conducted in the virtual space, it is just as susceptible to inadvertent escalation and uncertainty as if in the physical domain.[123] Russian political warfare tactics employed within the information space have far reaching implications for international security. They seek to challenge the US-led unipolarity of the global world order, to further their regional interests, and to undermine the role of NATO. But unlike the Cold War where Soviets supported left-wing socialist narratives, today they seek to create an echo chamber by supporting opposing ideologies.[124]

**Summary**

The use of social media to bring about regime change in the Arab Spring in 2010 and 2011, which the Kremlin perceived to be an attempt by the West to threaten Russia's security, played on Russia's sense of paranoia.[125] This brought about heavy investment in capabilities to target audiences outside of Russia and, by 2014, had a centralised and coordinated media element to its propaganda machine.[126] Russian actions in the last decade have been commonly viewed as aggressive, but arguably they are more defensive in nature; a response to the perceived insecurity presented by Western states. Political warfare tactics are etched into the fabric of Russia's strategic culture and seemingly extant under President Putin.[127] The Kremlin are increasingly focused on political warfare waged in the information space to avoid direct military confrontation.[128] As a revisionist state, Russia recognised that to gain competitive advantage, the West's weaknesses could be exploited by operating in the grey zone. By weaponizing information, the Kremlin is "ahead of the game"[129] and Russia has learned that using a strategy of death by a thousand cuts exploits the power of the internet and social media platforms to manipulate people by sowing seeds of doubt and confusion.[130]

**Section Three:**
**Contemporary Political Warfare**

'We may see 2016 as the year in which Russia fired the starting gun on a global information arms race, in which our digital space is in a permanent state of conflict….'.[131]

Ukraine offers a valuable case study in which to analyse how Russia's political warfare strategies have adapted in the twenty-first century. Russia perceives Ukraine to be within its sphere of influence, or near abroad, and considered key to Russia's economic prosperity. The region also acts as a geographic buffer zone against potential military aggression from adversaries.[132] In the 2004 Ukraine elections, the pro-Western candidate Viktor Yushchenko, was peculiarly poisoned. On voting day, masked men appeared at polling stations to harass voters opposed to the Russian-backed candidate, and votes were mysteriously cast by Ukrainians long-since deceased.[133] These overt tactics resulted in mass protests called the 'Orange Revolution' and resulted in a repeat election which saw Yushchenko victorious.[134] This demonstrated how the 'globalization of perception – the ability of everyone to know what is happening in minute detail around the world and the increasing tendency to care about it – is another way the small can fend off the large'.[135] However, ten years later Russia had adapted its political warfare tactics in order to subvert the 2014 elections and used far more covert tactics in an attempt

to manipulate the outcome. Cyber hackers implanted a virus into the Ukraine Election Commission's computer systems designed to alter the election votes in favour of the far-right ultra-nationalist party. The malware was detected, but only an hour before the results of the vote were announced.[136]

As the conflict in Ukraine escalated, reports emerged of the Internet Research Agency located in St Petersburg, with an army of trolls 'employed to prowl social media, sowing discord and influencing opinion world-wide'.[137] These troll armies consisted of online bloggers, each maintaining numerous Facebook and social media accounts and posting on multiple news articles daily to flood the internet with pro-Kremlin and anti-Western narratives.[138] Russia reinvented reality by convincing citizens that 'fascists' were running the country of Ukraine and the lives of ethnic Russians were being threatened.[139] With a large proportion of people viewing Russian-owned television channels, such as RT, the Kremlin was able to create a parallel reality in which ethnic Russians were in grave danger.[140] Consideration of twenty-first century grey zone activity is well encapsulated by the Ukraine case study, with the use of covert information operations to subvert democratic election processes.[141] Political warfare is the term that best captures the depth and breadth of Russia's intent in its intervention in Ukraine.[142] The Russian political warfare campaign was described as 'the most amazing information warfare blitzkrieg we have ever seen' [143] and the power of the internet gave Russia the anonymity and ubiquity needed to exploit propaganda techniques in a multi-faceted political warfare campaign that was considered highly successful.[144] However, the West would soon come to realise that Russia was not simply interested in employing political warfare tactics in its near abroad, but also to interfere in democracies around the world.

In the decade between the two Ukraine elections, Russian political warfare became increasingly covert and moved from the physical domain to the information space. The intervention in Ukraine had proved to Russia that political warfare conducted using information operations offered a faster, cheaper alternative that allowed greater plausible deniability.[145] In 2016, the hacking of the US Presidential election demonstrated how Russian political warfare techniques had grown increasingly savvy, using psychological operations to exploit existing societal tensions on social media platforms.[146] Disinformation was used to play on the fears of voters and to influence both their behaviours and voting choices.[147] Data stolen from the Democratic National Committee, as well as other political systems, was used to disrupt the election at various key points throughout the democratic process. This dissemination of information, coupled with their own propaganda and disinformation, was alleged to have been conducted by Russia to weaken the faith the US population held in their governmental institutions and to challenge established norms.[148] Exploiting social media platforms for propaganda and disinformation campaigns, these psychological operations offered the additional benefit of plausible deniability.[149] Overwhelming evidence exists that the election interference activity was directed by the Russian government at the highest level and, whilst difficult to measure the effectiveness of disinformation campaigns, Kathleen Hall Jamieson argues that it is extremely likely that Russian activity influenced the result of the election in favour of President

Trump.[150] President Trump characterised the Russian interference as a 'made up story' created to discredit his re-election; his statement was ranked as 2017's 'lie of the year'.[151] The political warfare campaign waged by Russia was not to gain re-election for Trump per se, but to discredit his rival who was considered anti-Russia.

Russia had already learned, from techniques employed by the Department for Active Measures, that for a disinformation campaign to be successful, it must contain some basis of truth for the campaign to be trusted.[152] The 'Pizzagate' conspiracy theory was created to undermine Trump's opponent. The theory that suggested Hilary Clinton was linked to a paedophile sex ring, operating from the basement of a pizza shop, was highly irrational. However, the shop *did* exist and could be verified with a simple internet search, and this gave enough credibility to the story that an outraged member of the public went to the shop to stop the atrocities being committed, opening fire with a semi-automatic weapon, despite it not even having a basement where the paedophiles were supposedly operating from.[153] A demonstration of how actors can use social media to influence populations on a grand scale, '#Pizzagate' was mentioned 1.4 million times on Twitter alone.[154] Back in 2010, Hilary Clinton had stated that the introduction of social media platforms had created a world where 'information has never been so free'; a statement that pointed to the ways these platforms spread democracy. The Russian political warfare campaigns carried out in 2016 highlighted that it also presented a new threat to the very democracy they were designed to promote.

The Russian disinformation campaigns conducted through social media spread falsehoods that played upon racial divisions and the resentments of the American voters to sway election results.[155] This disinformation was reinforced by images of social unrest and race riots to convince the US electorate that drastic changes were needed, and that Donald Trump would be the effector of these changes.[156] Between 2015 and 2017, over 30 million people shared social media posts created by the Internet Research Agency (IRA); posts designed to disrupt the democratic election by polarizing the American public.[157] But the IRA was not created to support a Trump re-election campaign, but to drive irreconcilable differences in the perception of the public because 'if we grow incapable of compromising, there can be no meaningful democracy'.[158] The extensive activities of the IRA were also accused of interfering in democratic processes of other Western nations, including the UK's EU Referendum.[159]

The UK's decision to leave the EU in 2016 was in the interests of Russia, to fragment Europe and weaken its strategic relationship with the US.[160] Credible evidence suggests that Russia used pro-Brexit disinformation campaigns, promulgated on RT and by social media trolls online, to influence the outcome of the Referendum.[161] Some Russian experts claim that Russia had little to gain from interfering in the Referendum and argue that giving the notion credibility greatly overestimates the power of Russia. If there was interference at all, it was likely to have been low level nuisance rather than a coordinated attack,[162] however, it was noted that 'the people of the United Kingdom were the targets of a scaled information operation'.[163] Arguably the Brexit result may have been the same without Russian interference

but, as the outcome was exceptionally close, it may well have tipped the balance. Inciting indignation and anger amongst the voting public put them in a more 'indiscriminately punitive mindset'.[164] Even though voters were aware that the economy was likely to suffer if the UK left the EU, the anger provoked by the Leave campaign was enough to override any fear that the consequences may induce. In the lead up to the Referendum, there were twice as many Brexit supporters on Instagram as there were Remain activists, and they were five times more active.[165] Social media companies facilitated the spread of propaganda and disinformation in sowing the seeds for chaos and disrupting democratic processes by failing to conduct any checks of the advertising campaigns performed on their platforms.[166] And whilst the UK government suspected that Russia had interfered in the Referendum, it failed to carry out a full assessment of the political warfare tactics deployed.[167] It may be politically more attractive to supress activity than acknowledge it has crossed a threshold, and it is true to say that highlighting Russian political warfare gives it greater impact, but pretending it doesn't exist at all potentially threatens democracy further.

More recently, Russia has capitalised on the COVID-19 pandemic as a tool to destabilise democratic states, in particular the US. Using disinformation and conspiracy theories to target a wide variety of audiences, Russia accused the US of creating and deliberately spreading the virus in order to maintain its world domination and weaken Russia.[168] This activity is reminiscent of the disinformation activity conducted under 'Operation Infektion'[169] conducted in the 1980s, but aided by online media and social networks, the effects of the COVID-19 disinformation narratives could be calculated in hours rather than years and reached millions of people.[170] These subversion techniques were also supported by the use of propaganda to spread negative messaging regarding how the US was dealing with the effects of the pandemic, to promote a view that democratic-led states were less able than Russia to deal effectively with a crisis.[171] Russia's objective was not to promote a different narrative per se, but a continuation of the 2016 electoral disinformation campaign to sow division and create mistrust and chaos within democratic societies.[172]

The COVID-19 pandemic offers an exemplar of how propaganda can be used to undermine an adversary. Because scientific data or facts during an emergency are rapidly changing or indeed missing, the constantly evolving narrative leaves room for disinformation to flourish where confusion exists.[173] Whilst the effects of Russian political warfare activity are difficult if not impossible to measure, recent surveys found that as high as 30% of US citizens believed that COVID-19 was either intentionally created or the severity of the virus highly exaggerated.[174] People who experience fear of uncertainty during a pandemic naturally gravitate towards disinformation, including conspiracy theories, as it fills a void of knowledge during an emerging crisis. Russia's aim was to sow discord amongst liberal nations and to create a narrative that drowns out its own failings in dealing with the pandemic.[175] Some of these narratives are preposterous, such as the social media posts and memes that appeared on the internet in October 2019, suggesting that the UK vaccine AstraZeneca had the ability to turn human being into monkeys. This activity was attributed to Russia with the UK Foreign Secretary

describing the propaganda as a significant attempt by the Kremlin to disrupt the production and dissemination of life-saving vaccines.[176]

### Summary

Russia has a long history of utilising political warfare campaigns to further its interests, but the character of twenty-first century conflict means it can be conducted at an unprecedented scale, reach and speed. Learning from the failure of the political warfare campaign conducted in the Ukraine elections is 2004, Russia turned to covert operations in its interference in the 2014 elections. The success of Russia's information operations in Ukraine may well have afforded Russia a template in which to conduct political warfare campaigns in the future. Russia used techniques developed in the Soviet era to undermine the credibility of the US election process, but with greater sophistication afforded by the technological advancements of twenty-first century conflict.[177] In the US elections, Russia sought not only to undermine the confidence of the voters regarding the integrity of the democratic process, but to influence the outcome. Though created prior to 2016, the IRA used disinformation and conspiracy theories via social media platforms to sow discord and play on societal tensions. These tactics were also demonstrated in Russia's meddling in the EU Referendum against the voting public of the UK. More recently, Russia has capitalised on the confusion generated during the COVID-19 pandemic, filling the void of scientific data and government advice to incite confusion in Western democracies. For Russia, conflict in the twenty-first century is now focused on influencing the minds of the people, rather than military victory on the battlefield.[178] The interconnectedness of populations makes it far easier for Russia to penetrate the societies of Western nations.[179] The political warfare tactics explored within the case studies are not isolated events, but part of a longer-term strategy to undermine democracy and challenge the stability of Western institutions.[180]

### Section Four: Challenges To The International Order

Russia's actions in Ukraine and interference in democratic processes has renewed focus on political warfare campaigns conducted against democratic values. This reflects a desire by Russia to restore its status as a great power within the international order and the use of subversive political warfare campaigns furthers Russian strategic objectives. By demonstrating that Russia cannot be ignored, and by discrediting the US as a suitable hegemonic power to lead the international order, the West becomes weaker and a less attractive partner than Russia for other states.[181] The political warfare campaigns waged in Ukraine may well be aimed at suppressing NATO enlargement, which Russia perceives as a great threat to its own security. By creating division amongst Western allies, the Alliance is weakened, potentially destabilising Europe.[182] Interference in democratic processes, such as the 2016 Presidential election and the UK Referendum, demonstrate how Putin views the spread of democracy as a threat to his authoritarian regime. By decreasing the stability of democratic nations, Putin therefore creates greater stability for Russia. Russian political warfare may seem to be waged in an unpredictable and reckless manner but is arguably less random or irrational than first viewed. When looking

to Russian strategic culture and its history of propaganda tactics, patterns of behaviour emerge that point to a view from Russia that foreign policy is a zero-sum game; where they can only gain if other states lose.[183] When considering the objectives of political warfare campaigns, and the features of those conducted in the grey zone in twenty-first century conflict, they present several challenges to the current global world order.

As explored in chapter one when evaluating the concept of grey zone conflict, ambiguity is a defining characteristic; who is conducting it, what they seek to gain, and when activity warrants a response.[184] Contemporary political warfare is one feature of grey zone conflict that is shrouded in deception, through the inherent nature of propaganda and disinformation activity waged, making it hard to attribute. Clear attribution of political warfare activity can reduce its effectiveness and actors seek to conduct it in a covert manner.[185] If the target audience knows that the information originated from the Kremlin, and not other like-minded citizens, they may not be receptive to sympathising with the narrative, or indeed sharing it further to increase its spread.[186] As seen in the case study of the US election and the UK's EU Referendum in 2016, Russian narratives often mirror those already dividing a populous, and are therefore difficult to disaggregate from those of a legitimate political party.[187] Attribution is also a challenge as political warfare campaigns waged in the information space offer anonymity and therefore plausible deniability. It is these features that make it attractive to revisionist actors seeking to challenge the US-led liberal international order, but understanding why they desire change is also complex.[188] The gradual approach adopted by Russian political warfare tactics makes it difficult for democratic states to identity when it is being attacked and how to delineate between legitimate and illegitimate behaviours. The case study of Russian interference in the Brexit Referendum demonstrates that 'by the time target states are in a position to retaliate or investigate, the damage has been done'.[189]

Some scholars argue that if we want to end grey zone conflict with Russia and counter its political warfare campaigns, we need to understand their motivations.[190] This paper has examined the strategic culture of Russia which identified two potential drivers in its desire to undermine the international order; security concerns over the sanctity of borders within its near abroad, and the perceived right to great power status. This presents a further challenge to the international order as understanding the primary of these two concerns arguably drives the response options that need to be considered, as both have different policy implications.[191] Without knowing whether Russia is principally motivated by concerns over security or a desire for recognition makes it difficult to know which strategies are more or less likely to be successful. If it is the former that is the dominant driver for Russia's revisionist tendencies, then it may be possible to alleviate these concerns with collaborative policies, such as arms control treaties or information sharing agreements.[192] However, potential solutions are far more complex if the desire to regain global power status is principal for Russian political warfare activity. It is much harder to establish a common ground and, as concerns over status are relational, the increase in power is likely to come at a cost to other states.

Identifying Russia's principal motivation is difficult, but understanding its long-term strategy is arguably more so. Cohen and Radin assess tactics adopted by Russia to be part of a 'soft strategy' where a linear path between actions and desired outcomes is unnecessary.[193] Instead, Russia wages contemporary political warfare with strategic patience; the hope that one day they may advance the Kremlin's objectives.[194] This in turn makes the long-term effect of Russian political warfare campaigns incredibly difficult to both identify and evaluate. Galeotti popularised the term the 'Gerasimov doctrine' (but later clarified that such a document did not exist), adding that Russia's 'campaign is dangerous precisely because it has no single organising principle'.[195] He argues that the behaviour of Russia is opportunistic and it is unclear whether an overarching strategic intent exists at all.[196] The political warfare tactics conducted by the Kremlin have been characterised as a 'firehose of falsehoods' as a way to describe the sheer volume of propaganda activity conducted by Russia.[197]

Whilst this paper does not make recommendations for response options, it is important to highlight the complexities in their consideration. Western democracies are unable to engage in the type of grey zone conflicts that revisionist states conduct as they are responsible for upholding the values and norms of the post-Cold War international system, which in turn limits the range of options available to counter Russian political warfare.[198] This presents a challenge to the liberal world order in not only understanding the threat these tactics present, but how to respond.[199] If you respond in strength this may inadvertently support Russia's claims of injustice and its 'narrative of grievance'.[200] Failure to respond at all may signal to Russia, and other revisionist powers, that we live in an age of impunity where aggressive actions conducted in the information space go unchallenged by the international community. Both courses of action hold a dangerous risk of escalation.

Operations conducted in the grey zone are deliberately designed to deny the ability to respond with certainty that a violation has occurred.[201] Russian activity in Ukraine was conducted over a protracted period, gradually unfolding rather than presenting an obvious decision point for action. Carrying out aggressive behaviour over years, or even decades, these 'salami' tactics provide less ability for decisive responses – and thus 'less ability to make unambiguous deterrent threats'.[202] The US has recently imposed sanctions against Russia over alleged election interference in 2016 (and subsequently 2020). Whilst the expulsion of diplomats from the US is unlikely to be of concern to Putin,[203] the economic sanctions are potentially more damaging to his resolve. Russia, in response to the announcement of the sanctions, responded with a threat that 'such aggressive conduct will of course get a decisive response'.[204] As the US received statements in support of its actions by NATO, the EU and the UK, there appears to be general agreement from the international community that a hard line needs to be taken to defend the democratic values of the global world order. The sanctions may feel warranted by societies in the West, but it is unknown how the perception of proportionality will be felt in the Kremlin. However, given Russia's strategic culture and view that it is merely a victim of the West, the sanctions may be unlikely to act as a deterrence to Putin's desire to further undermine the US-led liberal system that denies Russia its rightful status as a great power. The sanctions may

be seen by Russia as the West's own political warfare campaign, aggravating it into responding in increasingly aggressive ways. The difficulty of knowing when a threshold has been reached is complex, and the fact that these sanctions have been announced five years after the event, proves again how difficult attribution is when considering grey zone political warfare. The damage has already been done and Russia has already gained the strategic advantage it sought. Even where attribution is relatively clear, a further challenge is that of how to respond to Russian political warfare tactics with proportionality, and a greater challenge yet is whether responses are perceived to be proportional.

In most Western states, the right to free speech is sacrosanct and whilst it is the greatest strength of democracy, in the information age it is also its greatest weakness. Online propaganda created by Russia can be spread by citizens who are merely exercising their right to express their political opinion. By targeting pre-existing divisions amongst voters in both the US Presidential election and UK Referendum, Russia was able to influence democratic society. As an authoritarian state, Russia is not concerned with being a 'truth-teller', so even if the source of the disinformation can be directly attributed to the Kremlin, highlighting the activity does not undermine Russia's credibility.[205] Political warfare was not always the preserve of authoritarian states and was a widely used tactic by the US during the Cold War. But in today's era of transparency in liberal democracies, the 'dark arts' of political warfare are hard to reconcile with democratic values.[206] The West holds democratic values as inviolable, whereas Russia holds sovereign statehood as the primary focus and therefore both hold significantly different views on what underpins world politics, and therefore the legitimacy of its strategic behaviours.[207]

The current international system's foundations are based upon democratic values and cooperation through international institutions.[208] As a key feature of the liberal rules-based order, operating within an alliance can also pose a potential challenge for Western nations combatting contemporary political warfare. Whilst NATO is seeking to develop collective responses, individual nations will arguably need to maintain the ability to react, as waiting for collective agreement could mean losing the opportunity to respond; either because the response moves from countenance to punishment, or because the adversary has already gained the advantage.[209] NATO members will each have varying degrees of risk appetite and differing relations with an aggressor state. With regards to Russia, some countries rely upon workable relations for national interests, whereas others do not.[210]

## Summary

The information era of the twenty-first century has undermined the belief that more information would lead to greater democracy.[211] Malign actors, such as Russia, exploit the interconnectedness of the globe as a means of projecting influence in the grey zone and minimising conventional escalation. The challenge with countering Russian aggression conducted in the information space is self-perpetuating as the difficulties in deciding how and when to respond can lead to inaction by Western nations. The lack of political will to

counter political warfare activity emboldens Russia to continue its operations in the grey zone, which in turn reinforces to Russia that it can act with impunity, and therefore threatens the stability of the international world order.[212] Arguably, Russia's use of political warfare is unchanged and builds upon tactics employed during the Cold War, focussing on obfuscation and deniability.[213] What has changed is Russia's standing on the world stage and its place in the international order. A once great power, Russia cannot compete militarily with the US or NATO and has sought out methods in which it can destabilise democracies. By undermining liberal institutions, Russia increases its own security by making others less so.[214]

Seemingly unconcerned with how these actions are viewed by the international community, this brings a great challenge in how Western nations should seek to challenge these behaviours. As explored throughout this paper, Russia seeks both recognition of great power status and security over its perceived sphere of influence. How much is down to strategic culture is debatable, but the influence of Putin, with his experiences of operating in the KGB and preference for covert political warfare, is arguably key in the geopolitics of Russia. Whilst Russian meddling in the affairs of Western nations is challenging the international order to some degree, it is better than an attempt to topple Putin and potentially create a Russia in chaos, which is arguably far more dangerous to the global world order.[215]

## Conclusion

'By persistently injecting doubt into citizens' minds regarding the integrity of their democratic institutions, Russian activities may erode confidence in liberal democracy itself'.[216]

This research paper first defined the character of conflict in the twenty-first century, which is increasingly waged in the information space where technological advancements have transformed the notion of the battlespace. Not only do states need to be prepared for traditional military conflict, but they also need to consider how the war of the narrative is carried out online to destabilise the global world order; commonly characterised as a US-led rules based international order that has endured since the end of the Cold War. IOpC 2025 identified the challenge revisionist states pose to this order and proposes ways to respond to Russia's use of contemporary political warfare by building on the strengths of the UK's people, allies and through innovation, whilst respecting the norms of the rules-based system. Competing with an adversary for whom there is no distinction between war and peace, the UK also needs to adopt a pre-emptive strategy in countering political warfare and consider actions as part of a continuous campaign, as Russia does. Whilst the concept looks at how to respond, it fails to address the challenges in doing so. In identifying how contemporary political is waged in the modern era, chapter one of this research paper examined the discourse on the operational space used in twenty-first century conflict, including hybrid warfare and the grey zone. Whilst hybrid warfare offers some utility in defining contemporary conflict, it focuses on armed conflict as the dominant feature where information operations are a supporting function to military.

The grey zone encompasses the strategic level, concerned with the revisionist ambitions of the actor that conducts it, and where traditional military methods are less dominant and information operations can be conducted as stand-alone activity over a protracted period.[217] The grey zone can be defined as the space between peace and war where conflict is waged below the threshold that would warrant an armed response and where attribution is difficult.[218] As the Russian activity examined throughout the case studies point to a revisionist state seeking to disrupt the US-led international order, it is the definition that has been used throughout this paper. The Kremlin do not necessarily consider activity conducted within the grey zone as a prelude to conventional armed conflict, but as an alternative.[219]

Also explored in chapter one was the term political warfare, first coined in 1948 to describe the use of any means available to the state, short of actual war, to achieve strategic goals.[220] This definition is too broad and by stating that 'all means' can be utilised goes beyond the political component. As this research paper has been concerned with activity conducted in the information space, a narrower definition of political warfare has been adopted. Political warfare encompasses psychological operations, often conducted via social media, to manipulate information, and therefore opinions, to shape political outcomes.[221] In support of the desired outcomes of political warfare, information warfare is a tool for hostile actors where the use of narratives shape perceptions and influence the actions of the target audience. One technique commonly used by Russia is the use of psychological operations to manipulate these audiences in the cognitive battlespace through propaganda and disinformation. Political warfare is not new, but the anonymity and ubiquity of the online information space offers a greater challenge to the US-led liberal world order by targeting democratic values. The objective of political warfare is to sow confusion amongst a populous. In twenty-first century conflict, propaganda and disinformation techniques are used to distort reality and influence the minds and behaviours of the target audience. The two techniques have many overlapping characteristics, but one distinction is that disinformation specifically relates to false information whereas literary discourse on propaganda falls short of calling its messaging dishonest. This paper briefly touched on the age-old tactic of using conspiracy theories to mobilise passions by harnessing the power of cognitive bias, but what is new is the term fake news, widely used since the US Presidential elections in 2016 as a form of disinformation deliberately spread via social media. The advent of social media was deemed to be a revolution in the sharing of free speech, but in twenty-first century conflict it has been described as 'an instrument of war', that challenges the existing norms of our political systems.[222]

In chapter two, this paper examined Russia's strategic culture as a way to understand Russia's principal motivation in explaining behaviours, and its history of political warfare to add context to the way it conducts it today. Russia's contemporary political warfare tactics have similarities to those waged during the Cold War, but now exploit the power of the internet and social media platforms as tools to exert influence in Western politics. Russia employs a multitude of instruments to wage political warfare in the twenty-first century. As demonstrated during the

case studies, not only does Russia exert influence in its near abroad as seen in the Ukrainian elections, it also seeks to create division amongst Euro-Atlantic nations, by exploiting the openness of democratic systems by interfering in the processes that underpin them and waging political warfare in the information space.[223] As examined when considering the meddling conducted in the EU Referendum, Russia's aggressive political warfare campaigns further Putin's view that the EU is weak and ineffective, and any decline only strengthens the conditions for a revision of the international order in Russia's favour.[224] Capitalising on the chaos created during the COVID-19 pandemic, Russian opportunism used conspiracy theories in an attempt to discredit democratic institutions and sow confusion and discord amongst their populaces. Russia's zero-sum approach to international relations sees attempts to undermine adversaries and, in turn, promote its own security.

Whist this paper did not seek to make recommendations for response options, it aimed to identify the complexities in their consideration. Political warfare activity conducted in the grey zone, which is often shrouded in deception, makes attribution difficult and the examples explored highlight how anonymity and plausible deniability make it an attractive option for revisionist states seeking to challenge the international order. Understanding a state's primary motivation for conducting political warfare campaigns can be useful in devising strategies to counter grey zone conflict but, as identified when exploring Russia's strategic culture and throughout the case studies, it is difficult to identify and therefore developing an effective strategy is complex. One of the greatest challenges is the consideration of response options. The West is guided by the principals of free speech and freedom of information which underpin democracy, which in turn limits its response options. However, failure to respond at all may signal to Russia that it can act with impunity and demonstrate to other potential revisionist powers that conducting political warfare in the grey zone goes unchallenged. President Biden has subsequently issued sanctions to Russia for interference in Presidential elections, but it is too early to analyse their effectiveness in reducing Russia's aggressive actions. Russia increasingly expresses dissatisfaction with the power balance of the international order, and by using political warfare campaigns conducted within the grey zone, it can exert influence by attempting to undermine Western democracies.[225]

Whilst political warfare is not a new concept, technological advancements have irrevocably changed the way states and other actors conduct political warfare in twenty-first century conflict. The use of propaganda tactics and disinformation subvert democratic processes and challenge the post-Cold War liberal world order. The information age should have been an advantage to open democratic societies where freedom of speech is central and should have, in turn, hampered the ability of authoritarian states to control the narrative.[226] Instead the ability to wage political warfare with plausible deniability has grown with each advancement in technology, increasing the speed, reach and range of subversive tactics and number of actors that can operate in the information space. The introduction of the internet and social media platforms has made political warfare far more effective and pervasive. Russian political warfare campaigns sow doubt and confusion and force voters to question the validity of the

democratic systems that promote freedom of speech, leaving voters to question what is truth and what is mendacity, and severely threatens the political legitimacy of democracy.[227]

There is a consensus that Russia seeks to challenge the US-led international order, but a failure to agree on the extent to which it undermines the democratic values that underpin it. Some scholars and commentators suggest that Russia is a purely defensive power, seeking changes within the global world order rather than a revisionist state wishing to overturn it.[228] Russian political warfare campaigns, as demonstrated by the case studies, challenge the legitimacy of democratic processes that underpin the liberal world order. The extent to which these campaigns pose challenges to the international order is debatable, but simply talking about them undermines the faith people hold in democracy. Western nations, such as the UK, have recently given the threat posed by Russian political warfare attention where previously they assumed "our adversaries would see the world as we did".[229] If, as Kennan stated in 1948, political warfare encompasses all instruments of power, the UK's integrated approach to the way each government department operates recognises that a purely military response is not the answer. Some authors judge Russia to be slowly embracing European values, albeit this is likely to take decades.[230] The best the international order can hope for is containing Russia's actions by minimising the opportunities available for meddling in Western democracy, however unpalatable that appears.[231] Other actors are watching this exchange with interest, and learning how tactics can be employed with a similar strategy to further their own interests without contest.[232] The real challenge for the international order may be yet to come.

## Notes

[1] Carter, N. *Annual Chief of Defence Staff Lecture 2018* (London: RUSI, 11 December 2018). Available at: https://rusi.org/event/annual-chief-defence-staff-lecture-and-rusi-christmas-party-2018 (accessed 1 February 2021).
[2] Ibid.
[3] Ministry of Defence. *Introducing the Integrated Operating Concept* (London: Ministry of Defence, 2020). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/922969/20200930_-_Introducing_the_Integrated_Operating_Concept.pdf (accessed 12 March 2021): 5
[4] Gelven, M. *War and Existence: A Philosophical Inquiry* (Pennsylvania: Pennsylvania State University Press, 1994).
[5] NATO. *NATO Summit Guide: Brussels, 11-12 July 2018*. (Brussels: NATO Public Diplomacy Division, 2018).
[6] Tsygankov, *A. P. The Revisionist Moment: Russia, Trump, and Global Transition, Problems of Post-Communism* (2020), DOI: 10.1080/10758216.2020.1788397.
[7] Cottle, D., Keys, A., and Costigan, T. 'Contemporary Challenges to the US-led Liberal International Order from the United States and the Rising Powers of China and Russia', *Rising Powers Quarterly* (2009), 4(1): 57-75. Available at: https://risingpowersproject.com/quarterly/contemporary-challenges-to-the-u-s-led-liberal-international-order-from-the-united-states-and-the-rising-powers-of-china-and-russia/ (accessed 14 February 2021).

[8] Ikenberry, G. J. 'Liberal Internationalism 3.0: America and the Dilemmas of Liberal World Order'. *Perspectives on Politics* (2019), 7(1): 71–87. DOI: 10.1017/S1537592709090112.
[9] Kupchan, C A. No One's World: The West, the Rising Rest, and the Coming Global Turn. (New York: Oxford University Press, 2012).
[10] Fridman, O., Kabernik, V., and Pearce, J. C. (eds.), Hybrid Conflicts and Information Warfare: New Labels, Old Politics (London: Lynne Rienner Publishers, 2019). Available at: http://ebookcentral.proquest.com/lib/kcl/detail.action?docID=5541147 (accessed 12 May 2021):14.
[11] NATO. Framework for Future Alliance Operations 2018. Available at: https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf (accessed 13 May 2021): 10.
[12] Diplomatic, Information, Military and Economic.
[13] Robinson, L., Helmus, T. C., Cohen, R. S., Nader, A., et al. The Growing Need to Focus on Modern Political Warfare (Santa Monica: RAND Corporation, 2019). Available at: https://www.rand.org/pubs/research_briefs/RB10071.html (accessed 22 May 2021): 2.
[14] Chivvis. 'Hybrid War': 319.
[15] Silverman, D. Doing Qualitative Research: A Practical Handbook (London: Sage, 2013).
[16] Williams, M. Key Concepts in the Philosophy of Social Research (London: Sage, 2016).
[17] Cresswell, J. W. Research Design: Qualitative, Quantitative, and Mixed Methods (London: Sage, 2018).
[18] Fridman. Hybrid Conflicts and Information Warfare: 9.
[19] Galeotti, M. 'Takeaway Interview – Russia & Putin in the Age of COVID-19 with Mark Galeotti'. Centre for Historical Analysis and Conflict Research, 9 June 2020. Available at: https://chacr.org.uk/2020/06/09/podcast-chacr-take-away-interviews-episode-10-russia-putin-in-the-age-of-covid-19-with-mark-galeotti/ (accessed 27 April 2021).
[20] Ball, J. 'What is Hybrid Warfare', Global Security Review (2019). Available at: https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/ (accessed 2 April 2021).
[21] Rusnakova, S. 'Russian New Art of Hybrid Warfare in Ukraine', Slovak Journal of Political Sciences (2017), 17(3-4): 343-380. Available at: https://www.researchgate.net/publication/321955926_Russian_New_Art_of_Hybrid_Warfare_in_Ukraine (accessed 12 April 2021).
[22] Munteanu, R. 'Hybrid Warfare - The New Form of Conflict at the Beginning of the Century', Strategic Impact (2015), (56): 19-26. Available at: https://search.proquest.com/scholarly-journals/hybrid-warfare-new-form-conflict-at-beginning/docview/1753209782/se-2?accountid=11862 (accessed 10 April 2021).
[23] Piotrowski, M. A. 'Hezbollah: The Model of a Hybrid Threat', The Polish Institute of International Affairs (2015), 24(756):1. Available at: https://www.pism.pl/files/?id_plik=19320 (accessed 7 April 2021).
[24] Ministry of Defence. Allied Joint Doctrine for Psychological Operations: Allied Joint Publication-3.10.1 (Swindon: Development, Concepts and Doctrine Centre, 2014). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (accessed 5 April 21).

[25] Gow, J., Dijxhoorn, E., Verdirame, G., and Kerr, R, (eds.). *Routledge Handbook of War, Law and Technology*. (Milton: Taylor & Francis Group, 2019). Available at: https://ebookcentral.proquest.com/lib/kcl/reader.action?docID=5773084 (accessed 13 April 2021): 3.
[26] Puyvelde, D van. 'Hybrid warfare - does it even exist?', *NATO Review* (2015). Available at: https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html (accessed 24 May 2021).
[27] Hoffman, F. 'On Not-So-New Warfare: Political Warfare vs. Hybrid Threats', *War on the Rocks* (2014). Available at: http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybridthreats/ (accessed 3 May 2021).
[28] Betz, B. *The Idea of Hybridity. In, Fridman, O., Kabernik, V., and Pearce, J. C. (eds.), Hybrid Conflicts and Information Warfare: New Labels, Old Politics* (London: Lynne Rienner Publishers, 2019). Available at: http://ebookcentral.proquest.com/lib/kcl/detail.action?docID=5541147. (accessed 12 May 2021): 23.
[29] Wither, J. K. 'Making Sense of Hybrid Warfare', *Connections: The Quarterly Journal* (2016), 15(2). Available at: https://search.proquest.com/scholarly-journals/making-sense-hybrid-warfare/docview/1784582336/se-2?accountid=11862 (accessed 18 April 2021): 79.
[30] Radin, A., Demus, A., and Marchinek, K. 'Understanding Russian Subversion: Patterns, Threats and Responses', Perspective (Santa Monica: RAND, 2020). Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE331/RAND_PE331.pdf (accessed 2 June 2021): 2.
[31] Carment, D., and Belo, D. *War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare* (Calgary: Canadian Global Affairs Institute, October 2018). Available at: https://www.researchgate.net/figure/Comparison-between-Grey-Zone-and-Hybrid-Warfare-Characteristics_tbl1_334959464#:~:text=In%20gray%20zone%20conflicts%20states,(Carment%20and%20Belo%202018)%20. (accessed 27 May 2021): 5.
[32] Ibid.
[33] Hoffman, F. G. 'Examining complex forms of conflict: Gray zone and hybrid challenges', *Prism: A Journal of the Center for Complex Operations* (2018), 7(4): 30-47. Available at: https://search.proquest.com/scholarly-journals/examining-complex-forms-conflict-gray-zone-hybrid/docview/2156325964/se-2?accountid=11862 (accessed 10 April 2021).
[34] Lyle, J., Morris, L., Mazarr, M., Hornung, J., et al. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica: RAND Corporation, 2019). Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf (accessed 25 May 21): 8.
https://www.japcc.org/electromagnetic-operations-in-grey-zone-conflicts/
(accessed 10 April 2021): 8.
[35] Elkus, A. '50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense,' *War on the Rocks*, 15 December 2015. Available at: https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/ (accessed 21 May 2021).
[36] Mazarr, M. J. 'Struggle in the Gray Zone and World Order', War on the Rocks, 22 December 2015. Available at: https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/ (accessed 21 May 2021).

[37] Matisek, J. 'Shades of Gray Deterrence: Issues of Fighting in the Gray Zone', *Journal of Strategic Security* (2017), 10(3). Available at: https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1589&context=jss (accessed 25 May 2021): 2.
[38] Bensahel, N. 'Darker Shades of Gray: Why Gray Zone Conflicts Will Become More Frequent and Complex', *Foreign Policy Research Institute*, 13 February 2017. Available at: https://www.fpri.org/article/2017/02/darker-shades-gray-gray-zone-conflicts-will-become-frequent-complex/ (accessed 21 May 2021).
[39] Ibid.
[40] Payne, K. 'The Media as an Instrument of War', *Parameters* (2005), 35(1): 81-93. Available at: https://search.proquest.com/scholarly-journals/media-as-instrument-war/docview/198026659/se-2?accountid=11862 (accessed 16 April 2021): 81.
[41] Dowse, A., and Bachman, S-D. 'What is 'hybrid warfare and what is meant by the "grey zone"?', *The Explainer*, 17 June 2019. Available at: https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841 (accessed 12 May 2021).
[42] Kennan, G. F. *Policy Planning Staff Memorandum 269 dated 4 May 1948* (Washington: U.S. State Department, 1948). Available at: http://academic.booklyn.cuny.edu/history/johnson/65ciafounding3.htm (accessed 15 April 2021).
[43] Hoffman. 'On Not-So-New Warfare'.
[44] Cohen, R and Robinson, L. 'Political Warfare is Back with a Vengeance', *The RAND Blog*, 13 April 2018. Available at: https://www.rand.org/blog/2018/04/political-warfare-is-back-with-a-vengeance.html (accessed 15 April 2021).
[45] Jensen, B. 'The Cyber Character of Political Warfare', *The Brown Journal of World Affairs* (2018), 24(1). Available at: https://search.proquest.com/docview/2096550014/fulltextPDF/109ABA66993E4DC8PQ/1?accountid=11862 (accessed 15 April 2021): 168.
[46] Gross, M and Meisels, T. (eds.). *Soft War: The Ethics of Unarmed Conflict* (Cambridge: Cambridge University Press, 2017): 10.
[47] Wither. 'Making Sense of Hybrid Warfare'.
[48] Galeotti. '*Takeaway Interview*'.
[49] Paterson, T., and Hanley, L. 'Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'', *Australian Journal of International Affairs* (2020), 74(4). Available at: https://www.tandfonline.com/doi/pdf/10.1080/10357718.2020.1734772?needAccess=true (accessed 24 May 2021): 440.
[50] Paterson. and Hanley. 'Political warfare in the digital age': 444.
[51] Giles, K. *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016). Available at: https://www.natolibguides.info/hybridwarfare/reports (accessed 1 Apr 2021): 6.
[52] Giles. *Handbook of Russian Information Warfare*: 6.
[53] Gross and Meisels. *Soft War*: 88.
[54] NATO. Framework for Future Alliance Operations 2018. Available at: https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf (accessed 13 May 2021): 14.
[55] Galeotti. 'The "Gerasimov Doctrine" and Russian Non-Linear War'.
[56] Danesi. *The Art of the Lie: How Manipulation of Language Affects our Minds* (Lanham, MD; Prometheus Books, 2020): 204.

[57] Ibid: 206.
[58] Schleifer, R. 'Psychological Operations: A New Variation on an Age Old Art: Hezbollah Versus Israel', *Studies in Conflict & Terrorism* (2006), 29(1): 1-19. DOI: 10.1080/10576100500351185.
[59] Ministry of Defence. *Allied Joint Doctrine for Psychological Operations: Allied Joint Publication-3.10.1* (Swindon: Development, Concepts and Doctrine Centre, 2014). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (accessed 5 Apr 21).
[60] Waltzman, R. *Weaponization of Information: The Need for Cognitive Security* (Santa Monic, California: RAND Corporation, 2017). Available at: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf (accessed 23 February 2021).
[61] Danesi. The Art of the Lie: 86.
[62] Jackson, D. 'Distinguishing Disinformation from Propaganda, Misinformation, and "Fake News"', National Endowment for Democracy (2018). Available at: https://www.ned.org/wp-content/uploads/2018/06/Distinguishing-Disinformation-from-Propaganda.pdf (accessed 4 June 2021).
[63] Fetzer, J. H. 'Disinformation: The Use of False Information', Minds and Machines (2004), 14: 231–240. Available at: https://link.springer.com/article/10.1023/B:MIND.0000021683.28604.5b (accessed 24 May 2021).
[64] Floridi, L. 'Semantic Conceptions of Information', Stanford Encyclopedia of Philosophy (2005). Available at: http://plato.stanford.edu/entries/information-semantic (accessed 24 May 2021).
[65] Monmonier, M. How to Lie with Maps (Chicago: University of Chicago Press, 1991).
[66] House of Commons. Disinformation and 'fake news': Interim Report (London: House of Commons, 2018). Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf (accessed 12 May 2021): 4.
[67] Danesi The Art of the Lie: 102.
[68] Shinar, C. 'Contemporary Narratives in Russian Politics: From Stalin to Putin', *European Review* (2018), 26(4): 649. Available at: https://www.cambridge.org/core/journals/european-review/article/conspiracy-narratives-in-russian-politics-from-stalin-to-putin/4E0BD0A98746D696A5D6A2D41AD1642C (accessed 16 May 2021).
[69] Shlapentokh, V. 'Fear of the Future in the Modern world: a Russian Case', *International Journal of Comparative Sociology* (1998), 39(2): 161.
[70] Cummings, W. 'Conspiracy Theories: Here's what drives people to them, no matter how wacky', *USA Today*, 23 December 2017. Available at: https://eu.usatoday.com/story/news/nation/2017/12/23/conspiracy-theory-psychology/815121001/ (accessed 19 May 2021).
[71] Paxton, R. The Anatomy of Fascism (New York: Vintage, 2004): 44.
[72] Danesi. *The Art of the Lie*: 89.
[73] Dice, M. *The True Story of Fake News: How Mainstream Media Manipulates Millions* [Kindle version]. (The Resistance Manifesto, 2017)): 35.
[74] Ofcom. *News Consumption in the UK: 2020*. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0013/201316/news-consumption-2020-report.pdf (accessed 12 May 2021); 9.
[75] Danesi. *The Art of the Lie*: 86.

[76] House of Commons. *Disinformation and 'fake news': Final Report* (London: House of Commons, 2019). Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/2184/2184.pdf (accessed 12 May 2021): 5.
[77] European Commission. 'Fake News and Disinformation Online', *Eurobarometer Report FL6464* (European Union, March 2018). Available at: https://europa.eu/eurobarometer/surveys/detail/2183 (accessed 20 May 2021).
[78] Ibid.
[79] Singer, P. W., and Brooking, E. T. *LikeWar: The Weaponization of Social Media* (New York: First Mariner Books, 2019): 130.
[80] Dice. *The True Story of Fake News*: 639.
[81] Ofcom. *News Consumption in the UK: 2020*. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0013/201316/news-consumption-2020-report.pdf (accessed 12 May 2021): 6.
[82] Allen, R. 'Social Media Marketing Trends 2020', *Smart Insights*, 8 January 2020. Available at: https://blog.gwi.com/chart-of-the-day/9-in-10-getting-news-online/ (accessed 26 May 2021).
[83] McGrath, F. '9 in 10 Getting News Online', *GWI*, 8 January 2020. Available at: https://blog.gwi.com/chart-of-the-day/9-in-10-getting-news-online/ (accessed 27 May 2021).
[84] Payne. 'The Media as an Instrument of War': 81.
[85] Moore. *Democracy Hacked*: xi.
[86] Bradshaw, S., and Howard, P. N. 'Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation', *The Computational Propaganda Project report* (2018). Available at: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf (accessed 28 May 2021): 3.
[87] Danesi. *The Art of the Lie*: 205-206.
[88] Gray, R. 'Lies, Propaganda and Fake News: A Challenge for our Age', BBC, 1 March 2021. Available at: https://www.bbc.com/future/article/20170301-lies-propaganda-and-fake-news-a-grand-challenge-of-our-age (accessed 18 May 2021).
[89] Cull, N. J., Pomerantsev, P., Applebaum, A., and Shawcross, A. *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It* (London: LSE Consulting, 2017). Available at: https://www.lse.ac.uk/business-and-consultancy/consulting/consulting-reports/soviet-subversion-disinformation-and-propaganda-how-the-west-fought-against-it (accessed 24 May 2021): 33.
[90] Bradshaw and Howard. 'Challenging Truth and Trust': 4.
[91] Kaempf, S. In: Gross, M and Meisels, T. (eds.). *Soft War: The Ethics of Unarmed Conflict* (Cambridge: Cambridge University Press, 2017): 104.
[92] Galeotti. 'The "Gerasimov Doctrine" and Russian Non-Linear War'.
[93] Galeotti, M. *Russian Political War: Moving Beyond the Hybrid* (Milton: Taylor & Francis Group, 2019) Available at: https://ebookcentral.proquest.com/lib/kcl/reader.action?docID=5721531 (accessed 10 April 2021): 103.
[94] Gerasimov, V. 'The Value of Science is the Foresight', *Military Review*, January-February 2016.. Available at: https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf (accessed 17 May 2021): 3.
[95] Galeotti. Russian Political War: i.

[96] Kremlin. Speech and the Following Discussion at the Munich Conference on Security Policy, 10 February 2007. Available at: http://en.kremlin.ru/events/president/transcripts/24034 (accessed 27 May 2021).
[97] Moore. Democracy Hacked: 75.
[98] Geneva Centre for Security Sector Governance. National Security Policy. DCAF Backgrounder. Available at: https://securitysectorintegrity.com/defence-management/policy/ (accessed 1 March 21).
[99] Skak, M. 'Russian Strategic Culture: The Role of Today's Chekisty', Contemporary Politics (2016), 22(3): 324-341.
[100] Moore. Democracy Hacked: 76.
[101] Baylis, J., Wirtz, J., and Gray, C. Strategy in the Contemporary World: An Introduction to Strategic Studies (6th ed.). (Oxford: Oxford University Press, 2016).
[102] Ibid: 84.
[103] Schmitt, O. 'When are Strategic Narratives Effective? The Shaping of Political Discourse through the Interaction between Political Myths and Strategic Narratives', Contemporary Security Policy (2018). Available at: https://www.tandfonline.com/doi/abs/10.1080/13523260.2018.1448925?journalCode=fcsp20 (accessed 20 May 2021).
[104] Galeotti, M. 'Takeaway Interview'.
[105] Moore. *Democracy Hacked*: 78.
[106] Danesi. *The Art of the Lie*: 102.
[107] Moore. *Democracy Hacked*: 79.
[108] Cull, Pomerantsev, Applebaum and Shawcross. *Soviet Subversion, Disinformation and Propaganda*: 17-18.
[109] Singer and Brooking. *LikeWar*: 104.
[110] Rid, T. *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020): 302.
[111] Ellick, A.B., Westbrook, A., and Blackwell, A. 'How Disinformation is Taking over the World'. YouTube video, posted by *The New York Times*, 20 November 2018. Available at: https://www.youtube.com/watch?v=yA-FCxFQNHg (accessed 4 May 2021).
[112] Rid. *Active Measures*: 306.
[113] Singer and Brooking. LikeWar: 109.
[114] US Department of State. 'Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-1987' (August 1987). Available at: https://www.globalsecurity.org/intell/library/reports/1987/soviet-influence-activities-1987.pdf (accessed 4 May 21): 33.
[115] Dickey, J.V., et al. *Russian Political Warfare: Origin, Evolution, and Application* (Monterey, California: Calhoun, 2015). Available at: https://calhoun.nps.edu/handle/10945/45838 (accessed 16 April 2021): 2.
[116] Organization for Security and Co-operation in Europe. *Propaganda and Freedom of the Media* (Vienna: OSCE, 2015). Available at: http://www.stratcomcoe.org/~/media/SCCE/NATO_PETIJUMS_PUBLISKS_29_10.ashx (accessed 17 May 2021): 11.
[117] Pomerantsev, P and Weiss, M. 'The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money', *The Interpreter* (New York: Institute of Modern Russia,

2014). Available at: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf (accessed 24 April 2021): 15.
[118] Russia Today. 'About Us'. RT [Website]. Available at: https://www.rt.com/about-us/ (accessed 10 May 2021).
[119] Singer and Brooking. *LikeWar*: 107-108.
[120] Ibid: 108.
[121] Moore. *Democracy Hacked*: 85-86.
[122] Jensen. 'The Cyber Character of Political Warfare': 159.
[123] Ibid.
[124] Pomerantsev and Weiss. 'The Menace of Unreality': 10.
[125] Gow, Dijxhoorn, Verdirame and Kerr. *Routledge Handbook of War, Law and Technology*: 344-345.
[126] Giles, K. *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power* (London: Chatham House, March 2016), Available at: https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf (accessed 4 May 2021): 29-30.
[127] Paterson and Hanley. 'Political warfare in the digital age': 447.
[128] Galeotti. 'The "Gerasimov Doctrine" and Russian Non-Linear War'.
[129] Galeotti, M. In Pomerantsev, P and Weiss, M. 'The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money', *The Interpreter* (New York: Institute of Modern Russia, 2014). Available at: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf (accessed 24 April 2021): 14.
[130] Ressa, M. A. 'Propaganda: Weaponizing the Internet', *Rappler*, 3 October 2016. Available at: https://www.rappler.com/nation/propaganda-war-weaponizing-internet (accessed 26 May 2021).
[131] Moore. Democracy Hacked: 77.
[132] Radin, Demus and Marchinek, 'Understanding Russian Subversion': 5.
[133] Polyaka, A., and Boyer, S. P. The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition (Washington: Brookings Institute, 2018). Available at: https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf (accessed 20 May 2021): 2.
[134] Karpyak, O. 'Ukraine's Two Different Revolutions', BBC, 3 December 2017. Available at: https://www.bbc.co.uk/news/world-europe-25210230 (accessed 20 May 2021).
[135] Libicki, M. 'The Mouse's New Roar?', Foreign Policy, 117: 30-43. Available at: https://www.jstor.org/stable/1149560?seq=1 (accessed 24 May 2021): 41.
[136] Polyaka and Boyer. The Future of Political Warfare: 2.
[137] Grimes, D. R. The Irrational Ape: Why We Fall for Disinformation, Conspiracy Theory and Propaganda (London: Simon & Schuster, 2019): 13.
[138] Seddon, M. 'Documents Show How Russia's Troll Army Hit America', *BuzzFeed*, 2 June 2014. Available at: https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america?utm_term=.vfBjqD48#.lsKMAzx9 (accessed 22 May 2021).
[139] Pomerantsev and Weiss. 'The Menace of Unreality': 30.

[140] Ibid.
[141] Hoffman. 'On Not-So-New Warfare'.
[142] Dickey et al. *Russian Political Warfare*: 8.
[143] Wither. 'Making Sense of Hybrid Warfare'.
[144] Liaropoulos, A. *Russian Information Operations: A Pillar of State Power*. In: Filis, C. *A Closer Look at Russia and Its Influence in the World* (New York: Nova Science Publishers, 2019). Available at: https://www.researchgate.net/publication/346266493_Russian_Information_Operations_A_pillar_of_state_power (accessed 18 May 2021): 197.
[145] Polyaka and Boyer. 'The Future of Political Warfare'.
[146] Ibid: 2.
[147] House of Commons. Disinformation and 'fake news': 4.
[148] Jensen. 'The Cyber Character of Political Warfare': 166.
[149] Polyaka and Boyer. The Future of Political Warfare: 2.
[150] Jamieson, K. H. Cyberwar: How Russian Hackers and Trolls Helped Elect a President - What We Don't, Can't and Do Know (New York: Oxford University Press, 2018).
[151] Cummings. 'Conspiracy Theories'.
[152] Moore. Democracy Hacked: 80.
[153] Cummings. 'Conspiracy Theories'.
[154] Singer and Brooking. LikeWar: 128.
[155] Danesi. The Art of the Lie: 89.
[156] Ibid: 86.
[157] Howard, P.N., Ganesh, B., Liotsiou, D., Kelly, J., et al. The IRA, Social Media and Political Polarization in the United States, 2012-2018 (Oxford, UK: Project on Computational Propaganda). Available at: https://philhoward.org/the-ira-and-political-polarization-in-the-united-states/#:~:text=The%20IRA%20and%20Political%20Polarization%20in%20the%20United,computational%20propaganda%20to%20misinform%20and%20polarize%20US%20voters. (accessed 27 May 2021).
[158] Linvill, D., and Warren, P. 'That Uplifting Tweet You Just Shared? A Russian Troll Sent It', University of Clemson Tiger Prints (2020). Available at: https://tigerprints.clemson.edu/communication_pubs/18 (accessed 24 April 2021).
[159] Moore. Democracy Hacked: 73.
[160] Polyakova, A et al. The Kremlin's Trojan Horses: Russian Influence in France, Germany and the United Kingdom (Washington: Atlantic Council, 2016). Available at: https://www.atlanticcouncil.org/wp-content/uploads/2016/11/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf (accessed 4 May 2021):18.
[161] Sabbagh, D., Harding, L., and Roth., A. 'Russia report reveals UK government failed to investigate Kremlin interference', The Guardian, 21 July 2020. Available at: https://www.theguardian.com/world/2020/jul/21/russia-report-reveals-uk-government-failed-to-address-kremlin-interference-scottish-referendum-brexit (accessed 1 June 2021).
[162] Lis, J. 'Was there Russian meddling in the Brexit Referendum? The Tories just didn't care'. The Guardian, 21 July 2020. Available at: https://www.theguardian.com/commentisfree/2020/jul/21/russian-meddling-brexit-referendum-tories-russia-report-government

(accessed 1 June 2021).
[163] Wylie. Mindf*ck: 272.
[164] Wylie. Mindf*ck: 272.
[165] Polonski, V. 'Impact of social media on the outcome of the EU referendum', EU Referendum Analysis, 2016. Available at: https://www.referendumanalysis.eu/impact-of-social-media-on-the-outcome-of-the-eu-referendum-eu-referendum-analysis-2016/
(accessed 25 May 2021).
[166] Wylie. Mindf*ck: 273.
[167] Sabbagh, Harding, and Roth. 'Russia report reveals UK government failed to investigate Kremlin interference'.
[168] Matthews, M., Migacheva, K., and Brown, A. *Superspreaders of Malign and Subversive Information: Russian and Chinese Efforts Targetting the United States* (Santa Monica: RAND Corporation, 2021): 7.
[169] Singer and Brooking. *LikeWar*: 109.
[170] Ibid.
[171] Matthews, Migacheva and Brown. *Superspreaders of Malign and Subversive Information*: 12.
[172] Baker, B,. Kavanagh, K., and Helmus, T. C. 'A Crisis of Disinformation', *RAND Remote COVID-19 Briefing Series*, 22 May 2020. Available at: https://www.rand.org/multimedia/video/2020/05/22/covid-19-briefing-series-1.html (accessed 9 May 2021): 13.28.
[173] Grimes. The Irrational Ape: 278.
[174] Baker, Kavanagh and Helmus. 'A Crisis of Disinformation': 02.22.
[175] Grimes. The Irrational Ape: 279.
[176] Coble, S. 'UK in Cyber-War Against Anti-Vaccine Propaganda', *Info Security*, 9 November 2020. Available at: https://www.infosecurity-magazine.com/news/uk-in-cyber-war-against-anti/
(accessed 20 May 2021).
[177] Cormac, R., and Aldrich, R. J. 'Grey is the New Black: Covert Action and Implausible Deniability', *International Affairs* (2018), 94(3). Available at: https://academic.oup.com/ia/article/94/3/477/4992414 (accessed 2 April 2021): 490.
[178] Liaropoulos. Russian Information Operations: 192.
[179] Chivvis. 'Hybrid War': 316.
[180] Polyaka and Boyer. The Future of Political Warfare: 3.
[181] Radin, Demus and Marchinek. 'Understanding Russian Subversion': 4.
[182] Ibid: 5.
[183] Mathers, J. 'Vladimir Putin: how to understand the Russian president's view of the world', *The Conversation*, 18 March 2018. Available at: https://theconversation.com/vladimir-putin-how-to-understand-the-russian-presidents-view-of-the-world-93212 (accessed 1 June 2021).
[184] Bensahel. 'Darker Shades of Gray'.
[185] Radin, Demus and Marchinek. 'Understanding Russian Subversion': 3.
[186] Ibid: 1.
[187] Ibid: 14.
[188] Bensahel. 'Darker Shades of Gray'.
[189] Cormac and Aldrich. 'Grey is the New Black': 491.

[190] Galeotti, M. 'I'm sorry for creating the Gerasimov Doctrine', Foreign Policy Magazine, 5 March 2018. Available at: https://news.yahoo.com/m-sorry-creating-gerasimov-doctrine-190438481.html (accessed 1 February 2021).
[191] Schmitt, O. 'How to challenge an international order: Russian diplomatic practices in multilateral security organisations', *European Journal of International Relations* (2020), 26(3). Available at: https://journals.sagepub.com/doi/pdf/10.1177/1354066119886024 (accessed 13 March 2021): 923.
[192] Ibid.
[193] Cohen, R., and Radin, A *Russia's Hostile Measures in Europe: Understanding the Threat* (Santa Monica: RAND Corporation, 2019). Available at: https://www.rand.org/pubs/research_reports/RR1793.html (accessed 4 May 2021): 13-14.
[194] Radin, Demus and Marchinek. 'Understanding Russian Subversion': 6.
[195] Galeotti. "I'm sorry for creating the Gerasimov Doctrine".
[196] Ibid.
[197] Paul, C., and Matthews, M. *The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica: RAND Corporation, 2016). Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf (accessed 20 May 2021).
[198] Matisek. 'Shades of Gray Deterrence': 7-8.
[199] Ibid.
[200] Galeotti, M. *Russian Political War: Moving Beyond the Hybrid* (Milton: Taylor & Francis Group, 2019). Available at: https://ebookcentral.proquest.com/lib/kcl/reader.action?docID=5721531 (accessed 10 April 2021): 13.
[201] Lyle, Morris, Mazarr, Hornung, et al. *Gaining Competitive Advantage in the Gray Zone*: 9.
[202] Ibid: 9.
[203] Corera, G. 'US imposes sanctions on Russia over cyber-atacks', *The BBC*, 16 April 2021. Available at: https://www.bbc.co.uk/news/technology-56755484 (accessed 1 June 2021).
[204] Ibid.
[205] Cull, Pomerantsev, Applebaum and Shawcross. *Soviet Subversion, Disinformation and Propaganda*: 33.
[206] Paterson, T. 'The "grey zone": Political warfare is back', *The Interpreter*, 3 September 2019. Available at: https://www.lowyinstitute.org/the-interpreter/grey-zone-political-warfare-back (accessed 27 May 2021).
[207] Clunan, A. L. 'Russia and the Liberal World Order', *Ethics and International Affairs* (2018): 32(1). Available at: http://hdl.handle.net/10945/57361 (accessed 18 January 2021): 50.
[208] Nieto, I. 'Electromagnetic Operations in "Grey Zone" Conflicts: The Tool of Revisionist Countries to Confront the International Order', *Joint Air Power Competence Centre Journal* (2021), 31. Available at: https://www.japcc.org/wp-content/uploads/JAPCC_J31_screen.pdf (accessed 5 May 2021): 76.
[209] Lyle, Morris, Mazarr, Hornung, et al. *Gaining Competitive Advantage in the Gray Zone*: 35.
[210] Chivvis. 'Hybrid War': 11.
[211] Pomerantsev, P. 'The disinformation age: a revolution in propaganda', *The Guardian*, 27 July

2019. Available at: https://www.theguardian.com/books/2019/jul/27/the-disinformation-age-a-revolution-in-propaganda (accessed 30 May 2021).
[212] Nieto. 'Electromagnetic Operations in 'Grey Zone' Conflicts': 76.
[213] Paul and Matthews. *The Russian 'Firehose of Falsehood' Propaganda Model*: 1.
[214] Giles, K. *Moscow Rules: What Drives Russia to Confront the West* (London: Chatham House, 2019). Available at: https://ebookcentral.proquest.com/lib/kcl/detail.action?docID=5253422. (accessed 1 February 2021): 23.
[215] Galeotti, M. 'We Need to Talk About Putin: How the West Gets Him Wrong' (London: Ebury Pres, 2019): 141.
[216] Chivvis. 'Hybrid War': 317.
[217] Carment and Belo. *War's Future*: 5.
[218] Lyle, Morris, Mazarr, Hornung, et al. *Gaining Competitive Advantage in the Gray Zone*: 8.
[219] Galeotti. 'I'm sorry for creating the Gerasimov Doctrine'.
[220] Kennan. *Policy Planning Staff Memorandum 269 dated 4 May 1948*.
[221] Jensen. 'The Cyber Character of Political Warfare': 168.
[222] Ibid: xi.
[223] Götz, E., and Merlen, C-R. 'Russia and the question of world order', *European Politics and Society* (2019), 20(2). Available at: https://www.tandfonline.com/doi/pdf/10.1080/23745118.2018.1545181?needAccess=true (accessed 24 May 2021): 135.
[224] Dibb, P. *How the geopolitical partnership between China and Russia threatens the West* (Barton: Australian Strategic Policy Institute, 2009). Available at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-11/SR%20148%20China%20and%20Russia%20threatens%20the%20West.pdf?VersionId=D40qjgxThyiCjbwzDPmQb8H49YF0hAmW (accessed 3 May 2021).
[225] Lyle, Morris, Mazarr, Hornung, et al. *Gaining Competitive Advantage in the Gray Zone*: xiv.
[226] Freedman, L. *The Transformation of Strategic Affairs* (Abingdon: Routledge, 2006). Available at: https://ebookcentral.proquest.com/lib/kcl/detail.action?docID=1207127 (accessed 1 May 2021): 75.
[227] Omand, D. 'The Threats from Modern Digital Subversion and Sedition', *Journal of Cyber Policy* (2018), 3(1). Available at: https://www.tandfonline.com/doi/full/10.1080/23738871.2018.1448097?scroll=top&needAccess=true (accessed 1 May 2021): 5-7.
[228] Götz, E., and Merlen, C-R. 'Russia and the question of world order', *European Politics and Society* (2019), 20(2). Available at: https://www.tandfonline.com/doi/pdf/10.1080/23745118.2018.1545181?needAccess=true (accessed 24 May 2021): 133.
[229] Nicholls, D. 'Britain will regain mastery of 'political warfare' after taking 'eye off the ball' over Russian threat', *The Telegraph*, 21 May 2021. Available at: https://www.telegraph.co.uk/news/2021/05/21/exclusive-britain-will-regain-mastery-political-warfare-taking/ (accessed 24 May 2021).
[230] Galeotti. *We Need to Talk About Putin*: 141.
[231] Ibid: 141.
[232] Nieto. 'Electromagnetic Operations in "Grey Zone" Conflicts': 79.

Article

# To What Extent Does China's Increasing Influence in the Black Sea Region Promote Stability?

By Wing Commander Sarah McDonnell

**Biography:** Wing Commander Sarah McDonnell joined the Royal Air Force as a Fighter Controller, specialising as a weapons controller. She has completed several operational tours, including an exchange tour with the Royal Navy, and is a qualified Air Battlespace Manager. Latterly an E-7 Wedgetail programme manager, she graduated from the Advanced Staff Course in 2021 and will take command of Number 8 Squadron at RAF Lossiemouth, following operational conversion training on to the E-7 Wedgetail with the Royal Australian Air Force.

**Abstract:** China's economic expansionism through its Belt and Road and 17+1 initiatives has enhanced its influence in the Black Sea Region (BSR). Despite the inherency of regional instability, this influence has brought economic stability by providing alternatives to Russian investment, encouraging domestic development, and stimulating investment from the EU and US. China's growing status as a global power, and increasingly strong relationship and influence with Russia, has provided stability in deterring Russian aggression, although more complex in the longer-term. This paper considers China's geopolitical relationships with Russia, Ukraine, Georgia and Bulgaria, assessing its influence on stability, highlighting examples of China the investor, China the deterrent and China the intermediary. Whilst the Ukraine war has irrevocably altered the geopolitical dynamics of the region, if China continues to play the mediator, carefully balancing its relationship with the US and its asymmetric relationship with Russia, it will likely maintain its influence. Thus, in the long term, China is likely to promote stability in the BSR.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

## Section 1
## Introduction and Context Introduction

China is almost a global superpower and continues to grow across all facets of state power. Whether the future of China follows Pompeo's prediction of an 'authoritarian nightmare, intent on destroying democracy'[1] or Jinping's attempt to paint the 'quaint picture of Chinese pacifism,'[2] the realist, and to some extent liberalist view[3] suggest that the Western Liberal International Order (LIO) is in decline, within which China is a likely contender to US hegemony.[4] China's most obvious challenge to hegemony, has been through its growing economy, which has afforded it the economic power to be more assertive within the global economy. China now has the world's second largest economy, 'accounting for over 12 per cent of global trade and 15.5 per cent of the world's GDP.'[5] Indeed, Magalhães argues that China has become a 'globaliser'[6] in that it is able to 'affect the increase or decrease of globalism and shape its characteristics.'[7] To date, this expansion has been somewhat limited within Europe, however, under its Belt and Road Initiative (BRI), coupled with an increasing desire to access European markets, the Black Sea Region (BSR) has become a new area of interest.

It follows, that this paper does not contend the proposition that China does have influence within the BSR. Sanders, as one of the leading commentators proposes that through the BRI, China has increased its 'economic and political influence'[8] and has become an 'important player in the region.'[9] The 'economic weight, as the world's largest trading power'[10] and its global influence as a permanent member of the UN Security Council means that China has significant 'political leverage'[11] and thus even relatively modest investments in the BSR (compared to central Asia for example) have a disproportionate influence on the geopolitical environment.

This paper will evaluate the impact of this influence and examine to what extent it has been able to promote stability and whether it will continue to promote stability in the future. Although Western literature is somewhat limited, Sanders suggests that through economic investment, China is able to offer a counter to Russian investment, stimulate domestic growth, and draw continued Western investment into the region, all of which provide economic stability. Further, owing to China's growing status as a global power, and its increasing relationship with Russia, this influence, for the most part, has also been able to provide stability in deterring Russian aggression.[12] Ghisay and Zhou support this position, stating the BRI has the 'potential to support the conditions for stability…[if it can] foster inclusive and sustainable socioeconomic growth,'[13] and stimulate 'greater cooperative efforts…to address common security threats.'[14] However, they also state that it could be a source of instability by exacerbating political instability and adding financial risks.[15] Other literature suggests it could add friction to an already fraught region[16] (Russia-Ukraine and Russia- Georgia wars are cases in point) as the addition of further competition increases the likelihood of misperception of intent, and thus decrease stability should this result in retaliation.

This paper is divided into three sections. The first section, beyond the introduction, aims to contextualise the subject of China in the BSR. Specifically, it discusses the cause of instability, why the BSR is of strategic importance and China's BRI. It will show that Russia, due to its strategic culture and its perception of an existential threat through NATO expansionism, is the root cause of instability. It will then discuss how the BSR, at the confluence of major global trade routes, has developed into a region of renewed great power competition, within which China is evolving as a key competitor. This section concludes by evaluating China's BRI and discusses its strategy for the BSR. The second section considers China's geopolitical relationships with the littoral states of the BSR, focusing on Russia, Ukraine, Georgia and Bulgaria. For each it will outline the extent of China's BRI investment and discuss its immediate impact on state stability, as well as considering the long-term impact of Chinese influence in terms of how coalescing or antagonistic this may become within the future geopolitical situation.

For Russia, it discusses the complexities of their relationship with China, particularly noting the current Ukraine war. Ultimately, the asymmetry between an increasingly powerful China and a declining Russia enables China to exercise some control over Russian actions in the region, including acting as both a deterrent (in Georgia) and a mediator (in Ukraine) against military aggression. For Ukraine, despite significant investment which has provided economic stability, the war has shown that China lacks the absolute ability to temper Russia, suggesting that China's influence has limitations for stability. For Georgia, it will show how China's investment has provided stability by prompting US economic investment, limiting Russian influence. Unlike Ukraine, the sustainability of this arrangement is likely to endure, although the coexistence of China and the US in the same geography may cause friction if China attempts to translate economic influence into geopolitical dominance. Finally, for Bulgaria, counter to the proposition of this question, it will highlight that China's influence has been limited, owing to Bulgaria's membership of NATO and the EU. As a result, China has had limited opportunity to promote stability, however, in light of the Ukraine war, China may look to exploit Russian unpopularity which could increase its economic influence, and by deduction, its ability to promote stability.

The third section will conclude that China's influence in the BSR does promote stability, albeit this is not absolute and is complex. China's ability to have a long-term stabilising effect will be determined by its ability to balance its national interests whilst also maintaining its relationship with the West and managing an asymmetric relationship with Russia. The war in Ukraine will undoubtedly complicate China's ability to achieve this, and whilst the full determination of China's part in the aftermath is yet to be realised, the reassertion of US dominance into the BSR may limit China's options and therefore its means to promote stability. Here, China's actions may prove deterministic. It if remains neutral, carefully balancing its position as a mediator, it may secure its long-term influence, and therefore its ability to promote stability. Whilst economic power and influence certainly translate into geopolitical influence, Western security assurance will likely be the stronger deterrent against Russian

aggression. Therefore, until such time that China can also compete militarily, the stabilising nature of China in the BSR in the long-term may be limited.

### Methodology, Scope, Assumptions and Limitations

There is limited academic literature on China's activity within the BSR, therefore, a full literature review would yield fairly narrow analysis. Further, as much of the existing discussion has only been published within public discourse, peer review of the content is unlikely. This is particularly evident in the discussions surrounding the current Ukraine crisis. To mitigate bias of opinion, this paper has targeted arguments that are either corroborated or published by credible sources. The result, however, is that the analysis has had to be more expansive, drawing conclusions from peripheral geopolitical debates in lieu of direct evidence. Specifically, the extrapolation of literature that discusses China, Russia and Western relationships has been used to ascertain the likelihood of stability in the BSR based on observed interactions between these powers in other areas.

There are six littoral states within the BSR of which this paper explores China's relationships with Russia, Ukraine, Georgia and Bulgaria, as each of their engagements with China are all subtly different and thus offer the richness of a full discussion. Romania and Turkey are out of scope.

Romania has already firmly chosen West over East, resulting in negligible Chinese influence, thus offering little value to this discussion.[17] Turkey, however, would overpower the discussion in terms of the volume of analysis. The amalgamation of its strong Chinese allegiance, its continuing dependence on Russia, its NATO membership, its declining relationship with the West and its custodian responsibility of the Montreux convention has generated a powerful geopolitical status.[18] Thus, to try and analyse the stabilising impact of China's influence in Turkey would require a far fuller argument than could be made within this paper.

This paper will focus on China's influence through its economic power. Whilst the use of diplomatic power and subthreshold activity could provide valuable discussion, China, through the BRI, has used economic power as its primary lever of influence; examining through this lens is likely to provide the most tangible evidence for the impact on stability. This paper also works on the premise, as argued by Wagner and Deller, that a strong economy is a key proponent of stability; 'as a region's economy becomes more diversified, it becomes less sensitive to fluctuations caused by factors outside the region…[and] promotes stability.'[19] Furthermore, whilst acknowledging Nye's statement that, 'economic strength has not replaced military security,'[20] this paper predominately focusses on economic power and influence. Noting, that for now, China's main interest in the BSR has been economic.

## Context

### The source of instability

Valinakis describes the BSR as inherently prone to conflict owing to the collapse of the Soviet Union, issues over territorial claims and ethnically driven animosity.[21] Kuimov and Wezeman

concur, describing the region as an 'unpredictable and high-risk environment.'[22] Russia can be considered the common denominator for this instability, predominately as a derivative of its strategic culture. Whilst the full extent of Russia's strategic culture will not be discussed in this paper, its history, geography, and Putin are some of the key components which dictate Russian action. 'Defensiveness bordering on paranoia on one hand, combined with assertiveness bordering on pugnacity, on the other;'[23] this potent mix of psychology has repeatedly caused Russia to challenge in the physical, virtual, and cognitive domains within the BSR, all of which result in instability as these actions threaten the sovereignty of the targeted state. Putin considers NATO expansionism (12 to 30 states since 1949) to be a significant threat to Russia. Within the region, Romania, Bulgaria and Turkey are all members perpetuating Russia's threat perception,[24] aggravated by the belief that the BSR is firmly within its sphere of influence. Although in his discussion, Sankey states that 'conceptually, spheres of influence are security-enhancing because they serve as buffers to secure vital interests,'[25] this assumed deterrence, is reliant on a recognition and acceptance of their boundaries by other great powers, essentially making them 'spheres of restraint.'[26]
Whilst this arrangement held in the Cold War, the BSR does not enjoy the same neutrality. Thus, the myriad of influences in an area where Russia thinks it should dominate has already laid the foundations of instability. With the entrenched need to protect itself, Russia believes it is able to justify aggressive behaviour as defensive.[27] According to Russia, the wars with Georgia (2008) and Ukraine (2022), as well as the alleged cyber-attacks and spread of disinformation throughout the region,[28] have all been 'necessary to prevent the strategic balance from shifting decisively in NATO's favour.'[29] Putin is also keen to 'stoke fissures between alliance members along the Black Sea,'[30] and uses influence gained through energy ties as a 'geopolitical weapon.'[31] The West, as the traditional competitor in the region, has aimed to maintain regional stability through diplomacy and engagement with Russia, as well as providing the BSR states with military support.[32] For China, the composition of its economic influence and its relationship with Russia, should dampen the threat of Russian induced instability; however, in the long-term, until such time when China can exercise the full suite of state power (diplomatic, military etc), it may find that its economic influence, and stabilising nature therein, has limits.

## Why the Black Sea Region?

The BSR is a region of strategic importance due to its geographical link between Europe and Asia and the Middle East.[33] As such it has become a scene of renewed great power competition between Russia, China and the West. 'Consequently, instability, the potential for conflict, its resources and its economic prospects matter to the [entire] international community,'[34] although interestingly the perceived merits of influence in this region are subtly different for Russia and China in the context of its intentions for Eurasia. Russia needs the BSR 'to build a shell round itself to ensure its strategic security,' whilst 'China…sees the future of Eurasia as a vast corridor of trade.'[35] Russia, historically has been the biggest player in the region and 'has long seen the Black Sea as essential for projecting power and influence in to the Mediterranean and beyond.'[36] In forcing economic and energy

dependence, coupled with the threat of military action, Russia hopes it can secure allegiance, and deter further NATO expansion.[37] China, however, only see opportunity for further economic growth. Over the past 10 years the European Union (EU) has worked to deepen economic ties with China with a view to securing better access to Chinese markets. China has also made significant inroads to the BSR, through its 17+1[38] programme and its BRI, and is 'now the EU's biggest trading partner, [having] overtaken the US in 2020.'[39] Thus, the region is ripe for continued Chinese expansion. To some extent, Russian and Chinese intentions are mutually supportive in that each aims to reduce Western influence, however, Russian aggression 'may re-strengthen Euro-Atlantic ties and fracture China's ability to keep trade flowing…into Europe.'[40] Consequently, the region is likely to become more unstable, as these intentions compete. Ultimately, 'China wants to open the space…Russia wants to close it.'[41] For the West, the region can be viewed as an extension to the aims of US strategy since the end of the First World War; to ensure that 'no single state or coalition of states would dominate either Europe or East Asia.'[42] The contenders have varied; East Germany, Russia and now China, however the strategy of building a strong, neoliberal alliance through which to preserve the LIO continues to be a 'top geostrategic priority for the United States.'[43]

### China's Belt and Road Initiative

Coupled with the 17+1 mechanism, China's expansion under the BRI is likely to have significant impact in the BSR. Announced in 2013 by Jinping, the BRI is often referred to as a rejuvenation of the historic silk road,[44] and aims to provide China with increased economic corridors through investment in infrastructure. There is also hope of 'reduced physical and political barriers to trade [which should] open new markets for exporters and foster regional security through enhanced cooperation.'[45] Undeniably, improvements in infrastructure and increased connectivity are welcome investments for BSR states as they continue their growth post the collapse of the Soviet Union. Further, the digital silk road has been announced which aims to improve global connectivity through the export of communication technologies.[46] Although out of scope for this paper, the implications of this initiative are likely to yield even more complex outcomes for geopolitics as the traditional concepts of terrain and territory become increasingly obsolete.

Beyond economic gain, literature that discusses the long-term intent of the BRI is varied. Wang Jisi, China's most prominent and influential international relations scholar, described the Strategy as China's 'March West' in response to the US pivot to the South China Sea.[47] China, however, has said the BRI promises to offer benefits beyond China's borders, with no 'geopolitical gains, beyond the reputational benefits'[48] of the BRI. Carminati corroborates this statement, stating China's intent is 'firstly economic and only secondly ideological and political.'[49] In contrast, some Western critics, see the BRI as China's push to challenge the LIO; an initiative that could see developing countries indebted to China in order to 'gain strategic assets through "debt-trap diplomacy".'[50] China's investment in the Hambantota Port Development in Sri Lanka, for example. When Sri Lanka could not repay China for its

investment in Hambantota Port, they had to agree to 'sell an 80% stake [of]…the port to China,'[51] further expanding China's sphere of access and influence.

Whilst such negative connotations of the BRI exist, China's biggest limitation in successful implementation of the initiative is its lack of transparency and its inability to harness soft power relationships.[52] Culturally and ideologically China still stands as an outsider to neoliberalism. Despite China's attempt to reconcile its image,[53] Orientalism[54] still resonates globally; cognitively therefore, China still has some way before it presents an attractive alternative to Russia for the BSR. In the short-term therefore, the BRI will likely remain as a mechanism for economic investment. However, China's increasing global power, will likely mean that this economic influence gives China disproportionate geopolitical influence, thereby increasing its ability to promote stability within the BSR.

## Section 2
## China's Geopolitical Relationships China-Russia

China and Russia 'are joined not by ideology, but the avoidance of it.'[55] Under Putin and Jinping, common objectives, such as their antipathy to liberal values and their ambition to challenge the LIO, has seen their relationship mature, and strengthen. Recently the two leaders declared that their relationship has 'no limits.'[56] However, scholars such as Sutter, are not so optimistic for the future of this unconditionality. He suggests that 'economic asymmetry…limits on arms sales and defense cooperation…[and a] divergence of foreign relations'[57] create 'unevenness in their relationship,'[58] sowing resentment in Russia and caution in China, both of which may hamper their continued cooperation.

Economic asymmetry is likely the greatest source of tension; Russia is certainly the dependent junior partner. A declining Russia and a growing China has allowed China to dominate the relationship economically, from which it has also yielded geopolitical influence.[59] This dynamic is likely to become more prevalent as Russia navigates out of economic decline, exacerbated by recent sanctions; China is likely to become Russia's lifeline.

However, China's response to the war may prove deterministic for the future of the relationship. On the one hand, as China has not openly condemned the invasion and abstained from the UN General Assembly vote,[60] this could be evidence of the 'no limits' narrative and a message to the West of the strength of this partnership. Alternatively, this could be less because they owe Russia political allegiance, and more because China needs to maintain a good relationship with Russia to exploit their increased dependence on China and secure opportunity to fill Russian investment voids without fear of Russian retaliation. Furthermore, noting China's strong view on territorial integrity, abstinence could be viewed as China effectively condoning Russia's actions. Indeed, it will likely be 'interpreted [by the West] as China's indirect support for Russia's use of military force.'[61] China will, however, most likely wish to avoid such blatant support for Russia, to avoid being subject to secondary

sanctions,[62] or risk their already fragile reputation. However, to the contrary the abstention could be seen as China isolating Russia and signalling its disapproval.

China, however, persist that they remain neutral.[63] With the interdependency of the two states, coupled with the regional and global implications as a result of the war, China is currently striking a careful balance, exercising patience with Russia on one side and the West on the other before it acts decisively in the BSR. For the BSR, perceptions will be important. If the BSR states perceive China to be siding with Russia, then this will likely frame their interaction with China, and it is unlikely to be positive.

For Russia, as a consequence of its aggressive action in Syria and Ukraine, its cooperation with its near abroad, including the BSR has lost momentum.[64] This may mean they are willing to accept further Chinese economic expansion as a compromise for its own economic support from the East, as well as acceptance that if it is unable to hold economic or political influence in the region, it would rather China, over the US fill the void.

Other opportunities for China as a result of the Russia-Ukraine war could be China's ability to influence Russian military sales. In return for supporting Russia, China may demand access to Russia's top military equipment, especially, 'submarine and air-defence technology.'[65] They may also pressure Russia to limit sales to China's rivals, such as Vietnam and India.[66] There is also literature to suggest that Russia will be more malleable to China if they remain 'strategic partners' against the West. This could see China benefit from strategically positioned locations in Russia, notably the Arctic.[67] Whilst this may not immediately impact stability in the BSR, as China's hold over Russia increases, they will become even more subservient, which in turn will play out in all regions where the two countries have cooperation and influence. For the BSR, this is likely to increase stability in the near term as China capitalises on a weakened Russia. China's increased influence over Russia and within the BSR will limit Russia's aggressiveness in the region.

In summary, the increasingly asymmetrical relationship between China and Russia, exacerbated by the war in Ukraine is likely to subordinate Russia to subservience, at least in the short-term. For the BSR, this exaggerated influence beyond the BRI should mean an increase in stability. China favours a secure environment to foster economic growth, thus, with a stronger influence over Russia in the BSR, it should be able to curtail any suggestion of future or enduring aggression. Further, as the BSR states denounce Russia's invasion of Ukraine and subsequently withdraw from Russian influence, China is likely to be an increasingly attractive investment partner, which should increase economic stability and thicken the buffer to Russian influence. This, however, is dependent on the palatability of China's continued support for Russia, and whether renewed Western favourability to assure security offers China any opportunity for continued economic influence. Geopolitically, the asymmetric power relationship between China and Russia could make the BSR more of a stable environment. The war in Ukraine undoubtedly presents China with an opportunity to act as a stabilising mediator. If China,

through the deepening dependence of Russia, can curtail Russian aggression, limit subthreshold activity, whilst maintaining a healthy relationship, China, without considering the impact of individual state actions and responses, has the potential to promote long-term regional stability.

## China-Ukraine

China's relationship with Ukraine has strengthened since 1991,[68] and 'by 2019, China had replaced Russia as Ukraine's largest trading partner.'[69] Further, since 2017 an estimated $3bn has been invested in construction contracts under the BRI. Specifically, ports in Mariupol, Yuzhny and Chornomorsk have all seen large-scale investment.[70] These, coupled with the development of transport infrastructure, led Zelensky to announce in 2021 that 'he hoped Ukraine would become a bridge to Europe for Chinese business.'[71] Outside of the BRI, agriculture and defence industries have also seen Chinese investment.[72] Ukraine is now China's largest supplier of corn,[73] and China's development of its 'first aircraft carrier…is a refurbished Soviet carrier purchased from Ukraine.'[74] Generally, this economic investment, and thereby influence is seen as a stabilising factor. It acts as a catalyst for domestic development; promotes economic growth which attracts other investors and offers alternatives to Russian investment tempering Russian influence.

However, the impact of this influence on stability is fragile. Firstly, China's investment may not be economically sustainable. Secondly China's decision making may fuel geopolitical instability, and Russia has proven that, in Ukraine specifically, China is unable to deter Russian territorial and geopolitical ambitions. In terms of sustainable economic stability, even before the war, concerns over Ukrainian entrenchment with Chinese investment, meant it was at risk of becoming a 'hidden debtor'[75] to China. Revelations of debt could degrade investor confidence and the Ukrainian government may need to shoulder the remainder,[76] both of which risk economic stability. Although Gelpern suggests that lending could be serviced 'through the proceeds of commodity exports,'[77] although, the destruction of Ukraine and the ongoing naval blockade are unlikely to make this viable. Thus, China's economic influence, which promoted stability prior to the war, may potentially become a source of instability post the war. For commentators who argue that the BRI serves to 'debt trap' the invested states and allow China to exploit the dependency for geostrategic gain, Ukraine is quickly becoming an acute example. Post the pandemic, as China grapples with an overstretched lending portfolio, it may have to rebalance its existing, and curtail future lending,[78] potentially affecting BRI investments. China's investment could become destabilising for economic stability if China is unable to sustain its lending.

China's decision making over existing investments could also prevent its influence from continuing to promote stability. As discussed, China has long hailed that the BRI exists solely for economic gain.[79] However analysts such as Chang[80] and Cai[81] contend that the BRI is a tenet of grand strategy designed to reassert China's dominance in pursuit of multipolarity. Ukraine may be the test case to ascertain China's true intent. If the BRI is solely to generate economic wealth, China could well curtail its investment in Ukraine in favour of more

economically settled environments. In this scenario, China's abandonment coupled with the already muted nature of China's condemnation against Russia could lead Russia to perceive its ambivalence as acceptance, cementing the no limits narrative and consenting to continued Russian aggression. China's action and its lack of sustained economic investment thus becomes destabilising and potentially prolong the war. However, if the BRI is indeed a tool for global dominance, and it continues to support its investments in Ukraine, the sustainability of its stabilising nature is more complicated. Pursuing Ukrainian investments with at least some conscious knowledge that this is likely to engender debt, may result in regional criticism and confirm Western suspicions that the BRI is a tool for geopolitical dominance. Alternatively, continuing to support Ukrainian investment could play to its cooperation narrative, as per the headline of Jinping's speech to the United Nations in 2017,[82] and therefore enable sustained stability. China's decision making in Ukraine is therefore key. Seeking alternative investment may curtail its stabilising nature and prolong the war. Persisting in its investment may on the one hand allow for a cooperation narrative and aid stability, in contrast, maintaining economic investment in the face of expected economic loss, could confirm Western nervousness of China's long-term intent to challenge US hegemony making long-term stability less likely.

Ukraine is unlikely to simply play the onlooker and its action towards China may affect whether China's influence can promote continued stability. Sanders highlights that prior to the war, Ukraine had a difficult task in balancing its East vs West allegiances.[83] Post the war however, despite Zelensky's frustrations with NATO's rejection of a no-fly zone,[84] he is likely to emphasise his relationship with the West in order to assure continued security support. Thus, China becomes the losing partner with limited ability to promote stability in future. Further, Ukraine may find it unpalatable to continue its engagement with China, should China continue to support Russia.[85] Again, in this case, China will likely lose its influence in Ukraine and therefore cannot continue to promote stability.

Finally, the Ukraine war has potentially proven that China may have limited ability to deter Russian territorial and geopolitical ambitions. Although there is some suggestion that Putin made Jinping aware of his intentions, it is unclear whether he was seeking Jinping's approval; thus, potentially giving Jinping influence, or whether Putin was simply informing Jinping of his plans.[86] Owing to the escalatory NATO-Russian rhetoric in November-December 2021, it is likely to be the latter. To that end, the assumption made throughout this paper could be irrevocably flawed, as despite the significant Chinese investment in Ukraine, it seemingly held insufficient deterrence against Russian aggression. It would follow therefore, that China's influence does not promote stability in the BSR as Russia has proven it will prioritise countering NATO over the preservation of its relationship with China. However, this seems naïve. Russia's miscalculations in the strength of the Ukrainian response, and/or the severity of Western sanctions has made China their 'lifeline.' The criticality of that dependency should provide strength against future aggression in the BSR. Further, the annexation of Crimea in 2014, the Russian control of the Kerch Strait and the 18 Ukrainian ports (more than double the

amount located in any other BSR state), suggests that Ukraine is sufficiently important to Russia to justify conflict, whereas other BSR states might not be. On this basis, the conclusion for China's stability in the BSR has four avenues. Russia is unlikely to act with the same aggression again in other BSR states and thus China's influence is immaterial for stability, the Russian dependency allows China to become more assertive over Russia, curtailing any future aggression and ensuring long-term stability, China becomes excluded from the region as the West increase their military presence, meaning its influence is inconsequential, or NATO and the US realise that China is the only real contender for 'mediation' and thus its level of influence becomes a critical dependency for regional stability. Of these, the latter is potentially the most likely for the BSR.

In summary, prior to the war China's influence likely aided stability in Ukraine. Significant investments allowed for alternatives to Russian investment and the investments themselves fuelled domestic growth. However, following the conflict, China is likely to lose its ability to maintain stability in Ukraine. The severity of the West vs Russia conflict will have overshadowed any ability for China to maintain influence, its decision making against existing investments will likely result in mixed messages as to its intent, and Ukraine may itself denounce China if it continues to support Russia. All of which removes China and its stabilising influence in the long-term. Alternatively, the resultant dependency of Russia on China following the war, and China's role as a mediator may allow China's influence to continue to promote regional stability in the long-term, even if this excludes Ukraine.

## China-Georgia

Since Georgia's independence from the Soviet Union, China has slowly increased its relationship with Georgia. This has largely been through economic investment with cooperation now at its peak.[87] In 2021, Georgia exported more to China than any other country, totalling $615 million.[88] Georgia's geographic position in the BSR, coupled with its border with Azerbaijan providing a land route to the Caucasus without the need to use Iran or Russia, makes Georgia of strategic importance to China's BRI.[89]

Some literature suggests that China's interest in Georgia has also had a positive effect on US economic commitments.[90] Although the Foreign Policy for Research Institution describes the trend as 'somewhat counterintuitive,'[91] owing to the US 'pivot' to Asia,[92] and Smolnik, a Senior Associate in Eastern European and Eurasia research, describes the US-Georgia relationship as lacking in a strategic vision;[93] this support could well be a manifestation of US grand strategy. The US is quickly realising that 'as competition with China becomes increasingly central to US grand strategy, the US is likely to look at different regions…through the lens of that competition.'[94] As such, Georgia has been able to use its developing relationship with China 'to boost Georgia's strategic…partnership with Washington.'[95] Georgia's 'strategy' is therefore win-win. Chinese investment increases their economic stability and attracts US economic and security assurances. Further, China's engagement specifically counters Russia's involvement; it is able to 'limit Russia's freedom of manoeuvre and will begin

to mitigate its geostrategic dominance.'[96] In the short-term, if the principles of economic liberalism (economic interdependence reduces the likelihood of hostility as the cost of disruption outweighs the justification for conflict)[97] holds, China and US co-habitancy is likely to assure stability, unless this coexistence becomes problematic. 'According to power transition theory, the onset of war between a dominant and a rising power grows more likely as the gap in relative strength between them narrows and the latter's grievances with the existing order move beyond any hope of peaceful resolution.'[98] Whilst neither side has shown any intention of aggression in the region, an increasingly powerful China coupled with resultant US uneasiness, could lead to tension, potentially causing China's influence to negatively affect stability. Brands, in his discussion of ideological competition between China and the US, argues that autocracy vs democracy is a line of great power competition which, in the long-term will not simply resolve.[99] Whilst the realisation of this tension is unlikely to result in military conflict both because the foreign policy on each side favours diplomacy, and because Georgia is unlikely to be revered as a cause over which each side should go to war; any suggestion of subthreshold activity between the US and China in Georgia may limit the sustainability of China's stabilising influence in the long-term, should it feel that its position becomes untenable.

Nonetheless, China will likely want to retain its investment in Georgia for as long as is feasible, as without NATO or EU membership, China still has room for significant influence. China's ability to promote stability in the long-term will be dependent on how attractive it becomes as an investor and thereby how much influence it can yield over other actors. Russia likely believes that Georgia should remain firmly within its sphere of influence, and the 2008 war clearly signalled 'their determination to prevent further expansion of the Alliance into former Soviet republics.'[100] Indeed since the war, the 'Abkhazia and Tskhinvali regions are still under Russian occupation'[101] and although written in a US policy paper, Welt claims that since the war, 'Russia has used a variety of means to undermine and challenge Georgia's security, including…establishing military bases, and reinforcing their military strength.'[102] Georgia, acutely aware of the Russian threat, has ensured that the US remain its security guarantor and when Wang Yi, the Chinese Foreign Minister, visited Georgia in 2019, the importance of seeking 'Chinese support for Georgia's sovereignty and territorial integrity'[103] was raised, potentially indicating that Georgia expects China to become a strategic ally as well as an economic investor. China's investment in Georgia therefore complicates this power play for which Russian action in response to China's growing influence may test the limits of the current stability. China's investment in Belarus may give some indication of Russia's temperament. As well as BRI investments, China invested a $500bn 'general loan' into Belarus after Russia's Eurasian Fund for Stabilisation and Development refused to pay a $200M instalment of a $2bn loan,[104] which saw a negligible response from Russia suggesting that even investments outside of the BRI curtail rather than aggravate Russian aggression. Although Russia undoubtedly would like to counter China's investment, it 'does not have the deep pockets to match Beijing's,'[105] thus, it must accept interventions, even in states with long standing socio-political ties to Russia. It would seem that China's economic investment could have significant resilience for assuring stability against Russia in Georgia.

The final test against China's stability in Georgia may be realised in analysing Russia's likely intent post the Ukraine crisis. Some commentary has suggested that the risk of Russian escalation has increased.[106] Indeed, fearing invasion, 'the Georgian government has tiptoed round the crisis,' and filed for EU membership on 03 March 2022. In the event of military action, China is unlikely and probably unwilling to intervene, clearly limiting its ability to promote stability. However, if Russia pursued military intervention, China's inaction may act as a stabilising factor as any action that directly disrupts China's BRI may cause Russia to fall out of favour with China,[107] something Russia can ill afford. By proxy therefore, China may now be able to temper Russian aggression in Georgia even in a heightened escalatory environment.

In summary, China's influence is likely to promote stability in Georgia in both the short and long term. China's economic investment and resultant US investment has provided Georgia with a win-win strategy for countering Russian aggression. Further, China has been able to expand its investment beyond construction and thus has proven it can act with impunity without Russian retaliation, proving the significance of China's influence as a stabilising factor. Though the threat of Russian occupation has potentially heightened following the war and the long-term co-habitancy of the US and China in a small geographic space may give rise to future tension, these are unlikely to result in large scale conflict.

## China-Bulgaria

Bulgarian geopolitical relationships are complex. Traditionally a strong ally of Russia; however, since joining NATO in 2004 and the EU in 2007, it has continued to establish and uphold strong relations with the West, owing to its reliance on financial and economic security from the EU.

China, a 'geopolitical latecomer to Bulgaria,'[108] has found it difficult to gain influence in the country due to Bulgaria's NATO/EU membership, and legacy Russian influence. This is beginning to change. China realises the potential of using Bulgaria as a 'logistics and transportation hub into Europe,'[109] and as Bulgaria is one of only two states within the region to officially be a member of the 17+1 construct, it offers China a particular advantage.[110] As such, since 2016, BRI investments have been forthcoming. The ports of Burgas and Varna have seen large scale investment, as well as multiple commitments to improve transport infrastructure more generally (a tunnel under the Balkan mountains and investments in Plovdiv airport are examples).[111] This investment has acted as a catalyst for commitment to a domestically led ambitious transport strategy, in order to accommodate the likely increase in maritime traffic.[112]

Despite these investments and public announcements to continue to 'lift China-Bulgaria relations to a strategic partnership,'[113] in real terms, China holds little influence in the macroeconomy, which is dominated by the EU. Bulgaria trades in excess of 60% of both its exports and imports with the EU, compared to a maximum of 3% with China.[114]

Although Shopov, a visiting fellow of the European Council on Foreign Relations, does document a compelling suite of investments and engagements beyond the infrastructure and energy sectors, citing examples in cultural, educational, agricultural and research projects.[115] The aggregate effect however, has seen little movement away from the EU. This is unsurprising as 'the availability of EU funds for primary infrastructure…remains sufficient and comes at little or no cost to the Bulgarian exchequer.'[116] As such, in the near-term, and counter to the proposition of this paper, China lacks influence in Bulgaria limiting its ability to promote stability.

However, the war in Ukraine has affected Bulgaria's relationship with Russia for which China may exploit. Interestingly, unlike other European countries that are punishing Russia, Russia has punished Bulgaria.[117] In failing to meet Russian demands to pay for natural gas in roubles (knowing that this is against sanction regulations), GazProm turned off Bulgarian gas supply[118] for which the Energy Minister, Nikolov's, response was to suggest that 'natural gas is being used…as a political…weapon.'[119] Russia knows that European dependency on Russian gas gives them leverage, and although Nikolov has a resolute tone, he is also mindful of the need to carefully balance Russia's perception of Bulgaria such to prevent further aggression; 'my heart says we do not leave Ukraine alone…[but]…I don't think I can send Bulgarian planes flying over Ukraine, fighting with Russian jets.'[120] Indeed, in terms of support to Ukraine, Bulgaria has pledged humanitarian support but not weapons.[121] This changing dynamic potentially puts China in a precarious position. It also needs to balance Russian and EU interests in Bulgaria to ensure its economic growth goes unhindered. It has learned from its investments in Central Asia that it can comfortably co-habit with Russia in an economic sense,[122] however, although Russia looks like it is content with dismemberment from Bulgaria, it may well be relying on China to fill the void to prevent deeper EU dominance. In this case, China's increasing influence could remain a vector for future stability. Indeed, there has already been some illustrative evidence of this when in 2019, China's bid to restart development on the previously abandoned Russian nuclear facility in Belene,[123] yielded negligible Russian reactions. However, as the trade statistics show, and the post war trend to turn Westwards, China may find its influence shrinking. In this instance, Russia loses its ally, and the perception of NATO expansion strengthens. Whilst this is unlikely to result in Russian vs Western conflict (owing to Bulgaria's NATO membership), an environment with decreasing Chinese influence could encourage Russia to pursue persistent subthreshold activity as a means to exploit Bulgarian nervousness and prevent Western absolutism. China is unlikely to intervene as Bulgaria is a small state and already a member of NATO and the EU, and as such China may lack motivation to act as a mediator. Thus, with a decreasing influence, its ability to promote stability also declines. However, as Shopov highlights, a significant part of China's investment strategy has been to consider sub-national ties, exploiting the 'stalled process of fiscal decentralisation'[124] to local municipalities. Fostering pro-Chinese sentiment from the ground up may help China retain its influence and thereby its ability to promote stability in demonstrating to Russia that these relationships can temper further NATO concreting, ultimately reducing the likelihood of Russian aggression.

In summary, although against the premise of this paper, China has struggled to grow influence in Bulgaria, limiting its ability to promote stability. Bulgaria, as a member of the EU and NATO has limited need for Chinese investment and post the war in Ukraine, this Western preference is likely to strengthen. China may be able to fill some of the void left by Russian overpromise or future unpopularity, as per the example of the Belene facility, instances which Russia will likely encourage in order to prevent Western involvement. However, even these such investments are unlikely to yield any sway over the Western preference although China may look to grow pro- Chinese sentiments at the local level such to maintain a foothold. As such, China's already limited influence is likely to decrease further. Its long-term ability to promote either economic or political stability looks increasingly limited as shown by the subthreshold aggression in the cessation of gas supply. Further, Bulgaria's membership to NATO, over China's tempering of Western dominance will likely act as the greater deterrent to Russian aggression.

## Section 3
## Conclusion

In conclusion, the BSR has become an important region for China, for which the discussion of whether the impact of its influence can promote stability is complex. Plagued by an interwoven fabric of conflict-ridden history and a globally strategic geography, the BSR is a uniquely unstable region that has evolved into an environment of renewed great power competition between Russia, China, and the West.

Russia remains the greatest source of instability, evidenced by attacks in the cognitive, virtual and physical domains of the targeted states. The concept of Western encirclement entrenched in Russian strategic culture, and the perception of an existential threat through NATO expansionism is likely to continue to provoke Russian aggression; the BSR is likely to remain unstable.

In the short-medium term, China, through the 17+1 construct and the BRI, is likely to continue its expansion in the BSR, under the premise of economic growth and increased access to European markets; strengthening China's influence. Whether this influence allows China to promote stability in the BSR will likely be decided by its ability to pursue its national interests whilst navigating its geopolitical engagements with Russia, the West and the BSR states themselves. China's relationship with Russia has strengthened since the collapse of the Soviet Union to the extent that the Sino-Russian rhetoric suggests their allegiance has no limits, although this narrative may be tested within the BSR. Russia, the junior partner, may find the asymmetry of power difficult in a region that historically has socio-political allegiance with Moscow. However, as Russia struggles with a declining economy, exacerbated by imposed economic sanctions since the Ukraine invasion, it will have to accept China's expansion into its perceived territory in order that it can assure its own financial support. The war in Ukraine has ultimately made China, Russia's lifeline. For the BSR specifically, this has accelerated China's role as the mediator between Russia and the BSR states and thus the influence of its asymmetrical power advantage has increased stability in the BSR by curtailing Russian aggression. China has

a difficult game to play to ensure this is sustainable. In not openly condemning the invasion, it has proven to Russia the credibility of the no limits statement. China could therefore expect to continue its economic growth in the BSR without fear of Russian reprisal with the hope of assuring future access to military technology and the Arctic. Further, China's general silence also suggests it is trying to avoid Western backlash. The preservation of both these relationships should help assure its influence in the BSR and thus its ability to promote stability.

For the BSR states considered in this paper (outside of Russia), Ukraine, Georgia and Bulgaria have all increased their cooperation with China, largely through economic investments in logistics and transport infrastructure. Increased economic investment has had a threefold stabilising effect in all three countries; increased economic stability, provided alternative avenues to Russian investment, and stimulated investment from the West. All of which reduces the dependency on Russia which reduces Russian influence. Further, buoyed by a nervousness of Chinese investment, increased Western investment has by proxy assured access to Western security. For each state however, the sustainability of this stabilising nature is more difficult to ascertain.

For Ukraine, whilst the severity of the West vs Russia conflict may overshadow any ability for China to maintain direct influence, China's decision making is likely to prove deterministic for regional stability; critically whether it prioritises economic growth or acts to assure geopolitical dominance. If it opts for the former, it may withdraw from Ukraine in pursuit of more settled investment environments which may prove destabilising as it removes any ability to temper Russian aggression and possibly signals to Russia its indifference to the war. However, if China maintains its commitment to Ukraine investment, this may stoke Western perceptions of the true intent of the BRI aggravating Western-China tensions. Alternatively, if China maintains its investment and disseminates a mediator, reconstructionist narrative, it may continue to offer stability. Irrespective, Ukraine is unlikely to simply observe. If China continues to support Russia, Ukraine may find future Chinese interaction unpalatable, potentially reject their continued investment, thereby reducing China's influence and thus its ability to promote stability.

For Georgia, the future looks more settled. The Georgian strategy of using its relationship with China to boost Georgia's strategic significance with Washington has resulted in a stable win-win environment. Though the threat of Russian aggression continues in the occupied territories, the coexistence of Chinese and US investment looks resilient enough to repel any escalation. Further, even China's exploitation of investment gaps caused by Russian over-promise, resulted in a negligible Russian reaction, suggesting that China will be able to operate with impunity in Georgia for the foreseeable future and thus assure sustainable stability. China will have to be careful to avoid US misperception of geopolitical dominance to prevent US-China tensions, although the likelihood of a full-scale conflict on these grounds is small.

Finally, for Bulgaria, China remains an inconsequential actor. Since entering NATO (2004) and the EU (2007), Bulgaria has affirmed its Western allegiance, and thus China has had difficulty in

cultivating influence. Although China's investment is increasing, its ability to promote stability is limited, highlighted by China's inability to prevent the recent cessation of Russian gas supply. The Ukraine invasion will also likely force Bulgaria to deepen its Western ties to assure its security, further reducing the ability for China to promote stability. China may continue to exploit Russian unpopularity, as per its investment in the Belene nuclear facility, but this is unlikely to challenge Western dominance which will continue to provide economic and security stability beyond anything China can offer.

Overall, whether the impact of China's influence can promote stability in the BSR in the long-term is complex. In terms of its economic influence; offering alternatives to Russian investment, stimulating domestic growth, and drawing continued Western investment into the BSR all provide economic stability, which by proxy act as a deterrent against Russian aggression owing to Russian dependencies on China and the need for Russia to maintain this relationship. However, the war in Ukraine is likely to irrevocably change the geopolitics of the region within which China will need to carefully navigate the changing dynamics in order to retain its influence and thereby its ability to promote stability. China likely has three courses of action to assure this influence; support Russia, support the West or remain neutral. If China supports Russia under the no limits narrative, it will jeopardize its relationship with the West and will further force BSR states to turn West. It therefore loses influence in the BSR, and the region becomes increasingly unstable becoming a theatre for a new Cold War. If China supports the West, the BSR is likely to become more stable as China and the US offer a united front against Russia. Finally, and potentially the most likely, China will remain neutral, aiming to balance its position as a mediator showing sufficient support to Russia to future proof its long-term objectives, but with enough support for the West in order to continue to expand in the BSR and Europe. What is likely however, is that irrespective of China's overall grand strategy, for which the academic discussion remains inconclusive, China is likely to be constrained to economic influence until it can also compete militarily. Although this economic influence gives China disproportionate geopolitical influence as it nears superpower status, the BSR, underpinned by Western liberalism ideology, will likely continue to seek security from the West as security assurance over economic influence is likely be the stronger deterrent against Russian aggression. Thus, the stabilising nature of China, in the long-term may be limited as it lacks the means to provide stability through security. Interestingly, this may be China's preferred outcome. The war may have enabled Jinping to pursue his preferred strategy; exploiting the Russian investment void without the burden of security responsibility allowing it to play the quaint pacifist until such time that it declares otherwise.

## Notes

[1] Michael Schuman, 'What Happened When China Leads the World,' The Atlantic, 2020. https://www.theatlantic.com/international/archive/2020/10/what-kind-superpower-will-china-be/616580/ (Accessed May 20, 2022).
[2] Ibid.
[3] Jasper M. Trautsch, 'Who's afraid of China? Neo-conservative, realist and liberal-internationalist

assessments of American power, the future of the West and the coming new world order,' *Global Affairs* 1, No.3 (2015):235-245. DOI: 10.1080/23340460.2015.1077609. (Accessed May 22, 2022).

[4] John G. Ikenberry, 'The end of the liberal international order?,' *International Affairs* 94, no.1 (2018):17. DOI: 10.1093/ia/iix241. (Accessed May 23, 2022).

[5] Deniz Unver, 'Growing Chinese Presence and Interests in the Black Sea,' AVIM, https://avim.org.tr/Blog/GROWING-CHINESE- PRESENCE-AND-INTERESTS-IN-THE-BLACK-SEA (Accessed April 14, 2022).

[6] Diego Trindade d'Ávila Magalhães, 'The globaliser dragon: how is China changing economic globalisation?,' *Third World Quarterly* 39, no.9 (2018):1729, DOI: 10.1080-01436597.2018.1432352 (Accessed May 5, 2022).

[7] Ibid.

[8] Deborah Sanders, 'Can China promote stability in the Black Sea Region?,' *Southeast European and Black Sea Studies* 21, No.3 (2021):415. DOI: 10.1080/14683857.2021.1935771 (Accessed May 01, 2022).

[9] Ibid.

[10] Gideon Rachman, 'China is still a long way from being a superpower,' *Financial Times*, 2021. https://www.ft.com/content/bdaad457- 9e22-4d74-b614-6cc44a613a0c. (Accessed May 25, 2022).

[11] Ibid.

[12] Deborah Sanders, 'The Black Sea Region Caught Between East and West,' *The Journal of Slavic Military Studies*, 34, No.2 (2021):202-225. DOI: 10.1080/13518046.2021.1990561 (Accessed April 14, 2022).

[13] Richard Ghiasy and Jiayi Zhou, 'The Silk Road Economic Belt,' Report, SIPRI, 2017. https://www.sipri.org/sites/default/files/The-Silk- Road-Economic-Belt.pdf (Accessed April 21, 2022).

[14] Ibid.

[15] Ibid.

[16] Unver, 'Growing Chinese Presence.'

[17] Sanders, 'Can China promote stability?.' 421.

[18] Suat Kiniklioglu, 'Necessary friends: Turkey's improving relationship with the West,' European Council on Foreign Relations, 2022. https://ecfr.eu/article/necessary-friends-turkeys-improving-relationship-with-the-west/ (Accessed May 24, 2022).

[19] John E. Wagner and Steven C. Deller, 'Measuring the Effects of Economic Diversity on Growth and Stability,' *Land Economics* 74, no.4 (1998):542. https://www.jstor.org/stable/3146884?seq=1 (Accessed April 28, 2022).

[20] Joseph S. Nye, *Understanding International Conflict*, (New York: Pearson Longman, 2007).

[21] Yannis Valinakis, 'Cooperation and Security in the Black Sea Region,' European Institute for Security Studies, (1999), https://www.jstor.org/stable/pdf/resrep07042.6.pdf?refreqid=excelsior%3Abb9597accb1db4104c410080ef9fc3f8&ab_segments=0%2FS YC-6294%2Ftest_segment_2&origin= (Accessed April 21, 2022).

[22] Alexandra Kuimov and Siemon T. Wezeman, 'Russia and Black Sea Security,' Report, SIPRI, 2018. https://www.jstor.org/stable/resrep24424 (Accessed April 21, 2022).
[23] Fritz W. Ermath, '*Russian Strategic Culture: Past, Present and in Transition*,' Defense Threat Reduction Agency Advanced Systems and Concepts Office, (2006):6. https://irp.fas.org/agency/dod/dtra/russia.pdf (Accessed April 30, 2022).
[24] Paul Stronski, 'What is Russia Doing in the Black Sea?,' Carnegie Endowment for International Peace, 2021. https://carnegieendowment.org/2021/05/20/what-is-russia-doing-in-black-sea-pub-84549 (Accessed April 28, 2022).
[25] Evan Sankey, 'Reconsidering Spheres of Influence,' *Survival* 62, No.2 (2020):40. https://www.tandfonline.com/doi/epub/10.1080/00396338.2020.1739947?needAccess=true (Accessed May 20, 2022).
[26] Ibid., 44.
[27] Valentin Maxim and Lucian Valeriu Scipanov, 'Considerations on the Russian Doctrine for a New Warfare Model in the Black Sea Region,' *Strategic Impact* 78, No.1 (2021):63-73.
[28] Andy Greenberg, *Sandworm: A new era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, (New York: Doubleday, 2019).
[29] Stronski, 'What is Russia Doing?.'
[30] Ibid.
[31] Ibid.
[32] Marius Serbeszki, 'The Black Sea Militarisation,' *Romanian Military Thinking* special, No.4 (2019):150-159. https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=141745788&site=eds-live (Accessed May 29, 2022).
[33] Ibid.
[34] Valinakis, 'Cooperation and Security.'
[35] On Geopolitics, 'The Ukraine War Exposes Russia and China's Competing Visions for Eurasia,' On Geopolitics, 2022. https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=155581629&site=eds-live. (Accessed May 23, 2022).
[36] Stronski, 'What is Russia Doing?.'
[37] Ibid.
[38] Cooperation between China and Central and Eastern European countries aiming to enhance economic and infrastructure investments.
[39] BBC, 'China overtakes US as EU's biggest trading partner,' BBC, https://www.bbc.com/news/business-56093378 (Accessed April 15, 2022).
[40] On Geopolitics, 'Competing Visions for Eurasia.'
[41] Ibid.
[42] Ibid.
[43] Simon Luis, Linde Desmaele and Jordan Becker, 'Europe as a Secondary Theater? Competition with China and the Future of America's European Strategy,' *Strategic Studies Quarterly* 15, No.1 (2021):90-115. https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=149301836&site=eds-live.
(Accessed May 24, 2022).
[44] Andrew Chatzky and James McBride, 'China's Massive Belt and Road Initiative,' Council on

Foreign Relations, 2020. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative (Accessed April 14, 2022).
[45] Eurasia Programme, 'On the Fault Line: Georgian Relations with China and the West,' Foreign Policy Research Institute, 2019, https://www.fpri.org/wp-content/uploads/2019/09/on-the-fault-line.pdf (Accessed April 20, 2022).
[46] Richard Ghiasy and Rajeshwari Krishnamurthy, 'China's Digital Silk Road and the Global Digital Order,' The Diplomat, 2021. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/ (Accessed May 29, 2022).
[47] Wang Jisi in Yun Sun, 'March West: China's Response to the US rebalancing,' Brookings, (2013), https://www.brookings.edu/blog/up- front/2013/01/31/march-west-chinas-response-to-the-u-s-rebalancing/ (Accessed April 20, 2022).
[48] David F. Gordon, Haoyu Tong and Tabatha Anderson, 'Beyond the Myths – Towards a Realistic Assessment of China's Belt and Road Initiative: The Security Dimension,' Report, The International Institute for Strategic Studies, 2020. https://ispmyanmarchinadesk.com/wp-content/uploads/2020/12/BRI-Report-Two-Beyond-the-Myths-Towards-a-Realistic-Assessment- of-Chinas-Belt-and-Road-Initiative.pdf (Accessed April 14, 2022).
[49] Daniele Carminati, 'The State of China's Soft Power in 2020,' E-International Relations, 2020. https://www.e-ir.info/2020/07/03/the- state-of-chinas-soft-power-in-2020/ (Accessed April 28, 2022).
[50] Gordon, Tong and Anderson, 'Beyond the Myths.'
[51] Ibid.
[52] Julie T. Miao, 'Understanding the soft power of China's Belt and Road Initiative through a discourse analysis in Europe,' *Regional Studies, Regional Science* 8, No.1 (2021):162-177. DOI: 10.1080/21681376.2021.1921612 (Accessed May 29, 2022).
[53] Falk Hartig, 'How China Understands Public Diplomacy: The Importance of National Image for National Interests,' *International Studies Review* 18, No.4 (2016):655-680. DOI: 10.1093/isr/viw007. (Accessed May 29, 2022).
[54] Shehla Burney, 'Chapter One: Orientalism: The Making of the Other,' *Counterpoints* 417 (2012):23–39, http://www.jstor.org/stable/42981698 (Accessed April 30, 2022).
[55] Kadri Liik, 'It's complicated: Russia's tricky relationship with China,' European Council on Foreign Relations, 2021. https://ecfr.eu/publication/its-complicated-russias-tricky-relationship-with-china/ (Accessed April 25, 2022).
[56] Vladimir Putin and Xi Jinping in Shannon Tiezzi, 'What Putin and Xi said (and didn't say) about Ukraine,' The Diplomat, 2022. https://thediplomat.com/2022/02/what-putin-and-xi-said-and-didnt-say-about-ukraine/ (Accessed April 14, 2022).
[57] Robert Sutter, 'America's Bleak View of Russia-China Relations,' *Asia Policy* 13, no.1 (2018):42. https://www.jstor.org/stable/26403229 (Accessed April 15, 2022).
[58] On Geopolitics, 'Competing Visions for Eurasia.'
[59] Alexander Gabuev, 'A soft alliance?: Russia-China Relations after the Ukraine Crisis,' Report, European Council on Foreign Relations, 2015. https://www.jstor.org/stable/resrep21546 (Accessed April 19, 2022).
[60] UN Affairs, 'UN General Assembly votes to suspend Russia from the Human Rights Council,'

UN Affairs, https://news.un.org/en/story/2022/04/1115782 (Accessed April 19, 2022).
[61] Natasha Kuhrt and Marcin Kaczmarski, 'Ukraine Invasion: Why China is more likely to support Russia then in the past,' KCL, 2022. https://www.kcl.ac.uk/ukraine-invasion-why-china-is-more-likely-to-support-russia-than-in-the-past (Accessed April 28, 2022).
[62] The Economist, 'Ukraine and the lessons of the cold war,' *The Economist*, (March/April 2022):33-35.
[63] Lijia Zhang, 'How the Ukraine crisis is hurting China's soft power ambitions,' *South China Morning Post*. https://www.scmp.com/comment/opinion/article/3173272/how-ukraine-crisis-hurting-chinas-soft-power-ambitions (Accessed April 20, 2022).
[64] K. Khudoley, 'The Baltic Sea Region and Increasing International Tension,' *Baltic Region* 8, no.1 (2016):4-16. https://www.researchgate.net/publication/301741862_The_Baltic_Sea_region_and_increasing_international_tension/fulltext/573a125b0 8ae9ace840dc4c4/The-Baltic-Sea-region-and-increasing-international-tension.pdf?origin=publication_detail (Accessed April 30, 2022).
[65] The Economist, 'Testing the Limitless,' *The Economist*, (19-25 March 2022):52.
[66] Ibid.
[67] Trym Eiterjord, 'What Does Russia's Invasion of Ukraine Mean for China in the Arctic?,' The Diplomat, 2022. https://thediplomat.com/2022/03/what-does-russias-invasion-of-ukraine-mean-for-china-in-the-arctic/ (Accessed May 29, 2022).
[68] Sanders, 'Caught Between East and West.' 209.
[69] Zongyuan Zoe Liu, 'What's at Stake for China's Economic Relationship with Ukraine,' Council on Foreign Relations, 2022. https://www.cfr.org/in-brief/whats-stake-chinas-economic-relationship-ukraine (Accessed May 14, 2022).
[70] Sanders, 'Can China promote stability?.' 419.
[71] Liu, 'What's at Stake, China-Ukraine.'
[72] Ibid.
[73] Olena Mykal, 'Why is China interested in Ukraine,' The Diplomat, 2016. https://thediplomat.com/2016/03/why-china-is-interested-in- ukraine/ (Accessed May 10, 2022).
[74] Liu, 'What's at Stake, China-Ukraine.'
[75] Zeneli in Sanders, 'Can China promote stability?.' 425.
[76] Sanders, 'Can China promote stability?.' 424.
[77] Sebastian Horn, Carmen Reinhart and Christoph Trebesch, 'China's overseas lending and the war in Ukraine,' VoxEU/CEPR. https://voxeu.org/article/china-s-overseas-lending-and-war-ukraine (Accessed May 16, 2022).
[78] Ibid.
[79] Zamir Ahmed Awan, 'BRI – a mega initiative for peace, harmony and prosperity,' China Daily, 2018. http://www.chinadaily.com.cn/a/201807/05/WS5b3d8f56a3103349141e0de1.html (Accessed May 16, 2022).
[80] Y-Y Chnag, 'Understanding the Belt and Road Initiative,' *European Journal of East Asia Studies* 18, No.1 (2019): 7-35. https://www.researchgate.net/publication/334324647_Understanding_the_Belt_and_Road_Initiative_BRI (Accessed May 12, 2022).
[81] Kevin G. Cai, 'The One Belt One Road and the Asian Infrastructure Investment Bank: Beijing's

New Strategy of Geoeconomics and Geopolitics,' *Journal of Contemporary China* 27, No.114 (2018):831. https://www.tandfonline.com/doi/pdf/10.1080/10670564.2018.1488101?needAccess=true (Accessed May 16, 2022).

[82] Andrew J. Nathan, 'What Exactly is America's China Policy?,' *Foreign Policy* Spring, No.244 (2022):32-39. https://eds.s.ebscohost.com/eds/detail/detail?vid=0&sid=782917af-abe2-442a-aec7-d628d8549c6b%40redis&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=156306742&db=mth (Accessed May 10, 2022).

[83] Sanders, 'Caught Between East and West.'

[84] BBC, 'War in Ukraine: Zelensky slams Nato over rejections of no-fly zone,' BBC, https://www.bbc.co.uk/news/world-europe-60629175 (Accessed May 15, 2022).

[85] Bonnie Girard, 'The Cost of the War to the China-Ukraine Relationship,' The Diplomat, 2022. https://thediplomat.com/2022/03/the- cost-of-the-war-to-the-china-ukraine-relationship/ (Accessed May 14, 2022).

[86] Vincent Ni, 'China denies it asked Russia not to invade Ukraine during Winter Olympics,' *The Guardian*, https://www.theguardian.com/world/2022/mar/02/china-russia-invade-ukraine-winter-olympics-beijing (Accessed May 27, 2022).

[87] Revaz Topuria, 'Georgia: The Key to China's Belt and Road,' The Diplomat, 2016. https://thediplomat.com/2016/04/georgia-the-key- to-chinas-belt-and-road/ (Accessed April 20, 2022).

[88] Trading Economics, 'Georgia exports and imports to China,' Trading Economics, https://tradingeconomics.com/georgia/exports/china (Accessed April 20, 2022).

[89] Dante Schulz, 'China-Georgia Bilateral Relations,' Caspian Policy Center, 2022. https://www.caspianpolicy.org/research/security-and- politics-program-spp/china-georgia-bilateral-relations. (Accessed April 20, 2022).

[90] Eurasia Programme, 'On the Fault Line.'

[91] Ibid.

[92] Mark Landler, 'Leaving Asia, Obama Predicts U.S Tilt Towards Region Will Be Lasting,' *NYT*, 2016. https://www.nytimes.com/2016/09/09/world/asia/obama-laos-asia-asean-tour.html. (Accessed May 24, 2022).

[93] Franziska Smolnik, 'The Strategic Partnership between Georgia and the United States' Vision Wanted, Research Paper. SWP, 2020. DOI: 10.18449/2020RP15. (Accessed April 20, 2022).

[94] Luis, Desmaele and Becker, 'Europe as a Secondary Theater?.' https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=149301836&site=eds-live. (Accessed May 24, 2022).

[95] Smolnik, 'The Strategic Partnership.'

[96] Sanders, 'Can China promote stability?.' 431.

[97] Yuleng Zeng, 'Does Money Buy Friends? Evidence from China's Belt and Road Initiative,' *Journal of East Asian Studies* 21, No.1 (2021), DOI: 10.1017/jea.2020.34 (Accessed May 19, 2022).

[98] Xiaoyu Pu, *Rebranding China*, (California, Stanford University Press, 2018):6. https://eds.s.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzE5MjA2NTZfX0FO0?sid=31d2e016-1507-4952-b8a3- ede572b3d8bd@redis&vid=5&format=EB&rid=1 (Accessed May 19, 2022).

[99] Hal Brands, 'Democracy vs Authoritarianism: How Ideology Shapes Great-Power Conflict,'

*Survival* 60, No.5 (2018):61-114. DOI: 10.1080/00396338.2018.1518371 (Accessed May 20, 2022).
[100] James Dobbins, Raphael S. Cohen, Nathan Chandler, Bryan Frederick, Edward Geist, Paul DeLuca, Forrest E. Morgan, Howard J. Shatz, and Brent Williams, *Extending Russia: Competing from Advantageous Ground* (Santa Monica: RAND Corporation, 2019),14.
[101] Alexis Mrachek, 'Top Five Priorities for the U.S-Georgian Relationship in 2020,' Report, The Heritage Foundation, 2022. https://www.heritage.org/global-politics/report/top-five-priorities-the-us-georgian-relationship-2020 (Accessed May 07, 2022).
[102] Cory Welt Sanders, 'Caught Between East and West.' 209.
[103] Emil Avdaliani, 'China Set to Increase its Influence in Georgia,' Georgia Today, http://gtarchive.georgiatoday.ge/news/15824/China- Set-to-Increase-its-Influence-in-Georgia (Accessed May 05, 2022).
[104] Dominik Istrate, 'Belarus continues China pivot,' Emerging Europe, https://emerging-europe.com/news/belarus-continues-china- pivot/ (Accessed May 10, 2022).
[105] Saibal Dasgupta, 'Putin Demands a Role in Eurasian Part of Belt and Road,' VOA, https://www.voanews.com/a/putin-demands-a- role-in-eurasian-part-of-belt-and-road/4903625.html (Accessed May 09, 2022).
[106] Olesya Vartanyan, 'In Ukraine, Georgia Sees Powerful and Worrying Parallels,' Crisis Group, https://www.crisisgroup.org/europe- central-asia/caucasus/georgia/ukraine-georgia-sees-powerful-and-worrying-parallels (Accessed May 08, 2022).
[107] Smolnik in Sanders, 'Can China promote stability?.' 426.
[108] Valdimir Shopov, 'Let a thousand contacts bloom: How China competes for influence in Bulgaria,' European Council on Foreign Relations, 2022. https://ecfr.eu/publication/let-a-thousand-contacts-bloom-how-china-competes-for-influence-in-bulgaria/ (Accessed May 01, 2022).
[109] Sanders, 'Can China promote stability?.' 419.
[110] Ibid., 416.
[111] Ibid., 419-420.
[112] Ibid., 420.
[113] TendersInfo News, 'Bulgaria, China: Xi Jinping Holds Talks with President Rumen Radev of Bulgaria,' TendersInfo News, 2019. https://link.gale.com/apps/doc/A592745655/STND?u=jscscoll&sid=ebsco&xid=421a650c (Accessed May 03, 2022).
[114] EU, 'Bulgaria: Overview,' EU, https://european-union.europa.eu/principles-countries-history/country-profiles/bulgaria_en (Accessed May 06, 2022).
[115] Shopov, 'Let a thousand contacts bloom.'
[116] Ibid.
[117] Zosia Wanat, 'Poland and Bulgaria start life with no Russian gas,' Politico, 2022. https://www.politico.eu/article/poland-bulgaria-life- no-russia-gas/ (Accessed May 06, 2022).
[118] BBC, 'Ukraine war: Russia halts gas exports to Poland and Bulgaria,' BBC, https://www.bbc.co.uk/news/business-61237519 (Accessed May 05, 2022).
[119] Wanat, 'Poland and Bulgaria start life with no Russian gas.'

[120] Lili Bayer, 'Bulgarian PM: We're no longer "soft" on Russia,' Politica, 2022. https://www.politico.eu/article/bulgaria-not-soft-russia- prime-minister-kiril-petkov/ (Accessed May 03, 2022).
[121] Boryana Dzhambazova, 'Ukraine war exposes the Kremlin's lingering reach in Bulgaria,' Politico, 2022. https://www.politico.eu/article/ukraine-war-kremlin-reach-bulgaria-kiril-petkov/ (Accessed May 05, 2022).
[122] News Central Asia, 'Central Asia and BRI could open opportunities for "combining efforts" between Russia and China,' News Central Asia, 2019. https://link.gale.com/apps/doc/A583362986/STND?u=jscscoll&sid=ebsco&xid=636a359d (Accessed May 03, 2022).
[123] Sanders, 'Caught Between East and West.' 217.
[124] Shopov, 'Let a thousand contacts bloom.'

Article

# Female Radicalisation and ISIS: What are the Implications for UK Domestic Security?

By Wing Commander Siân English

**Biography:** Wing Commander Siân English joined the Royal Air Force in 2003 as an Intelligence Analyst before commissioning as a Personnel Support Officer. Having served in a variety of overseas theatres she completed the Advanced Command and Staff College in September 2020 and was made an MBE in the same year. She is a Charactered Member of the Institute of Personnel Development and was part of the Chief of Defence Personnel Team who received the 'Inclusive Teamwork' award in the Women in Defence 2021. She presently works in the MOD Defence People Strategy Team.

**Abstract:** It has long been the assumption that radicalisation and subsequent violent activity emanating from a terrorist group was predominantly from the male protagonists. Indeed, societal opinion and cultural bias asserts women involved in such activity have either been coaxed or hoodwinked by male predators, or that they are mentally or physically unwell and thus unable to make intellectual informed decisions; equally their involvement is peripheral. In 2015, three London school girls left the UK to join ISIS. Headlines then portrayed three innocent girls, lured, groomed and/or brain washed by an insidious organisation. The paper will focus on the increase of UK females radicalised by ISIS, who subsequently voluntarily travel to the Islamic State, examining the factors which made these women become more susceptible. It will offer that 'some' women, who are radicalised can pose a threat to domestic security, needing greater attention from the UK Government, Security Services and Partners Across Government to understand the impact gender has on security to ensure preventative strategies and policies are considered through a gendered lens.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

## Introduction

Islamist radicalisation has been at the forefront of the Western security agenda since the aftermath of 9th September 2001 (9/11) terrorist attack in the U.S., and the emergence of the term 'radicalisation' has shaped the actions of governments, practitioners, and scholars alike to understand and combat terrorism.[1] As such, it has become core policy and central to terrorism studies and counter-terrorism policymaking. The consequences of radicalisation and the existential threat posed by those who would carry out acts of terror is well documented and indeed much of the literature and research discourse within terrorism studies focuses on the subject. However, the link between female Islamist radicalisation and domestic security is not as apparent as much of the literature is centred on violent radicalisation and acts carried out by men rather than women. In addition, academic literature, governmental policies and strategies, and government security enforcement agencies all focus on preventative measures that have been written largely by men for men, and therefore are 'gender-blind'[2] which has serious implications when implementing counterterrorism, deradicalisation, and re-integration programs.

This research project will examine the link by focusing on the rise of UK females radicalised by Islamic State (IS) in Iraq and Syria (ISIS) and the potential implications for UK domestic security. The paper has two main objectives: 1) to critically analyse the contributing factors why ISIS was able to recruit UK females to its ideology and to highlight the primary reasons why these women were more susceptible to radicalisation; 2) to assess the potential impact to UK domestic security as women radicalised by ISIS integrate back into society by examining the current preventative measures and deradicalisation programs. This paper will begin with setting out the parameters of the research by outlining the methodological approaches used and the theoretical framework that has formed the foundations of the project. Throughout the paper the term female radicalisation, radicalisation and Islamist radicalisation will be used interchangeably, and IS, ISIS, Da'esh and Caliphate will be used in the same manner and will have the same meaning, but the focus will only be on the period 2014-2018 when the group was most active and in conflict with Western Forces. However, it must be noted that the group remains an active terrorist organisation with an online presence capable of radicalising states' citizens across the globe, including those from the UK.

This paper will only focus on Islamist radicalisation and not violent extremism, and it is primarily centred on examining the non-violent political motivations which made up the larger percentage of UK females who joined ISIS but acknowledges that a smaller percentage did want to bear arms and fight. The final point to note is that when defining UK domestic security, due to the classification of this paper, detailed counter-terrorism strategies and policies adopted by the security services cannot be included and instead the UK Government websites and online definitions in the public domain will be used when citing and referencing current preventative and deradicalisation initiatives. For the purposes of this research paper both *Prevent* and *Channel* will be referenced interchangeably as both are intended to tackle radicalisation in all communities, regardless of the ideology behind the radicalisation; however,

they are also different because one is only referred to Channel if, and only if, they are identified or flagged at various stages during Prevent.

This paper will conclude that the increase of UK females radicalised by ISIS does have implications for domestic security, as many of those women who travelled to IS witnessed terrorist attacks, potentially helped to plan attacks or condoned atrocities, committed acts of violence, or were directly involved in the establishment of the Caliphate by supporting its fighters, bearing their children, and lastly promoting the ideology's narrative and therefore hold the same extremist beliefs as the men in the group. Similarly, some women actively recruited other women online, promulgated ISIS' narrative across social media and were crucial players in the radicalisation of UK females. Whilst many of these women did not carry out a violent act or attack themselves, they did carry out key roles which gave the caliphate state-like properties, along with strength and power, and undoubtedly helped the ideology grow on a global scale. Further, for the most part these women were not victims or forced to travel, and academic research to date highlights that the vast majority voluntarily left to join a terrorist organisation who were fighting against Western democracy and international rules-based order in the name of religion, and therefore like their male counterparts they pose a threat to UK domestic security.

Despite the current measures in place to tackle radicalisation – *Prevent* and *Channel* - this paper will contend that greater focus must be given to the gendered lens of security if the UK Security Services and Partners Across Government (PAG) are to adequately support those females radicalised by ISIS through the de-radicalised programmes, the judiciary process, and subsequent reintegration into society. This latter point is key if the UK Government and security agencies hope to prevent further radicalisation in our communities when these women return from Iraq, Syria, or refugee camps, or are released from prison. Therefore, the part the UK Government, media, and social media plays in its narrative to society by rebranding the 'them vs Islam' segregation over the past 10 years is crucial to prevent the 'ISIS effect' reoccurring should another ideology offer young people the same opportunities. Ultimately, the roles women play in an ideology, a radical or terrorist group must be reframed in security literature, polices and military doctrine to appropriately assess risk through a gendered lens to mitigate against any potential threat to UK domestic security.

## Research Framework

Whilst the research approach is qualitative drawing on existing literature from the field of terrorism studies, the analysis does include the expert views of two leading scholars who have both published work in terrorism and radicalisation, with specific focus on the gendered lens. The primary aim of this research is to answer a defined question by exploring if there is a potential connection between the rise of female radicalisation in the UK and an increased threat to domestic security. By using a methodical framework and theoretical ideas from Identity Crisis Theory, Hyper-Masculinity Theory and Hyper-Femininity theory a positive research approach will be used to 'describe, understand and explain the links between

empirical phenomena, and the potential relationships between the theoretical concepts and the empirical facts'[3] which are required to test the hypothesis. Further, the research will share some of the views of Dr. Katherine Brown and Dr. Joana Cook from the expert interviews which will be used to fill gaps in existing International Relations and feminist theory literature on the potential connections between gender and security, and the implications for UK domestic security.

To ensure the research has originality and validity, both ontological and epistemological views have been considered and balanced by the input from expert interviews to ensure the research and information has been interpreted with neutrality.[4] The most relevant paradigm for this research is constructivism based on the fact there is no single truth or reality as distilled by Lincoln and Guba (*The constructivist Credo 2008*) 'constructivism is defined in such a general way that it can relate to a wider range of sociological theories.'[5] Indeed, within the academic field there is very limited quantitative statistics and research discourse about female Islamist radicalisation, specifically in relation to how many UK females joined ISIS and the implications for domestic security. Therefore, this paper aims to draw on both the extensive academic literature and content from the elite interviews and explore theoretical frameworks to test hypothesis whilst acknowledging that there are vast and differing opinions rather than truths.

## Section 1
## Defining Terms

This section will define the key terms in the research question: Radicalisation and UK Domestic Security.

### Radicalisation

Radicalisation and its concept have gained increased popularity since 2004 after bomb attacks in Madrid and London and it has become central to terrorism studies and counter-terrorism policy making.[6] As U.S. and European governments focused on 'home-grown' Islamist political violence and coined the term 'violent radicalisation' it has featured in much academic literature and discussion and become a 'political shibboleth.'[7] Kundnani (2012) comments:

> 'The introduction of policies designed to 'counter-radicalise' has been accompanied by the emergence of a government-funded industry of advisers, analysts, scholars, entrepreneurs and self-appointed community representatives who claim that their knowledge of a theological or psychological radicalisation process enables them to propose interventions in Muslim communities to prevent extremism.'[8]

Sikle et al define the term radicalisation as a process of how people become involved with terrorist causes or movements but argue that in the past it was often referred to as 'becoming' a terrorist, 'joining', a terrorist group, or of being 'recruited'[9] and that the term has been embellished and expanded by politicians and academics due to 9/11 and the shift in focus

to Islamist political violence. Schmid supports this notion that the term has been heavily politicised by Western governments and often applied one-sided to non-state actors who fall to adhere democratic processes and principles, laws and who use violence to achieve political ends.[10] This view is reinforced by Sedgewick who highlights that the term is linked too freely with terrorism by politicians which has created a multitude of obstacles.[11]

Horgan and Bradcock offer one of the most recent definitions which is widely cited in modern literature and define it as 'the social and psychological process of incrementally experienced commitment to extremist political or religious ideology.' [12] This latter definition will be used in this research paper as the description is befitting to ISIS in that the ideology was able to attract followers who were both radicalised in opinion and action. McCauley and Moskalenko argue that their two pyramids 'radicalisation of opinion' (beliefs, attitudes and feeling) are cognitive which is importantly different from 'radicalisation in action' (which is physical behaviour) however, the principle for both models is that for the vast majority 'radical ideas do not take radical action.' [13]

**UK Domestic Security**

The policy for UK Domestic Security is captured in the National Security Strategy (NSS) which outlines how the national capabilities are used to build a prosperous Britain through influence in the world and to strengthen our security by using all the instruments of national power to prevent conflict and avert threats beyond our shores. Fundamentally, the security of the UK is the foundation of our freedom and our prosperity.[14] Within this strategy one of the key areas is titled 'Risks to our Security' captures those threats which have the potential to become an existential threat to the state, undermine the core foundations of the society, or endanger the lives of our citizens.[15] Radicalisation, terrorism and extremism form part of the strategy and the policies and formal doctrine for UK Defence and the Security Services also lists Islamist Radicalisation as a continued threat to the UK. The National Security Strategy and Strategic Defence Review 2015 states:

> 'the increasing threat posed by terrorism, extremism and instability. Whether inspired by Islamist extremism, the far right, or the situation in Northern Ireland, the overarching goal of individual terrorists and the groups that support them is the same – to inflict harm, to inspire fear and, in so doing, look to undermine the very fabric of our society.' [16]

To mitigate against these threats, the UK Counterterrorism and Security Act received Royal Assent on 12 February 2015 and contains powers to help the UK respond to the threat of terrorism. The act has the power to do the following: disrupt the ability of people to travel abroad to engage in terrorist activity and then return to the UK; enhance the ability of operational agencies to monitor and control the actions of those who pose a threat, and combat the underlying ideology that feeds, supports and sanctions terrorism.[17] Within the Act, the UK Government introduced the *Prevent* strategy as part of the Government's wider counter-terrorism and deradicalisation strategy, known as CONTEST.[18] *Prevent* aims to

safeguard and support those vulnerable to radicalisation to stop them engaging in violent extremism or supporting terrorism, in all its forms including when it is inspired by Islamist or right-wing ideologies.

The purpose of *Prevent* is early engagement to encourage individuals and communities to challenge radicalisation, violent extremist ideologies and behaviours.[19] The strategy is reliant on the society, or someone working in schools, colleges, universities, hospitals etc who can raise their concerns to the police, or local authority safeguarding teams about a person they know who has or is susceptible to being radicalised.[20] The *Channel* programme which is a voluntary initiative provides a multi-agency approach to safeguarding, supporting and protecting children, young people and vulnerable adults at risk of radicalisation, extremism or terrorist related activity, and which delivers this strategic aim of *Prevent*.[21]

## Section 2
## The Rise of ISIS

This section will provide a summative overview of ISIS, its history, how it emerged and how it exploited the Western Media to create divisions in UK society to further its gains, before examining why the group posed a threat to international and domestic peace and security.

ISIS is a terrorist organisation that emerged only three years after 9/11 from the remnants of al-Qaeda in Iraq in 2004.[22] After the surge of U.S. troops in Iraq in 2007, the group was on the peripheral edges in the area, but not active and it did not pose a threat to the international community.[23] In 2013 the group changed its name to ISIS and launched an offensive on Mosul and Tikrit in June 2014. On June 28, Abu Bakr al Baghdadi, announced the end of ISIS and the birth of the IS on the first day of Ramadan; however, the UK and most of the West continued to refer to the group as either ISIS or Daesh.[24] The declaration of the caliphate was motivated by its military momentum, the size of its forces and the takeover of Sunni Iraq at the onset of the holy month of Ramadan, and saw Baghdadi call upon all Muslims throughout the world, including all existing jihadi groups, to accept IS supreme authority.[25]

Following several terrorist attacks by ISIS in the UK and across Europe in 2014, the group was assessed by the security services, and governments to pose a significant threat to international peace and security and was formally recognised as a 'terrorist organisation with considerable military and territorial and financial resource.'[26] As such, in August 2014 the U.S. and its allies resumed Air Strikes over Iraq. Whilst ISIS started in Iraq in 2004, it was the Syrian civil war in 2011 that saw the group grow exponentially benefiting from the instability in the country to gain territory and enabling it to recruit as many as 30,000 foreign fighters, mainly from the region but also from Europe.[27] The group seized strategic territory in Syria and Iraq, acquired a revenue estimated at $2 billion annually and created Islamic laws, including its own judicial system which included courts and a police force enforcing the 'Islamic Laws', and it was also able to 'claim the responsibility for over 90 terrorist attacks in more than 21 countries including France, Belgium, Turkey, Australia, the UK, and the USA.'[28]

It was this global reach that presented the greatest threat to international peace and security, including the UK, who viewed ISIS emergences as posing an existential threat to their state, their citizens, and international order. However, it was also this same factor that attracted large numbers of Westerners to join ISIS as it was able to make itself internationally accessible irrespective of geographical boundaries. This global reach was also one of the primary reasons it could portray the caliphate as an Islamic utopia, and a functioning state 'where *sharia* (Islamic law) would be implemented according to the principles of *al-salaf al-salih* (the righteous predecessors) or the first three generations of Muslims.'[29] The Internal Centre for Counter-Terrorism – The Hague - estimated in 2016 that between 663 and 883 women and young girls, including three London schoolgirls Amira Abase, Shamima Begum and Khadiz Sultana all aged between 15 and 16 travelled to join IS.[30] Since 2014, ISIS aggressively recruited Western women through their propaganda campaigns and narratives of *Dabiq* which called on Western women to perform *hijrah* to its territories, and in 2016 it released its first English-language magazine, 'Rumiyah' directly targeting UK females.[31]

From the outset, the UK media coverage on the British military's return to Iraq was extensive which heightened ISIS's profile and brought the group's presence on to the centre stage with minimal effort. The extensive literature on ISIS' propaganda machine highlights its far reaching, influential and immensely adaptive capabilities which in turn helped to radicalise, recruit and infiltrate Western society.[32] From broadcasting the group's violent, brutal actions such as streamed execution videos or armed fighters killing citizens who refuse to covert to the caliphate, to including videos and blogs, or celebrating the large number of Western fighters that left their homelands to join the fight for an IS, the Western Media unwittingly reinforced another dimension which enhanced the group's ability to recruit members and sympathisers, instil fear in its opponents, and promote its legitimacy as an IS.[33] This heightened global media presence, coupled with the group's extensive use of online platforms such as YouTube, Twitter, Telegram and online magazines in both English and Arabic was disseminated in-real-time on a scale not previously achieved by other terrorist organisations.[34] The media created sensationalist spectacles of violence which appealed to those seeking stardom, and popular culture and this narrative became the spectacle for the news media.[35] Hoffman explains, 'through the publicity generated by their violence, terrorists seek to obtain the leverage, influence, and power they otherwise lack to effect political change on either a local or international scale.'[36] Ultimately ISIS was able to use Western media to advance its political agenda, and improve its media strategies with a constant output merging 'pre-modern religious ideology with 21st Century communication management.'[37]

Using online media, ISIS was able to create a camaraderie and belonging which appealed to those individuals searching for a meaningful political, religious or personal identity.[38] A recent study by Cook & Vale found that many of the women who migrated to Iraq and Syria were attracted to the caliphate because of the purported sense of belonging and sisterhood which they felt lacking from the West, and the sense of unity, purpose and empowerment offered by ISIS and its ideology was a powerful recruitment tool.[39] Jeffry et al highlight that

'Ideology plays an important role in that it can provide the true believers with a license to kill'[40] and that ideology plays an important and constant factor in the radicalisation process towards terrorism. In contrast, Schmid argues that whilst ideology is a major factor for some, he cites McCauley and Moskalenko by noting that there are many paths to radicalisation that do not involve ideology.[41] However, it was ISIS' ideology that acted as a key pull factor in the recruitment of Western women who were drawn to the notion of building utopia, the so-called 'Caliphate' in the hope to live Islamic lives without the restrictions of Western laws, societal pressure, judgement and victimisation; these narratives were important drivers of female radicalisation.[42] It was ISIS' ideology and propaganda machine that attracted and empowered UK women to join the group.[43]

## Section 3
## Radicalisation: Primary Motivations and Factors

This section will explore the primary reasons for radicalisation and the factors associated with the radicalisation process by examining McCauley and Moskalenko's 12 mechanism model and McClauley's Two Pyramids Model looking at Radicalisation of Opinion and Radicalisation of Action. The expansion of theoretical models over the past decade has been fuelled by a plethora of theories around what factors and processes drive radicalisation.[44] The models all provide different perspectives on the issue, but for the purposes of this paper the McCauley and Moskalenko's 12 mechanism model will be used as a framework to understand the primary reasons why ISIS was able to radicalise many Western females, specifically UK females, to join the caliphate. Published in 2008, the McCauley and Moskalenko's model argues that radicalisation can happen at three levels: individual, group, and mass.[45] The primary argument in their work is that normal people can be radicalised and move towards criminal and violent behaviour, and that radicalisation is not an abnormality or psychopathology. The focus on Individual radicalisation features heavily in their works, and six of the twelve mechanisms

**Table 1: McCauley and Moskalenkos 12 mechanism model**[46]

| Level of radicalisation | Mechanism |
|---|---|
| Individual | 1. Personal victimization |
| | 2. Political grievance |
| | 3. Joining a radical group—the slippery slope |
| | 4. Joining a radical group—the power of love |
| | 5. Extremity shift in like-minded groups |
| Group | 6. Extreme cohesion under isolation and threat |
| | 7. Competition for the same base of support |
| | 8. Competition with state power—condensation |
| | 9. Within-group competition—fissioning |
| Mass | 10. Jujitsu politics |
| | 11. Hate |
| | 12. Martyrdom |

Table 1 above outlines the level of radicalisation and the mechanism.

are identified by the process of political radicalisation centred around Western culture and psychology that behaviour reflects an individual's beliefs, feelings, and preferences.[47] Within their framework, each level is considered as a pathway leading to radicalisation, and the 12 mechanisms within the model describe how the process can happen.

At the Individual level, mechanisms one to four outline grievances, either directly or indirectly through affiliation with a group whom the individual identifies with, that leads an individual to move from sympathizer to activist which sees radicalisation of opinion (behaviour) develop to radicalisation of action (carrying out violent acts). However, in most cases this process is normally slow and gradual, and cases of individual radicalisation to political violence, highlights that more often than not an individual will act as part of a group, or on behalf of the group, rather than on their own.[48] Mechanisms three and four are particularly relevant in this paper as ISIS was able to successfully attract individuals to embrace the violent ideology in support of a political and religious cause which led to some moving through the process from sympathy (cognitive radicalisation) to extreme violence in a single giant step. However, Silke and Brown argue that radicalisation is complex and dynamic, and there is no single route to an individual carrying out a violent act[49] and that more than 200 different factors have been identified by research that play a role in the radicalisation process.[50]

The path that leads an individual to join a radical group is often via personal connections through a trusted network of friends, lovers, and family to prevent betrayal to the authorities. This was particularly true in the ISIS recruitment campaign as many young UK females were contacted online through friendship groups, by other trusted women and through family and friends. In the case of the three London School girls, it is alleged they were recruited online by an old schoolfriend, Aqsa Mahmood, who had already made the journey to Syria in 2013 and that she facilitated their journey, which indicates the importance of the 'sisterhood' to escape the feelings of oppression, isolation, and identity which they believed lacking in the West.[51]

At the Group Level, mechanisms five to nine outline how individuals can be radicalised through affiliation with likeminded people, through shared values, beliefs, opinions, and feelings which can result in conflict, competition and resentment against other groups, political and societal opinions or even state governance and rule of law. These changes in behaviour are often referred to as 'risky shift,' 'group extremity shift,' or 'group polarization' [52] and outlines the process where strangers with shared political opinion come together and adopt two types of behaviour.[53] More often, the shift towards increased extremity occurs on the balance of which opinion is favoured most by those within the group.[54] In the case of ISIS the 'group extremity shift' is particularly relevant as despite the vast array of differing motives that shaped individual aspiration and motivations to migrate to the IS, the group was able to fuse diversity of opinion of its recruits persuading them to follow its idealistic goals of religious duty and to build a utopian 'Caliphate state'.[55] The power of group radicalisation is especially evident regarding Western women who joined ISIS with many citing social and

cultural isolation within communities being a key push factor in their decision to leave in search of a Muslim sisterhood and to find a sense of belonging and identity with individuals who shared their opinions, values and beliefs.[56]

At the Mass level, mechanisms nine to twelve outline a much larger phenomenon of radicalisation which sees exceptionally large numbers (thousands upwards), or multiple groups with similar shared characteristics joining forces. These small, combined groups lead to increased group cohesion, increased respect for ingroup leaders, the acceptance of established structure and idealisation of group norms.[57] Mass radicalisation was a concept used by ISIS to create a 'State like' identity by pushing the extremist narrative that cast the other side (the West) as evil, as 'enemies,' and that individuals joining the group must fight at all costs in order to preserve their way of life. By building the Caliphate, ISIS was able to convince its recruits that it was their mandatory religious duty to assist in the process of State-building and its narrative was that all Muslims must travel to build IS.[58]

Historically, mass radicalisation took time as the outlet for information and dissemination was slow through newspapers or political speeches in towns and cities etc. However, that is no longer reality with the power of the internet as a radicalising message can be broadcast to hundreds of millions of people in a matter of seconds. ISIS effectively embraced the full power of this tool by using social media platforms to maximum effect reaching individuals worldwide, via their mobile phones or other electronic devices with relative ease.[59] The internet, media outlets and social media companies set the perfect conditions for mass radicalisation for the ideology and between 2014-2017, ISIS was able to recruit over 41,000 citizens from 80 countries, and a quarter of these were women and minors.[60] Further, its use of slick videos, online messages, extensive Vlogs and Blogs on YouTube and Twitter, and the creation of an app that all aimed to radicalise and create a new generation of cyber jihadists, fighters and terrorists suggests that its reach, goals and ideology extended beyond the 'state' it had built.[61] Cook and Vale argue that these modern-day tools helped ISIS spread their propaganda and ideology to thousands of online sympathisers across the world, and despite ISIS' loss of territory many of its supporters are likely to carry on its ideology, mostly online.[62]

Whilst the influence of the internet is cited extensively throughout literature on ISIS as being a key component in the radicalisation process of its recruits in the most part this is the first step which sees an individual's behaviour, beliefs or values change as described in the model above.[63] McCauley and Moskalenko refer to this first step as 'Radicalisation of Opinion' and this process is illustrated by a 'Radicalisation in Opinion Pyramid' which demonstrates how individuals or groups can move upwards from neutrality to sympathiser, to justifier to personal moral obligation to act (violently in most cases). Further, that the pyramid represents the front line in the 'war of ideas' between terrorist and government.[64] This later point is especially true for individuals who joined ISIS as many of those radicalised by the group cite political motivation directly linked to their treatment by Western governments, and the UK Foreign Policy, as their primary factor for deciding to travel to the IS.[65]

## Section 4
## How ISIS Recruited Western Women?

This section will analyse how ISIS was able to recruit Western women to support its ideology by exploring some of the key reasons how the ideology deliberately targeted and directed their recruitment campaigns to attract UK/Western women to the Caliphate.

Although foreign fighters joining an Islamist extremist organisation is not a new issue, the call from ISIS resonated with greater numbers of Westerners to travel and join the Caliphate than in the past.[66] This was especially true in relation to the number of Western females who migrated to join ISIS, and Bakker and de Leede argue that the conflict in Iraq and Syria introduced a new dimension which saw Western citizens of Muslim origin, or converts to Islam, travelling to Iraq and Syria voluntarily to fight against their own society. Indeed, their research suggests around 10-12% of the individuals who travelled from Western countries were women, of which around 80-90 were from the UK.[67] However, this number is disputed as most western countries, including the UK, did not track the gender of those that travelled and therefore the number could potentially be higher.[68]

The 'International Centre for the Study of Radicalisation' at King's College London estimates that the women were mainly aged between 16 and 24 years old, and that the women fall into two main groups: those that travelled as a family unit, and those that travelled alone.[69] One of the most important reasons cited in the report prepared by the Institute for Strategic Dialogue (ISD) is that ISIS was able to recruit greater numbers of women to join because of its state-building project.[70] Indeed, the call from the leader al-Baggdadi directly calling upon Muslim females to travel to help build the new territory, and how they would play an important role in its society by assuming the traditional roles as wives and mothers. Offering Western women, the opportunity to be part of the fight by adopting *jihad* off the battlefield by raising *mujahid* children, and by supporting their husbands in the fight to create the foundations for the new proclaimed caliphate was a major driver for women who travelled because the narrative empowered them to act.[71]

### The Importance of Western Women to the Ideology, and the Caliphate

Spencer expands on the importance of women in the ideology and highlights that the ISIS leadership viewed women, especially Western women, as an 'untapped resource and it was increasingly willing to make concessions in its ideology to fold women into its ranks.'[72] Peresin and Cervone reinforce this notion and highlight that ISIS recognised that women produced sensational international media attention as media outlets became fascinated by the roles women filled within the territory, especially those women who were well-educated, professional from well-established families and who generally had bright prospects of life in the West.[73] This enhanced attention, and media coverage saw ISIS actively use women for propaganda purposes which generated a new swath of potential recruits who became alerted to the ideological cause with minimum effort.[74] Further, the promise and hope ISIS portrayed online appealed especially to Western women as they were given the opportunity to do more

than simply play a peripheral role as they were actively encouraged to undertake physical action by travelling to join the group in the creation of an ideologically pure state.[75]

The traditional role of a woman in most Islamist terrorist groups is to serve her husband and previous groups such as al Qaeda clearly emphasized that men and women were not equal and therefore women were not permitted to leave their homes unless there were legitimate reasons, such as having to wage jihad when no men were available.[76] ISIS from the outset depicted the importance of women in building the State and whilst women were recruited to fulfil traditional roles, they were also recruited to take on active roles such as policing official, recruiter, and in armed roles.[77] Gan et al state that ISIS used these enhanced roles as a form of empowerment which helped in the recruitment of Western women to join its ranks.[78] This was particularly evident when ISIS created an all-female police unit, Al-Khansaa Brigade, in 2014 to enforce strict rules and regulations women living in the State.[79] Again, these high profile armed roles normally preserved for men acted as key recruitment tool as women were offered directive roles in the governance of the Caliphate, and thus demonstrated the importance of their presence to the group. However, for some women it was the opportunity to carry out acts of violence in the name of ISIS which lured them into making the journey,[80] which reinforces that some women want to bear arms and carry out violent attacks like their male counterparts, and therefore can pose a threat to domestic security.

## Section 5
## Identity Crisis Theory and the Push/ Pull Factors of Radicalisation

This section will analyse the 'push and pull factors'[81] that influenced UK citizens to become radicalised by ISIS looking at Identity Crisis Theory to critically examine the role of the British Governmental decisions, strategies and polices played and that of UK society in the radicalisation process.

### Identify Crisis Theory

The term identity 'refers to a complex theoretical construct involving elements originating at three levels: cultural, social and personal.'[82] Identity crisis theory played a key part in the motivations of UK women who decided to travel, and many cited when interviewed that they felt isolated from society (personal), isolated culturally by British norms and way of life (societal), and uncertain of their place within a Western culture which made them question their identity (cultural).[83] Hamid highlights that 'studies on radicalisation find identity to stand at the forefront of the radicalisation process'[84] and Stroink states this is especially true for Muslims living in Western democracies where public displays of religiosity go against mainstream views.[85] These feelings of exclusion, and discrimination in some cases, can lead certain individuals to draw heavily on their religion in their search for identity because the mainstream society threatens their 'self-identity.'[86] Liht and Savage argue that European Muslims face '*self-definitional uncertainty*' and the solution for many was an intensification of Islamic identity.[87] Certainly, one of the major pull factors for UK women was ISIS' ideology and the creation of a pure-IS where individuals believed they could find a sense of belonging, unity and self-identity.

## The Push Factors

> 'The motivations for women to travel were diverse and generally referred to as drivers or 'push' and 'pull' factors – factors in their individual lives that 'pushed' them out of their society and 'pulled' them toward IS.' [88]

The factors, processes and rate of radicalisation for both men and women is not linear but Cragin and Daly argue that there are distinct patterns.[89] The 'Push Factors' are those that 'prime certain women to be more vulnerable to extremist propaganda' [90] and from the extensive research by the ISD report 'Till Martyrdom Do Us Part' highlights that the factors which motivated Western women to migrate to ISIS-controlled territory were similar, if not the same, as their male counterparts.[91] This notion is supported by Bakker and de Leede who argue that the motivations of young women and young men who joined ISIS were broadly similar.[92]

The major push factors cited during the extensive interviews and research of men and women were: 'feeling isolated socially and/or culturally, including questioning one's identity and uncertainty of belonging within a Western culture; feeling that the international Muslim community as a whole is being violently persecuted; and, an anger, sadness and/or frustration over a perceived lack of international action in response to this persecution.' [93] Hoyle et al expand the concept by adding that like men, women saw it as their ideological and religious duty to support jihad and live their lives by the laws of Alah in a pure IS because Western culture did not offer this opportunity or prospect, and for many this was seen as a push factor in the search of self-identity.[94]

Research suggests that most females radicalised in the UK were second or third generation who are shaped by their parents' views at home, which were often in conflict with their own, and who struggled to integrate into British society and be accepted. Many stated they felt in conflict between their religion and the cultural norms of society.[95] This was further exacerbated by the UK Government's emphasis on 'political correctness and Muslim cultural sensitivity' which appears to have unintentionally aggravated feelings of difference and separation.[96] Equally, other societal pressures on identity such as socioeconomic status, higher unemployment and low social standing caused individuals to become disenfranchised due to a perception of unfair treatment.[97] Tahir states that 'Muslims may fall prey to radicalisation as they suffer from economic inequality, social disparity, discrimination and acts of Islamophobia' [98] and Roy (2004) supports this notion by arguing that ISIS was able to target individuals in doubt of their identity and faith, and that ISIS appealed to an '*uprooted, disaffected youth in search of identity beyond the lost cultures of their parents and beyond the thwarted expectations of a better life in the West*.' [99] These individuals strongly believed that ISIS could provide them with a chance to build a new and positive identity and be part of a pure IS or a 'imaginary ummah.' [100]

Studies in Britain illustrate that personal negative experiences, such as attacks on fellow Muslims in Iraq and Afghanistan, the death of loved ones, or close relatives also fostered cognitive openings and extremist visions.[101] Hasan argues that revenge theory plays a part as

individuals are outraged by Western actions, foreign policy and that the oppression of Muslims can trigger radicalisation, which links directly to one of the Push Factors outlined above – 'feeling that the international Muslim community as a whole is being violently persecuted.'[102] The feeling of persecution and being under attack from the West was echoed by female migrants who talked of the oppression of Muslims internationally as a motivating push factor.[103] In addition, anger and frustration over international inaction, on issues such as racism, inequality within society etc broadens the divide between Muslims and non-Muslims, and the 'us versus them' narrative heightens, for some, feelings which justify violence against this perceived enemy force.

Another factor during the early stages saw some Western women migrating in the name of humanitarianism and their process of radicalisation was accelerated due to the perception that the West was in some way responsible for the atrocities on the ground, and in the suffering of innocent Muslims.[104] The empathy that women undergoing radicalisation feel for victims of violence is a highly influential factor for individuals choosing to leave, and it was seen as a key push factor.[105] Finally, the rigid patriarchal values in parts of UK Muslim communities was cited by female participants as a push factor, with many suffering from low self-esteem, a feeling of restriction of opportunity due to their gender, and how they were perceived as being less educated, less 'streetwise' and less resilient.[106]

### The Pull Factors

While the push factors for men and women were broadly similar, the primary 'Pull Factors'[107] for women were more gender specific and predominately shaped by the roles that they could fill once inside the IS. Recent academic research identifies that the pull factors were much more specific and individualised and shaped by incentives, motivations and goals for each woman who left to join the Caliphate.[108] However, the most cited by those interviewed in existing literature are: Idealistic goals of religious duty and building a utopian 'caliphate state'; belonging to a sisterhood; and romanticisation of the experience, which are all gendered. Lahoud reinforces this notion by highlighting that the major pull factors were diverse and ranged from ideological motivations, the opportunity for empowerment and adventure, seeking a husband or joining one in country, the perceived 'obligation' to make hijra and live under strict Islamic jurisprudence and governance, and play an active and supportive role in the State-building project.[109]

Whilst the vast majority of Western women appeared willing and eager to travel, often evading their families in the bid to make the journey, there is also evidence to suggest some were coerced or forced to travel by their family unit, through marriage.[110] Sherwood et al argue that given the age of the females that travelled, particularly from the UK (the London school girls were 14 and 15 at the time), that they were groomed online and that they made the decision to leave because they were too young and naïve to understand the consequences of their actions.[111] Sjoberg and Gentry highlight that the Western media were quick to victimise these girls for travelling by belittling their actions to simply the pursuit of romance, to find husbands

and to be wives and mothers. These perceptions were reinforced by UK media outlets, and governmental departments to potentially avert the real reasons girls had been radicalised by ISIS by removing the issue from the political agenda or preventing questions around governmental commitment to ethnic minorities, societal or community divisions or failure in radicalisation policies.[112] These narratives made the actions of UK women seem irrational and non-credible as potential terrorists, and for some, the lack of recognition was a driver that shaped their reason for leaving, and for others it was a rebellion or demonstration of defiance towards society.[113]

The most captivating pull factor for UK women was the prospect of a new world, a utopian society and many travelled in search of the opportunity to live freely as a Muslim without victimisation, intimidation, threats of violence and Islamophobia they received in their daily lives in British communities.[114] The ISIS propaganda and official speeches by al-Bagdadi reinforced this pull factor as females felt they were an essential part of the State-building process, and thus the sense of personal and societal identity relating to the 'Sisterhood and Belonging' lured women to travel to the caliphate.[115] Hoyle et al highlight how the strong bond with other 'sisters' formed online, especially for those women seeking sanctity, acceptance, or a sense of belonging which they felt was missing in the UK/Western culture was a key pull factor, and those cited in the ISD report consistently referenced a feeling of belonging, of unity and community as their motivation.[116]

The final major pull factor which was captured extensively in the media was the romantic notion of adventure and finding romance. As most UK females who travelled were aged between their late teens and early twenties, the promise of marriage and status after being married to a jihadist was their reason.[117] In addition, some saw the opportunity as a chance to rebel against their family, a way of starting their freedom of expression, and the possibility to make the transition from childhood to adulthood on their own terms.[118]

Despite the many factors which mirror their male counterparts, the UK media portrayed the females as 'Jihadi Brides' and therefore simply dismissed them as hopeless romantics. Schröter warns against this assumption by stating that 'the women of ISIS may have been partly attracted by romantic ideas of finding a soul mate, but like the male jihadists, they also see themselves as part of a grand movement that will completely change the world.'[119] This view is supported by Ingram who argues that the media has portrayed a simplistic understanding of female radicalisation and recruitment which does not match reality, and the notion of the 'jihadi bride: the idea that females are motivated to join ISIS solely for romantic and sexual motives'[120] significantly undervalues the importance of women. Equally, it miscalculates the potential for women to be regarded as a security threat in the future and undermines the principles of CONTEST strategies.[121]

Brown reinforces this notion that the consequence of gender and radicalisation is holistically overlooked and that the 'policies not only fail to prevent radicalisation and terrorism, but it

further reinforces the insecurities of women driving them to groups such as ISIS.'[122] Further, Brown & Cook agree that the link between gender, radicalisation and security is not given the appropriate resource, funding, training or attention by the UK Government or the Security Services and therefore *Prevent* and *Channel* both overlook the threat radicalised women pose to domestic security.[123]

## Section 6
## Gender and Radicalisation

This section will analyse the importance of Gender in the ISIS radicalisation process by exploring the similarities and differences between men and women including their roles in the Caliphate. Similarly, it will examine the impact and relevance of UK societal gendered perceptions and stereotypes.

Gender describes the socially constructed characteristics and rules that construct masculinity and femininity.[124] This includes behaviours and roles associated within the social construct such as power dynamics, and gender will vary within societies and can change over time. As such, it plays a considerable role on daily life for citizens as it defines power relations throughout socio-political domains in sometimes rigid and restrictive ways depending on regime type, societal and cultural factors.[125] Studies of female and male radicalisation often consider them in isolation, but Sageman argues that in fact women, like men, join extremist groups for both personal and political reasons and that organisational factors, such as ideology, motives, aspirations and group unity are strong influences for both.[126] However, by linking men and women's motivations as similar, Pearson & Winterbotham argue that the societal assumption about 'women's "natural" propensity for peace is challenged.'[127] This was particularly relevant in the UK as the Government would not accept that females left freely, and that they had the same motivations as men because this narrative would likely cast doubt on their deradicalisation strategies, and potentially highlight divisions within society.[128] Similarly, the shift in the rise of females being radicalised challenged the perceived recognised societal behavioural and stereotypical norms depicted of UK women.

Within societies, gender perceptions will differ depending on the regime type, religion, culture etc. but in general terms men are often depicted as adventurous, aggressive and rebellious and therefore joining ISIS to fight for a cause befitted this narrative, whereas women are viewed as obedient and compliant[129] and therefore their decisions to join ISIS was viewed as irrational and based on unhappiness, bad relations at home, tension with parents, education, conflict with the rise of identity around feminism, or mental health.[130] Loken and Zelenz argue that the rise of female participation in ISIS challenged Western perceptions on gender norms in relation to violence, as women are often seen as victims rather than perpetrators.[131] As such, their participation in the group has continued to perplex policymakers, government officials and researchers, and the Security Services and it is also these gendered norms and perceptions within UK society that have shaped deradicalisation programmes resulting in preventative strategies which have overlooked understanding security through a gendered lens.[132]

Another push factor cited by UK females who joined ISIS was the Islamophobia they faced within their communities, and online.[133] The predominant identification of a Muslim woman is a visual one as they wear religious symbols (hijab, burqa) which makes them more susceptible to victimisation and discrimination within Western society; the same cannot be said for a Muslim man as their relationship with religion does not require them to wear external religious attire.[134] Indeed, UK Muslim women are often viewed as oppressed and passive victims of Muslim men and this narrative has been fuelled by the 'War on Terror',[135] and terrorists attacks on home soil which have generated a one-dimensional perception within society which has exacerbated Muslim women's feelings of isolation from communities and society. Moreover, these narratives were intensified by the international community who responded with abject condemnation as Western women migrated to join ISIS and governments and media outlets regularly referred to them as 'mothers, monsters (and) whores.'[136] Despite the growing awareness of the varied roles, and importance, women play within conflict,[137] many of the labels and narratives were centred on gender stereotypes such as victim, mothers, wives and sisters of radical men which denied these women agency as an individual actor.[138] Brown focuses on the narrative of 'hypersexualized warriors' which again reinforces motivation based purely on romance, and highlights how women were perceived as being ill, dangerous and potentially mentally unstable.[139]

In contrast to these ideas of romance and vulnerability, Yilmaz argues that the great majority of Western women joined ISIS to 'escape the alleged pressure and denigration they have encountered living in the West'[140] and that their motives like men, were more political than psychological.[141] Likewise, Gan et al argue that many young Western women who voluntarily joined ISIS shared the same motivations as men: 'motivated by ideology; motivated by alienation and equality motivated by romance; motivated by peer influence; and motivated by sense of security'[142] and that they were both educated and fully aware of their decisions.[143] Their deep grievances at the treatment of Muslims worldwide, the political and social resentment towards the West's foreign policy, the lack of opportunities in society and the isolation from their community were broadly the same motivations shared by men online.[144] Ingram reinforces this notion that some of the major motivators for Western men and women were similar and equally as complex: 'personal experiences, a range of politico-historical and psychological factors such as identity crisis, feelings of marginalization, perceived erosion of gender roles in society due to emerging feminist movements, and unequal opportunities in society in comparison to non-Muslims.'[145]

Bloom challenges the assumption that women are drawn into violence by men, by arguing that women are driven by political motivation in the same manner as men, and that 'some women are just as blood thirsty as the male members', and like a man.[146] Although women were initially recruited for more domestic roles, ISIS' Manifesto did not exclude combat roles for women, and indeed the Al-Khansaa Brigade was responsible for policing the IS territory which often involved undertaking acts of violence for those not abiding to the caliphate rules.[147] Indeed, Cottee highlights that during interviews with ISIS women they mocked the Western concept of Jihadi Bride by stating that no women would leave the comfort of their

home just to marry a man, and that these views were held only by Western men, or Western media to belittle their agency and alliance to the caliphate.[148]

### Women's Roles in ISIS and Gender Perceptions Around Femininity and Masculinity in UK society

As women are generally assessed as less risk to domestic security or viewed as periphery in the terrorist groups, ISIS was able to exploit this resource with limited scrutiny.[149] Brown states that ISIS Western women were seen with weapons or dressed as a suicide bomber in ISIS propaganda videos to signify their support to violent 'jihad' and to highlight that women had made a 'political choice' as much as a personal one to join the group, which was aimed to challenge Western values, society and gender norms.[150] Whilst the day-to-day roles between men and women differed, current research across the field suggests that like men, women's motivations were borne out of a devotion to gendered religious and political ideology to the creation of the IS.[151] Cook and Vale highlight that the women who were radicalised online were made to feel empowered and crucially important to the existence of the caliphate, and even though the roles would be predominately domestic, they were also numerous and diverse: Wife, Mother, Operational (Al-Khansaa Brigde), Recruiters, State-Building and Skilled Workers such as doctors, and teachers. Women joining ISIS viewed these opportunities as meaningful employment which many lacked in the West.[152] The diversity of these roles undoubtedly shaped ISIS' recruitment campaign, articles and propaganda messaging which led to the largest number of Western women to join its ranks than any Islamic group in history.[153]

A recent study by Pearson and Winterbotham emphasises that some women joined ISIS because of the growth of Western feminism, gender equality and consumerism and that their decision to leave was based on the rejection of these Western values.[154] Their research suggests that many Western women believed a new enhanced status in the State would serve as dual functions: it could constitute rejection of traditional family norms which see women restricted more than men, and it could offer independence and a new identity which rejected Western norms which does not value religion and the role of women to raise the family.[155] Unsurprisingly, the loss of status in their communities in the West and a desire to attain greater prominence in a society was strongly linked with female rather than male radicalisation.[156] The sense of worth and value in society was a firm part of ISIS' narrative to depict women as valued supporters with agency within their families, who gain status from their husbands' perceived glory, and this was reflective in a specific policy for women widowed which further heights the status the group placed on women within its ranks.[157]

For some Western women, their exclusion from wider society due to governmental partial banning of religious dress left them feeling unable to express their religion how they wished. Further, the UK media often associated religious items of clothing, particularly Islamic headwear such as the veil with oppression, terrorism, fundamentalism, and victimhood.[158] A consequence of this narrative left some women believing they must choose between their Muslim identity and their belief in gender equality; one that involved betraying either

their faith or their feminist conscientiousness. This was a key pull factor for Western women as the group offered them the opportunity to do both.[159] These feelings were aggravated by the UK Governmental policy to limit religious headdress in the community, places of work and educational environments which led to greater segregation and further marginalised Muslim women as 'different' to the societal culture thus promoting a new wave of Islamophobia both within society and actively online.[160]

Whilst there were gendered motivations for the men and women who joined ISIS, Topping and Gani (2015) argue that men and women were motivated by 'idealistic reasons' [161] and this view is shared by Pearson who argues that the shock within societies stems from the disbelief that women, like men, appear to have an appetite for violence. The fact UK women willingly joined a violent and extremist group which violated women shocked society as it did not align with gendered norms,[162] and Brown argues that these gendered perceptions have wrongly shaped the UK Governmental approach to female radicalisation.[163] Similarly, that the UK Governmental Departments have significantly overlooked the role women played in ISIS, and in most cases they were considered peripheral based on the assertion that historically women have carried out fewer attacks than men and therefore their participation is viewed as somehow a lesser threat to domestic and international security.[164] The perception that UK female Muslims who joined ISIS had less agency than men demonstrates a lack of understanding of the importance gender plays in the radicalisation process, and the significant role women can have in terrorist groups, which has led to an inevitable assumption that women pose less of a security risk.[165]

## Section 7
## Female Radicalisation and Threats to UK Domestic Security

This section will analyse the link between gender and security by exploring elements of the UK CONTEST Strategies, and to identify the potential risk from women radicalised by ISIS and the implications to domestic security.

Peresin and Cervone aptly summarise why women who join a terrorist organisation should be considered as much of a security threat as their male counterparts:

> 'Female suicide bombers may conceal explosives and evade security checks better than their male companions and have more chances to hit with precision their targets, because they are considered less suspicious than men.' [166]

Current research shows that the UK Counterterrorism and Deradicalisation programmes are gender-blind and that the integration of gender perspectives during the design, implementation and review processes is extremely lacking in substance.[167] Brown argues that:

> 'there is little explicit consideration of the role of gendered norms and impacts in these programs for either men and women, rendering such efforts unreflectively focused on men's security needs and priorities.' [168]

The European Radicalisation Awareness Network highlights that while motives into radicalisation appear similar for both men and women, the mechanics are influenced by gender but that this is often overlooked because the gender norms of society hinder the success of the programmes; women are seen as victims and men as aggressors.[169] Jacobs reinforces this notion that empirical evidence of female motivations and the factors in the radicalisation process is problematic as it denies women agency and fails to acknowledge their perceived grievances, and most importantly that it creates a dangerous gap in the security response.[170] Pearson and Winterbotham support this view by arguing that '*if policy-makers ignore the variety of women's motivations in favor of stereotypes, this will limit the reach of any policy designed to counter or prevent their involvement*' [171] and therefore detecting radicalisation in communities will be difficult because reality contradicts assumptions and norms about how women should behave.

Whilst female Islamist radicalisation is not a new phenomenon, the number of young UK females who left to join ISIS was unprecedented, and with many unaccounted for possibly still living in Iraq, Syria and Turkey, or in refugee camps and yet to return, the threat they pose to domestic security remains unclear.[172] Furthermore, as the UK did not track the gender of those who travelled so the exact numbers who left to support ISIS is unknown, it is very difficult for the Security Services and PAG to appropriately assess the potential implications or threat to domestic security, and equally to introduce mitigation methods, strategies or policies to minimise such threats.[173] Similarly, those females that left but who travelled as part of a family network remain broadly undetected as their reason for travel at the time could be legitimate such as visiting family, and therefore it is unlikely they were stopped from leaving, or returning, by boarder control agencies as their activity was not deemed suspicious.

Brown states that the potential security threat posed by these females is the most difficult to assess, but that it is likely to be much lower than those who travelled alone as association with a terrorist does not mean an individual will carry out a violent act themselves.[174] However, Cook holds a different view that women who have spent time in conflict zones who have been facilitators or supported foreign fighters or terrorists, whilst not directly engaged in the fight on the frontline, have been invaluable facilitators and provided essential information on Western culture and security practices which can be used by the group, and their direct inputs are likely to increase the success of terrorist activity, and therefore these women could pose a threat to UK domestic security.[175]

Given that several young British women were reportedly active in the support of the Al-Khasaa Brigade, concerns have been raised about the level of threat they pose to the UK as they have been closely linked to brutal and violent atrocities and punishment of women, and associated with, or supported the group in many ways.[176] This group is assessed as having the greatest potential to carry out a lone attack in the West given their extremist behaviour in the name of ISIS.[177] Focusing on this group who were predominately young single women it must therefore be assumed that the vast majority left voluntarily. As this group made informed decisions to leave their home and join a terrorist organisation, Brown and Cook agree that this group

could potentially pose the greatest risk to UK domestic security.[178] This notion was introduced by Briggs and Silverman who argue that there are three type of threats to domestic security that originate from individuals involved in terrorist groups: directed plots by individuals acting upon group instructions; individuals who carry out lone attacks without direction, but pledge alliance to the group; and individuals, or a network, that provide support and infrastructure to terrorist plots.[179] Indeed, a 2018 RUSI report highlighted that a small portion of those who voluntarily travelled are more likely to target the West, especially since ISIS has lost territory leaving many resentful to the UK and U.S. Governments for their military intervention in Syria and Iraq.[180]

Although ISIS may have lost most of the territory it acquired, the *MOD Regional Threat Outlook: Daesh, Iraq and Syria* report reinforces that the group remains a threat to UK domestic security.[181] The report states that Daesh remains a global ideology driven by a long-term objective of re-establishing the caliphate and therefore it will continue to employ violence to achieve its objective.[182] Further, the report highlights that the group maintains its global network of affiliates who are active in employing its Islamic governance to ensure the group maintains its leading position within the global Salafi-jihadist movement.[183] Brawn agrees that UK women living in the Middle East in areas still largely controlled by ISIS are still part of this active network, and as they have already been exposed to brutal war experiences and established contacts, formulated networks and adopted ISIS' way of life, this makes them a particular threat to domestic security if they try to return.[184] Hegghammer argues that whilst his 'tentative data' does not indicate that all foreign fighters return to carry out domestic terrorist attacks, there is a small minority who are motivated overseas, who have acquired terrorist combat skills and are therefore more effective operatives on their return; this group does have implications for domestic security and counterterrorism strategies.[185] Therefore, those females who travelled from the UK to join ISIS voluntarily, and who have chosen to remain living overseas or in refugee camps waiting to return home, like Shamima Begum, should not be underestimated as even a small number of returnees with the skills and desire to carry out terrorist attacks pose a very real threat to domestic security.[186]

In the four years of ISIS control, it is highly likely that many UK women will have been further radicalised, married to a jihadi fighter, remain living in a war-torn country or a refugee camp, and potentially support the group online or regionally. Whilst some women have chosen to remain, others are unable to leave having surrendered their passports upon arrival as a sign of dedication to the caliphate.[187] Further, the lack of support provided by the UK Government for those wanting to return could potentially exacerbate feelings of resentment, abandonment, and betrayal which are all motivating factors in the radicalisation process. Indeed, these feelings are likely to have intensified by the change in 2015 to the UK Counter-terrorism and Security Act which was amended to introduce new powers to remove British citizenship from any individual who travelled to join ISIS who has appealed to return if they are assessed as a security threat.[188] This was the case for Begum who asked for leave to return to the UK from a Syrian refugee camp but her appeal was denied due to her links with ISIS, and the

fact that she displayed little remorse for leaving the UK and for her actions. As such she was deemed an unacceptable candidate for deradicalisation and not granted permission to return.

While senior political figures, the Security Services and the Metropolitan Police Commission all agreed that Begum, and others like her, do pose a security risk to the UK, the temporary measure of citizenship deprivation whilst effective in the short term to reduce the immediate threat, is likely to be counterproductive in the longer term as a Counterterrorism approach.[189] An individual's sense of betrayal from having citizenship removed, the potential disillusionment with the radical cause itself and the psychological scars faced by those who have witnessed fighting could pose a greater threat if these disenfranchised, isolated and aggrieved individuals chose to seek retaliation.[190] Furthermore, their personal identity and moral image of the world and belief system could have been altered making them significantly more vulnerable, and a target for further radicalisation,[191] and whilst the scale of the threat posed by those yet to return, or held in refugee camps awaiting return, is not yet known it is predicted to be substantial.[192]

As the women who joined ISIS are largely viewed by the UK government, its agencies, and society as being less of a risk to security than the men who joined the group, those who do manage to return (legally or illegally) are likely to pose a threat because they are likely to remain undetected by the security enforcement agencies.[193] Indeed, Brown (2020) agrees with this notion that gendered motivations for women's participation in conflicts, and their underlying grievances especially at the political level are ignored and those in charge of programmes such as *Prevent* and *Channel* are not qualified to interact or advise in relation to gender specific requirements. As such, women are not given the appropriate support which often results in them being a higher risk as they are left unwatched in society.[194] Spalek reinforces Brown's argument that *Prevent* and counter-terrorism policies 'affirm and reinforce Islamophobia and have created a suspect community' which has formed a greater divide in society and left UK Muslims feeling socially, culturally, and personally isolated from society and thus more likely to be radicalised as they search for belonging.[195]

A further challenge of UK deradicalisation programmes is that the judiciary system is unable to prosecute women because there is predominately insufficient evidence they were contributing towards an act of terrorism and therefore the link between their behaviour and criminal activity is tenuous.[196] Women are more likely to be charged with kidnapping, child abuse or child neglect rather than terrorism related charges which means they often do not qualify for deradicalisation support in the same way their male counterparts do.[197] Similarly, many women find that because the practitioners are men, they cannot build a rapport or trust due to cultural boundaries, and their religious beliefs are called into conflict which causes the programme to be unsuccessful, and they stop attending.[198]

For the UK women who have returned from Iraq and Syria and are arrested, prosecuted and imprisoned for terrorist related offences, the prison system can be a breeding ground for

network building or further radicalisation resulting in greater resentment towards the government and society on their return to normal life, and thus an increased security threat.[199] Moreover, UK women who returned were sentenced differently (often more leniently) than men which sends a message to terrorist groups, extremists or radicals that the UK does not treat men and women who participate in terrorist activity equally.[200] This could see young females and women deliberately targeted in future as it could be perceived they can achieve greater success in a terrorist attack because they are less likely to be detected, suspected, or tracked by the Security Services. Cook and Vale argue that almost all women, and children born in the Caliphate, will face social stigma within society, potential rejection from their families and community and have far limited opportunities in society because of their time in the IS which makes them a greater security threat as they are isolated from society, likely to be easily radicalised and more paradoxically a potential motive to strike back at the society they believe has failed them.[201]

Whilst the UK has adopted the approach to strip or deny citizenship for those individuals who travelled to join ISIS who pose a threat, and to leave them in refugee camps in the Middle East, this approach can only be short-term and only temporarily mitigates the risk. It is likely that these individuals' sense of 'non-belonging and unbelonging' [202] will magnify and potentially manifest into a greater threat to UK domestic security in the form of retaliation, resentment or the potential to radicalise others online who might be sympathetic to the cause and prepared to carry out violent acts on the group's behalf.[203] This could potentially generate a longer-term wave of new young females radicalised, and children born to these women, especially as Islamist terrorist groups continue to praise attacks carried out by women that align with their goals, which in turn empowers women to join their ranks.[204]

## Chapter 8
## Conclusion

The rise of ISIS highlights the complexity of radicalisation both in relation to how individuals, groups and mass levels of people can be radicalised by both opinion and action, but it also highlights how motivational factors will differ depending on the societal, cultural, political, and personal status. The theoretical model by McCauley and Moskalenko provides a useful framework to demonstrate how individuals can move from radicalisation of opinion to radicalisation of action, and to understand the importance and power of group radicalisation in the process. ISIS was able to use group radicalisation to recruit greater numbers of UK women to join its caliphate than any other Islamist group before them by reaching and influencing its supporters irrespective of geographical boundaries. They achieved this by using online channels to sell its propaganda narrative, social media forums to recruit, and blogs and videos to enhance the profile, ISIS captivated those in the UK society who felt excluded whether that be personal victimisation, political grievance, disenfranchised with the lack of opportunities, or a rejection of families and cultural norms with relative ease. By portraying a sense of belonging and camaraderie within the ideology, the promise of a utopian Islamic Caliphate appealed to many young women in search for a 'sisterhood' of likeminded Muslim women, and an opportunity to live a life where their religion and societal values were not in conflict.

For these women who joined ISIS, identity crisis theory played a key part in their radicalisation process and was the primary push factor for those travelling in search of self-identity, belonging and unity which was fuelled by ISIS' deliberate targeting online via women only forums and trusted friendship groups to capture those individuals who displayed feelings of isolation both socially and culturally from society, and therefore more vulnerable and susceptible to be radicalised. This paper has highlighted that the push factors for both men and women radicalised by ISIS were similar and broadly shaped by political motivations, ideology, and a sense of unity around religion which led to large numbers making the journey. Equally, that some women like men joined ISIS to carry out acts themselves and therefore the perception by the Western media and governments that all women who joined ISIS were victims, oppressed by Muslim men or mentally unstable fundamentally overlooks the importance of understanding gendered motivations in the radicalisation process. Not only did these narratives deny these women agency, but it also reinforced gender stereotype within UK society that women involved with an extremist group do not pose the same threat to security as their male counterparts.

However, the pull factors were more gendered and for the women who joined ISIS, they were centred on the roles they could undertake in the IS, and the importance placed by al-Bagdadhi on their value to building the Caliphate, and its future. Critically, this provided UK Muslim women with a sense of belonging, purpose and empowerment and an opportunity to be more than just a peripheral element to the ideology. The primary pull factor was the 'sisterhood', a sense of belonging and to live freely as a Muslim by overtly following their religion without victimisation or subject to the Islamophobia which they faced in the UK, and for some a chance to rebel against their family's cultural way of life. These similarities and differences identify why gender should play an important part in future Counterterrorism and Deradicalisation programmes, and that understanding security through a gendered lens is critical to the effectiveness of UK security strategies and policy in the future.

This paper has identified that there is a connection between the UK females radicalised by ISIS and a threat to UK domestic security, and whilst the firm-hand narrative the government has adopted to deal with those returning or wanting to return is understandable as the level of risk is undetermined, adopting an aggressive and resolute stance is unlikely to be the answer. Neither is arresting our way out of the problem leaving citizens in refugee camps or in Iraq and Syria to make their own way home, removing citizenship or detaining in prison as this does not stop the risk to UK security, it only delays the threat. Understanding the motives of those radicalised by ISIS must be at the forefront of future UK deradicalisation and counter-terrorism strategies and policies if the UK Government and the Security Services are to properly assess the threat and then implement mitigation measures in the NSS to appropriately monitor, support and where necessary detain those radicalised by ISIS who pose a threat to domestic security.

ISIS was able to implant a message to potential followers unlike any other Islamist group whilst gaining territory across Iraq and Syria, revenue and income and introduced state-like attributes

in just four years. Their global reach and ability to attract large numbers of Western women was unprecedented and therefore the UK Government and its Security Services need to reevaluate preventative strategies and polices to better understand the link between gender and security and to assess the implications with greater numbers of women within society either radicalised by ISIS or who are susceptible to being radicalised to ensure the 'ISIS Effect' is not relived in the future.

Whilst female radicalisation is not new, the number of UK women who joined ISIS between 2014-2018 was unprecedented, and the ages of those who left voluntarily was also concerning but their movements were not tracked by the Security Services, and PAG, the actual threat they pose is undetermined, and potentially underestimated. Having been exposed to life within an extremist organisation, it is likely these women have been involved in operational and tactical level planning, carried out or supported acts of violence, and most likely been involved in the group's recruitment campaign, therefore the skills they have acquired can be dangerous if not controlled appropriately. Similarly, these women are likely to be susceptible to further radicalisation in future as they are largely undetected by security agencies and displaced within society.

As the exact numbers of women still living in Iraq and Syria or embedded in refugee camps either wanting to return or denied access remains unknown, this factor alone is concerning as it denudes governmental departments assessing threats and establishing mitigation, or preventative measures. Equally, those women who have returned and been processed through the judiciary system or *Prevent* programme have been given very little tailored support to integrate back into society which could result in these individuals being further isolated from society which is a key driver to radicalisation. With so many unknowns, the UK could be potentially at risk in the future from either a lone attack (with or without group instruction), or a more collaborated event as we have already seen in London if these women chose to provide infrastructure, networks, or safe spaces within our communities for the group to launch such attacks.

As the *Prevent* and *Channel* programmes have been designed to tackle extremist radicalisation which is primarily aimed towards violence (radicalisation of action) and therefore overlooks the risks from cognitive radicalisation (radicalisation of opinion), many women often slip through the net, or do not engage with these voluntary programmes as they are not tailored in any way to their specific requirements. Moreover, as the programme practitioners are predominately men, Muslim women struggle to build rapport due to cultural sensitivities and they often drop out of the programmes and are left largely unmonitored. The gendered perception that women are victims of violence rather than perpetrators, and that society does not view the women radicalised by ISIS with the same metrics as the men could mean that new extremist groups, or existing ones, start to actively target and recruit larger numbers to their ranks as they are an untapped resource, with the ability to enhance a groups profile and influence.

As such, this paper has demonstrated that the link between gender and radicalisation needs to be better understood in academia and at the UK governmental level as 'some' UK women radicalised by ISIS can, and do, pose the same threat to domestic security as 'some' of their male counterparts, noting that radicalisation does not always resort to extremist behaviour. Therefore, security preventative measures, the judiciary system and the deradicalisation programmes should not be gender blind if they want to mitigate against any future threats to UK domestic security.

An area for further research is to understand the potential risk that children born within the Caliphate might pose when they reach adulthood to UK domestic security. Whilst there is early academic research by Cook and Vale this is limited due to the vast number of unknowns because the UK government, and its PAG, did not accurately track the gender of those who joined ISIS. Similarly, whilst revision of UK CONTEST strategies is not the intent of this paper, it has demonstrated that *Prevent* and *Channel* need to be redesigned through a gendered lens if they are to be successful in tackling female radicalisation with greater emphasis placed on the role women can play in terrorist groups, and why they should not automatically be discounted as posing a threat to security because of societal gendered perceptions. The actions of the Security Services and the Government in supporting and facilitating the reintegration of ISIS women back into society is critical for them, their community, and potentially future generations if the UK hopes to mitigate against radicalisation in our communities.

## Notes

[1] Arun Kundnani, 'Radicalisation: the journey of a concept,' *Race & Class, Vol. 54*, No. 2 (Oct.-Dec. 2012): 3.
[2] Dr. Katherine Brown, interview with author, Appx 1, Q1.
[3] Dimiter Toshkov, '*Research Design in Political Science*,' (London: Macmillan Education UK, 2016), 24.
[4] James Scotland, 'Exploring the Philosophical Underpinnings of Research.' *English Language Teaching 5*, no. 9 (2012): 9-16.
[5] George Ritzer and Guba, Egon, Paradigm Dialog, '*Canadian Journal of Sociology 16*', no. 4 (1991): 446-448.
[6] Alex P. Schmid, 'Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion & Literature Review.' *ICCT Research Paper* 4.2 (2013): 1.
[7] Ibid.
[8] Kundnani, 'Radicalisation: the journey of a concept'.:3.
[9] Andrew Silke, Katherine Brown and S Jayakumar, *Radicalisation: The Transformation of Modern Understanding of Terrorist Origins, Psychology & Motivation*. (World Scientific, 2016), 1.
[10] Schmid, *Radicalisation, De-Radicalisation, Counter-Radicalisation*. 22.
[11] Mark Sedgwick, 'The Concept of Radicalisation as a Source of Confusion', *Terrorism & Political Violence, Vol. 22*, No. 4 (2010): 480.
[12] John Horgan and Kurt Braddock, 'Rehabilitating the Terrorists? Challenges in Assessing the Effectiveness of Deradicalization programs', *Terrorism & Political Violence*, Vol. 22, No. 2, (2010): 267-291.

[13] Clark McCauley and Sophia Moskalenko, 'Toward a Profile of Lone Wolf Terrorists: What Moves an Individual from Radical Opinion to Radical Action.' Terrorism & Political Violence 26.1 (2014): 69-71.
[14] A Strong Britain in an Age of Uncertainty: The National Security Strategy (2010).
[15] Ibid. 25-33.
[16] National Security Strategy: Strategic Defence & Security Review 2015.
[17] UK CONTEST & Security Act, Nov 2014.
[18] UK CONTEST Strategy (2011). The aim of CONTEST is to reduce the risk to the UK & its interests overseas from terrorism.
[19] Home Office - Prevent Strategy (2011).
[20] Ibid. 'Individuals referred to and supported through the Prevent Programme', April 2017 to March 2018.
[21] Ibid.
[22] Michael Weiss and Hassan, Hassan, *Isis: Inside the Army of Terror* (First Regan Arts Paperback ed. 2015), 1-8.
[23] *Timeline: Rise and Spread of the Islamic State* (2016): Woodrow Wilson International Centre for Scholars.
[24] Weiss and Hassan. 1-8.
[25] Mashail Haydar Ali 'The Language Policy of the Caliphate State.' *Middle Eastern Studies* 57, no. 2 (2020): 391-405.
[26] Devorah Margolin, 'The Changing Roles of Women in Violent Islamist Groups,' *George Washington University Program on Extremism*, (2019).
[27] Ibid.
[28] Ibid.
[29] Daveed Gartenstein-Ross, Nathaniel Barr and Bridget Moreng, 'The Islamic State's Global Propaganda Strategy.' *ICCT Research Paper (Online)* 7.1 (2016): 9.
[30] Mark Singleton, Bibi van Ginkel and Eva Entenmann eds., 'The Foreign Fighters Phenomenon in the European Union: Profiles, Threats & Policies,' International Centre for Counter-Terrorism – The Hague 7, no. 2 (2016).
[31] Kiriloi Ingram, 'IS's Appeal to Western Women: Policy Recommendations.' *ICCT Research Paper (Online)* 8.4 (2017): 4.
[32] Jan Christoffer Andersen and Sveinung Sandberg, 'Islamic State Propaganda: Between Social Movement Framing & Subcultural Provocation.' *Terrorism & Political Violence* 32.7 (2020): 1506-526.
[33] Ibid.
[34] *Handbook of Terrorism & Counterterrorism Post 9/11*, edited by D. M. Jones, et al., Edward Elgar Publishing Limited, 2019:26-38.
[35] Audrey Courty, Halim Rane and Kasun Ubayasiri, 'Blood & Ink: The Relationship between Islamic State Propaganda and Western Media.' *Journal of International Communication* 25.1 (2019): 69-94.
[36] Bruce Hoffman, *Inside Terrorism* (New York: Colombia University Press, 2006).
[37] Chris Galloway, 'Media Jihad: What PR Can Learn in Islamic State's Public Relations

Masterclass.' *Public Relations Review* 42.4 (2016): 582-90.
[38] Ibid. 23
[39] Joana Cook and Gina Vale, 'From Daesh to Diaspora: Tracing the Women & Minors of Islamic State,' *International Centre for Study of Radicalisation* (2018): 7-20.
[40] Jeffry R, Halverson, Lloyd H, Goodall & Steven R. Corman, *Master Narratives of Islamist Extremism*. 1st ed. (New York: Palgrave Macmillan, 2011).
[41] Schmid, 'Radicalisation, De-Radicalisation, Counter-Radicalisation:':89.
[42] Cook and Vale, 9-20.
[43] Anne Speckhard and Molly Ellenberg, 'ISIS in Their Own Words: Recruitment History, Motivations for Joining, Travel, Experiences in ISIS, & Disillusionment over Time,' *Journal of Strategic Security* 13.1 (2020): 82-127.
[44] Randy Borum, 'Radicalization into Violent Extremism II: A Review of Conceptual Models & Empirical Research', Journal of Strategic Security, Vol. 4, No. 4, (2011), 7-62; M. King & D. Taylor, 'The Radicalization of Homegrown Jihadists: A Review of Theoretical Models & Social Psychological Evidence', Terrorism & Political Violence, Vol. 23, No. 4, (2011), 602-622.
[45] McCauley and Moskalenko, 'Mechanisms of Political Radicalization: Pathways Toward Terrorism', Terrorism and Political Violence, Vol.20, No.3 (2008),415-433.
[46] McCauley and Moskalenko, (2008), 418.
[47] McCauley and Moskalenko, Friction: How radicalization happens to them and us. Oxford: Oxford University Press, 2011, 4.
[48] Ibid. 419.
[49] Silke and Brown, 'Radicalisation,': 7.
[50] University of Amsterdam, Empirical Study (revised). SAFIRE: Scientific Approach to Finding Indicators for & Responses to Radicalisation (2013).
[51] Ruth Gan, Loo Seng Neo, Jeffery Chin and Majeed Khader, 'Change Is the Only Constant: The Evolving Role of Women in the ISIS.' *Women & Criminal Justice* 29.4-5 (2019): 214.
[52] McCauley and Moskalenko, 'Mechanisms of Political Radicalization': 422.
[53] Ibid.
[54] Roger Brown, 'Group Polarization,' in *Social Psychology*: The Second Edition (New York: Free Press, 1986).
[55] European Parliamentary Research Service. Radicalisation and counter-radicalisation: A gender perspective.
[56] Anita Peresin and Alberto Cervone, 'The Western Muhajirat of ISIS.' *Studies in Conflict and Terrorism* 38.7 (2015): 495-509.
[57] John Duckitt and Kirstin Fisher, 'The Impact of Social Threat on Worldview & Ideological Attitudes,' Political Psychology 24, no. 1 (2003): 199–222.
[58] Peresin and Cervone, 497.
[59] Imran Awan, 'Cyber-Extremism: ISIS & the Power of Social Media.' *Society* 54.2 (2017): 138-149.
[60] Cook and Vale, 'From Daesh to Diaspora.': 7-12.
[61] Ibid.
[62] Awan. (2017): 138-149.
[63] Ibid. 140.

[64] McCauley and Moskalenko, 'How radicalization happens to them and us,': 268.
[65] Ibid. 270.
[66] Peresin and Cervone, 'The Western Muhajirat of ISIS.' 498.
[67] Edwin Bakker and Seran De Leede, 'European Female Jihadists in Syria: Exploring an Under-Researched Topic.' *ICCT Research Paper* 6.2 (2015): 1-13.
[68] Peresin and Cervone: 499.
[69] Ibid.
[70] Carolyn Hoyle, Alexandra Bradford and Ross Frenett. 'Becoming Mulan?' Institute for Strategic Dialogue (2015): 8.
[71] Yılmaz Zehra. (2017). Critique of ISIS' women policy. *Turkish Journal of Middle Eastern Studies, 4*, 2. (2017): 29.
[72] Amanda Spencer, 'The Hidden Face of Terrorism: An Analysis of the Women in Islamic State.' *Journal of Strategic Security* 9.3 (2016): 74-98.
[73] Peresin & Cervone, 'The Western Muhajirat of ISIS': 509.
[74] Spencer. 78.
[75] Hoyle et al, 'Becoming Mulan?': 13.
[76] Gan et al, 'Change Is the Only Constant.': 209-212.
[77] Ibid, 209.
[78] Ibid. 211.
[79] Amanda Spencer, 'Behind the veils: The forgotten women of ISIS.' (Orchard Research Group, 2017).
[80] Joana.Cook, *A Woman's Place: US Counterterrorism since 9/11*. (Oxford Scholarship Online, 2020).
[81] Schmid, 'Radicalisation, De-Radicalisation, Counter-Radicalisation.':1-91.
[82] Seth J. Schwartz, Curtis S. Dunkel and Alan S Waterman, 'Terrorism: An Identity Theory Perspective.' *Studies in Conflict & Terrorism* 32.6 (2009): 540.
[83] Erin et al, '*Till Martyrdom Do Us Part*'. 11.
[84] Hamid Sadek. 'The Attraction of "Authentic Islam": Salafism & British Muslim Youth,' in Roel Meijer (ed.), Global Salafism: Islam's New Religious Movement (New York: Columbia University Press, 2009), 384-403.
[85] Mirella L. Stroink, 'Processes and Preconditions Underlying Terrorism in Second-Generation Immigrants,' Peace & Conflict: Journal of Peace Psychology 13:3 (2007): 293-312.
[86] Catarina Kinnvall, 'Globalization and Religious Nationalism: Self, Identity, and the Search for Ontological Security' Political Psychology 25:5 (2004): 742.
[87] Sara Savage Hampson and Jose Liht Boyd-Macmillan. 'Turning the Telescope Round: Reciprocity in Psychology-Theology Dialogue.' *Archive for the Psychology of Religion* 30.1 (2008): 8.
[88] Joana Cook and Gina Vale. 'From Daesh to "Diaspora"II: The Challenges Posed by Women & Minors After the Fall of the Caliphate', *CTC Sentinel*. (2019).
[89] Kim Cragin and Sara Daly, A. *Women as Terrorists Mothers, Recruiters, and Martyrs*. Westport, Conn.: Praeger Security International, 2009.
[90] Marie Erin, Melanie Saltman-Smith and Lawrence Freedman. Institute for Strategic Dialogue,

and International Centre for the Study of Radicalisation Political Violence. '*Till Martyrdom Do Us Part*': *Gender and the ISIS Phenomenon*. 2015: 8.
[91] Ibid. 9-12.
[92] Bakker and de Leede. 'European Female Jihadists in Syria.': 5.
[93] Susanne Schröter, 'Between romance & Kalashnikovs – the women of "Islamic State"', 11 February 2015, Deutsche Welle.
[94] Hoyle el al. 'Becoming Mulan?':12.
[95] Matenia Sirseloudi, 'The Meaning of Religion & Identity for the Violent Radicalisation of the Turkish Diaspora in Germany,' Terrorism and Political Violence 24:5 (November 15, 2012):813-14.
[96] Munira Mirza, Senthilkumaran, Abi, Ja'far, Zein, and Policy Exchange. *Living Apart Together: British Muslims & the Paradox of Multiculturalism*. London: Policy Exchange, 2007.
[97] Savage Hampson and Liht Boyd-Macmillan. 75-113.
[98] Tahir Abbas. *Islamic Radicalism & Multicultural Politics: The British Experience*. Taylor & Francis, 2011.
[99] Oliver Roy. 'FT.com Site: Radical Islam Appeals to the Rootless.' FT.com, 2004: 1-4.
[100] Ibid.2.
[101] Quintan Wiktorowicz. *Radical Islam Rising*. (Lanham: Rowman & Littlefield Publishers, 2009), 20-24.
[102] Erin et al. '*Till Martyrdom Do Us Part*': 8-10.
[103] Ibid.
[104] Cook and Vale, 'From Daesh to 'Diaspora.': 7-9.
[105] Ibid. 12-14.
[106] Ibid. 66-68.
[107] Cook and Vale. 'From Daesh to Diaspora,':20.
[108] Ibid. 22
[109] Nelly Lahoud, 'Empowerment or Subjugation: An analysis of ISIL's gendered messaging' UN Women, June 2018.
[110] Cook and Vale. 24.
[111] Harriet Sherwood, Sandra Laville and Kim Willsher *in Paris*, Ben Knight *in Berlin*, Maddy French, 'Schoolgirl Jihadis: the Female Islamists Leaving Home to Join ISIS", *The Guardian, September 29 2014*.
[112] Laura Sjoberg and Caron E. Gentry *Beyond Mothers, Monsters, Whores: Thinking about Women's Violence in Global Politics*. London: Zed Books (2015).
[113] Ibid.
[114] Brown. Interview, Appx 1, Q2.
[115] Erin et al. '*Till Martyrdom Do Us Part*'. 14-15.
[116] Hoyle et al. 'Becoming Mulan?': 12-18.
[117] Erin et all. 16.
[118] Bakker and de Leede. 'European Female Jihadists in Syria.': 7.
[119] Schröter, 'Between romance & Kalashnikovs.'
[120] Ingram, 'IS's Appeal to Western Women.': 1-13.
[121] Ibid.

[122] Brown, '*Gender and Countering Islamic State Radicalisation*'. E-International Relations (2016): 1-4.
[123] K Brown and J.Cook, Interview with authors, Appx 1 and 2.
[124] Laura Sjoberg, Grade D. Cooke and Stacy Reiter Neal. 'Introduction: WOMEN, GENDER, AND TERRORISM.' *Women, Gender, and Terrorism*. Athens; London: U of Georgia, 2011,6.
[125] Srobana Bhattacharya, 'Gender, Insurgency, and Terrorism: Introduction to the Special Issue.' *Small Wars & Insurgencies* 30, no. 6-7 (2019): 1077-088.
[126] Marc Sageman, *Leaderless Jihad Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2011, 81-82.
[127] Emily Winterbotham and Elizabeth Pearson, 'Different Cities, Shared Stories: A Five-Country Study Challenging Assumptions Around Muslim Women & CVE Interventions.' *The RUSI Journal* 161, no. 5 (2016): 61-63.
[128] Winterbotham and Pearson. 62.
[129] Alice Martini, 'Making Women Terrorists into "Jihadi Brides": An Analysis of Media Narratives on Women Joining ISIS.' *Critical Studies on Terrorism* 11, no. 3 (2018): 469.
[130] Ibid.
[131] Mereidth Loken and Anna Zelenz, 'Explaining Extremism: Western Women in Daesh.' *European Journal of International Security* 3, no. 1 (2018): 47.
[132] Brown and Cook. Interviews with authors, Appx 1 and 2.
[133] Ibid.
[134] Cook, Interview, Appx 2, Q3.
[135] Richard Jackson, *Writing the War on Terrorism: Language, Politics & Counterterrorism*. New Approaches to Conflict Analysis. Manchester: Manchester University Press, 2005.
[136] Laura Sjoberg, 'The Women of ISIS: Gender and Political Violence', Political Violence at a Glance, 28 August 2017.
[137] United Nations Security Council, Resolution 1325 (2000).
[138] Sofia Patel and Jacqueline Westermann, 'Women and Islamic-State Terrorism: An Assessment of How Gender Perspectives Are Integrated in Countering Violent Extremism Policy & Practices.' *Security Challenges* 14, no. 2 (2018): 54.
[139] Katherine Brown, 'Gender & Countering Islamic State Radicalisation',18 February 2016.
[140] Zehar Yılmaz, İsmail Numan Telci and Kemal İnat, 'Critique of ISIS' Women Policy.' *Türkiye Ortadoğu Çalışmaları Dergisi* 4, no. 2 (2017): 13-40.
[141] Ibid. 36.
[142] Gan et al. 'Change Is the Only Constant': 204-20.
[143] Nabeelah Jaffer. 'The Secret World of Isis Brides: U Dnt Hav 2 Pay 4 ANYTHING If U R Wife of a Martyr'; What Draws Western Women to Islamic State's Violent Jihad? *The Guardian (London, England)*, 2015.
[144] Gan et al. 211.
[145] Ingram, 'IS's Appeal to Western Women.': 19.
[146] Mia Bloom, 'Bombshells: Women & Terror.' *Gender Issues* 28, no. 1 (2011): 11.
[147] Peresin and Cervone, 'The Western Muhajirat of ISIS.': 502.
[148] Simon Cotte, 'What ISIS Women Want,' *Foreign Policy*, 17 May 2016.

[149] Cook. Interview, Appx 2.
[150] Katherine Brown, 'Utopian Vision in Jihadi Gender Politics'. *Durnstein Symposium*, Austria 2015.
[151] Loken & Zelenz, 'Explaining Extremism: Western Women in Daesh,': 59.
[152] Spencer, 'Behind the veils,': 80-88.
[153] Cook. Interview, Appx 2, Q2.
[154] Pearson and Winterbotham. 'Different Cities, Shared Stories.': 60-80.
[155] Ibid.
[156] Ibid.
[157] Ibid.
[158] Fraihi Hind, 'The Future of Feminism by ISIS Is in the Lap of Women.' *International Annals of Criminology* 56, no. 1-2 (2018): 23-31.
[159] Brown, Interview, Appx 1, Q3.
[160] Hind. 30.
[161] Alexandra Topping and Aisha Gani. School reaction to 'Syria-bound' schoolgirls: 'It doesn't make sense.' The Guardian. (23 February 2015).
[162] Emily Pearson, The case of Roshonara Choudhry: Implications for theory on online radicalization, ISIS women, and the gendered jihad. Policy & internet, 8(1), (2015): 5–33.
[163] Brown, Interview, Appx 1, Q3.
[164] Ibid.
[165] Pearson and Winterbotham, 'Women, Gender & Daesh Radicalisation,' *The RUSI Journal*, Vol. 162.2, 2017, 65.
[166] Peresin and Cervone, 'The Western Muhajirat of ISIS': 500 – 502.
[167] Patel and Westermann, 'Women and Islamic-State Terrorism.':55.
[168] Brown, *Gender, Religion, Extremism*. Oxford Studies in Gender & International Relations. 2020, 12.
[169] European Commission - RAN EXIT Gender-specific approaches in exit work, 22-23 October 2019.
[170] Anne Jacobs, 'The Evolution of Women in The Islamic State,' Washington institute for Near East Policy, 26 September 2016.
[171] Pearson and Winterbotham, 'Different Cities, Shared Stories.':65.
[172] Cook, Interview, Appx 2, Q4.
[173] Ibid.
[174] Brown, Interview, Appx 1, Q4.
[175] Cook, Interview, Appx 2, Q4.
[176] Pearson and Winterbotham, 60.
[177] Katherine Brown, *Gender, Religion, Extremism*. 42.
[178] Brown and Cook, Interview, Appx 1&2.
[179] Rachel Briggs and Tanya Silverman, Western Foreign Fighters Innovations in Responding to the Threat' *Institute for Strategic Dialogue* 2014: 37.
[180] Raffaello Pantucci & Clare Elis, 'The Threat of ISIS to the UK', *Rusi Threat Assessment*, October 2018.

[181] Mod.Gov.UK. MOD Regional Threat Outlook: Daesh, Iraq & Syria, 16 December 2020.
[182] Ibid.
[183] Ibid.
[184] Kerstin Braun, '"Home, Sweet Home": Managing Returning Foreign Terrorist Fighters in Germany, The United Kingdom & Australia.' *International Community Law Review* 20, no. 3-4 (2018): 311-46.
[185] Thomas Hegghammer, 'Should I Stay, or Should I Go? Explaining Variation in Western Jihadists' Choice between Domestic and Foreign Fighting. (Report) (Author Abstract).' *American Political Science Review* 107, no. 1 (2013): 1.
[186] Bruan. 321.
[187] UNSC - CTED Trends Report – Gender Dimensions of the Response to Returning Foreign Terrorist Fighters. 8.
[188] Helen Fenwick, 'Responding to the ISIS Threat: Extending Coercive Non-trial-based Measures in the Counterterrorism & Security Act 2015.' *International Review of Law, Computers & Technology* 30, no. 3 (2016): 175.
[189] Institute on Statelessness & Inclusion (2020). Citizenship striping as a security measure. *World Statelessness Report 2020*.
[190] Ibid.
[191] Briggs and Silverman, 'Western Foreign Fighters Innovations in Responding to the Threat.': 39.
[192] Ibid.
[193] Mia Bloom, 'Death Becomes Her: The Changing Nature of Women's Role in Terror. (Conflict & Security).' *Georgetown Journal of International Affairs* 11, no. 1 (2010): 95.
[194] Brown, Interview (2021).
[195] Basia Spalek, 'Radicalisation, De-radicalisation & Counter-radicalisation in Relation to Families: Key Challenges for Research, Policy & Practice.' *Security Journal* 29, no. 1 (2016): 39-52.
[196] Organization for Security and Co-operation in Europe (OSCE). (2019). OSCE Secretariat. Vienna: Organization for Security and Co-operation in Europe.
[197] Spalek, 40.
[198] Schmid, 'Radicalisation, De-Radicalisation, Counter-Radicalisation:':90.
[199] Ibid.
[200] Brown, Interview, Appx 1, Q4.
[201] Cook and Vale, 'From Daesh to Diaspora' II. 2019.
[202] Briggs and Silverman, 'Western Foreign Fighters Innovations in Responding to the Threat.': 45-49.
[203] Ibid.
[204] Ibid.

## Appendix 1

### Elite Interview conduct on Wednesday 3rd March 2021 with Dr. Katherine Brown, Senior Lecturer in Islamic Studies University of Birmingham.

This appendix (appx) is a summative overview of the answers to the four questions posed ahead of the interview which was recorded on Teams. Whilst I do not have permission to share the entire script, the author has given authority for me to summarise the key points from the interview. In addition, some of the author's professional opinions discussed during this interview have been used as primary evidence in the Research paper and these have been footnoted accordingly.

### Q1. What role, if any, has gender in the radicalisation of British women supporting ISIS?

Dr. Brown stressed that the general perception, not just in the UK, but in academic literature, at the political level and within the security domain is the assumption that women are largely insignificant in terms of the radicalisation process as the numbers involved with terrorist groups is small in comparison to men. Therefore, why would governmental strategies, funding and deradicalisation programmes be shaped around the minority. Further, that UK deradicalisation programmes have been designed to tackle Counterterrorism with the primary objective to maintain physical security in society and preventing harm to citizens. Dr. Brown stated that even though there has been a shift since 9/11 towards tackling radicalisation in the UK, the focus has remained on understanding how people (predominately men) behave and think which is designed to prevent them undertaking physical acts of violence. In the past, most attacks have been carried out by men which has led to the perception that women are less violent or likely to be a security risk; women have carried out a small number of physical acts, but they remain an outlier.

### Q2. If there is a potential link, what part do you think gender perception and stereotypes within UK society plays in how men and women were radicalised by ISIS. Do you think there are similarities and differences?

Dr. Brown stated that until the emergence of ISIS, British women were largely not carrying out acts of violence and therefore they remained unnoticed – Dr. Brown used the example that you do not notice that most of the world leaders are predominately men until you see women in the photo. ISIS has shone a light on the importance of understanding gender in the radicalisation process, and only when the UK Government started to see its female citizens engage with ISIS' ideology and voluntarily willing to travel in support of an extremist terrorist organisation did the narrative start to migrate towards understanding 'why and how' women were radicalised - but this is still very limited. Dr. Brown states that UK domestic security polices, programmes and strategies are gender blind. Therefore, British policy has been shaped around preventing men from carrying out acts of violence, rather than focusing on radicalisation and the part gender plays in this process.

Lengthy discussion took place on the role of the UK society and the importance of the ideological component and what ISIS offered to young females. Dr. Brown stated that the

prospect of living in a Muslim state and being part of this new pure-State, which valued religion and Muslim culture was for many a key driving factor for why younger females migrated. She stated that many felt oppressed and restricted in the West due to the Islamophobia they faced daily, and due to societal perceptions about all Muslims. In addition, Dr. Brown stated that some young women made the journey in the fight for jihad but that this concept has been overlooked almost entirely by the UK government, and the Security Services.

### Q3. What was the role of British society, if it did have one, in driving Islamist radicalisation, and what were the primary factors that lead women leaving to join ISIS?

The focus during the meeting was on the role the UK media played, and at the governmental level which shaped the narrative that UK females who joined ISIS were motivated by romance and were simply termed as 'Jihadi Brides.' This oversimplified term, Dr Brown argues removes agency from their decisions and somehow makes them less of a risk to security. Dr. Brown stated that the general Western perception is that women should 'not be doing it anyway' and therefore by using the narrative that they were coerced or lured reinforces the UK societal and cultural perception that women are forced into violence by men; violent behaviour is accepted of men, but not of women. Dr. Brown agreed that there were similarities and differences that motivated men and women to join ISIS which are covered in the paper.

Dr. Brown introduced the Shamima Begum case as an example of how women who participated are framed as needing psychological help, and that their motivating factors are medicalised unlike their male counterparts where its culturally and societally accepted that some men will fight for a cause. Dr. Brown stated that this perception has also shaped our national security policies as women are viewed as less of a risk to the society as they are deemed unlikely to fight or carry out acts of violence.

### Q4. What do you foresee are the primary security implications of potential amounts of increased British females radicalised by ISIS, especially those that do return?

Dr. Brown discusses at length the UK CONTEST programmes and stated that Prevent and Channel have been designed mostly by men, and that these interventions are delivered predominately by male practitioners which not only overlooks gendered factors in the radicalisation process but results in women not fully engaging or they are dropping out as it does not meet their needs. She uses the term 'designed by men for men' – and stated that the deradicalisation and Counterterrorism strategies, programmes and governmental policies are largely unsuccessful in supporting women involved in terrorist organisation as they do not consider the gendered aspect – they are 'gender blind.' Further, Dr Brown stated that the UK judiciary system is not equipped to deal with women who support a terrorist group as often the offences they are charged with are reduced to child abuse/neglect or linked to terrorist related offensives but only as a supporter or an affiliate. Due to gender perceptions and stereotypes of a woman's role in a terrorist organisation, Dr. Brown states that the UK women radicalised by ISIS are not given the appropriate support, scrutiny, or risk assessment

in the same way as their male counterparts, as the role is normally viewed as peripheral or supportive – victims rather than perpetrators.

Dr. Brown's opinion was that the women who lived in the Islamic State are likely to have been trained in defensive measures, and there is evidence of them wearing suicide vests and bearing arms. Similarly, that they had training in field triage and involved in the planning of operations which does give them some battle skills. However, Dr. Brown stated that these extra skills or their affiliation to ISIS does not necessarily make them a security threat by association, but she did agree that the level of threat posed by women who joined ISIS is undetermined, especially for younger women who travelled alone as it is reasonable to expect they made the decision based on the facts available online, in the media and globally; these women were aware that ISIS were a violent extremist group and yet they still decided to participate. Dr. Brown stated that these motives are likely to mirror that of the men who travelled and therefore they could potentially pose a similar, if not the same, threat to domestic security.

## Appendix 2

### Elite Interview conducted on Friday 26th February 2021 with Dr. Joana Cook, Assistant Professor Terrorism and Political Violence, Faculty of Governance and Global Affairs, Leiden University.

This appendix (appx) is a summative overview of the answers to the four questions posed ahead of the interview which was recorded on Teams. Whilst I do not have permission to share the entire script, the author has given authority for me to summarise the key points from the interview. In addition, some of the author's professional opinions discussed during this interview have been used as primary evidence in the Research paper and these have been footnoted accordingly.

### Q1. What role, if any, has gender in the radicalisation of British women supporting ISIS?

Dr. Cook stated that in her book, *A Woman's Place*, and in her recent current research *Daesh to Diaspora* with Gina Vale she looks at the role gender plays in the radicalisation process. She stated that if you look at the question through the counterterrorism lens, and across the full spectrum which includes everything from preventative to direct engagement, disengagement, rehabilitation, and reintegration, and you consider each of these different groups, gender has a role to play in every aspect. Dr. Cook stated that gender influences the trajectory of radicalisation and is present throughout an individual's entire journey. Specifically, gender plays an essential part in how an individual accesses radical ideology, what roles are on offer within a group, how that role will be present in the organisation, and how the organisation has evolved; these factors are all shaped by gender stereotypes within societies and what attracts an individual to a particular terrorist group will be shaped by gendered cultural, societal, and personal beliefs. Dr. Cook highlighted that gender plays a part in how individuals are targeted, and in the case of ISIS, the propaganda campaigns and online recruiting was extremely gender focused. Dr. Cook stated that this gendered targeting in ISIS' Manifesto, during their recruitment campaigns, how it was portrayed online by its followers

and from the direct call from its leader all empowered Western women, including those from the UK, to travel on a scale not seen by any other Islamist Terrorist group in history. Dr. Cook stated that the gender lens offers insight into the lived experience, allows us to understand factors or pathways into radicalisation and what accelerator radicalisation is – what are the motivating factors that cause men and women to be radicalised.

### Q2. If there is a potential link, what part do you think gender perception and stereotypes within UK society plays in how men and women were radicalised by ISIS. Do you think there are similarities and differences?

Dr. Cook focuses on a chapter in her recent book and explains how Muslim women in the UK tend to face Islamophobic attacks, particularly women who wear religious symbols. She explains that a division in society whereby these women are feeling excluded, rejected, or increasingly targeted based on gender, compounds their feelings of cultural, societal, and personal separation from the society and communities where they live. These factors are key drivers for radicalisation as evidence suggests these individuals are likely to seek like-minded groups as part of self-identity, and to find a sense of belonging. Dr. Cook raises a key point that gender stereotypes and roles within communities shape the way in which individuals exist, behave and who they form networks with.

Dr. Cook touched on her recent research *Daesh to Diaspora* to explain that in almost all cases that she looked at, the motivations for radicalisation have been multifaceted, but the ideology and the opportunity to live in a Caliphate was a key factor for women. The opportunity to live in a kind of hegemonic organisational structure and ideology where very idealised gender roles is supported and facilitated appealed to many young women. In addition, that ISIS offered UK women the opportunity to live in a State which valued their belief system and rejected the femininity movement growing in the UK. Therefore Dr. Cook argues that the UK societal perceptions on roles of men and women, with males being leaders and fighters, and women being private, inward facing, and supportive was exploited by ISIS as a key recruitment tactic and pull factor as they projected a utopian Muslim State were the traditional roles of men and women were firmly accepted and encouraged in their ideology.

### Q3. What was the role of British society, if it had did have one, in driving Islamist radicalisation, and what were the primary factors that lead women leaving to join ISIS?

We discussed the impact of recent conflicts in the Middle East, the history of terrorist activity from the IRA and more recent terrorist attacks in London and how they have influenced British perception that Muslim men are terrorists, and that women are oppressed by men, and the general view that they are forced to wear the hijab etc reinforces the notion that they are weak, brain-washed, and vulnerable. Dr. Cook stated that for many UK young females, the feelings of isolation, disenfranchisement, and lack of opportunity within the society, along with day-to-day verbal and in some cases physical attacks were both push and pull factors in each individualised radicalisation journey. Similarly, that the Shamima Begum case demonstrates how the public view Muslims in UK society, as even though she is British

born and bred the debate around her citizenship was fuelled by the media coverage that she did not deserve this status, and society largely supported this notion. Dr. Cook states that the UK society, and Media platforms and UK Government all played a key role in the radicalisation process for many UK females who felt that the British state did not care about them, or their identity which for many just validated their feelings of isolation from the society and reaffirmed their decision to leave. ISIS was able to give these women a sense of empowerment to choose the life they want to live, and for some to rebel against society or fight back.

### Q4. What do you foresee are the primary security implications of potential amounts of increased British females radicalised by ISIS, especially those that do return?

Dr. Cook stated that around 900 UK individuals travelled to the Islamic State (but this number could be higher) and that the gender was not accurately tracked. In addition, Dr. Cook stated that unlike European countries, the UK was the only country that has not actually differentiated the women who have returned, but that they have for the men. She stated a few questions, How many women remain in camps in northeast Syria? How many are confirmed dead? How many have drifted off to other parts of Iraq and Syria? We discussed these questions but the answer to all three question is the statistics are not accurate and the number remains unknown. However, Dr. Cook did state that of the women who have returned, no attacks have yet been conducted but that does not mean they should not be viewed as potential threats and treated as such. Dr. Cook stated that many of these women have been trained by ISIS to use guns, accustomed to battle tactics, supported the network, facilitated attacks, part of the State building process and indoctrinated children to the ideology's cause and therefore they do have the potential to pose a threat to UK domestic security, and must be given the appropriate attention. She did stress that the judiciary system is not the only mechanism to support these women but that the social services, and other government departments must be involved if the threat is to be appropriately mitigated.

Dr. Cook stated that the biggest areas of concern for the UK is the deradicalisation programmes and disengagement programmes which do not factor gender in their design, delivery, or measures of success. She stressed that there must be a strong gendered lens when creating programmes or approaches to manage these individuals as they return, and that they must be gender sensitive. Lastly, Dr. Cook stated that the UK judiciary system is often more lenient on women involved in terrorist groups, and many are not brought to justice for their actions which does have consequences as they are not offered deradicalisation or reintegration support, therefore potentially making them a greater threat.

Article

# Evaluate the Potential Effectiveness of Air Power in Sub-threshold and 'Grey Zone' Operations

By Wing Commander Clare Mummery

**Biography:** Wing Commander Clare Mummery joined the Royal Air Force in 2008 as an Aerosystems Engineer. She's since carried out tours on and in support of multiple aircraft types, including fast jets, transport aircraft and support helicopters, with two deployments on Operation Herrick in Afghanistan. Following OF3 Command, as XO Air Wing Engineering at RAF Brize Norton, she was promoted to Wing Commander in 2021 and attended the Advanced Command and Staff Course, during which she wrote the following Defence Research Paper.

**Abstract:** Conflict in the grey zone has ever been part of geo-political rivalry, but despite this, hasn't until recently been given adequate consideration. This paper expands the narrative on the effective use of air power in the grey zone through a literature review and two cases studies of Iran and Japan. At the strategic level it concludes there is an important role for air power in the grey zone, both in support of deterrence by punishment and deterrence by denial strategies. However, the nature of grey zone conflict leads to several fundamental requirements for effective use of air power. Namely strategic patience, a finely tuned risk calculus and integration within a holistic cost imposing strategy.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

## Section 1
## Introduction

In a 2019 RAND study, notable political scientists stated:

> The United States is entering a period of intensifying strategic competition with several rivals, most notably Russia and China. U.S. officials expect this competition to be played out primarily below the threshold of armed conflict, in what is sometimes termed the gray zone between peace and war.[1]

As identified within the statement, sub-threshold and 'grey zone' operations are one and the same. They are operations which intentionally 'remain below thresholds that would generate powerful… response, but nonetheless are forceful and deliberate, calculated to gain measurable traction over time.'[2] The central aims of grey zone strategies are often the same, with revisionist powers seeking to undermine the international order and gain greater control over spheres of influence.[3] However core features of this competition vary between aggressors.

> 'Russian gray zone campaigns in Europe...consist primarily of disinformation campaigns meant to undermine political institutions. Other Russian gray zone tactics include the use of economic tools to extract concessions or hold countries at risk of being coerced through an over-reliance on Russian energy; the demonstration of military threats through exercises near the borders of certain states; and...the infiltration of Russian security forces to exert de facto control over disputed territory.'[4]

While Chinese grey zone tactics focus on deterrence or denial of resources through use of law enforcement and maritime militia, and expansion and militarisation of artificial islands to further tilt the regional balance in China's favour. In addition, to support these tactics, China employs broad economic coercion and political subversion including diplomatic pressure, legal warfare, disinformation campaigns and cyberattacks.[5, 6]

As argued by Michael Eisenstadt, the rise of actors who see conflict as a continuum, while the West has been constrained by binary thinking of peace or 'all-out' war, has allowed space and opportunity for actors such as China and Russia to exploit the grey zone.[7] This was highlighted by the UK Secretary of State for Defence, Ben Wallace, in 2020 when he said 'Our values and interests are being challenged in the grey zone all over the world.'[8] Western nations and defence communities are now waking up to the realisation they are inadequately prepared to counter grey zone conflict. As stated by Morris et al, '[The] United Stated and its allies…have yet to come to terms with the challenge of the [grey zone] threat, let alone fashion a strategy to neutralize or roll it back.'[9]

This dawning realisation has led to an increased narrative and analysis of grey zone conflict. However, this been predominantly focused on non-military tactics including Russia's cyber and disinformation campaigns, and China's fait accomplis and 'whole-force' use of fishermen

and the Coast Guard to deter and deny access to resources.[10] Less focus has been given to the use of conventional military forces in the grey zone and particularly on the use of air power. With China's increasing use of air power in the South China Sea, as evidenced by the recent deployment of 16 aircraft from the People's Liberation Army Air Force (PLAAF) near Malaysian airspace, there is increasing debate over whether this is a new tactic for China to assert its claims.[11] In addition, increasing PLAAF incursions into Japanese and Taiwanese Air Defence Identification Zone,[12] and expansion in the use of drones in grey zone conflict by Russia, China and Iran,[13] highlights the relevance of further study. This paper aims to provide greater thinking and expand the narrative on the utility of air power in the grey zone, both as an offensive grey zone component and as an effective strategic countermeasure.

The core thesis of this paper is that air power has significant utility across a range of grey zone operations, due to its ability to effectively support both a strategy of deterrence by punishment and deterrence by denial. However, effective application relies on a number of key factors. Firstly, a need for strategic patience and recognition that gains will be gradual over extended timeframes, likely appearing more as a maintenance of the status quo. Secondly, that the risk of escalation from the use of military force, combined with the need to signal commitment and intent, requires a finely tuned risk calculus. However, the non-binary nature of the grey zone supports nuanced, incremental objectives and a greater risk tolerance than the West currently employ in the grey zone. Thirdly that, as grey zone aggressors have adopted highly sophisticated, holistic grey zone strategies where many elements cannot be targeted by air power, successful strategies to counter grey zone aggression must rely on an equally comprehensive approach. However, these strategies must retain a focus on legitimacy and proportionality to support the objective of undermining the reputation and support for grey zone aggressors.

To explore this thesis, the paper will first undertake a literature review of the debate on the use of military force in the grey zone, identifying three key themes for the effective use of air power. It will then move on to two case study reviews structured around those three key themes. The first case study of Iran will focus on the effectiveness of an offensive use of air power as part of a strategy of deterrence by punishment. The second Japan case study focusses on the effectiveness of air power as part of strategy of deterrence by denial, to prevent fait accompli. These case studies will allow conclusions to be drawn on the effective use of air power across both strategies, providing insight in to how the West can better integrate air power into an effective grey zone strategy.

## Section 2
## Literature Review

The title of this paper potentially covers a very wide scope, with the grey zone spanning political, diplomatic, informational, social, economic and military activity, often synchronised and integrated.[14] To gain sufficient focus on the effective use of air power in the grey zone, this review does not outline the debate on the origins of the grey zone concept, nor does it focus

on the debate around its characteristics or definition. For insight into these areas, works such as Michael Mazarr's *Mastering the Gray Zone*,[15] Javier Jordan's article 'International Competition Below the Threshold of War'[16] or Jahara Matisek's *Shades of Gray Deterrence*[17] offer comprehensive insight. Instead, this review focusses on scholarship on the effectiveness of military force in the grey zone. It has been elected to keep the literature review at the level of military effectiveness, rather than contracting further to air power only, to avoid a loss of sufficient breadth and number of texts for review and to avoid an overly tactical analysis. In undertaking this review, three themes on the effective use of military force in grey zone operations have been identified. Namely short- termism and the idea of victory, elevated risk and risk tolerance, and holistic cost-imposing strategies. These three key themes will provide the framework for the rest of the paper.

## Short-termism and the idea of victory

The first theme for review is political or policy maker short-termism prejudicing the effectiveness of grey zone strategies. This can be compounded by a failure to recognise the different nature of victory in the grey zone, contributing to difficulty in measuring attainment of objectives and frustration from perceived or real lack of progress. Mazarr and Jordan highlight the challenge that persistent and gradual grey zone activity poses to effective Western military response.[18] Grey zone activities occur in the order of decades, or as described in the US National Defense Strategy, in an enduring competition continuum.[19] But Western militaries, in particular, are reliant on the approval of politicians, with a focus on the immediate and short-term, dictated by election calendars to the detriment of support for long-term commitments.[20] Mazarr also describes how grey zone campaigns are likely to play out: 'generating occasionally clear advances, frequent reversals, and no final objective outcomes.'[21] Further highlighting the challenge this will pose for Western states 'more comfortable with simple, traditional conflicts with well-defined objectives, a defined time frame, and a clear winner.'[22] Votel et al outline the notion of winning, stating 'a gray zone "win"' is not a win in the classical sense. Winning is perhaps better described as maintaining the US Government's positional advantage, namely the ability to influence partners, populations, and threats towards achievement of our regional or strategic objectives.'[23] Matisek goes further suggesting grey zone conflicts are a 'catch-22', stating 'Trying to robustly "win" in the near term against gray zone actors is not only infeasible but also undermines prospects of "winning" the conflict over the long-term…[but] Playing the long game is equally frustrating for domestic audiences (and politicians).'[24]

This review has highlighted strong consensus on the extended and flexible timeframe associated with a grey zone win, which is characterised by incremental gains that look more like a maintenance of the status-quo rather than a notable victory. There is also consensus on the challenge this poses to Western militaries in particular. For military effectiveness, politicians, supporting departments, partners and allies will need to exercise strategic patience to avoid miscalculation and counter-productive heavy handedness when competing priorities apply pressure to grey zone strategies.

## Elevated Risk and Risk Tolerance

The second theme in the literature review is elevated risk and risk tolerance in military grey zone strategies, fundamental to the debate over what extent the military should be engaged in grey zone activity. There is a view that, of the levers of power that can be wielded in the grey zone, military ones have the greatest risk of miscalculation and escalation, and of being counterproductive.[25] Mazarr argues that grey zone strategies increase risk of conflict by their ambiguous nature and risk taking. That their very success depends on remaining below key thresholds, but as these thresholds are rarely clearly articulated, there is an increased risk of inadvertent war if key thresholds are crossed and are of unexpected vital interest.[26] Jordan outlines the direct, limited and sporadic use of force as the highest level of escalation in a grey zone conflict and often a pre-war situation.[27]

In addition to the elevated risk of military activity in the grey zone, theorists also argue that the use of military force in the grey zone can be counterproductive. Matisek outlines how the ambiguity of grey zone activity blurs the lines of sovereignty and law, leading to issues with legality of military response.[28] Mazarr also highlights how use of military force in such situations can undermine legitimacy, cause backlash over perceptions of heavy-handedness if pursued too aggressively and support the aims of the aggressor.[29] As Johnson argues with reference to actors such as Russia, those who 'subvert international norms and use force, forfeits… international status and the protection of peacetime norms.'[30] So the same applies to the US and allies in the use of military force in the grey zone. Matisek expands on this by stating 'This normative expectation [from US hegemony] undercuts the United States ability to engage in gray zone activities, as it is much easier for various actors to highlight some United States actions as hypocritical…to Western values.'[31]

## Risk Tolerance

This selection of views offers some academic consensus that the use of military force in the grey zone comes with greater risk of miscalculation, escalation and counter-productivity. However, the avoidance of its use may signal limited interest. As stated by Bothwell, 'signalling is necessary to communicate specific red lines over vital interests through credible commitments, such as sunk costs.'[32] Takahashi goes further, claiming there is an inherent need to 'develop a robust posture to win the possible war in the case of escalation, and to make the challengers recognise the possibility of unfavourable military conflict.'[33] Taken together, this implies that the use of military force may not always be appropriate and requires careful consideration in its application, but failure to integrate its use as part of a strategy of deterrence may be seen as an indication of limited commitment and encourage further aggression.

Noting these arguments of miscalculation, escalation and counter-productivity, it is unsurprising then that opinion is split over the effectiveness of military involvement in grey zone conflict. Arguments range from military involvement as part of a conventional deterrence strategy only, moving to limited use as secondary to other levers of power, and

finally an argument that military power should play a significant role in the grey zone as interconnectedness now prevents effective use of other levers in the grey zone. The following paragraphs will outline each of these arguments.

## The Three Opinions on use of Military Force

A number of scholars argue that risks and limited effect mean military force should not be used in grey zone strategies, instead retaining a focus on conventional deterrence. Monahan outlines that 'gray zone aggression seeks to degrade and subvert existing rules to change the very paradigm of the competition.'[34] He argues that normalisation of grey zone tactics favours aggressors such as Russia and China, undermining Western competitive advantage which lies in upholding the rules-based international order. He further expands to state that 'Tit-for-tat responses offer minor returns and exposure to downside risk.'[35] Monahan's view is supported by Mitre and Gellerman who claim with reference to the US, 'The Department of Defense's primary role in great power competition should be to deter war, not engage in daily competition.'[36] Further arguing that 'The risks of not doing so are the militarization of foreign policy, potential escalation of competition, and distraction from deterrence.'[37]

Moving to the second opinion, there is support for an argument that military responses should be utilised as a secondary and less important component of grey zone strategies. This is based on strategic penalties such as sanctions, diplomatic condemnation and isolation better targeting the many non-military elements of grey zone aggression.[38] As stated by Johnson, 'Anxiety …[has resulted in] a search for tactical solutions, or an escalation of existing techniques: more airpower, more Special Forces operations, the recruitment of local forces en masse.'[39] But he goes on to say that 'Rather than trying to counter the techniques at the operational and tactical level, it has been far better to assert strategic penalties through sanctions, diplomatic condemnation, isolation and strategic positioning alongside allies and partners.'[40] However, Jordan addresses the need for military integration by highlighting that 'The comprehensive and synchronized use of strategic lines of action combined with the different levels of escalation offers advantages to an actor who resorts to the gray zone over a rival whose defensive strategy is based on classic, linear and inflexible military deterrence.'[41]

Finally, addressing the opinion that military force may be the most important lever in the grey zone. Votel et al advocate for 'unconventional warfare' using special operations forces to support local state and non-state actors to achieve objectives. They argue that economic and social interdependence has become so powerful that alternate ways are required to achieve political goals. As stated by Votel et al, 'The complex nature of the future operating environment will often render traditional applications of the diplomatic and economic instruments ineffective or inappropriate.' 'At such times, unconventional warfare might be the only viable option through which the U.S Government can indirectly achieve political objectives.'[42]

Drawing together these conflicting views, the most developed argument with the greatest support is for a considered use of military force, integrated with the other levers of power. The limited impact of sanctions targeting Russia in 2014, and failure to deter the recent invasion of Ukraine, highlights the limitations of such diplomatic and economic measures.[43] Thus, while economic and diplomatic levers will continue to have an important role in applying cost, psychological pressure and signalling commitment, it would be a disadvantage if military force was not also effectively leveraged. As stated by Weissmann 'It is crucial to understand the role of the military in the grey zone. Unless [grey zone threats] can be handled there, the war is likely to have been lost before a conventional war breaks out.'[44]

### Holistic cost-imposing strategies

Moving away from the theme of elevated risk and risk tolerance, and the fundamental connection to the argument on use of military force in the grey zone, the final theme for review expands on the need for holistic cost-imposing strategies. Existing grey zone strategies adopted by aggressors such as China and Russia use a wide range of grey zone concepts, approaches and technologies, of which most are non-military in character, to pursue revisionist intent.[45] Brister[46] and Matisek[47] outline how many of these potential objectives, not least due to purposeful avoidance of direct confrontation, are isolated from interdiction by military force. As such, an equally holistic and comprehensive strategy is required to counter grey zone strategies, targeting multiple lines of operation, of which military will be just one element. This is supported by Mazarr, who argues for alignment with departments, multilateral processes and institutions, to achieve the required cooperation and coordination of a multicomponent strategy that renders aggressor 'gray zone campaigns toxic drains on resource and reputation'.[48]

Drawing together the three key themes identified in the literature review, an analysis of academic opinion suggests that the effective application of military force relies on long-term rather than short- term strategies with an expectation of incremental gains rather than grand victories. That the use of military force in the grey zone comes with risk of escalation and miscalculation, however this must be balanced against a need for risk tolerance to signal intent and deter further grey zone activity. Underpinning the first two themes is the need for a holistic cost-imposing strategy that leverages all aspects of power to counter equally comprehensive strategies by aggressors, while maintaining legitimacy and legality. These three key themes of short-termism and the idea of victory, elevated risk and risk tolerance, and holistic cost-imposing strategies, identified as key to effective application of military force in the grey zone will now be used as the framework to analyse the effective use of air power in two relevant and ongoing grey zone conflicts in Iran and Japan.

## Section 3
## Iran Case Study

This section will analyse Iran's application of air power as part of its grey zone strategy, using the three key themes identified as a framework. The focus is on contextualising and expanding

the relevance of those themes to analyse the effective use of air power in the grey zone. Iran has been selected as the first case study due to being one of the World's foremost grey zone actors who has challenged US ability to respond effectively.[49] As stated by Mazarr, 'Iran has wielded… [an] impressive array on unconventional, gray zone tools to bolster its influence in the Middle East and beyond.'[50] These tools have incorporated significant elements of air power, including precision strikes against US bases in the Middle East, but in doing so it has demonstrated both effective and ineffective use of air power to advance its objectives.[51] As such it yields relevant study, particularly in the effective application of a more offensive use of air power in the grey zone.

## Short-termism and the idea of victory

This first section will analyse how Iranian key decision makers have contributed to effective use of air power in the grey zone. In analysing Iran's grey zone activity through the first theme of short- termism and the idea of victory, it is argued that Iran have not suffered from short-termism and have been appropriately focussed on incremental gains over a more conventional victory. Since the creation of the Islamic Republic in 1979, Eisenstadt argues Tehran has progressed a consistent asymmetric strategy against US influence in the Middle East.[52] While diversifying and expanding its grey zone options, for example in response to new technologies, the strategy has retained its core principle of deterrence by punishment.[53] As further stated by Eisenstadt, 'Tehran has relied on the same dog-eared playbook for nearly 40 years now.'[54]

This consistency, and its positive impact on the use of air power in the grey zone, is highlighted by Iran's drone programme. Nadimi describes how, 'After decades of steady development, Tehran now uses drones to complement its missiles and broader effort to bring the entire Middle East within its range.'[55] With development dating back to the 1980s, organisational reform and continued academic and financial support, Iran's weaponised drones now pose a credible threat of punishment throughout the Middle East.[56] The benefits derived from Iran's long-term strategy of drone development for precision strike are further highlighted by comments from the Commander of US Central Command, General Kenneth McKenzie. Addressing the Senate Armed Services' Committee, he stated that the drones being proliferated by Iran and its proxies 'present a new and complex threat to our forces and those of our allies…until we are able to develop and field a networked capability to detect and defeat [UAVs], the advantage will remain with the attacker.'[57]

This ability to maintain a long-term strategy is argued by Eisenstadt to be due to 'Iran's key decisionmakers…[being] unelected and therefore can often ignore public opinion when it comes to national security matters.'[58] For example, Ayatollah Khamenei has been Supreme Leader since 1989 and Qassem Soleimani had been the Islamic Revolution Guards Corps-Qods Force Commander since 1998 until his death by US drone strike in 2020.[59] Additionally, it is argued that Iran believes it is fighting for its survival, but that following the near quarter-million Iranians killed in the Iran-Iraq war, this must be done without escalation to conflict.[60]

These factors are argued to lead to Iran's consistency in progressing revisionist aims it considers essential, but through a nuanced and incremental grey zone strategy that doesn't escalate to war.

In contrast, Western decision makers are often politicians constrained by re-election timeframes.[61] Western decision makers also do not view Iranian grey zone aggression as an existential threat and counter-strategies suffer from many competing commitments, not least from Russia and China.[62] Taken together, this hampers Western ability to form a coherent long-term strategy. This is then further constrained by erroneous views of the black and white nature of war and peace. Symonds argues that 'the West tends to think about conflict in a binary way: you are either at war or at peace.'[63] Eisenstadt supports this view, arguing, 'U.S. decision makers tend to conceive of war and peace with Iran, as well as with other state actors link China and Russia, in stark, binary terms, and have frequently been constrained by fear of escalation.'[64]

Drawing this theme together, analysis highlights key elements that have contributed to the effectiveness of Iran's long-term strategy. Namely, a long-term goal of incremental gains, below the threshold of war, and an early recognition of the asymmetric advantage drone technology could provide. Presently the West is constrained in many ways, hampered by short-termism and on overly simplistic view of peace and war. While the democratic nature of Western nations, and re-elections, will inherently drive an element of short-termism, the West needs to work toward a culture that better recognises the characteristics of the grey zone. This will enable more effective, enduring strategies, that recognise the non-binary nature of the grey zone, and work toward removing the greater freedom currently allowed to aggressors such as Iran.

## Elevated risk and risk tolerance

Moving to an analysis of the second theme of elevated risk and risk tolerance. Despite a significant offensive strike component to Iran's grey zone strategy, this rarely leads to miscalculation and unintended escalation, despite frequent reciprocal engagements with the US. As such, Iran poses a compelling example of where offensive military action, including the use of air power, is used as part of a grey zone strategy, while apparently managing the associated risks. This next section will outline the differing arguments on the contribution that Iran's use of offensive air power poses to the risk of escalation and miscalculation, and thus its effectiveness in supporting the regime's aims and objectives.

The first argument is that Iran's development and proliferation of drones to its own forces and proxies has reduced the risk of escalation. Views in support of this include Esfandiari who argues 'Drones have allowed Tehran to maintain plausible deniability even as it carries out covert operations in the region.'[65] Ostovar further outlines how 'Iran's ability to strike at its opponents through clients provides it a mechanism of retaliation that can have a deterrent effect.'[66] He expands to state that, funding and support of proxies, including through proliferation of

drones, has enabled Iran to establish a network that has 'transformed into a sophisticated system of power projection that has afforded Tehran immense strategic value.'[67] These views support an argument that Iran's use of air power, including through its use of weaponised drones, has not only supported its objective of increasing its influence in the region, but has also reduced the risk of escalation through the considerable deterrent effect the precision strike capability poses.

The opposite opinion is given by Lamson, who argues that 'evidence of Iran's new precision-strike weapons capability has been raining down across the Middle East.'[68] He contends this success means Iran are now at greater risk of miscalculation through over confidence and perception of advantage. He states, 'Iran's reliance on precision-strike weapons to conduct quick, decisive, and offensive responses to enemy actions could easily drive a fast, escalatory cycle of tit-for-tat attacks.'[69] However, the evidence to date suggests this may be an overly pessimistic assessment. While Iran has demonstrated miscalculation, such as in air strikes on Saudi Arabian oil infrastructure which provoked many countries dependent on Gulf oil, this is one of few examples and saw rapid recognition and adjustment.[70] For the most part, Iran has shown patience and caution in its decades long struggle against US influence in the Middle East. This was highlighted in the exchanges which led to General Soleimani's death by US drone strike. Despite the potentially severe provocation, the Iranian response involved calibrated missile attacks on an American base in Iraq, with warning to allow US service members time to seek shelter.[71] This clear demonstration of retaliatory strength, followed up by signalling of desire to de-escalate, epitomises Iran's proportional use of force and focus on protraction rather than escalation of conflict.[72] Votel et al describe this as Iran's 'finely tuned risk calculus'.[73]

Drawing this theme to a close, it has been shown that Iran demonstrates an effective use of weaponized drones in the grey zone, managing the risk of escalation and miscalculation. This has been to the benefit of increased influence in the region through its proliferation of drones to proxies, associated increased ambiguity of attacks and contribution to highly credible deterrence. For a revisionist State who has elected to pursue an aggressive strategy against US influence, this risk tolerance has likely contributed to preventing US military escalation. However, while this has proved to be an effective use of air power for a regime with reduced interest in legality and upholding international norms, it doesn't necessarily follow as an argument for similar application by the West. Previous experience has highlighted the counter-productive nature of drone strikes that undermine legitimacy and have associated 'blowback' for Western nations upholding international rules and norms.[74] As such, while the use of drones in the grey zone remains a useful option to be exploited, its use needs to be very carefully considered as miscalculation may have more enduring ramifications for the West. Finally, drones offer a low-cost way for a country, such as Iran, suffering from years of crippling US sanctions to compensate for a lack of a modern Air Force. As such, the West should expect further proliferation and develop an enduring, long-term strategy to counter.

## Holistic cost-imposing strategies

This final element of the Iran case study will analyse the extent to which Tehran has integrated the use of air power as part of a holistic cost-imposing strategy and the extent to which this has impacted the attainment of Iran's aims and objectives. To a great extent the literature supports a view that Iran has pursued a wide range of grey zone concepts, approaches and technologies, to support its revisionist intent. Eisenstadt outlines how Iran has 'created a complex institutional setup for projecting influence abroad consisting of both civilian and military entities.'[75] He expands to explain the setup provides Iran 'with tools and options unavailable to its adversaries-such as terrorism and intimidation, bribery, and unbridled disinformation activities.'[76] Further adding that Iran is now adding offensive cyber operations to its strategy and 'relies on a variety of nonmilitary means to bolster deterrence-creating economic dependencies in neighbouring states,…[and] building external bases of support for Iranian policy.'[77] Eisenstadt's analysis is supported by Mazarr who outlines an 'impressive array of unconventional, gray zone tools to bolster its influence in the Middle East and Beyond.'[78] He states that Iran 'deploys a…extensive network of covert operatives and quasi-military forces through its embassies and other locations. It uses energy diplomacy and the proceeds of oil riches to fund its various causes… It has a well-developed network of proxies…to help carry out its strategic ambitions.'[79] These measures are argued to have given Iran an advantage in shaping the strategic environment and expanding its influence in the Middle East.[80] From this overview of Iran's grey zone strategy, it can be seen that many of the tools of Iran's approach cannot be targeted by military means. As such, it follows that an equally holistic approach is required to effectively counter Iran's grey zone aggression.

In summary, this case study has identified that Iran have effectively avoided short-termism to the benefit of progressing an enduring drone development strategy that is now providing significant benefit in supporting Iran's aims of increased influence in the region and protection of the regime. In contrast, the West suffers from short-termism and has been risk averse due to inaccurate and binary perceptions of war and peace, providing Iran with greater freedom for aggression in its use of air power. In considering the accusation that the use of air power increases the risk of escalation and miscalculation in the grey zone, this was not found to be the case with Iran. Instead, it was identified that Iran pursues a highly patient, consistent and finely tuned risk calculus that enables the effective use of offensive air power without escalation to war. Finally, Iran has demonstrated a holistic cost-imposing strategy in its grey zone activity, much of which cannot be targeted by military means. This supports the theme identified in the literature review that the use of air power must be integrated as part of a wider comprehensive strategy to effectively counter the sophisticated grey zone strategies employed by aggressors.

## Section 4
## Japan Case Study

This section will now analyse a second case study on the effective use of air power as part of Japan's deterrence of Chinese grey zone operations. As with the first case study, the three

key themes identified in the literature review will be used as the framework, with the focus on contextualising and expanding the relevance of those themes to further analyse the effective use of air power in the grey zone. Japan has been selected for this second case study as 'territorial disputes with Japan in the East China Sea (ECS) have been a significant focus of China's grey zone efforts.'[81] While this has predominantly played out in the maritime domain, there has been considerable activity in the air domain also.[82] The dispute revolves around the Senkaku Islands, which are administered by Japan but claimed by China. Since the Japanese government purchased three features in the Senkaku's from a private owner in September 2012, China has expanded its military, paramilitary, diplomatic and political campaigns to alter the status quo of the Senkaku islands.[83] Japan's response to China's grey zone activity in the ECS was one of the first examples of the development of a conceptual framework of grey zone deterrence, laid out within its National Defense Program Guidelines (NDPG) in 2010.[84] Since then, it has developed this framework further, in 2013 and again in 2019, progressing the adoption of a more responsive and integrated defence force, including increasing use of conventional air power to deter Chinese grey zone aggression.[85] With the dispute ongoing and growing opinion that 'the trends do not bode well for Japan',[86] it yields a highly relevant case study in analysing the effective use of air power in deterring sub-threshold and grey zone operations.

## Short-termism and the idea of victory

Addressing Chinese grey zone aggression in the ECS and the effective use of air power as part of Japan's response, this next section will consider the first theme of short-termism and the idea of victory. In analysing this theme, and how Japan's use of air power has been influenced by changing priorities or inaccurate perceptions of victory in the grey zone, contradictory arguments have emerged. The scale of change in Japan's Security and Defense Forces (JSDF) since 2010, and increased frequency of NDPG publication,[87] supports an argument of short-termism. Force posture changes include 'the re-location of defense capabilities…from the northern to the southern part of the country, including the southern island chains.'[88] Increasing capabilities are highlighted such as the 'acquisition of 147 F-35 fighter jets…an increase of 105 planes from the previous plan,'[89] and 'first time acquisitions of capabilities [standoff missiles and hyper velocity gliding projectiles] that go beyond Japan's exclusively defence-oriented security doctrine.'[90] Further that Japan's intent to have both defensive and offensive cyber capabilities 'is a significant change from Japan's previous strategies.'[91]

Nevertheless, it is argued that despite these changes, Japan's strategic objectives towards China have been highly consistent and always combined both deterrence and engagement.[92] Berkofsky supports this view stating, 'the restructuring of Japan's armed forces…is comprehensive and ambitious, but does not change the fundamentals of decade-old Japanese security and defense policies.'[93] An example in support of the view that Japan has successfully balanced strategic patience with necessary reform, is given by the enduring deterrence by denial concept introduced in 2010. 'As outlined by Liff, the strategy included

the deployment of additional forces to address a defence vacuum and surveillance gap around the Senkaku islands to prevent a Chinese fait accompli.[94] The use of air power to provide persistent intelligence, surveillance, and reconnaissance (ISR), and air interception, has successfully contributed to a view that, 'Japan thus far has been able to successfully counter Chinese attempts to alter the status quo by monitoring, shadowing, and warning off Chinese intrusions…[around the] Senkakus.'[95]

On balance, academic opinion supports the view that Japan's policy makers have effectively balanced long-term consistency with necessary reform, and in doing so have achieved the strategic aim of retaining the Senkaku Islands. However, while the evidence supports a lack of short-termism at the strategic level, Japan have demonstrated a failure to recognise the enduring nature of grey zone competition in tactical elements of its response. This is exemplified by Japan's policy of intercepting and shadowing all Chinese air incursions, to considerable detriment of their F-15 fleet.[96] This highlights a lack of adequate consideration of the costs this policy would exact over the prolonged timeframe associated with grey zone competition. However, Japan subsequently recognised the unsustainable toll the policy was having, citing in the 2019 NDPG that the policy 'is exacting a chronic burden in its personnel and equipment, generating a concern that JASDF may not be able to maintain proficiency and the volume of its activities.'[97] The policy was subsequently amended, to reduce the numbers of aircraft scrambled for each incursion and adoption of other measures of surveillance.[98] However, concern remains that Japan are not planning for the long term and will 'waste its F-35s shadowing Chinese Planes.'[99]

Drawing this section together, the majority of Japanese strategic decision making has recognised the long-term nature of grey zone conflict, setting realistic aims and objectives for the retention of the Senkaku Islands and seen the exercising of strategic patience. However, there are elements to Japan's response that highlight areas for improvement. While the strategy of deterrence by denial around the Senkaku's has been successful so far, including in its application of air power, Japan have yet to adopt an air interception strategy that appropriately mitigates the attrition of China's incursion rate. Unless this is addressed, Japan is playing into China's alleged attrition strategy for altering the status quo of the Senkakus.[100]

## Elevated Risk and Risk Tolerance

While the previous sub-heading analysed how short-termism and the idea of victory have influenced the effective application of air power in Japan's grey zone deterrence strategy, this next sub-heading analyses the case study from the theme of elevated risk and risk tolerance. Reviewing the literature on this theme, there are two opposing views on the elevated risk of escalation and miscalculation posed by Japan's use of air power. Starting with the argument that Japan's use of air power in the grey zone has elevated risk, to the detriment of Japan's strategic aim of deterring Chinese aggression. As part of a strategy of persistent presence around the Senkakus to prevent a fait accompli by China, in February 2016, Japan 'established

the 9th Air Wing in Naha…the enhancement effectively doubled the number of fighters dedicated to responding to Chinese incursions.'[101] However, this strategy is critiqued as having led to escalation and more scope for miscalculation, with 2016 subsequently a year of rising tensions. This was highlighted in June 2016, when Japan claimed that a PLAAF aircraft nearly fired at a JASDF fighter in the ECS, and again in July 2016 when China accused Japan of aggressive behaviour nearly resulting in a dogfight.[102]

The counter argument however states that China's disinformation campaigns elaborate or fabricate these incidents,[103] and stresses the need to demonstrate 'a will to protect Japan's sovereignty and independence.'[104] Bothwell supports this position stating, 'signalling is necessary to communicate specific red lines over vital interests through credible commitments, such as sunk costs.'[105] Takahashi goes further, claiming there is an inherent need to 'develop a robust posture to win the possible war in the case of escalation, and to make the challengers recognise the possibility of unfavourable military conflict.'[106] On balance, noting Japan denied the allegations of a near dogfight,[107] Japan's balance of risk tolerance appears appropriately measured to China's growing military assertiveness in the region.

## Holistic cost imposing strategies

This final section will provide an analysis of Japan's use of air power as part of a holistic cost-imposing strategy, in response to China's highly sophisticated and comprehensive approach. An analysis of the literature highlights that Japan's current strategy 'lacks several important elements.'[108] Ueki outlines these as a 'lack of strategy for multilateral security institution building',[109] and lack of a 'clear and shared objective with countries such as Australia and the United States'[110] on a free and open Indo-Pacific. Further that Japan has been 'slow to react to threats in cyberspace even though the United States has been pushing Japan in that direction for some time.'[111] In contrast, Japan can be seen to have recognised the limitations to its ability to deal with the grey zone challenge in isolation, through clear signalling within the NDPG of the importance of the regional security ties and the US alliance.[112] This was highlighted by President Biden recently reaffirming the Senkaku Islands are covered by the collective defence obligation of the Japan-US Security Treaty.[113] In addition, Japan has played a significant role in the recent resurgence of the Quadrilateral Security Dialogue for cooperation with the United States, Australia and India.[114] In turn this has led to the reinforcing of the security partnership with the first joint exercises for 13 years.[115] Finally, Japan also continues to engage China thorough business cooperation and other economic and diplomatic measures.[116]

In analysing this debate, it is argued Japan can improve its grey zone strategy for countering China with a greater focus on a truly comprehensive approach that increases the costs imposed on China. However, Japan has achieved success beyond preventing a fait accompli. As argued by Mazarr, 'Japan's new defense guidelines alone, and the tighter partnership it implies with the United States, has probably cost China more in the overall balance of power than it has gained with its rhetoric and land reclamation.'[117] Further, that Japan's restraint and proportionality in its strategy has maintained its reputation for upholding international rules

and norms, just as China has undermined its own reputation through its threatening behaviour and failure to abide by such rules.[118]

In summary, this case study has identified that Japan has been largely effective in avoiding short- termism to the benefit of progressing an enduring strategy of persistent surveillance and defence around the Senkaku Islands. This strategic patience, and recognition that winning in the grey zone looks more like a maintenance of the status quo, has enabled the prevention of a fait accompli by China. In considering the accusation that the use of air power increases the risk of escalation and miscalculation in the grey zone, there was evidence to support this. However, this was contrasted with Japan's need to signal clear commitment to protect its territorial integrity, to avoid Chinese miscalculation and act as a deterrent to further escalation. Finally, Japan has demonstrated elements of a holistic cost-imposing strategy in its grey zone activity, including through effective alliance and regional security measures. However, there is evidence that Japan needs to expand its approach to inflict greater cost on China as existing measures haven't prevented increasing aggression in the ECS.

## Section 5
## Conclusion

In conclusion, this research paper has evaluated the effectiveness of air power in sub-threshold and grey zone operations, arguing that air power has significant utility both as part of a strategy of deterrence by punishment and of deterrence by denial. However, this paper has also identified the need for the use of air power to be integrated into an enduring, risk aware, and holistic cost- imposing strategy to be effective and impose greater cost on an aggressor.

Section one of this paper introduced the concept of grey zone competition. Arguing that, while the grey zone is the manifestation of strategic competition below the threshold of war by actors such as Russia and China, core features may vary between aggressors. This was highlighted through Russia's focus on cyber and disinformation campaigns to undermine political institutions, in contrast to China's focus on expansion and militarisation of artificial islands coupled with deterrence and denial of resources in the SCS and ECS. However, the introduction identified that, regardless of differences in core features and tactics applied by some grey zone aggressors, the central aim of an aggressor's strategy will be the same. Namely the aim to undermine the current international order and gain greater influence and control over spheres of influence.

Following the introduction of grey zone and sub threshold competition, the paper moved to a literature review in chapter two. The review identified three key themes critical for the application of military force to be effective in supporting a grey zone strategy. The first theme was argued to be political short-termism and misperceptions around the idea of victory in the grey zone, challenging the ability of Western democratic nations to adopt and maintain effective grey zone strategies. The second theme was identified as the risk of miscalculation and escalation posed by military activity in the grey zone, contrasted with the need for risk

tolerance to achieve effective signalling of commitment for deterrence. This second theme was found to be central to the debate over the extent to which military forces should be used within the grey zone. The third theme identified that grey zone aggressors have adopted highly sophisticated, holistic grey zone strategies, where many elements cannot be targeted by military force. As such, successful strategies to counter grey zone aggression must rely on an equally comprehensive approach. However, in adopting such an approach, the aim shouldn't be to likewise flaunt international rules and norms, but to maintain legitimacy and proportionality to support a strategy that drains reputation and support from the aggressor. These three themes were then used as the framework for the two case studies.

Expanding on the debate over military use in the grey zone, linked to second theme of escalation and miscalculation, the literature review identified three contrasting trains of thought. The first position argues that the risk of escalation and miscalculation is too high, only offers minor returns, is often counter-productive and other levers such as economic sanctions are far more effective. This position argues that militaries should only engage in conventional deterrence of grey zone aggression, as doing otherwise and targeting ambiguous grey zone activity risks undermining legitimacy through criticism of heavy-handedness and illegality, likely supporting the opponent's narrative. The second opinion argues that military force should be used as a limited and secondary element in grey zone strategies. That while strategic penalties such as sanctions, condemnation and isolation are likely to have greater effect, the synchronization of such activities with different levels of military escalation offers advantages over a strategy which only includes military force in a classic deterrence posture. The final position argues that economic and social interdependence have become so powerful as to render application of diplomatic and economic instruments ineffective or inappropriate. Arguing that, at times, 'unconventional warfare' through use of Special Operations Forces, operating with local state and non-state partners, may be the only viable option to achieve political objectives. This paper concluded that self-limitation to conventional deterrence only, noting the ambiguity of salami slicing tactics employed by aggressors such as China and Russia, is insufficiently nuanced to provide effective deterrence. Conversely it is argued that elevation of military activity in the grey zone above the other levers of power would be a flawed approach. This is based on the fact many aspects of aggressor grey zone strategies cannot be targeted by military means and use of extensive military force can too easily be construed as illegal and heavy-handed, further supporting aggressor revisionist aims. As such, this paper concludes that a balanced approach is required. That while economic and diplomatic levers will remain key, military force has an important role to play in a holistic strategy and as such it would be remiss and act as a disadvantage if not leveraged.

Section 3 moved on to the first of two grey zone case studies, analysing the effectiveness of Iran's use of air power as part of its deterrence by punishment grey zone strategy. Iran was selected as one of the World's foremost grey zone actors that has consistently challenged US and western ability to respond effectively, using one of the greatest amounts of lethal

force compared to other grey zone actors. The case study of Iran's use of air power in the grey zone argued it was however largely effective in progressing its objectives, with only limited evidence of counter-productivity. It was found that Iran effectively used drones as part of a comprehensive strategy to deter by punishment and gain influence in the region. When analysing Iran's strategy, while it has diversified and expanded its grey zone options over time, it has done so with highly consistent aims and objectives. This was found to have supported its effective application of air power through use of drones, highlighted by its successful development programme stretching back to 2011. With the weaponization of Iran's drones today posing a very credible threat of precision attack anywhere in the Middle East. Despite this offensive use of air power, lack of escalation to war was found to be due to Iran's effective pacing and spacing of measured activity in a predictable manner, supporting an effective deterrence by punishment strategy. Finally, Iran has effectively integrated its use of air power as part of a highly comprehensive grey zone strategy that blends capabilities and tactics across all domains to maximise leverage and cost imposed to opponents. While examples of miscalculation exist, Iran has demonstrated an effective ability to identify and adjust course, reinforcing its potent threat to deter and signalling desire for de-escalation at key times. However, Iran's aggressive strategy, while effective at progressing its aims of increasing its influence in the region and ensuring regime survival, has come at very significant cost through crippling economic sanctions and isolation. Thus, utilisation of air power for precision strike, as part of a grey zone strategy needs careful calibration to maintain legitimacy and support the objective of undermining the support and reputation of the aggressor.

While the first case study provided an analysis of the offensive use of air power, the second case study provided a very different analysis of Japan's defensive strategy against Chinese expansionism in the ECS. Analysing Japan's use of air power as part of its deterrence by denial strategy, a number of conclusions were drawn. Firstly, Japan has evidenced mixed recognition of the enduring timeframe associated with grey zone strategies, leading to adoption of some policies that exact a chronic burden on the JASDF. However, on balance, they have maintained long-term consistency, while undertaking necessary reform, and in doing so have achieved the strategic aim of retaining the Senkaku Islands. Early recognition and development of the grey zone as a concept from 2010, with enduring priority on addressing the surveillance and defence gap around the Senkakus, is argued to have been critical in preventing fait accompli by China. Secondly, this paper identified contradictory opinion around the escalatory risk of Japan's increased forward military presence, including its doubling of the number of fighters for interception. The risk of escalation has been highlighted by several confrontations and incidents between PLAAF and JASDF aircraft. However, this paper concluded that Japan has effectively managed this risk and furthermore, is evidence of appropriate risk tolerance. Japan's JASDF reform underlines its commitment and intent to defend its territorial integrity. The signalling of which aids the avoidance of miscalculation by China and acts as a further deterrent. Finally, it was identified that Japan's strategy required greater focus on a more holistic approach to exact greater cost on China. While Japan's use of military force, including

air power, has been successful in preventing fait accompli, it was argued that Japan's closer ties with the U.S. and regional partners had contributed most to imposing cost on China and its aims for increasing regional influence.

In conclusion, this paper has argued that air power is effective in the grey zone, both as part of a strategy of deterrence by punishment and a strategy of deterrence by denial. Further that failure to leverage air power's capability acts as a disadvantage to grey zone aggressors who utilise all aspects of power to form a comprehensive strategy. However, in order to compete in the grey zone, this paper identified three key themes for the effective application of air power. Firstly, a need for strategic patience and recognition that gains will be gradual over extended timeframes, likely appearing more as a maintenance of the status quo. Secondly, that the risk of escalation from the use of military force, combined with the need to signal commitment and intent, requires a finely tuned risk calculus. However, the non-binary nature of the grey zone supports a greater risk tolerance than the West currently employ in the grey zone. Thirdly that, as grey zone aggressors have adopted highly sophisticated, holistic grey zone strategies where many elements cannot be targeted by air power, successful strategies to counter grey zone aggression must rely on an equally comprehensive approach. However, these strategies must retain a focus on legitimacy and proportionality to support the objective of undermining the reputation and influence of grey zone aggressors.

## Notes

[1] Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Keep, *Gaining competitive advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War*, (Santa Monic: RAND Corporation, 2019), 1.
[2] Michael J. Mazarr. *Mastering the gray zone: Understanding a changing era of conflict*. (Morrisville: Strategic Studies Institute and U.S. Army War College, 2015): 1-2.
[3] Ibid., 11.
[4] Morris et al, *Gaining competitive advantage in the gray zone*, xi.
[5] Ibid., xii.
[6] Mikael Weissmann, Niklas Nilsson, Per Thunholm, and Björn Palmertz, eds. *Hybrid warfare: Security and asymmetric conflict in international relations*, (London: Bloomsbury Publishing, 2021), 173-184.
[7] Michael Eisenstadt, 'Iran's Gray Zone Strategy', *PRISM* 9:2, 2021: 78.
[8] *Sky News*. 'Defence review: UK's armed forces must be more 'nimble' as 'enemies study Britain's vulnerabilities', 15 September 2020. https://news.sky.com/story/ (accessed 10 Mar, 2022).
[9] Morris et al, *Gaining competitive advantage in the gray zone*, ix.
[10] Robert Johnson, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies*, 29:1, 2018: 142.
[11] Adam Leong Kok Wey, *Airborne Assault to Occupy South China Sea Features?*, *Commentary*, 15 July 2021, https://rusi.org/ (accessed 5 Mar, 2022).
[12] Sidharth Kaushal and Sam Cranny-Evans, *China's Taiwan Air Incursions: Reading the Tea Leaves*, *Commentary*, 19 October 2021 https://rusi.org/ (accessed 5 Mar, 2022) and Kosuke Takahashi,

Japan Scrambled Fighter Jets to Intercept Foreign Aircraft Over 1,000 Times in FY2021, 15 April 2022. https://thediplomat.com/2022/04/ (accessed 10 Mar, 2022).
[13] Won-June Hwang, 'How are drones being flown over the gray zone?', *Defense & Security Analysis* 37:3, 2021: 328-345.
[14] Javier Jordan, 'International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict,' *Journal of Strategic Security* 14:1, 2020: 3.
[15] Mazarr, *Mastering the gray zone*.
[16] Jordan, 'International Competition Below the Threshold of War'.
[17] Jahara Matisek, 'Shades of gray deterrence: Issues of fighting in the gray zone.' *Journal of Strategic Security* 10:3, 2017: 1-26.
[18] Michael J. Mazarr. *Mastering the gray zone: Understanding a changing era of conflict*. (Morrisville: Strategic Studies Institute and U.S. Army War College, 2015): 33 and Jordan, 'International Competition Below the Threshold of War'. 10.
[19] Department of Defense, 'National Defense Strategy 2020'. https://www.defense.gov/ (accessed 4 Feb, 2022).
[20] Jordan, 'International Competition Below the Threshold of War'. 10.
[21] Mazarr, *Mastering the gray zone*. 67.
[22] Mazarr, *Mastering the gray zone*. 67.
[23] Joseph Votel, Charles T. Cleveland, Charles T. Connett, and Will Irwin. 'Unconventional warfare in the gray zone.' *Joint Forces Quarterly* 80:1, 2016:108.
[24] Matisek, 'Shades of gray deterrence: Issues of fighting in the gray zone.' 26.
[25] Jordan, 'International Competition Below the Threshold of War'. 17.
[26] Mazarr, *Mastering the gray zone*. 109.
[27] Jordan, 'International Competition Below the Threshold of War'. 17.
[28] Matisek, 'Shades of gray deterrence: Issues of fighting in the gray zone.' 2.
[29] Mazarr, *Mastering the gray zone*. 67-68.
[30] Robert Johnson, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies*, 29:1, 2018: 151.
[31] Matisek. 'Shades of Gray Deterrence'. 8.
[32] Heather Bothwell, 'Gray Is the New Black.' *JFQ* 101:2 (2021): 29.
[33] Sugio Takahashi, 'Development of gray-zone deterrence: concept building and lessons from Japan's experience.' *The Pacific Review* 31:6 (2018): 800.
[34] Sean Monahan. 'Bad Idea: Winning the Gray Zone,' *Center for Strategic and International Studies*, December 17, 2021, last modified December 17, 2021, https://defense360.csis.org/ (accessed 15 Apr 22).
[35] Monahan. 'Bad Idea: Winning the Gray Zone.'
[36] Jim Mitre, and Andre Gellerman. 'Defining DoD's Role in Gray Zone Competition.' *Center for a New American Security*, August 24, 2020, https://www.cnas.org/ (accessed 15 Apr 22).
[37] Ibid.
[38] Mazarr, *Mastering the gray zone*. 50.
[39] Johnson, 'Hybrid War and its Countermeasures'. 144.
[40] Ibid.

[41] Javier Jordan, 'International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict,' *Journal of Strategic Security* 14:1, 2020: 17.
[42] Votel et al. 'Unconventional Warfare in the Gray Zone'. 105.
[43] Edward Hunter Christie, 'The Design and Impact of Western Economic Sanctions against Russia', *The RUSI Journal* 161:3 (2016).
[44] Mikael Weissmann, Niklas Nilsson, Per Thunholm, and Björn Palmertz, eds. *Hybrid warfare: Security and asymmetric conflict in international relations*. (London: Bloomsbury Publishing, 2021): 61.
[45] Mazarr, *Mastering the gray zone*. 91.
[46] Paul Brister, 'Revisiting the Gordian Knot: Strategic Considerations for Hybrid Warfare.' *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict* (2011): 51.
[47] Matisek. 'Shades of Gray Deterrence'. 5.
[48] Mazarr, *Mastering the gray zone*. 135.
[49] Michael Eisenstadt, 'Iran's Gray Zone Strategy', *PRISM* 9:2, 2021: 77.
[50] Mazarr, *Mastering the gray zone*. 44.
[51] Ibid., 81.
[52] Ibid., 81.
[53] Farzin Nadimi, 'Iran's Game of Drones.' *The Washington Institute for Near East Policy*, Mar 2, 2022, https://www.washingtoninstitute.org/ (accessed 9 Apr, 2022).
[54] Eisenstadt. 'Iran's Grey Zone Strategy', 90.
[55] Nadimi, 'Iran's Game of Drones.'
[56] Ibid.
[57] Kenneth McKenzie, Posture Statement Before the Senate Armed Services Committee April 22, 2021. https://www.armed-services.senate.gov/ (accessed 17 Apr, 2022).
[58] Eisenstadt. 'Iran's Grey Zone Strategy', 79.
[59] Ibid.
[60] Ibid., 78-79.
[61] Jordan, 'International Competition Below the Threshold of War'. 10.
[62] Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Keep, *Gaining competitive advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War*, (Santa Monic: RAND Corporation, 2019), 1.
[63] Matthew Symonds, Shades of grey – Neither war nor peace, The uses of constructive ambiguity. Special report, The Economist, Jan 25, 2018, https://www.ecenomist.com/special-report. (accessed 17 Apr, 22).
[64] Eisenstadt. 'Iran's Grey Zone Strategy', 78.
[65] Golnaz Esfandiari, 'Iran Deploys Drones to Target Internal Threats, Protect External Interests.' Radio Liberty, Jan 18, 2022, https://www.globalsecurity.org/ (accessed 9 Apr, 2022).
[66] Afshon Ostovar, 'The Grand Strategy of Militant Clients: Iran's Way of War', *Security Studies* 28:1 (2019) 172.
[67] Ibid.
[68] Jim Lamson, 'New Missiles, New Risks: The Escalatory Implications of Iran's Precision-Strike Weapons, War on the Rocks', Jan 14, 2022, https://warontherocks.com/2022/01/

(accessed 10 Apr, 2022).
[69] Ibid.
[70] Eisenstadt. 'Iran's Grey Zone Strategy', 88.
[71] Ibid.
[72] Ibid., 82, 88.
[73] Votel et al. 'Unconventional Warfare in the Gray Zone'. 102
[74] Aqil Shah. 'Do US drone strikes cause blowback? Evidence from Pakistan and beyond.' *International Security* 42:4 (2018): 47-84.
[75] Eisenstadt. 'Iran's Grey Zone Strategy', 81
[76] Eisenstadt. 'Iran's Grey Zone Strategy', 81.
[77] Ibid.
[78] Mazarr, *Mastering the gray zone*. 44.
[79] Ibid.
[80] Eisenstadt. 'Iran's Grey Zone Strategy', 81.
[81] Morris et al, *Gaining competitive advantage in the gray zone*, 92.
[82] Ibid., 96-97.
[83] Ibid., 93-94.
[84] Sugio Takahashi, 'Development of gray-zone deterrence: concept building and lessons from Japan's experience.' *The Pacific Review* 31:6 (2018): 787.
[85] Government of Japan. 'The National Defense Program Guidelines, for FY 2014 and beyond.' and 'The National Defense Program Guidelines, for FY 2019 and beyond.' https://www.mod.go.jp/en/d_act/d_policy/national.html (Accessed 12 Mar 2022).
[86] Morris et al, *Gaining competitive advantage in the gray zone*, 91.
[87] Axel Berkofsky, 'Japan's December 2010 'National Defense Program Guidelines (NDPG)': The 'Big Bang' of Japanese Security and Defense Policies?.' *Korean Review of International Studies* 14:1 (2011): 33.
[88] Berkofsky, 'Japan's December 2010 'National Defense Program Guidelines (NDPG).' 34.
[89] Ibid.
[90] Kawakatsu Ueki, 'Japan's China strategy.' *Security Challenges* 16:3 (2020): 61.
[91] Ibid.
[92] Ueki, 'Japan's China strategy.' 59.
[93] Berkofsky, 'Japan's December 2010 'National Defense Program Guidelines (NDPG).' 33.
[94] Adam Liff Japan's 2010 National Defense Program Guidelines – Reading the Tea Leaves Asia Pacific Bulleting.
[95] Morris et al, *Gaining competitive advantage in the gray zone*, 93.
[96] David Axe. 'Japan Is About To Waste Its F-35s Shadowing Chinese Planes', *Forbes*, https://www.forbes.com/ (accessed 11 Apr, 2022).
[97] Government of Japan. 'The National Defense Program Guidelines, for FY 2019 and beyond.'
[98] Axe, 'Japan Is About To about to Waste Its F-35s Shadowing Chinese Planes'.
[99] Ibid.
[100] Alessio Patalano, 'A Gathering Storm? The Chinese "Attrition" Strategy for the Senkaku/Diaoyu Islands.' *RUSI Newsbrief* 21:1 (2020): 21.

[101] Morris et al, *Gaining competitive advantage in the gray zone*, 106.
[102] Franz-Stefan Grady, China Accuses Japan of Endangering its Military Aircraft, The Diplomat, https://thediplomat.com/ (accessed 11 Apr, 2022).
[103] Masataka Oguro. *Ensuring Japan's Future Air Security: Recommendations for Enhancing the JASDF's Readiness to Confront Emerging Threats*. Brookings, 2018.
[104] Masataka Oguro. *Ensuring Japan's Future Air Security*.
[105] Heather Bothwell, 'Gray Is the New Black.' *JFQ* 101:2 (2021): 29.
[106] Takahashi, 'Development of gray-zone deterrence', 800.
[107] Grady, China Accuses Japan of Endangering its Military Aircraft.
[108] Ueki, 'Japan's China strategy.' 62.
[109] Ibid.
[110] Ibid., 63.
[111] Ibid., 61.
[112] Government of Japan. 'The National Defense Program Guidelines, for FY 2019 and beyond.'
[113] Newsweek, 'Joe Biden Vows to Defend Senkaku Islands If Attacked by China', May 10, 2021 https://www.newsweek.com/ (accessed 14 May, 2022).
[114] Emma Chanlett-Avery, *Japan, the Indo-Pacific, and the 'Quad'*. Chicago Council on Global Affairs., 2018.
[115] NIKKEIAsia 'Quad nations flaunt stronger ties with first drill in 13 years' November 7, 2020 https://asia.nikkei.com/Politics/International-relations/ (accessed 17 May, 2022).
[116] Ueki, 'Japan's China strategy.' 62.
[117] Mazarr, *Mastering the gray zone*. 128.
[118] Geraint Hughes, 'War in the Grey Zone: Historical Reflections and Contemporary Implications.' *Survival* 62:3 (2020): 133.

Article

# Artificial Intelligence Changing the Nature of War – Strategic Security Implications for the United Kingdom?

By Wing Commander Alison Morton

**Biography:** Wing Commander Alison Morton joined the Royal Air Force in 2008, as a Pers(Trg) Officer, following time in the Royal Navy Reserve, Crown Prosecution Service and as an English Teacher in China. As a Junior Officer she completed a variety of tours, including the RAF Presentation Team and Aide-De-Camp (ADC) to the Air Officer Commanding (AOC) 2Gp. After promotion to Squadron Leader, she took command of Base Support Squadron at MOD Boscombe Down before taking up Air Staff duties, including Clerk to the Air Force Board. Deployments have included, Op Telic, Unified Protector and Shader. Following further promotion in 2020, she attended the Advanced Staff Course prior to taking command as Officer Commanding Base Support Wing at RAF Cranwell. Wing Commander Morton is a CAS Fellow having completed the Henderson Fellowship at the University of Exeter in 2020.

**Abstract:** Artificial Intelligence (AI) is a rapidly growing area of technology which will impact societies, economies and national security; presenting strategic security challenges for the UK. As such, this article will first consider the extent to which the nature of war will change and explore the threat AI poses to UK security. It will then consider how the UK can achieve strategic advantage. The article argues that war's essence will continue to be a politically-directed human endeavour. Violence, chance and friction will endure. Nevertheless, whilst technological advantage is a necessary condition, it is not sufficient to claim strategic success. Accordingly, the UK must develop a defence-specific AI strategy in order to gain and maintain strategic advantage.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

## Introduction

**In September 2017, Vladimir Putin stated that whoever 'becomes the leader in this sphere [AI], will become the ruler of the world'.[1] Whilst few have posited AI's potential quite as strongly as Putin, AI will impact societies, economies and national security in the coming years. Therefore, whilst Putin's hyperbolic language could be subjected to strong critique, AI and the subsequent implications on UK security strategy is a relevant and important area of study.**

The debate surrounding AI's impact on national security has several stakeholders and aspects to it. This article will not address all challenges that AI will pose to the UK's national security, nor will it focus on the technical intricacies of AI, such as machine decision-making or cybersecurity which are covered extensively in existing multi-disciplinary literature. Furthermore, the widely contested legal, ethical and moral arguments surrounding the use of AI in warfare will not be explored, though certain ethical implications will be expanded in Part Two. Whilst the definition of 'security' is contested and broad; this paper will largely focus on the implications for UK 'defence' elites – namely MOD and will concentrate on the macro-question of the nature of war, which will then inform Parts Two and Three. Specifically, AI's emergence has highlighted several questions which this paper aims to answer. First: To what extent will AI change the nature and character of war? Second: What strategic security variables is the UK exposed to by the development of AI? Third: How can UK security elites improve upon current positioning to gain a strategic advantage?

This study is therefore structured in three parts. First, it will use Clausewitz's trinity as an analytical theoretical framework to study the impact of AI on the nature of war. Following this, previous Revolution in Military Affairs (RMA) will be analysed for any lessons that may be applicable to the autonomous revolution. Part Two will then consider the strategic variables and challenges that AI poses to the national security of the UK. This section will consider, AI's impact on the international order, as well as the effect regime type has on AI development. Finally, Part 3 will aim to provide the reader with an examination of the UK's current AI strategic positioning and what is required to gain and maintain strategic advantage.

## Part One

*Is Clausewitz really still relevant?* Since the publication of Clausewitz's *On War*, few would dispute that the ways and means of the battlefield have not adapted over time. Indeed, the Prussian's central thesis stated this - the character of war will change, but its nature will endure. Followers of Clausewitz, understand that the nature of war is absolute, war is without limits and violence will escalate until there is an eventual victor. We can (thankfully) reflect on history and realise such destruction is relatively rare, more theoretical than real. Clausewitz explains this is due to fog, friction and politics; armies are unsure what lies in the next valley, engines run out of oil and politicians will be indecisive.[2] It is for these reasons that we have been, more often than not, spared annihilation. It is the human being that provides war her nature, therefore, according to Clausewitzian theory, if machines were to replace humans on the

battlefield, it is a rational assumption that the nature of war would fundamentally change – this is why it is important to examine the future of war through the prism of history.

*Character versus Nature*. Villacres and Bassford convincingly suggest AI is an attempt to improve warfare, reduce human suffering, eliminate the fog of war and friction, leading to ultimately 'de-politicizing war, turning it from a phenomenon marked by an amalgam of rationality, irrationality, and non-rationality.'[3] Moreover, Ankerson suggests warfare will evolve towards hyper-rationality.[4] In this scenario, AI would perform strictly to reason and logic. Human flaws such as fear, biases and exhaustion would be eliminated – a compelling argument that the nature of war will itself change. However, central to Clausewitz's theory is that war is not logical and strategy has too many variables. If humans are removed from warfare, so too will the social and political context that it operates in. Ultimately, the nature of war is forged on human disposition, it is bounded by our failings. Human flaws provide a safety net and therefore should not be viewed as weakness - the brutality and sacrifice of war are necessary protections.

Clausewitz differentiates between the objective nature of war and the subjective character of war, highlighting components such as; technology, ethics, law and culture that will change across space and time.[5] In his book *Modern Strategy*, Colin Gray captures this well, 'There is a unity to all strategic experience: nothing essential changes in the nature and function [or purpose] in sharp contrast to the character—of strategy and war.'[6] Indeed, Clausewitz himself observed that every period has its, 'own kind of war, its own limiting conditions and its own peculiar preconceptions.'[7] Whilst Clausewitz was basing his theory of war over 200 years ago, in which the character of warfare was changed largely by social and political conditions, he was aware that technological advancement would change the character of war.[8] And like Gray, many contemporary theorists agree with Clausewitz. Murray believes that technology cannot dissipate war's nature and contends war's nature includes the fog and the friction of war, and any argument contending war's nature can be altered are false.[9] Further arguing, 'No amount of computing power can anticipate the varied moves and the implications of an enemy's capacity to adapt in unexpected ways.'[10] In security strategy - the enemy always has a vote.

Whilst Murray is rooted in his views, there is reason nevertheless to question Clausewitz's theory. Writing over 200 years ago, could the Prussian really be certain that 21st Century revolutionary technology would not alter or even eliminate the objective and subjective elements of warfare?[11] There is nuance to Clausewitz's theory though, as Echevarria has stated; elements of warfare do interact and influence each other, 'Under Clausewitz's concept, the objective and subjective natures of war are closely connected to one another and interact continuously. New weapons or methods can increase or diminish the degree of violence or uncertainty, though probably never eliminate them entirely.'[12] Clausewitz himself believed the nature of war did not exist in isolation, and, was in itself a product of interactions. Clausewitz did not limit war's reciprocal nature to a clash of opposing trinities, but asserted interaction with

the trinity, 'these three tendencies are like three different codes of law, deep-rooted in their subject and yet variable in their relationship to one another.'[13] Accordingly, all elements of the trinity must be appropriately considered, rather than view them as arbitrary to one another. It is this exchange between the three elements which shapes violence and causes war's uniqueness, this in turn provides context to each case.[14] Accordingly, a change in character, such as AI, could influence an essential element and therefore could affect the nature of war. Furthermore, the conduct of war affects its character and this amended character feeds back into the political ends that ultimately drive its conduct.[15] Given the separate elements of Clausewitz's trinity do not operate in isolation, but rather attract and repel each other,[16] it is therefore worth analysing the trinity in further depth in relation to AI.

*Violence (The People)*. As will be expanded in Part 2, China is one nation that has been forthright in adopting AI for not just military purpose, but to also control the wider population; 'The Communist Party of China (CPC) hopes AI will have utility in enhancing the 'intelligentization' of 'social management' and protecting social stability.'[17] Whilst the CPC does not have the constraints of parliamentary democracy (like the UK) to limit policy options, the widespread use of AI may see the relationship between government and the population it serves blunted, simultaneously reducing public interest in the armed forces and as a consequence damaging the relationship between the military and the people.[18] Hoffman expands on the consequences of this and suggests 'cabinet wars' will become more frequent as they will be perceived as politically low-risk. Consequently, this increase in conflict may ultimately result in machines being seen as a policy failure and a demand for humans to return to the battlefield. The rise of AI, and the increased anonymity of warfare, may ultimately erode professional military identity and in turn the 'unique social responsibility that involves risk and danger.'[19]

*Chance (The Armed Forces)*. The tactical predictability of AI is unlikely to reduce strategic friction; though, the effects on 'tactical chance' may decrease despite unpredictable interactions.[20] Clausewitz highlighted the importance of adaptation and organisational learning in warfare. A key capability of AI is the ability to rapidly process data and update programs – this will be of benefit. Nevertheless, Clausewitz observed 'knowledge cannot be forcibly produced by an apparatus of scientific formulas and mechanics; it can only be gained through a talent for judgment, and by the application of accurate judgment to the observation of man and matter.'[21] Clausewitz, theorised that it was only the blend of the practical experience of war and study that would result in 'applied military judgement.' Future commanders who have AI to rely on, will likely be at an advantage as their tactical understanding of the battlespace will increase; nevertheless, there will always be a need for a 'general's instinct' – often crafted over decades of combat experience. Clausewitz did acknowledge commanders could gain talent 'through the medium of reflection, study and thought,'[22] however, the quality he valued most in a commander was combat experience. So whilst AI will be able to learn and adapt quicker than humans, this will be an unlikely substitute for seasoned training, professional military education and combat experience.

*Reason (Political Direction)*. Whilst inevitably humans need time to process information in order to inform decision-making, AI decisions will likely be instantaneous which has led to warnings about 'hyperwar.'[23] The speed at which decisions are taken by machines will render human reaction time pedestrian and policy lagging behind; thus potentially removing political direction from warfare – a fundamental of the nature of war.[24] Nevertheless, as long as humans remain responsible for directing war, programming machines and fielding Autonomous Weapons Systems (AWS), which they will likely do so as politicians are unlikely to cede control to a machine; war's elements namely violence, chance and reason will remain, as will fog and friction.[25] As Lawrence posits, 'both friction and 'the flash of the kingfisher' will remain fundamental to war.'[26]

### *Revolution in Military Affairs*

As evidenced, the Clausewitzian trinity offers a relevant analytic framework as we enter the age of autonomy. This era will blend the advances of the industrial revolution and the information age, creating developments in machine learning, deep-learning AI and fully autonomous systems.[27] Such a revolution would unquestionably change the ordering of forces who employ such technology. Potential changes could include a reduction in military numbers, old organisations made redundant/new ones formed, force structures recast and savings reinvested into Research and Development (R&D).[28]

Previous military revolutions have produced changes in the way wars are deterred, fought and resolved, and as a result have reduced the value of existing military power including weapons, platforms and doctrine.[29] Krepinevich, posits that RMA's consist of four elements; technological change, systems development, operational innovation, and organisational adaptation. With each element in itself being necessary, but not a sufficient condition to military effectiveness.[30] Whilst it should be noted, Krepinevich wrote in 1994 (in the context of overwhelming US success in the Gulf War and the significant contribution of precision weapons), this is noteworthy in the present day especially as the debate surrounding technological advancement and the changing nature of war is not new. As Hickman notes, history is littered with predications; the machine gun, tanks, aircraft were all supposed to change warfare radically.[31]

However, history teaches us that this is not the case. Often, and within a short-time, less technologically capable forces were able to mitigate such advances through tactical innovation and frequently seize victory against their more technologically adept adversaries.[32] This is reinforced by research that demonstrates technological advantage does not significantly increase the likelihood of a military victory – it is as predictive as a 'toss of a coin.'[33] Analysis by Biddle, has shown that of 16 wars between 1956 and 1992, the technologically superior side was victorious just eight times.[34] Despite the lethality that tanks, air power and machine guns introduced to the battlefield, 20th-century technological advances did not fundamentally alter the way modern armed forces fight. Rather, it was human innovation that rapidly matched technological disadvantage through exploitation of the battlefield.[35]

A cursory qualitative glance at the UK's recent campaigns (Iraq, Afghanistan, Libya) proves that overwhelming technological advantage does not translate into success. Accordingly, whilst AI will be a powerful weapon in the armoury of a state, it is unlikely that said state will then go onto enjoy absolute military dominance. Hickman suggests there are two reasons for this. First is the 'glacially paced change of recent memory', suggesting the battlefield of 2035 may not look too dissimilar to now; and second, is the history of specious forecasting over the past 40 years suggesting revolutionary change is 'just around the corner.'[36]

### *Evolutionary versus Revolutionary*

Given recent technological transition periods have been between ten to twenty years,[37] it is a convincing argument to suggest that periods between technological advances are evolutionary, rather than revolutionary. Nevertheless, it is not just the speed at which technological shifts occur, but rather the appreciation that the character of conflict has changed - requiring change in military organisations and doctrine.[38] Strategic military analysts such as Gray, concluded that their contemporary period was on the brink of a revolution in military affairs.[39] Nevertheless, a researcher of the exponential growth in battlefield lethality in 1950 would be just as likely to predict a RMA in 2020, as the scale of the curve is identical.[40] Consequently, despite being seemingly always on the cusp of an RMA, this advises that advances in lethality are not revolutionary, but rather evolutionary. Furthermore, in peacetime especially, it is unlikely existing technologies will be fully exploited by militaries; this is due to military institutions normally evolving rather than committing to revolutionary change.[41]

*Organisational Structure and Culture*. There are numerous factors preventing military institutions from committing to rapid radical change. Organisational culture and structures however, play a central role. Cohen highlights this point well by analysing the evolution of the US Army with General Motors. Comparing the organisational charts between the two institutions in 1950, they would look broadly similar; namely, a classic pyramid with small units reporting up to larger units. Fast-forward seventy years and an army corps looks similar, whereas General Motors have stripped out middle management and vastly reduced the social and functional distinction between the 'labour force' and management.[42] Compare this to the UK Armed Forces today, and those hierarchical structures still very much exist, as does the social and functional distinction between commissioned and non-commissioned. It is the 'radical revision' of these structures that will be the last indication of an RMA and the most difficult to implement.[43]

Nevertheless, humans are able to adapt. When air power first targeted massed forces, opponents did not simply stay paralysed and succumb to mass vaporisation. Instead commanders dispersed forces and minimised exposure to aerial attack weapons. Whilst the learning curve is often steep and costly, tactical innovators will often succeed.[44] If militaries focus too much on developing AI, there is a danger that battle-winning essentials could be overlooked.[45] All elements of strategy are competitive meaning the employment of forces, doctrine and tactical decision-making will be as important as ever to gain the decisive

edge. Regardless of who has the technological superiority, the likely victor will be those that develop strategic, operational and tactical innovators who then leverage the battlespace to their advantage – 'Human intelligence and creativity will win the next war, not technology.'[46] Blitzkrieg provides a compelling example of the consequences of failing to/successfully implementing the necessary organisational structures and culture.

*Blitzkrieg – A Case Study*. Whilst the concept of blitzkrieg is widely known as a German doctrinal approach, the raw conceptual elements can be traced back to 1918 and J.F.C. Fuller's plan for a final assault by the British Army into Germany. Nevertheless, it took a further two decades to put the British military strategist's theory into practice – by the Germans. Despite the Germans having a comparable number of tanks to the British and French in 1940, they succeeded not because of technological superiority, but due to organisation, operational concepts and command and control structures.[47] As Cohen highlights, 'military organizations that did not adapt in a rapidly changing, highly competitive environment have declined, often quite quickly.'[48] The British and French failed to adapt and suffered grievously.[49]

The creation of a panzer division reflected the requirements of the modern battlefield, building combined arms around the tank. In contrast, the Allies had armoured divisions consisting almost entirely of tanks. Not only did the Germans field engineers, infantry and air power with their tanks, they also bred a 'climate of command.'[50] As a US liaison officer in Germany highlighted in a 1930's report, 'the Germans point out, that often a Commander must make an important decision after only a few minutes [a fair decision on this basis] is much better than one wholly right but too late. They visualize rapidly changing situations in modern warfare and are gearing their command and staff operations accordingly.'[51] The examination of Blitzkrieg as a case study, demonstrates that intellectual innovation combined with organisational flexibility, provides a competitive advantage and a decisive strategic edge.

*Is this Revolution Different?* Historically, superiority on the battlefield has been determined by two conditions; quality and quantity. In traditional warfare, quantitative advantage was prized, but with technological breakthrough, numbers became less important and qualitative aspects became more relevant.[52] Nevertheless, one element that has endured throughout history is that all superpowers gained and retained hegemony through unmatched technological advancement.[53] Yet, with AI technology likely to be ubiquitous, the 'offset strategy' faced by many defence ministries may no longer be relevant as AI will be widely available to lone-terrorists and adversary states alike. Unlike exquisite technology such as the F-35, the ubiquitous nature of AI will not necessarily be able to offset adversarial strength. There are also other elements that distinguish AI from previous periods of weaponry development. Caton suggests that due to AI generating perception, cognition and action in weaponry, weapons will no longer be a means of warfare, but rather the driving force of warfare.[54] This may certainly be the case if humans cede control as 'predictable tasks are being performed, where reaction time is critical.'[55] Therefore, it is likely that some of the greatest benefits to come from AI are not AWS, but rather mundane everyday tasks where AI does not replace, but rather augments

human-decision making. Former US Deputy Secretary of Defense Robert Work made this exact point, 'Rapid advances in AI...are pointing towards new and more novel warfighting applications involving human-machine collaboration and combat teaming.'[56]

*Leveraging Technological Development*. Whilst the vast majority of military technological change derives from external source; occasionally it occurs internally. It was military R&D that facilitated the nuclear revolution, the early stages of space exploration and submarines.[57] Nevertheless, the majority of military technological change lies in the political and economic sphere.[58] The civil development of the railroad during the American Civil War, enabled the Union to transfer 25,000 troops, with artillery and logistics, over 1,100 miles from Virginia to Tennessee, in under twelve days.[59] The Interwar and Second World War years were dominated by states rapidly adapting civilian technology into military capability. There was then an interval during the Cold War which saw the rise of the defence industry. However, as Cohen wrote in 1996, just seven years after the fall of the Berlin Wall and the end of bi-polarity, he predicted the pendulum was beginning to shift back in favour of civil industry and indeed that economic strength will prove a great enabler to military power.[60] Whilst this is a compelling argument, the dawn of the autonomous era will not necessary need a strong state economy, but rather the ability to leverage the civilian AI technology sector and translate that into military power – after all, no one is going to have a monopoly on AI. It is up to humans to recognise and decide what the future characteristics of the battlefield will be, by employing the ever-expanding array of technological, operational, and organisational options.[61] To ignore this would risk strategic impotence.[62] Ultimately, it will be up to political leaders to link AI with strategy – and leverage the people, organisation, technology and process to gain a decisive edge – this will be expanded in Part Three.

The contemporary debate surrounding the extent to which RMA and AI will change warfare, is likely to endure, as this quote from the US's National Intelligence Council demonstrates, 'The nature of conflict is changing...with robotic systems.'[63] The US Army has also forecasted that technological revolutionary shifts 'may even challenge the very nature of warfare itself.'[64] Whilst a UK assessment noted 'the increased capability of robots is likely to change the face of warfare.'[65] Technological advances will change the character of warfare and do have the potential to impact the nature of war. Nevertheless, as long as humans remain responsible for directing war, programming machines and fielding forces, fog and friction will remain and so too will Clausewitz's enduring essence of war.

## Part Two

*The Balance of Power*. The study of Clausewitzian theory and past RMAs, have demonstrated that technological advantage is transient. There is no guarantee that technological leadership will be maintained in the battlespace. Furthermore, not all nations will follow the same developmental AI path; geostrategic disposition, strategic and economic position will lead to competitors taking different routes.[66] The case of Blitzkrieg also demonstrates that current technological advantage, does not translate into dictating the direction and pace

of future progress. In sum, western strategic technological-military dominance is far from guaranteed and there is convincing argument that AI will upset the balance of power in the international order.

The availability of AI will not provide a barrier to individual and state actors, as the 'cost of competition' is not likely to mirror that seen in previous RMAs, additionally the advantage of monopoly is likely to be shorter lived than ever. The use of AI could also undermine both conventional and strategic deterrence between states, by lowering the threshold of war.[67] Furthermore, the 'technological fog of war' could lead to a mismatch in planning and conduct given the speed and complexity of future operations; this could lead to a situation in which, 'militaries fail to take their political goals.'[68] Therefore as Singer wrote, it is a decision to 'embrace, technologies that make war safer, and...counter the trend that such technologies have to disengage us, to make war more acceptable or potentially more ubiquitous.'[69] So whilst AI has the potential to make the world a more dangerous place, it is the responsibility of people, military and politicians to ensure the 'most troubling features of the current revolution'[70] are controlled. Furthermore, a recent US Army War College study found, 'Human perceptions and the relative value of truth have increasingly become ripe territory for low risk/high impact manipulation of strategic outcomes.'[71] This convincingly suggests that actors with limited resource could effectively employ technology, such as AI, to achieve an asymmetric strategic effect. Correspondingly, as demonstrated in the recent publication of the UK's Intelligence and Security Committee's Russia report, state-on-state interference in electoral systems through disinformation[72] suggests the threshold of traditional forms of strategic control is lowering.

With the AI arms race firmly underway and a finite amount of resource, any increase in the UK's defence budget on AI would likely to lead to budgetary cuts from conventional forces - it is a zero-sum gain. As Matsumoto posits, this could result in the ill-preparedness of existing forces.[73] And, as Part One has demonstrated, technological advantage does not translate into guaranteed success. The winner of the AI race will need to; understand adversary capability, be fast enough to counter the adversary and have the economic resource to fund the capability.[74] If the UK fails to achieve these three necessary conditions, there is a danger of strategic impotence which will damage conventional power.[75] In an emerging multi-polar world, the UK needs well defined political goals that the military can follow. In a void of political direction, it is the nature of war that will result in defeat, rather than any adversary.[76]

*Great Power Competition*. The US, China and Russia are all modernising existing systems and weaponry by incorporating AI.[77] Additionally, the economic centre of gravity moving eastward[78] will likely disrupt the balance of power, threaten the liberal rules based order and challenge US political, economic and military dominance.[79]

*Russia*. In September 2017, Vladimir Putin professed (his now infamous) views on AI stating it was, 'the future, not only for Russia, but for all humankind' and the nation which, 'becomes the leader in this sphere, will become the ruler of the world'.[80] Russia is investing heavily in robotics

and AI, especially in the military arena, where investment is significant when compared to commercial efforts.[81] This, in comparison to the UK, US and China where AI development is largely emanating from commercial enterprise, will likely put Russia at a disadvantage given the dynamism of the US and Chinese innovative ecosystems.[82] Nevertheless, in 2012 Russia founded the Foundation for Advanced studies, largely in response to the US Defense Advanced Research Projects Agency (DARPA) which has taken the lead on AI including image recognition and human thought process.[83] As Putin made his 2017 speech, levels of state investment in AI technology stood at 700 million rubles (US$12.5 million). When compared to the US or China this is relatively low; however, Russia has been increasingly successful at leveraging private sector investment in recent years. AI investment was forecasted to be at 28 billion rubles (US$500 million) by 2020.[84] Given Russia's levels of investment in AI, it is not likely to single-handedly challenge US hegemon. However, Russia's increased use of hybrid warfare combined with AI technological advance, demonstrates how US conventional power will be increasingly challengeable[85] and UK interests could be threatened.

*China*. Two years ago, the UK's National Security and Capability Review stated 'The United States continues to be our single most important international partner,'[86] - it is therefore in the UK's national interest for the US to retain advantage over China. Furthermore, given NATO also remains the cornerstone of UK security posture,[87] NATO's Secretary-General Jens Stoltenberg, recent comments calling on the alliance to stand up to Beijing's 'bullying and coercion'[88] were pertinent. Given strategy is competitive and China is now challenging the US for primacy, it is important to examine China's surge in creating a 'Fog of Technology' that could rival US power.[89]

It was in 2017 that China launched the Generation Artificial Intelligence Development Plan (GAIDP) (新一代人工智能发 展规划) which headlined, 'AI has become a new focus of international competition. AI is a strategic technology that will lead in the future; the world's major developed countries are taking the development of AI as a major strategy to enhance national competitiveness and protect national security.'[90] Zhu and Long suggest the greatest risk to US power is the continuous development and application of AI weapons which could erode the foundation of strategic deterrence between China and the US – subsequently lowering the threshold for war.[91] Nevertheless, as with previous RMA's it should be noted that the US and China have varying strategic goals, access to different resources and different strategic cultures; therefore, any evolution in military AI is likely to take different routes.[92] Additionally, it is unclear whether China will be able to develop its capacity and strategy fast enough to challenge US conventional power.[93] Factors such as economic disruption as a result of COVID-19 and downturn in corporations linked to the Chinese state such as Huawei losing the UK 5G contract may all impact implementation – the most difficult element of strategy. Nevertheless, and in accordance with the GAIDP, China is emerging as a 'powerhouse in AI' and is seeking to become 'the world's premier AI innovation center.'[94] To achieve this China is currently investing in an AI industry of 1 trillion RMB (US$150 billion) by 2030.[95] Whilst this is an ambitious spending target, China is leveraging the dynamism of commercial enterprise wisely, whilst simultaneously synergising with national defence applications – resulting in a national

strategy of military-civil fusion.[96] It is this 'national team' ethos that will be so vital to China's progress. Companies such as Baidu, Alibaba and iFlytek[97] are developing dual-use technologies; suggesting a deep accord with the party-state, advancing the military-civil fusion strategy.[98] The People's Liberation Army (PLA) is capitalizing on these rapid advances.

Nevertheless, despite being one of the few nations to have an AI strategy that integrates political, economic and military elements, China still believes it is losing the AI battle to the US. It was AlphaGo's victory over Lee Sedol that was a catalyst for Chinese AI development, providing a 'Sputnik moment' for the Chinese military especially with regards to AI's capability to influence command and decision making.[99] The Chinese are right to be scrutinising US progress in AI. The US is well positioned and benefits from one of the world's best university systems and the most advanced AI researchers in academia.[100] This relationship between academia and commerce, forges the baseline of global US technological leadership. Meanwhile, the US military have declared that in the 2021 budget, US$841 million will be spent on AI (0.1% of the US$705 billion fiscal proposal).[101] However, this does fail to capture the AI integration costs throughout different weapons systems.[102] The Chinese military have been even less than transparent about AI strategic intentions, though it is clear they understand the importance of this RMA, which the PLA refer to as 'intelligentized warfare.'[103] However, an examination of this form of warfare suggests it is largely an extension of existing operational concepts; namely an information-centric approach. Whilst the US military are focussing effort on AWS, the Chinese are concentrating on the use of AI to dominate information systems and networks in an attempt to 'paralyse' an opponent's joint force – a systems confrontation approach.[104] The English-language translation[105] of China's 2019 Defense White Paper observes a change in modern warfare: 'War is evolving in form towards informationized warfare, and intelligent warfare is on the horizon.' However, a Chinese-language version is more revealing describing 'that the change is not about moving toward informationized warfare, it is about an evolution in informationized warfare.'[106] Regardless of the differences, what Western analysts should note is the Chinese are studying AI seriously, including how it will shape the character of war and from this analysis, doctrinal changes are likely.

### *Democracy versus Authoritarianism*

With a population nearing 1.4 billon, China enjoys the advantages of scale and can use entire cities as experimental grounds. In April 2020, Xi Jinping visited the 'smart city' of Hangzhou calling for more cities to become 'smarter,' to enhance city-wide management and security. However, as mentioned in Part One, this use of AI (as a control measure) could weaken public support and allow less democratic regimes to 'manipulate populations.'[107] Whilst the US can rely, to a certain extent, on companies such as Google and Amazon who have copious amounts of data, Chinese state control enables free and ready access to huge quantities of data, enabling them to generate machine learning algorithms. This is reinforced by state control of the internet, which enables a more efficient method to harvest data for algorithms when compared to the US.[108] Furthermore, autonomous weaponry is also confronting two major obstacles, first the vast economic costs needed for R&D, and second, ethical concerns.[109]

Project Maven provides an example of how ethical concerns within democratic states can thwart military progress.

*Project Maven – A Case Study*. In June 2018, Google cancelled a contract with the DOD as a result of thousands of Google employees signing a petition strongly opposing the partnership. If progressed, Project Maven would have supported algorithms that helped analysts to select military targets from video imagery.[110] The aim of the AI application was to increase the fidelity of battlefield information and in turn, increase military effectiveness and ultimately save lives.[111] Google pulling out of the contract is not an isolated incident. Amazon also recently refused to sell facial recognition software to the US police; this is a worrying trend for the US Government. US corporations such as Google, Facebook, Apple, Microsoft, and Amazon have driven technological innovation in the US, but they have also been the beneficiaries of a highly skilled and educated workforce comprised of thousands of US citizens. Indeed, many of the US's economic policies also favoured and accelerated the exponential growth of these tech-corporations.[112] Nevertheless, corporations are more than aware of the ethical concerns and public scepticism that associates with AI. As evidenced in leaked emails, by Dr. Fei-Fei Li, chief scientist for AI at Google Cloud, she advised her staff against mentioning 'AI' in relation to the Project Maven contract, referring to it as 'red meat to the media.'[113] When Google employees protested and asked their CEO to 'cancel [the] project immediately,' stating it would 'irreparably damage Google's brand,'[114] the DOD lost the strategic narrative. Commercial innovation will be vital to winning the AI war. Nevertheless, it seems democracies have some way to go to convince their citizens and corporations that AI will be vital for national security. Whilst the battle for the strategic narrative will be important in places with authoritarian regimes; the case study of Project Maven proves it is essential for democracies.

### *Control and Regulation*

Whilst there is concern about the rate at which adversaries are developing AI, the UK and allies should also be concerned with how they might use it. No international legal restrictions currently exist regarding the military application of AI, and it is unlikely China and Russia will be constrained by domestic concerns over ethics or morality. Accordingly, both states are developing military AI systems. This is unsurprising, given they view themselves as 'weaker militarily than the combined forces of NATO and its partner countries, and as such, have doctrinally declared that they will be seeking out any asymmetric advantage they can.'[115] Conversely, the UK's position on developing AWS is somewhat confused. At the Geneva UN Lethal AWS Conference 2019, the UK was amongst a group of states including Australia, Israel, Russia and the US, to speak against legal regulation for Lethal AWS.[116] Nevertheless, the MOD has also stated, 'The United Kingdom does not possess fully autonomous weapon systems and has no intention of developing them.'[117] This leaves the UK exposed as AI developments would likely mean an adversary could defeat the human-loop relationship by switching to fully autonomous systems, increasing reaction times - thereby defeating the more human system.[118] The UK is strategically communicating mixed messages in trying to prevent an international ban on one hand, whilst stating it has no intention to develop AWS on the other. The UK have

effectively ignited their own strategic constraints and made strategy more difficult than it needed to be; allowing adversaries to develop AWS whilst not doing so themselves.

Furthermore, unlike many conventional weapons that professional militaries use, AWS are likely to be widely available to states, corporations and individuals alike. Whilst states will have greater leverage over other entities, the extent to which this technology will be available for use is a cause for concern. A case in point being Ayoub Kara an Israeli politician who stated Israel is currently developing military robots as small as flies with nuclear capability.[119] As Horowitz posits, 'the sharper the competition, the greater the need...for a race to the bottom in AI safety.'[120] As competition increases between non-state actors and militaries alike, there is a risk that reliability and safety will be overlooked, heightening the potential for unreliable systems and accidents; this is especially the case if commercial and military sectors value 'first mover advantage.'[121] The promises of increased combat effectiveness, combined with reduced costs could prove to be seductive; nevertheless, some of the key benefits of AI are reliability, speed and accuracy, if corners were to be cut in Test & Evaluation (T&E) this could impact on both effectiveness, safety and value for money.

The balance between speed of development, procurement and ensuring value for money for taxpayers will be pivotal with AI. The UK Armed Forces have not always achieved the right balance. Throughout the Iraq and Afghanistan campaign, the British Army needed to procure equipment at short notice. They did this through urgent operational requirement (UOR) - defined as equipment bought due to the 'the identification of previously un-provisioned and emerging capability gaps because of current or imminent operations.'[122] Nevertheless, in subsequent evidence given to the Defence Select Committee, UOR was represented as, 'poor value for money...historically, within the defence sector, value only comes from well-planned work programmes.'[123] Additionally noting 'until the main equipment programme can be as agile, there will still remain coherency issues with running a UOR portfolio alongside the main, equipment programme.'[124] The speed at which AI is constantly developing is unlikely to tessellate with the current procurement practices of Defence Equipment and Support. An enhancement on capability delivery is needed – this will be explored in Part Three.

## Part Three

### *How is the UK Positioned – Current UK Strategy*

As discussed in Part Two, the US and China are leading the global race in AI by some margin. The UK's investment in AI is relatively low in comparison, with American spending outstripping the UK's by 50 times.[125] Conversely though, the UK ranks as one of Europe's leaders in AI development,[126] currently ahead of the EU-28 pack on AI Readiness.[127] A McKinsey report suggests this is because of relative strengths in science and policy leadership.[128] As the MOD Modernising Defence Programme report recently stated 'AI is a necessity, without which we risk losing our edge.'[129] It is therefore unsurprising that the UK has stated intentions to compete in AI given the impulse to prevail is 'entirely human and consists of twin desires: to avoid misery and to not be left behind.'[130] Subsequently, the UK has seen significant

investment in AI technology. In 2019 over £1 billion was committed to AI R&D,[131] a prudent investment, given gains in the AI global economy are predicted to be £12 trillion by 2030.[132]

Nevertheless, developing an AI industry is not easy or quick. To grow a successful industry multiple policy areas need to align to create successful conditions. These include: AI investments, building an AI talent pool, economic policies to mitigate displaced workers, establishing industry leadership and evaluating ethical and moral issues.[133] Therefore a successful approach is comprehensive and must encompass a variety of government departments, ranging from Education, Business, Energy and Industrial Strategy (BEIS), Digital Culture Media & Sports (DCMS). As Horowitz sensibly posits, the gap between the development of technology and the implementation of technology, is the strongest argument for a national approach to AI.[134] Accordingly, the UK has made significant progress in AI development. The Office for AI, a joint BEIS-DCMS organisation, was founded in 2018 and is responsible for overseeing implementation of the AI and Data Grand Challenge.[135] In the same year the UK government published its national AI strategy – the AI Sector Deal. The aim of the AI Sector Deal is to prepare the economy and society for AI development and provide the foundations to advance the UK's global position in AI technologies.[136]

The strategic narrative from the UK is consistent and is fervent in its support of AI, as the then Prime Minister laid out her ambition at the 2018 World Economic Forum, stating she wanted the UK to be, 'a world leader in AI, building on the success of British companies like Deepmind.'[137] Nevertheless, whilst the UK's strategy covers a wide range of AI societal impacts such as medicine, manufacturing and transport; at no point does the document mention Defence or military.[138] This exclusion of Defence from the national strategy is contrary to the MOD's own thinking on AI. The MOD's most recent *Global Strategic Trends* publication mentions AI no less than 72 times and states 'those who most effectively integrate the capabilities of machines and people, may derive decisive advantage.'[139] Subsequently, to make no mention of national security in a national strategy seems incongruous at best. Furthermore, the UK Government published 'A guide to using artificial intelligence in the public sector'[140] in 2019 and once again omitted any direction on how AI could be implemented by Defence or security agencies. Whilst the guide does provide generic advice on data and machine learning, there are no specifics on how the MOD could develop or implement AI in everyday tasks. This would have been useful, especially as the MOD does not have an 'AI literate' workforce. The MOD's Doctrine and Concepts Development Centre have produced a comprehensive and impressive Joint Concept Note – Human-Machine Teaming,[141] nevertheless, this is not a strategy. As stated in the Purpose and Aim of the document, it 'considers potential changes to the ways, as well as the means, with which we will fight,' but, 'is to guide coherent future force development and help frame Defence strategy and policy on automation and autonomy.'[142] This is an issue given there is currently no Defence strategy on AI. The MOD's own *Digital and Information Technology Strategy* admits there are 'unconnected systems' across defence, yet AI is only mentioned once, 'The CIO will provide the link for defence with…DCMS, interpreting central direction for defence regarding data

governance and AI exploitation, where appropriate.'[143] However, this does not mitigate that in 2020, there is no one consolidated strategy that brings together AI direction, ambition and resource for the security of the UK. The single services are developing their own projects,[144] however, there is not a coherent approach which would provide vital lessons as well as likely savings and efficiencies. Encouragingly, Defence Science and Technology Laboratory (DSTL) have established an AI Lab which works across DSTL's whole portfolio 'in the application of AI related technologies to Defence and Security challenges,'[145] nevertheless, this does not link to a MOD Head Office strategy.

In an anarchic international system, the UK is the sixth biggest economy in the world. Whilst strategy exists within the sphere of politics, economics and society, the UK still has relative power and has the ability to shape the future of war. But to do so requires strategic thought. The UK needs to ensure it has the right people, has the correct organisational structures, technology and processes in place to advance development and place the UK as a leading AI state.

*People and Organisation*. The investment battle in the forthcoming Integrated Review will be opportunity cost, there will have to be a loser. If AI sees significant investment, this will likely be at the expense of conventional capability or human resource. The MOD would need to redirect resource into AI R&D and train and sustain an AI capable talent pool. The human resource skills required to develop AI systems are rare. Newly qualified PhD's, in the relevant field, can often command starting salaries of $300,000 to $500,000 a year.[146] This remuneration package suggests the MOD will be unable to compete with industry to attract talent. Nevertheless, countries that have strong education domestically, and immigration policies that can attract talent, have an advantage over others. The UK is relatively well positioned and has a large pool of AI talent, including attracting skills from overseas,[147] though Brexit may have an adverse impact on this. Lithuania is one country whose dynamic national AI strategy created 'start-up visas' which have facilitated innovators from abroad to settle and work in the country.[148] Despite the threat of Brexit, the UK has the second-largest number of software developers in Europe, comprising 15% of the total.[149] Nevertheless, for the UK military, it is not just about software developers. As concluded in Part One, often force employment, doctrine and tactics can overcome technological advantage. Indeed, too much focus on software could lead to blind spots elsewhere, including neglecting conventional capability that once abandoned, can be all but impossible to recapitalise. It is worth noting that just as the nuclear revolution did not render conventional weapons obsolete; the AI revolution will not render, 'guerrilla tactics, terrorism, or weapons of mass destruction obsolete'[150] either.Therefore the MOD needs to ensure investment in its people. As highlighted over a decade previously, 'we must get smart people more engaged; not as corrosive critics, but as constructive contributors. This will develop the habit of thinking strategically…and tap into a deeper pool of strategic ideas.'[151] Furthermore, and as history has taught us, 'the best bet for future victory is developing the tactical, operational, and strategic innovators who will leverage battlespace conditions to achieve victory, regardless of

the tech balance. Human intelligence and creativity will win the next war, not technology.'[152] This will also require a transformation in organisational structures across MOD; strong strategic leadership and accountability will be vital.[153] As Porter convincingly argues, classical realism – especially Clausewitz and Morgenthau is a 'valuable resource' today for 'handling uncertainty more reflexively...[whilst] governments...should insure against the likelihood of predictive failure by developing the intellectual capability to react to the unknown.'[154]

At the national level, education to develop AI talent will also be vital and is a central tenet of the AI Sector Deal.[155] The Office of AI is establishing up to 20 AI Centres of Doctoral Training in UK universities.[156] However, China is also rapidly sustaining and growing home-grown capability, with 35 universities now teaching AI-related degrees – and over 100 degrees that combine AI and other subjects.[157] The UK simply cannot compete with the scale and rate of change that is taking place in the Chinese university system and will likely have to rely on international collaboration if it is to gain a strategic edge. At present, the MOD will have to rely on the AI Sector Deal to build domestic AI capability.

*Doctrine*. In his influential book *Wired for War*, Singer surveyed US military officers and found that they 'identified developing a strategy and doctrine [for using robots in combat] as the third least important aspect to figure out.'[158] Whilst this was not a study on the UK armed forces, Singer's findings suggest a more informed approach is needed. As demonstrated by the Blitzkrieg case study, doctrine is an essential element for a fighting force if it is to achieve its full potential. Whilst the Joint Concept Note on *Human-Machine Teaming* provides limited ways and means – it is not doctrine; nor does it expand on the use of AWS in-depth. Without renewed conceptual effort, AI may become the new Blitzkrieg, as Ader convincingly states, 'while R&D continues apace, rhetoric and doctrine has calcified. Major powers are conceptualising automation to augment and support existing force structures – not exploring how it might change the character of war. This is a mistake.'[159]

Whilst UK and NATO doctrine are widely published, AI is likely to change set assumptions. Wargaming is one tool that allows a diverse set of people to test novel capabilities in a safe environment. This forum would provide cooperation with military, civilian and commercial partners to test AI platforms whilst maintaining control over technical parameters.[160] Nevertheless, greater investment in multi-domain virtual training is needed.[161] Therefore, whilst the UK must develop AI specific doctrine, it must also review how AI will impact current doctrinal assumptions. To ignore this would risk exposure to adversaries. As the 2018 US National Defense Strategy stated, 'competitive military advantage has been eroding' and, if unaddressed, will allow adversaries to exploit these weaknesses to their own advantages.[162] This is important to note given the quantitative element (number of ships, tanks, aircraft) measurement of military effectiveness is more in question than ever. Platforms will become less important as munitions and information will result in increased difficulty for analysts to assess the military balance of adversaries.[163]

*Technology*. On the cover of the Economist in May 2017, was an article stating that data had replaced oil as 'The World's Most Valuable Resource.'[164] Whilst this is a controversial claim that has yet to be proven, states that are able to identify, acquire and apply data that is militarily important will be well positioned to develop high-performance AI systems.[165] However, there are worrying indicators that the UK is not maintaining a firm onshore tech-industry which will be vital to both national prosperity and security. Non-EU companies are acquiring AI technological firms, as demonstrated when a Chinese government-backed private equity firm, purchased Imagination Technologies, a UK semiconductor firm for £550 million in 2017.[166] Since the turn of the century, the UK's involvement in conflicts has proved unpopular. Risk appetite amongst generals and politicians have been called into question; this is part of the reason as to why AI technology is so attractive.[167] Moreover, with exquisite conventional technologies such as the F-22 costing $68,346 an hour to produce,[168] AI will be an attractive option for both treasuries and militaries alike, especially as the global economy takes a downturn due to COVID-19. Strategy is inherently competitive and with a recent UK economic recession, resource is evermore precious. As a consequence, the MOD needs a strategy that maximises the benefits of AI whilst minimising threat as the UK enters the Integrated Review.

*Process and Policy*. States must make regulatory choices regarding the use of AI, and balance trade-offs such as privacy versus efficiency. The AI Sector Deal is a solid foundation covering economic and societal development, however, as argued, the UK government has yet to state ambition or constraints on the use of AI by the UK armed forces. Until this happens the implications for national power will not be answered.[169] Nevertheless, even if policymakers were to remove all constraints, this would not guarantee effective and efficient implementation or regulate use.[170] As detailed in Part Two, it is likely democracies will face more constraints when compared to more autocratic regimes, therefore if UK policy was to be fixed as always having 'a man in the loop,' having an AI system that could do the Observe, Orient, Decide but then have to wait for a human to Act would give capable adversaries an advantage. This is why policy direction is vital; likewise, that policy needs to be accountable.

*Acquisition and Procurement*. For the UK government to harness the most out of AI for national security purposes, leveraging private sector innovation is needed. Though narrowing the AI gap inside and outside government will be a challenge,[171] China's military-civilian fusion strategy, is an example of how this can be achieved. There is also potential for strong economic gains through the leveraging of small and medium enterprise; in turn supporting Defence's prosperity agenda.[172] As former Undersecretary of Defense for Acquisition, Technology, and Logistics Frank Kendall states, 'Automation and AI are one of the areas where the commercial developments dwarf the military investments in R&D.'[173] Singapore is one state that is leading the South East Asia region in AI investments, having created a technology hub to attract significant investment.[174] The pace of change in commercial development requires agile capability delivery, or a 'fail fast' approach. Whilst there are elements of the MOD currently

practicing this conceptual and cultural shift in acquisition,[175] such innovation is isolated rather than the norm. Cook suggests that 'MOD...risks mission failure if agility is not injected into procurement and operating models rapidly.'[176] This is a compelling argument, especially as highlighted in Part 2, MOD procurement practices are often criticised. A conceptual and cultural shift will be needed across domains and headquarters. Procurement practices will have to work with onshore small tech start-ups, up to the likes of Boeing. This will require trained and capable staff that do not settle for 'nostalgia and comfort...to lull the [UK] into greater disadvantages against adversaries.'[177] Huntington correctly suggests that everyone involved in the human-machine interface, from politicians, commanders to watchkeepers will need to become more AI literate 'if they are to remain effective managers of violence.'[178] As Custons posits, 'successful commanders all [have] the ability to navigate government bureaucracy and understand acquisition processes.'[179] Whilst the lessons are Project Maven should be firmly in policymakers' minds, the UK does have levers to incentivise AI commercial partnership. These could include trade policies, infrastructure investment, and other economic stimuli.[180] Building trust and shedding bureaucratic constraints between the MOD and private enterprise is a necessary condition to facilitate AI into UK national security capability.[181] The status quo needs to be upset and the strategic narrative needs to stress that UK industry's success, relies on the national security of the UK.[182]

*Assurance*. Whilst the speed and agility of AI acquisition is important, so too, as highlighted in Part 2, is the assurance and safety of such systems. The MOD will likely have to manage more stakeholders and ensure the product it receives is both operationally effective as well as safe. The DOD have established strict test parameters for AWS and all systems must be certified by the Director of Operational T&E.[183] If the MOD is to move to an agile acquisition process, it will have to develop the capacity to 'test safe and controllable autonomous systems, especially those that fire weapons.'[184] Implementing an assurance organisation whilst understanding acquisition and bureaucracy[185] will be an enormous, but necessary challenge for UK Defence.

*Operating within Alliances and Interoperability*. The 1999 NATO-led war over Kosovo, provides a good example of issues that arise when alliance states have differing levels of capability. Many NATO states lacked precision-guided munitions (PGMs) and therefore many operational targets fell to a small number of states;[186] AI has the potential to increase such 'burden-sharing' tensions.[187] Whilst AI will likely increase military efficiency, there are significant issues that may arise whilst working in a multinational environment such as interoperability, information sharing and the speed of decision-making[188] which may heighten mistrust within a coalition.[189] Nevertheless, NATO has overcome interoperability challenges in the past and is taking action to address the challenges ahead. Several NATO allies have called for increased collaboration and Germany's 2019 National AI Strategy advocates 'work[ing] with the nations leading in this field … to conduct joint bilateral and/or multilateral R&D activities on the development and use of AI.'[190] Additionally NATO's Allied Command Transformation have implemented workshops recently 'to improve awareness and understanding of autonomous systems,

promote interoperability and provide guidance for the development of, use of, and defence against, autonomous systems.'[191]

Whilst AI alliance scenarios have yet to be explored in any great depth by militaries and scholars alike, there are existing alliance studies from the likes of Walt and McCalla that could inform potential challenges in the next RMA. This paper has not explored AI and alliances in depth, nevertheless, it is noteworthy given the likelihood of the UK participating in multilateral operations in the future is significantly higher than operating unilaterally. The UK should encourage NATO to develop policies and doctrine that streamline decision-making and data sharing, whilst mitigating procedural and technical gaps to bolster defences against adversaries.[192]

## Conclusion

While AI's potential in military application remains to be seen, recognition of the impact to the UK's society, economy and national security should be noted. Deciding and managing AI's rise and development is essential to prevent strategic impotence. This paper began by using Clausewitz as a theoretical framework and studied previous RMAs to establish the extent to which the nature of war would be changed by AI. It then went on to critically analyse some of the challenges and strategic variables that face the UK such as, the balance of power and international actors, regime type and control and regulation. Part Three summarised the UK's current strategy and approach to AI and progressed to prioritise 3 elements, namely, People and Organisation, Technology and Process and Policy. Whilst the future cannot be predicted, as long as humans remain responsible for directing war and programming and fielding machines; war's nature is likely to continue to be defined by violence, chance and reason. Fog and friction may dissipate at the various levels of warfare but will not be eliminated entirely. Clausewitz is as relevant today as ever. Analysis of previous RMAs, demonstrated that although technological advantage is a necessary condition, it is not sufficient to claim strategic success. Rather an adaptation of process, organisational structure and culture is needed to gain success. To ensure the UK maximises AI's contribution to national security and can compete in the international strategic environment, a comprehensive approach is needed. This strategic approach should be underpinned by strong leadership and communication. Furthermore, exploiting the civilian technology sector for military application will be vital, as well as agile acquisition and regulation. In sum, the MOD needs an AI strategy. A strategy would enhance the spectrum of Defence operations and would allow single services and allies to collaborate; enabling efficiencies and progress. Perhaps most significantly, an AI strategy would go some way to gaining a strategic decisive edge, by balancing risk of overestimating AI's potential to the cost and detriment of conventional force.

## Notes

[1] Vincent, 'Putin says the nation that leads in AI will be the ruler of the world.'
[2] Ankerson, 'Melancholic and Fascinated: Artificial Intelligence, Authentic Humanity, and the Future of War.'

[3] Villacres and Bassford, 'Reclaiming the Clausewitzian Trinity.'
[4] Ankerson, 'Melancholic and Fascinated: Artificial Intelligence, Authentic Humanity, and the Future of War.'
[5] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 23.
[6] Gray, *Modern strategy*, 362.
[7] Clausewitz, *On War*, 593.
[8] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 23.
[9] Owens and Offley, *Lifting the fog of war*, 9.
[10] Williamson, *America and the Future of War: The Past as Prologue*, 34-35.
[11] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 24.
[12] Echevarria, 'Globalization and the Clausewitzian Nature of War,' 318.
[13] Clausewitz, *On War*, 89.
[14] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 25.
[15] Beyerchen, 'Clausewitz, nonlinearity, and the unpredictability of war,' 87.
[16] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 25.
[17] Kania, 'China's artificial intelligence revolution.'
[18] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 27.
[19] Walsh, 'The effectiveness of drone strikes in counterinsurgency and counterterrorism campaigns,' 53.
[20] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 27.
[21] Clausewitz, *On War*, 97.
[22] Clausewitz, *On War*, 146.
[23] Allen and Husain. 'On hyperwar,' 31.
[24] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 29.
[25] Watts, 'Clausewitzian friction and future war,' 64.
[26] Lawrence, *Seven pillars of wisdom*, 193.
[27] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 20.
[28] Cohen, 'A revolution in warfare,' 37.
[29] Krepinevich, 'Cavalry to computer: The pattern of military revolutions,' 30.
[30] Ibid.
[31] Clifford, 'AI Will Change War, But Not in the Way You Think.'
[32] Hickman, 'The Future of Warfare Will Continue to Be Human.'
[33] Biddle, *Military power: Explaining victory and defeat in modern battle*, 21.
[34] Ibid.
[35] Biddle, *Military power: Explaining victory and defeat in modern battle*, 22.
[36] Hickman, 'The Future of Warfare Will Continue to Be Human.'
[37] Krepinevich, 'Cavalry to computer: The pattern of military revolutions,' 30.
[38] Ibid.
[39] Gray, '*Strategy for chaos: Revolutions in military affairs and the evidence of history*,' 17.
[40] Hickman, 'The Future of Warfare Will Continue to Be Human.'
[41] Cohen, 'A revolution in warfare,' 52.
[42] Cohen, 'A revolution in warfare,' 48.

[43] Ibid.
[44] Hickman, 'The Future of Warfare Will Continue to Be Human.'
[45] Biddle, *Military power: Explaining victory and defeat in modern battle*, 207.
[46] Hickman, 'The Future of Warfare Will Continue to Be Human.'
[47] Cohen, 'A revolution in warfare," 46.
[48] Krepinevich, 'Cavalry to computer: The pattern of military revolutions,' 30.
[49] Ibid, 36.
[50] Martinage, 'Toward a new offset strategy,' 15.
[51] Wedemeyer, 'Memorandum: German General Staff School Report,' 12.
[52] Khaqan. 'Artificial Intelligence and the Changing Nature of Warfare,' 66.
[53] Ibid, 71.
[54] Caton, 'Autonomous weapon systems: A brief survey of developmental, operational, legal, and ethical issues,' 17.
[55] Work and Brimley, 'Preparing for war in the robotic age,' 24.
[56] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 22.
[57] Ibid.
[58] Cohen, 'A revolution in warfare,' 39.
[59] Cohen, 'A revolution in warfare,' 42.
[60] Ibid, 51.
[61] Fitzsimonds, 'The Coming Military Revolution: Opportunities and Risks,' 32.
[62] Matsumoto, 'Defeating A Super Power: Challenges That Can Emerge Against American Conventional Warfare in an Age of Fog of Technology,' 19.
[63] National Intelligence Council, 'Global Trends: Paradox of Progress.'
[64] US Army Training and Doctrine Command, 'The Operational Environment and the Changing Character of Future Warfare,' 6.
[65] MOD, 'Strategic Trends Programme: Global Strategic Trends—Out to 2045,' 67.
[66] Krepinevich, 'Cavalry to computer: The pattern of military revolutions,' 41.
[67] Zhu and Long, 'How will artificial intelligence impact Sino–US relations?' 142.
[68] Matsumoto, 'Defeating A Super Power: Challenges That Can Emerge Against American Conventional Warfare in an Age of Fog of Technology,' 19.
[69] Singer, *Wired for War*, 337-338.
[70] Cohen, 'A revolution in warfare,' 53.
[71] Freier, 'Strategic Insights: Speed Kills, Enter an Age of Unbridled Hyperconnectivity.'
[72] Intelligence and Security Committee of Parliament, Russia Report, 13.
[73] Matsumoto, 'Defeating A Super Power: Challenges That Can Emerge Against American Conventional Warfare in an Age of Fog of Technology,' 14.
[74] Fitzsimonds, 'The Coming Military Revolution: Opportunities and Risks,' 35.
[75] Hoadley and Lucas, Artificial Intelligence and National Security, 36.
[76] Matsumoto, 'Defeating A Super Power: Challenges That Can Emerge Against American Conventional Warfare in an Age of Fog of Technology,' 19.
[77] Khaqan. 'Artificial Intelligence and the Changing Nature of Warfare,' 67.
[78] MOD, 'Strategic Trends Programme: Global Strategic Trends—Out to 2045,' 103.

[79] Horowitz, 'Artificial Intelligence, International Competition, and the Balance of Power,' 37.
[80] Vincent, 'Putin says the nation that leads in AI 'will be the ruler of the world.'
[81] Ibid.
[82] Horowitz et al, '*Strategic competition in an era of artificial intelligence*,' 15.
[83] Ibid.
[84] Bendett, 'Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems.'
[85] Matsumoto, 'Defeating A Super Power: Challenges That Can Emerge Against American Conventional Warfare in an Age of Fog of Technology,' 19.
[86] HM Government, 'National Security Capability Review.'
[87] Ibid.
[88] Speranza, 'China Is NATO's New Problem.'
[89] Matsumoto, 'Defeating A Super Power: Challenges That Can Emerge Against American Conventional Warfare in an Age of Fog of Technology,' 11.
[90] Allen, 'Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security,' 4.
[91] Zhu and Long, 'How will artificial intelligence impact Sino–US relations?' 150.
[92] Krepinevich, 'Cavalry to computer: The pattern of military revolutions,' 40.
[93] Matsumoto, 'Defeating A Super Power: Challenges That Can Emerge Against American Conventional Warfare in an Age of Fog of Technology,' 17.
[94] Horowitz et al, '*Strategic competition in an era of artificial intelligence*,' 12.
[95] Ibid.
[96] Ibid.
[97] Yi-Zheng, 'China, the Party-Corporate Complex.'
[98] Hoffman, 'The Communist Party's autonomic approach to managing state security,' 12.
[99] China Military Science, 'A Summary of the Workshop on AlphaGo.'
[100] Kania, 'Battlefield Singularity: AI, Military Revolution and China's Future Military Power,' 21.
[101] Dahm, 'Chinese Debates on the Military Utility of Artificial Intelligence.'
[102] Ibid.
[103] Ibid.
[104] Engstrom, '*Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*,' 16.
[105] Li, 'China's National Defense in the New Era,' Ministry of National Defense.
[106] Dahm, 'Chinese Debates on the Military Utility of Artificial Intelligence.'
[107] Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?,' 30.
[108] Horowitz et al, '*Strategic competition in an era of artificial intelligence*,' 13.
[109] Spiegeleire et al, 'Artificial Intelligence and The Future of Defense,' 75.
[110] Wakabayashi and Shane, 'Google will not renew Pentagon contract that upset employees.'
[111] Clifford, 'AI Will Change War, But Not in the Way You Think.'
[112] Shane et al, 'How a Pentagon contract became an identity crisis for Google.'
[113] Ibid.
[114] Shane and Wakabayashi, '"The Business of War": Google employees protest work for the

Pentagon.'
[115] Defence-In-Depth, 'One to Ponder: The UK's Ethical Stance on the Use of AI in Weapons Systems.'
[116] Gayle, 'UK, US and Russia among those opposing killer robot ban.'
[117] Ibid.
[118] Ankerson, 'Melancholic and Fascinated: Artificial Intelligence, Authentic Humanity, and the Future of War.'
[119] Khaqan. 'Artificial Intelligence and the Changing Nature of Warfare,' 70.
[120] Horowitz et al, '*Strategic competition in an era of artificial intelligence*,' 9.
[121] Ibid.
[122] HM Government, 'The EU Defence and Security Public Contracts Regulations (DSPCR) 2011.'
[123] UK Parliament, 'House of Commons - Defence Acquisition - Defence Committee.'
[124] UK Parliament, 'House of Commons - Defence Acquisition - Defence Committee.'
[125] McKinsey & Company UK and Ireland, 'Artificial Intelligence in the United Kingdom: Prospects and Challenges.'
[126] Bughin et al, 'Notes from the AI frontier: Modeling the impact of AI on the world economy.'
[127] McKinsey & Company UK and Ireland, 'Artificial Intelligence in the United Kingdom: Prospects and Challenges.'
[128] Ibid.
[129] Ministry of Defence, Mobilising, Modernising & Transforming Defence.
[130] Ankerson, 'Melancholic and Fascinated: Artificial Intelligence, Authentic Humanity, and the Future of War.'
[131] Ankerson, 'Melancholic and Fascinated: Artificial Intelligence, Authentic Humanity, and the Future of War.'
[132] PricewaterhouseCoopers, 'PwC's Global Artificial Intelligence Study: Sizing the Prize.'
[133] Horowitz et al, '*Strategic competition in an era of artificial intelligence*,' 10.
[134] Ibid.
[135] HM Government, 'Office for Artificial Intelligence, About Us.'
[136] HM Government, 'AI Sector Deal.'
[137] World Economic Forum, 'Theresa May's Davos Address in Full.'
[138] HM Government, 'AI Sector Deal.'
[139] UK MOD, 'Strategic Trends Programme: Global Strategic Trends—Out to 2045,' 145.
[140] Government Digital Service, 'A Guide to Using Artificial Intelligence in the Public Sector.'
[141] HM Government, 'JCN(1/18) Human-Machine Teaming.'
[142] Ibid, v.
[143] HM Government, 'Digital and Information Technologies Strategy.'
[144] HM Government, 'Revolutionary Artificial Intelligence Warship Contracts Announced.'
[145] HM Government, 'The Dstl Biscuit Book Artificial Intelligence.'
[146] Metz, 'Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent.'
[147] McKinsey & Company UK and Ireland, 'Artificial Intelligence in the United Kingdom: Prospects and Challenges.'
[148] Castro et al, 'Who is winning the AI race: China, the EU or the United States,' 55.

[149] McKinsey & Company UK and Ireland, 'Artificial Intelligence in the United Kingdom: Prospects and Challenges.'
[150] Cohen, 'A revolution in warfare,' 50.
[151] Newton et al, 'Reclaiming the art of British strategic thinking.'
[152] Hickman, 'The Future of Warfare Will Continue to Be Human.'
[153] Robertson and Robertson, 'Three Steps the UK's Ministry of Defence Can Take to Ensure It Makes the Most of Artificial Intelligence and Automation.'
[154] Porter, 'Taking uncertainty seriously: Classical realism and national security,' 239.
[155] HM Government, 'AI Sector Deal.'
[156] Shead, 'UK Government to Fund AI University Courses with £115m.'
[157] Bughin et al, 'Notes from the AI frontier: Modeling the impact of AI on the world economy.'
[158] Singer, *Wired for War*, 210.
[159] Ader, 'Are Automated Weapons the next Tank?.'
[160] Ibid.
[161] Hickman, 'The Future of Warfare Will Continue to Be Human.'
[162] Cohen et al, 'Peering into the Crystal Ball: Holistically Assessing the Future of Warfare.'
[163] Cohen, 'A revolution in warfare,' 53.
[164] The Economist, 'The world's most valuable resource is no longer oil, but data.'
[165] Horowitz et al, '*Strategic competition in an era of artificial intelligence*,' 4.
[166] CrunchBase, 'ARM.'
[167] Ankerson, 'Melancholic and Fascinated: Artificial Intelligence, Authentic Humanity, and the Future of War.'
[168] Spiegeleire et al, 'Artificial Intelligence and The Future of Defense,' 46.
[169] Metz, 'Google, Facebook, and Microsoft Are Remaking Themselves Around AI.'
[170] Horowitz et al, '*Strategic competition in an era of artificial intelligence*,' 11.
[171] Ibid, 17.
[172] Dunne, 'Growing the Contribution of Defence to UK Prosperity.'
[173] Scharre, *Army of none: Autonomous weapons and the future of war*, 91.
[174] Chitturu et al., 'Artificial Intelligence and Southeast Asia's Future,' 12.
[175] Royal Air Force, Rapid Capability Office.
[176] Cook, 'The Humble Task of Implementation is the Key to AI Dominance.'
[177] Ibid.
[178] Huntington, *The soldier and the state: The theory and politics of civil–military relations*, 112.
[179] Custons, 'Commanders Need to Know Innovative Acquisition.'
[180] Clifford, 'AI Will Change War, But Not in the Way You Think.'
[181] Custons, 'Commanders Need to Know Innovative Acquisition.'
[182] Ibid.
[183] US Department of Defense, 'Unmanned systems integrated roadmap FY2011-2036, 2015,' 87.
[184] Cummings, 'Artificial intelligence and the future of warfare,' 2.
[185] Cook, 'The Humble Task of Implementation is the Key to AI Dominance.'
[186] Larson et al, '*Interoperability of us and nato allied air forces: Supporting data and case studies*.'
[187] Lin-Greenberg, 'Allies and Artificial Intelligence: Obstacles to Operations and Decision-

Making.'
[188] Hartley, 'NATO, Standardisation and Nationalism: An Economist's View,' 57.
[189] Lin-Greenberg, 'Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making.'
[190] German Federal Government, 'Nationale Strategie Für Künstliche Intelligenz [AI Strategy].'
[191] Kuptel and Williams. 'Policy Guidance: Autonomy in Defence Systems,' 5.
[192] Firth, N, 'DeepMind's AI Has Used Teamwork to Beat Humans at a First-Person Shooter.'

Article

# Strategic Competition to Security Dilemma – The Language and Narrative of Space and Why it Matters

By Wing Commander Sas Duffin

**Biography:** Wing Commander Sas Duffin joined the Royal Air Force in 2005 as a Personnel Support Officer, prior to changing branch to Air Operations in 2018 to work within Space Operations. Having served in a variety of theatres including the Middle East, Afghanistan, Cyprus and Germany she completed the Advanced Command and Staff College in July 2021. Selected as a Space Fellow in 2022, her research considers space alliances and behaviours through the frame of international relations theories. She has been employed as Branch Head Enablement for the NATO Space Division in Ramstein, Germany since October 2022, and is a Women in Defence mentor for the 2022-23 programme.

**Abstract:** It was nearly 80 years ago that the first human made object, a V2 rocket, was launched into space. In the decades since, what started as a space race between two nation states has become an environment that is described as both a global commons and a war-fighting domain. Two space faring nations have become many, while an individual entrepreneur now owns more of the satellites that orbit the earth than any of the multiple nation states. The language and narrative of space has evolved in that time too. This essay considers how that language has evolved over the decades; how various actors promote their space narratives; the conflict not only in the use of space but also in the language of space, and what that might mean for the space domain and whether levels of strategic competition and misunderstood narratives could lead to security dilemmas between space actors in the future.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

## Introduction

> *'We think and behave not only because of who we are and what we believe we are, but also because of where we find ourselves, not necessarily by our own volition politically, morally and strategically.'*[1]
>
> Colin S. Gray

Outer space, the night sky and the planets have fascinated the human race for millennia. For centuries, although out of reach physically, it was utilised by mankind to understand anything from timings for harvests, celestial navigation, and the stories of Gods long gone.[2] It represented an aspirational domain for humanity; a place of infinite possibility. Yet when the novel *From Earth to the Moon* was published in 1889, it spoke of the fictional American conquest of the moon and adding it to the 'thirty-six States that compose this great Union,'[3] suggesting a desire for ownership of something outside of Earth's bounds even before much was known of the practicalities of getting there. Eighty years before humanity actually landed on the moon, science fiction of the time wrote of the wonder, excitement and opportunity of all that space could offer, yet it also focused on the proposed ownership of something outside this world. There was, it seemed, an inherent belief that space and the universe provided another area for mankind to explore, stake ownership of and mine for resources: and where there are resources, there is competition.

The space era of the 1950s and 1960s was a two horse race between the United States of America and the Soviet Union.[4] Competition and national pride drove development and achievement for both spacefaring nations, but it also saw the creation of some of the first space related treaties: the sentiment at that time (aided by the desire to maintain the status quo between two nations with nuclear capability) saw space as a global commons; somewhere that could be of benefit to all humanity. While there was little space discourse openly available at the time as so much of it was shrouded in secrecy and military classifications, the key events of the 'first time' achievements were front page news and on televisions around the world. The lack of transparency contributed towards the divide between the primary communist and democratic nation states, creating a level of political competition, rhetoric and a 'win at all costs' approach to space that created much of the mistrust and strategic behaviours between the US and Russia that remains today.[5] In the early decades of the 21st century, the number of players with an interest in operating in and maximising the benefits of accessing space has increased considerably. When considering the various narratives that each of those parties has brought to the space discussions, it is clear that many aspects of the '… political power of ideology and nationalism'[6] has translated from Earth to space. Given the additional parties with the desire to access or maintain access to space, and the currently limited impact of internationally accepted treaties regards behaviours in space, it is of little surprise that there are increased levels of strategic competition within the domain as each player works to understand or create their role within. Those increased tensions between spacefaring nations 'such as the US, Russia, China, Iran and North Korea pose security threats,' according to Dawson.[7] In addition, Lonsdale and Kane note that there are critical regions within space that are already

overcrowded with satellites and space debris, suggesting there is potential for 'conflict over the right to launch new satellites into them.'[8] As yet, however, 'battles beyond the atmosphere remain science fiction,'[9] and the space domain has remained relatively free from any potential security dilemmas spilling over into conflict. In respect of this paper, a security dilemma is defined as being when 'two or more states are drawn into conflict even though none of the states actually desires conflict.'[10] The challenge for the space domain in particular is that any conflict[11] could result 'not from the actual intentions and capabilities of a particular actor,[12] but rather from the uncertainty …'[13] That uncertainty could come from the language and narrative that a particular actor uses regards the space domain and any assets it may have.

As a result of the significant growth and reliance on space enabled technology, there has been an increase in the number of potential space powers and influencers within the last thirty years. This paper will therefore use the International Relations (IR) approach of constructivism, 'an approach to interpretive understanding,'[14] to ascertain whether space remains a global common for all or if it has become an area that is increasingly susceptible to becoming a security dilemma, via increased strategic competition, for all concerned. While IR theory will be a light touch throughout the essay, it will be highlighted as required, though as Kubalkova notes, 'different styles of constructivism fasten on different social phenomena, for example, language, rules, norms and structures.'[15] It is the varying examples of this, via the consideration of actors' language, culture and narrative, that will show how personal or national perspectives on space, can be constructed.

The key question behind this paper is concerned with how space actors; nations, leaders, industry, military forces or individuals, communicate about space and what messages, intended or otherwise, that might send to an audience regards an actor's intent towards space. In considering the language and narrative in popular use, the paper will consider the potential intent behind any message and whether the use of space by that entity is from the perspective of benefitting humanity (a global commons), for commercial competition, or security driven factors (strategic competition). The research will consider whether those narratives have changed since the beginning of the space race; who the key actors are within space today and how that differs from the early 1950s; whether those actors are working together as alliances and how that contributes towards international relations. Finally, it will consider whether space is still thought of as a global commons, or an area of strategic competition that is at risk of causing a security dilemma between some or all space actors. The paper will also discuss where the UK could position itself for a role within space, primarily from the perspective of defence.

This paper is broken down to five parts and will use discourse and content analysis from space and international relations academia; from national space strategies and the ensuing defence space strategies (where they exist); from space and security industry reports; and, from news stories and social media to consider the narrative of space. Part One will consider the space paradox and whether it is a global commons as originally intended, or if it has become an area

of strategic competition such that it could cause security dilemmas between actors. Part Two will discuss the actors involved in space, both nation state and non-state, and how that has evolved over the last six decades, including if there has been any impact to the narrative of space. Part Three will explore the language[16] and narratives surrounding space and how actors communicate their messages to their intended, and unintended, audiences. In addition, it will look at what those messages contribute towards the discourse in Part One. Part Four will consider both historical and current alliances and partnerships that the actors identified in Part Two are creating or disestablishing. Finally, Part Five will consider what might come next and suggest where UK Defence could have a function in contributing towards the UK space narrative, and the UK's role within the space faring nations.

Limitations within the paper are based around access to quality, unbiased information, the fast moving pace of developments within the space domain, and gaining a broad[17] perspective of the discourse that is available. The author, as a Western defence student from a space operations background, who is studying in a military training academy is susceptible to bringing an unintended bias towards interpreting the narrative via discourse analysis. The discourse itself is written by authors with a vested interest in the domain, and are therefore also not entirely neutral in approach. In addition, access to detail from nations such as Russia and China is limited: translated works are susceptible to misinterpretation and may have changed the original communication intent. Availability of written works are primarily limited to modern day and the early period of the Space Race while the pace of change in the space environment regards technology, actors and doctrine in the last few years alone means that even articles and books published within the last couple of years are already out of date in some aspects.

Overall, the paper concludes that words do, in fact, matter if the human race is to avoid falling into a downward spiral of rhetoric and poor behaviour that will drive space further towards becoming a domain of strategic competition, at risk of causing security dilemmas, rather than being a global commons with assured access for all. International collaboration and partnerships between spacefaring nations will only continue to grow in importance, therefore, understanding how best to communicate across language and culture will be vital to prevent escalation or misunderstandings. Key, trusted, interlocutors will be required if international agreements and norms of behaviours are to make any impact on future space endeavours; this could present an opportunity for UK Space and Defence to have a real position of relevance within the space domain in a role of space diplomacy.

## Part One: The Space Paradox – A Global Common or 'Star Wars' Part II?

> '*Since space is virtually unexplored, it becomes of great significance to man's future.*'
>
> Lt Gen James Gavin[18]

Gray suggests that there are four great commons on Earth: 'the sea, the air, Earth orbital space and cyberspace,'[19] while Sadeh expands those to describe the domains of '… space, the high

seas, the atmosphere and Antarctica … as global commons [that] lie beyond the jurisdiction of any state … and are available for all to use for the common good.'[20] A common, in this respect, is deemed to be an area 'beyond state dominion that hosts finite resources available to all or that provide non-excludable global benefits.'[21] This paper considers space, and whether it can be considered a global common, or if it has become an area of strategic competition, fraught with potential security dilemmas, despite the best intentions set out in treaties at the beginning of the Space Race.

Space and humanity have been interlinked for millennia and for the majority of that time, it was considered by many as something magical, mysterious and far out of reach. There was, prior to the beginning of the space age, a genuine desire to maintain space as a 'war free sanctuary.'[22] That is, until the United States and the Soviet Union commenced their competition with each other to gain the 'firsts' of human kind's explorations beyond earth's atmosphere. Thus, 'space and politics … [became] inseparably interlinked,'[23] with Sheehan noting that space has typically been considered from one of three perspectives: 'as a sanctuary; as an environment and; as a theatre of war.'[24] Though on 14 November 1957, the United Nations (UN) '… passed resolution 1,148 demanding to allow space flight for peaceful and scientific purposes only,'[25] the language used within documents such as this, or the Outer Space Treaty (OST) of 1967, are generally considered to be somewhat general in their vernacular and loose enough to allow for some interpretation.[26] Of interest, there is a 'strong linguistic dissonance, both in terms of translation and different interpretation of terminology,'[27] between the Western world and Russia. When words such as *peace*, *deterrence* and *détente* have quite different interpretations between two of the major space powers (US and Russia), there is certainly room for misunderstanding.[28]

Within the UK Ministry of Defence (MOD) publication on *Global Strategic Trends*, space is referred to as a 'global commons,'[29] alongside the earth's oceans. Mahan, a naval strategist, considered a global commons to be 'a great highway … or a wide common, over which men may pass in all directions.'[30] While Mahan was referring to the strategic use of terrestrial oceans, it has also been used to describe the Antarctic and space, both of which could provide unknown levels of mineral resources and are not claimed by any single nation. MOD doctrine for *UK Air and Space Power* states that space 'represents a source of power and influence in its own right … a critical weakness if not given appropriate protection.'[31] Silverstein and Panda, however, suggest that 'not all leading space powers have endorsed the concept of outer space as a great commons,'[32] with the US among those that have been inconsistent in their approach.[33] Where there are inconsistencies in narratives, that is likely down to the realisation that reliance on the space domain has created a vulnerability that needs protecting: but inconsistent language can lead to an inconsistent and, therefore, confusing approach to the use of space, and a misunderstanding of intent. As expansive as space is, there are elements that are a finite resource, such as orbital slots and the radio frequency spectrum, and it is these limitations that can create competition and make space the contested and congested domain that it is today. Sadeh notes that:

> 'As [a] commons becomes overcrowded and degraded, users must consume more just to get the same level of benefit, so a downward spiral begins that individual users are powerless to stop.'[34]

The modern day reliance, by many, on space enabled technology has created an environment where guaranteed access to those resources has become fundamental to day-to-day living, and nowhere is this more applicable than for a modern military. Outside of Defence circles, there has always been some concern regards what is seen as the militarisation and weaponisation of space, hence part of the original treaties were to ensure no placement of weapons in space. Dolman argues that space was both militarised and weaponised from the very beginning, at the moment that it became politicised.[35] Olsen suggests that it was later, at the beginning of the Global Positioning System (GPS) network upon which humanity has become so dependent, or the use of Joint Direct Attack Munitions (JDAMS) within terrestrial based military operations, saying: 'it is past time to drop the fiction that space, somehow, is a pristine environment untrammelled by the military art.'[36] Sheehan argues that outer space has always been perceived in a certain manner, a special realm whereby 'certain types of activity are possible … while others are frowned upon or specifically forbidden,'[37] while Gray proposes that space is simply the latest domain to be exploited by the military, like maritime, land and air before it.[38] Sadeh suggests that if space is seen purely in the context of military competition, 'the starting assumption is that players want to maximise their relative power.'[39] With the relatively recent growth of non-state actors creating substantial satellite constellations on orbit, that competition for access is no longer the preserve of nation state militaries. A commercial entrepreneur, Elon Musk, now controls more than 25% of all active satellites after launching more than a dozen Starlink missions since 2018.[40] China has already announced plans to launch an internet satellite constellation of its own, in competition. These substantial additions to the number of spacecraft on orbit, from both a nation state and commercial market perspective, provides further potential for strategic competition, miscalculation of intent and a change to any traditional space narrative.

Opinion on space as a global commons or an area of strategic competition is often polarised. Ziarnick suggests that this is simply down to human nature; that it is common to 'view a new environment in terms of the environment you are most familiar with.'[41] This could explain the propensity to link space strategies with naval and air power strategies from earlier centuries, as well as the divide between commercial industry, scientists, military leadership and public perceptions. Prior to humanity's successes in getting to space and reaching the moon, it was not difficult to consider something as vast as the expanse of space as being open and available to all. Sixty years later, with the significant reliance on space enabled technology, it is also easy to understand a desire for all nations to have assured space access, to want to protect any sovereign space based assets, and the nervousness over other actors' behaviours and intent regards space. Indeed, with all industrially advanced nations recognising that access to space, or delivery of space power, is critical to continued national security from a terrestrial

perspective, any concerns over military space programmes appear to have been cast aside.[42] As Gray notes, 'strategic history records many states misunderstanding their adversaries' concepts and plans, but often there has been time to learn and adjust to unanticipated revelations.'[43] Understanding others' approach and intent towards a valued domain is therefore of vital importance, for, as noted in the *NATO 2030* report, 'outer space is a new theatre for geopolitical competition.'[44]

In order to fully consider whether space can still be thought of as a global commons, or whether guaranteed access to space and its resources has become so fundamental to space faring nations that it has developed into a domain of strategic competition, it is important to understand who has a vested interest in space. It also requires an understanding of the cultures and approaches to communication by those actors, as that contributes towards how actions and intent are understood by others and supports the proposal that it is constructivism that determines how space activity is perceived. Meyer's body of work on culture is discussed more in Part Three, but highlights the importance of understanding how communication is done differently between nations, noting that 'Americans often tend to be more explicit and direct,'[45] which Monaghan suggests means 'the resulting commentary is often dramatised and hyperbolic – and misleading …'[46]

## Part Two: Who's Who In The Space Zoo?

> *'But today, many Americans look to the stars unsettled, fearing that they may soon be eclipsed in space by a foreign competitor.'*
>
> Brent Ziarnick[47]

The space age, Sheehan suggests, 'is the age of global politics,'[48] and the first real players in the space game were the US and the Soviet Union, as was. Their competitiveness as nations to achieve successful rocket launches, orbit the earth and get humanity to the moon was such that it earned it's own name: the 'Space Race'. While the launch of Sputnik in 1957 was celebrated by many, even outside the Soviet Union, for the Americans the message the launch sent drove fear into the national psyche, with it described as '… perhaps the most serious setback, both psychologically and technically, that [the US has] suffered since World War II.'[49] The publication in question was printed only two years after Sputnik launched and the tone of the entire book reads of national survival, and disbelief that the American way of life had not been able to beat the Soviets. That power balance for control of space between two significant nation states set the scene for the decades that followed, and the power struggle of the Cold War years,[50] though it also enabled four decades of 'consistent norms of conduct in space and strategic stability.'[51] The balance of space power may not be as equal as it once was between the US and Russia, but under Vladimir Putin 'the Russian leadership … continues to see space as a strategic asset that needs to be exploited for its potential.'[52] The issue of power, however, is not necessarily a characteristic in itself but rather a relationship[53] between two or more entities, where an active decision is made regards where the power balance lies; this will be covered in more detail in Part Four.

The US and Russia have been the known space actors over the last 65 years, with each nation competing with the other to gain those 'firsts' in space: for a time, Russia was very much the lead nation with the launch of Sputnik; Gagarin completing the first manned flight to space; Tereshkova as the first woman in space; and the Soviet space programme also saw them achieve the first space walk and send the first probes to the Moon, Venus and Mars.[54] Just days after Gagarin's successful orbit of the earth[55], President Kennedy held a cabinet meeting to discuss any options that the US might have in overcoming the Soviet lead in space.[56] This highlighted the level of competition in space at that time: Kennedy allegedly did not care what the specific programme might be, but he wanted something dramatic the US could succeed at, and send a message to the Soviets (and the world) while doing so. Thus started the planning for the moon landings, and when Armstrong stepped out onto the moon, 'the bi-polar space game was over.'[57] Ziarnick suggests that the competition between the US and Russia, or the Space Race as it was known, was a competition between the communist and free democratic systems, to 'win the popularity of the third world countries in a play for favouritism.'[58] What is less clear, is whether this was also the Soviet thinking of the time; that their space messaging from their accomplishments was merely designed to win favour with other nations and therefore expand Soviet influence. Over sixty years later, and the '… persistent friction between the West … and Russia'[59] continues, both on Earth and in space. Some of that friction could be attributed to the varying narratives and perceived intent behind actions within the domain.

Fast forward to the early 21st century, and there are now 'more than 50 countries [with] space agencies or other government bodies carrying out space activities.'[60] Space power: the ability to exert 'influence in, from, or through, space' [61] has traditionally focused on 'the activities of a nation's military and civil space programs,'[62] with Ziarnick suggesting there is an 'unhealthy preoccupation'[63] with the military form. However, even with the significant increase of other nations entering into space endeavours, the US still invests substantially more to their public space budgets: in 2017, at US$43.34 billion it represented more than twice that of the next 11 countries combined.[64] This level of investment shows no sign of abating as the recently formed United States Space Force (USSF) has announced a budget of $17.4bn for 2022, an increase of 13.1% over the previous year,[65] which highlights the US consistently messaging the importance that space has for them as a nation, both economically and as an investment in power status. Sheehan suggests that those nations with space capabilities can be divided into three tiers:[66]

1. Dedicated military and civilian space capabilities on the cutting edge of technology;
2. Develop and use dual use space systems for both military and civilian purposes;
3. Nations that lease or purchase space capability.[67]

While not necessarily an internationally accepted tier grading level, the parameters seem feasible when considered against the current global space actors. However, gradings or tiers can also suggest a level of competition or encourage a desire to reach a certain level. There can be little argument that nations such as the US, Russia and China are in Tier 1. The UK, for now,

is at Tier 2,[68] though that could change when UK sovereign space launch becomes a viable option, and if the planned ambition 'to develop a Sovereign low-earth constellation of responsive small satellites'[69] comes to fruition. The UK's narrative, however, would need to match its ambition and be accepted by the international space community. As Lonsdale and Kane posit, it is 'whether certain countries with certain cultures and certain political institutions are natural space powers …,'[70] and the UK's inability to match level of investment with nations such as the US, China and Russia will likely prevent it ever being perceived as a space power of equivalent value.

Confirming it's intent to become a space power of significance,[71] in October 2003 China became only the third country in the world to successfully launch and recover a human, its first *taikonaut*[72], from Earth's orbit.[73] China's growth within the space domain, over a relatively short period of time, has been impressive, 'exhibiting developments that eclipse many nations' entire accomplishments in space.'[74] Elsewhere, the United Arab Emirates (UAE), in less than a decade, has created a sovereign space agency, sent an astronaut to the International Space Station (ISS), launched a probe to Mars, founded a regional space alliance, and recently announced the first Arab female astronaut had been selected to train with NASA for future space flights.[75] While the UAE's focus is very much on the scientific and space industry side, rather than defence requirements, their messaging has been clear: they are a regional lead for space and will participate alongside the larger space powers, albeit through cooperative endeavour for the most part. This regional alliance, and its subsequent acceptance by the international space community, effectively adds strength to the UAE's geopolitical power position in the Middle East region and sends a message that they want to become part of the international space faring community. In addition, in the last three years, France, the UK, Germany and Australia have all announced and formally stood up, national Space Commands for their military services. All of these new commands are working closely with industry and across Government departments to ensure a cohesive national approach to space. This is a different approach to the early days of the space age when it was primarily seen as a military only endeavour: these efforts should go some way to securing consistent and transparent communications on a nation's space activity.

There is, however, no single nation state that is attempting to operate in space as a single entity. Partnerships and alliances have been steadily increasing over the years, though it has been a constant after the initial competition between the US and Russia. Kauppi and Viotti suggest that it is within these relationships and interactions that the approach of constructivism as part of IR, really comes to the fore, as the 'interests of actors are constructed and subject to change.'[76] The choice of partner(s) within space alliances and cooperative endeavours can also be used as a form of messaging. In recent years Russia, for example has created a regional space cooperative with several Asian neighbours: Japan, China, India, Korea, Indonesia, Malaysia and Thailand.[77] While some of those nations might not be considered significant space powers in their own right, it speaks to regional engagement and building alliances (non-Western) across multiple space activities. International cooperation in space

has long been the focus for Russia,[78] even from its days as the Soviet Union, primarily in getting astronauts and cosmonauts to space. The US were hugely reliant on this agreement in the years after the Space Shuttle Program finished, until Elon Musk and SpaceX provided an alternative with the Dragon capsule in April 2020. France, China, India and the UK have also benefitted from 'a demonstration of Soviet inclusiveness regarding its space programme.'[79] These relationships will be covered in greater detail in Part Four.

While nation states 'remain the principal actors in world affairs,'[80] there are an increasing number of non-state actors with a significant or growing presence within the space domain, all of whom are contributing towards the growth of the space industry and humanity's achievements outside of the Earth's atmosphere. Most notable among them is Elon Musk and SpaceX, whose advancements in reusable rocket boosters within the last couple of years has seen a substantial reduction in the cost of space launch, and a total of 65 rockets being reflown:[81] a concept that was unfathomable only a couple of years ago. In addition, SpaceX's Dragon capsule saw the US able to provide their own sovereign crewed space launch in 2020, sending astronauts to the ISS for the first time since 2011, and being the first private spacecraft to do so.[82] Jeff Bezos is another of the so-called 'Space Barons,'[83] who with his company Blue Origin is working to add to the commercial competition for astronaut shuttles, with the first launch of the New Shepard capsule expected in July 2021.[84] Musk and Bezos have traded competitive rhetoric over social media for some years as they compete to land substantial US government space contracts, which suggests the two horse Space Race of over six decades ago has shifted focus from nations to entrepreneurial individuals with commercial and government contracts in their sights.

## Part Three: How's Your Klingon?

> *'Our words matter to us. Simply by being spoken, our stated intentions and plans have some degree of normative force in their own right.'*
>
> Nicholas Onuf [85]

Space: often referred to as the high frontier, the final frontier or the next frontier; the ultimate high ground; a global common; as being both an enabler and a vulnerability; and then there are space races and space ages. The nomenclature surrounding space is certainly varied, and occasionally confusing, which potentially creates a situation where intent can be questioned, or certainly misunderstood. To consider how the narrative of space may have changed over the decades since even before Sputnik, Gagarin and Armstong were the headlines of the day, it is important to understand how the means of messaging have also evolved. In the 1950s, much of the general population's information was delivered to them via official news channels through authorised spokespeople and journalists. Today, news and information are provided 24/7; the majority via space enabled technology to a hand held device, and almost anyone with an opinion is able to create their own narrative with the global population as the audience. It is the narrative, according to Miskimmon et al, that is 'central to the identity and behaviour of actors in the international system, the structure of the system itself, and how

ideas, issues and policies are contested.'[86] Part Three of this paper will consider the language of space through rhetoric, doctrine, treaties, fiction and social media; it will also discuss how culture and trust can affect how communications are understood or interpreted, occasionally leading to friction.

The number of actors; that is nation states and, as seen in Part Two, entrepreneurial individuals that actively participate within the space environment has risen significantly since the early days of the Space Race. Scholarly articles, news headlines, company mission statements and military strategies with a reference to space are more commonplace now than they have ever been, even when considering the narrative around the height of the original Space Race during the Cold War. There are many similarities within those documents, regardless of origin: it is not possible, after all, to change the laws of physics regards operating in space. Yet there are also both subtle and significant differences in what is said, and the intent that might be understood. Gray noted that, 'between the scholar and the policy maker and strategist lies the zone of journalistic commentary,'[87] which is increasingly prevalent within space narratives. The option for Hollywood screen writer, enthusiastic entrepreneur, industry specialist and military leadership could also be added to the potential authors when it comes to adding to the language and narrative of space. In this section, language refers not only to the spoken and written word, but the actions taken[88]; all of which send a message to multiple audiences. Communication in this instance, is 'the sharing of meaning through the exchange of information,'[89] which can come in many guises such as the recordings of Sputnik's radio transmission signals, the audio and visual footage of the Apollo moon landings, or the launch of a Tesla Roadster into orbit. It is important to note that audiences are not simply 'a blank slate for narratives to be projected onto … [the] skilful practitioners of strategic narratives must take into account the political and media literacies of their target audiences,'[90] if they are to understand the messaging as intended. This is where conflicting messaging, such as how a nation state perceives the space domain, does not help an audience understand the environment.

Communication, in its simplest terms, is when an actor uses words, imagery and language in combination to form a narrative that describes an intent or action.[91] The language chosen invariably reflects an element of power; dependent upon the messenger and the message, that power may be perceived quite differently, as could be the reactions to what is said, or the message received which may not necessarily be the same thing.[92] An example of this is the relationship between the US and China: Johnson-Freese highlights that for the US, '[the] concern is primarily regards the ultimate intent of Chinese space ambitions, but deciphering such intent can be difficult for outsiders.'[93] Power relationships, such as those related to the space domain and particularly between the US and China, 'are largely constructed in people's minds through communication processes.'[94] When considered against the IR approach of constructivism, Kauppi and Viotti suggest that constructivists are, 'particularly interested in the key concepts of norms, rules and identities and how they affect the conception of ourselves and how we relate to the world.'[95]

A clear example of this for space is the work the UK undertook to get the membership of the United Nations (UN) to sign off the United Nations General Assembly (UNGA) resolution 75/36 which considered the 'reduction of space threats through norms, rules and principles of responsible behaviours.'[96] The additional 164[97] countries that signed up to the agreement show a clear intent to be seen as responsible users of space, but the UK leading that narrative also gives a strong message as to the role it wants to make for itself in space. Of note, China, North Korea, Iran and Russia were among the 12 countries that voted against the resolution, while India and Israel were among the six abstentions.[98] Sheehan notes that when states 'pursue policies designed to increase their prestige, they are seeking to confirm an evaluation of strength, excellence, even superiority,'[99] against others. It is feasible, then, to interpret the intent of those countries that abstained or refused the resolution to be less than responsible in their use of space. The language in the document, however, may also have contributed to the hesitancy of some nations to accept the proposal. Some consideration of cultural communication differences are made later in this section.

Where an actor sits within the arena of strategic space competition requires a narrative of some sort, whether that is softly spoken or shouted loudly. Constructing that narrative is 'shaped by domestic and international political contexts, the communication environment, and the goals of the political leadership.'[100] In the 1950s, space was a two horse race: in 2021, there are multiple nation states, and non-state actors (primarily entrepreneurs such as Elon Musk and Jeff Bezos) working to gain power within the space environment, each with their own narrative, identity and motivations. There are often disagreements between state leadership, military forces, industry professionals, academics and the civilian population on how space is referred to, what it is utilised for, the legitimacy of treaties and what the proposed 'norms of behaviour,'[101] i.e. any new international legal regimes or best practice guidelines for day-to-day operations, should be. Various factors will influence the development and consistency of any narrative: a nation state's leadership, matters of global significance, levels of strategic and commercial competition and technological advances to name a few. Space, however, has moved from something that was purely aspirational, to being of daily relevance to the majority of the developed world in little over 60 years. Expansive as it is, there are some aspects of space that have a finite capacity; the radio frequency spectrum and available orbital slots for satellite use being the best examples. According to Sadeh, this has the potential to cause issues at some point down the line:

> 'Despite the vastness of space, certain kinds of crowding and irresponsible use are already raising the risks that individual space users will inadvertently cause problems for each other.'[102]

Inadvertent problems in space are one thing, but how would one actor know if an action were unintended or otherwise; how does an actor determine whether or how to react; and how much faith does the spacefaring community have that an actor is being truthful in the

first place? Booth and Wheeler suggest this is how security dilemmas are created, with two levels of strategic predicament: 'a dilemma of interpretation (motives, intentions, capabilities), and a dilemma of response …'[103] This does not simply apply to physical actions, it can also come from the words or postures that are taken by individual actors, and highlights again how constructivism plays its role in how an actor perceives their reality. Constructivists, according to Kauppi and Viotti, build any personal understandings and frameworks from a cultural perspective; from social relationships and shared meanings, according to the level of priority or importance the subject may hold within their group.[104]

Given the role that Defence has within national security, regardless of nation state, it could be expected that any language used in messaging could be considered to be more aggressive or confrontational in nature against any communications that might be seen from an industry or scientific perspective. There are, however, differences even within defence organisations as to the choice of language or tone of message. For example, the US Department of Defense (DOD) released a summary of the *Defense Space Strategy* in June 2020; in the first paragraph it states 'space is now a distinct warfighting domain,'[105] and goes on to explicitly state that it is China and Russia that have 'weaponized space and turned it into a warfighting domain.'[106] There can be further differences in tone even within the same nation state; Gallagher notes that while the US DOD describes space as 'congested, competitive and contested,'[107] the US State Department 'uses more diplomatic terms … congested, multifaceted and interdependent.'[108] This, combined with Gray's suggestion that an absence of discipline and consistency over spelling of commonly used words such as space power, space-power or spacepower, is indicative of conceptual uncertainty and creates a 'strategic anxiety [that] has a way of propelling the creative imagination.'[109] Creative imagination could be another means of explaining a constructivist approach to the space domain, and the potential for creating security dilemmas.

While the US has openly stated that they consider space to be a warfighting domain, NATO[110] use the less contentious phrase of *operational domain*, as did the UK though that changed in 2020 when both the head of UK Strategic Command and the Chief of the Royal Air Force made reference to space as a warfighting domain and 'extending warfare into the novel domain of space.'[111] Although the language use is subtly different, Bowen suggests that the UK MOD has 'explicitly and unambiguously brought British space security policy and military doctrine in line with US doctrine,'[112] though this also contradicts the language within the previously mentioned *Global Strategic Trends* document, another MOD publication, which refers to space as a 'global common.'[113] What that potentially says to other space actors is that the UK will respond in the same manner as the US to any poor or aggressive behaviour in space, but it may also signal a confused approach to the domain by the UK, from other actors' perspectives. Silverman suggests that, 'language does not merely describe events or states of affairs. It also creates or performs them …[it] accomplishes the act itself,'[114] therefore what is said, how it is said, and consistency of message are of real importance when it comes to communicating about space.

Any form of communication is susceptible to misunderstanding, for a variety of reasons, and that can be purposeful or inadvertent. Communicating across cultures, in particular, '… can be fraught with invisible difficulties,'[115] and only some of that is attributed to any difference in the spoken or written language of origin. Huntington suggests that this is partially because people, '… interpret communications in terms of their own pre-existing values and perspectives.'[116] The choice of language in any communication is therefore very important, particularly in challenging domains such as space. The US has certainly varied its approach between the original Space Race era and now. Lonsdale and Kane highlight that at a time when Cold War antagonism between the US and the Soviet Union was at its peak, the US DOD specifically prevented the US Air Force (USAF) from publicly mentioning 'the possibility of equipping its proposed interceptor satellite with a "kill capability",'[117] which suggests a desire from the US perspective to prevent any possible escalation to conflict in space, certainly at that time, or to be seen as contravening the peaceful use of space. Contrast that with the approach and language of the recent Trump presidency, where it was stated: 'It is not enough to have American presence in space … we must have American dominance.'[118] This posturing, while understandable for a nation and society that is considered to have the greatest reliance on space enabled technology,[119] particularly for their military,[120] sends a message of intent that other space actors could react to, or might consider inflammatory. It does not send a message that space is for all.

The US has a potted history regards its communications on space, and whether or not it considers it to be a commons for all, but what has remained constant is its obvious desire to remain the number one space power. In August 2004, the USAF quietly issued a doctrine document entitled *Counterspace Operations*, in which it 'declared the strategic ambitions of the USAF in space.'[121] Johnson-Freese suggests that the low key release of such a document was done specifically to see how much attention other actors were paying to communications such as the doctrine release; effectively testing the water for any negative response to their military intent to protect their space assets on orbit. At the time, the document went virtually unnoticed. Move forward to 2020, and the US DOD issued a space strategy summary and fact sheet that called out Russia and China for 'weaponizing space and turning it into a warfighting domain.'[122]

In that same year, China released the latest version of its White Paper on space; Johnson-Freese describes the language within the paper as 'assertive.'[123] Within the document, it had added an additional component that focused on '… the promotion of international cooperation in Chinese space activities,'[124] and from the outset has stated that the 'Chinese government holds that outer space is the common wealth of all mankind.'[125] An independent review of that same paper highlighted that within the 11,000 word document, the word *security* was mentioned only three times, while the words *military* or *dual-use* had not been found at all.[126] This could be further reflection of Meyer's work, which suggests that the Chinese inclination for high context communication[127] leaves a lot left unsaid, with a need to read between the lines. As noted by Johnson-Freese: 'part of China's propensity toward secrecy is cultural. When intent

is ambiguous, failure is easier to avoid,'[128] but it also makes it far easier for other space actors, such as the US, to assume the worst.[129] Miskimmon et al propose that China has 'preferred to present an ambiguous identity and narrative to the West about its rise,'[130] both as a nation and a space power, though when linked to Meyer's[131] work, that could simply be considered as the manner in which China naturally communicates. Which leaves China's intent open to interpretation dependent on how the West and others want to perceive it, though this is equally true from the perspective of China looking at the US and the West.

China's key piece of global messaging regards its plans for the space domain came in 2003, when it became only the third nation to ever successfully launch a crewed space flight from Earth's orbit.[132] This, combined with an ambitious space strategy[133] that looks out to the next thirty years suggests that President Xi Jinping 'has embraced the idea of technology innovation and [is] adopting the idea of a Silk Road here on Earth and a Silk Road information corridor in space …'[134] China, therefore, 'presents itself in an ambiguous way. It is perceived alternately as an aspiring normal great power to balance others, or as a rising hegemon.'[135] This paper has previously covered the challenges of messaging towards different audiences, with Booth and Wheeler highlighting the difficulty that comes when the 'postures that one government claims to be defensive may appear potentially offensive from the perspective of neighbours and rivals.'[136] This would appear particularly true when it comes to the US interpretation of China's intent. The US simply does not trust China to have non-nefarious intent with its space activities; the reality it has constructed for itself regards China will not allow it to, unless something changes. Kissinger suggests that this is partly due to the US not having 'experience interacting on a sustained basis with a country of comparable size, reach, and economic performance [that embraces] a distinctly different model of domestic order.'[137] Both nations are constructing their own version of a World Order, with each seeing themselves at the centre; this could lead to increased competition within the space domain, misunderstanding of intent, and potentially, conflict due to an ensuing security dilemma.

This paper has previously covered how nations have a natural setting towards how communication is done: messaging and language use within a space narrative is no different and can be both obvious and subtle. Meyer highlights that both the US and UK, 'fall toward the low context end of the communicating scale,'[138] that is, communications that are precise and clear. The US much more so, which explains some of the language use in DoD space policy and strategy documents, but this also carries through to media releases on space behaviours. The US, according to Hitchens, 'messages about what it considers irresponsible milspace behaviour ...'[139] allowing for the reading or listening audience to deduce the norms of behaviour the state accepts. In April 2020 the US Space Force chief, General Jay Raymond, directly called out Russian behaviour following their testing of a ground based Nudal anti-satellite (ASAT) missile. Unusually, for the UK, the lead for the MOD Space Directorate, Air Vice Marshal Harvey Smyth, also decried the activity, 'marking the first time that the [MOD] has publicly criticised Russian actions in space.'[140] While effectively taking the same action, the language and tone between the two space leaders was subtly different: Smyth spoke of

*concern* and *threatening the peaceful use of space*, requesting that Russia 'continue to work constructively … to encourage responsible behaviour.'[141] Raymond 'strongly condemned'[142] the behaviour, speaking of *hypocrisy* and *aggression*, and *threats* to the US and its allies; yet did not, in this instance, suggest any means of working together to create the norms.

Transparency and consistency in communications, therefore, is significant. Without it, an actor is left to interpret the gaps and will invariably fall to what is known of the other actor; that is, they will construct what previous experience suggests is the likely intent. If the starting position is one of mutual distrust, it is unlikely either would consider the other to be a responsible partner within a space alliance.

## Part Four: Inter-Galactic Speed Dating

> *'An alliance is a temporary, mutually expedient arrangement within a rivalry … allies expect to eventually revert to a condition in which war between them is an option … Friends may fall out … but their expectation up front is that the relationship will continue.'*
>
> Alexander Wendt[143]

With so much competition between nations since the beginning of humanity's endeavours in space, it could be considered that there would not be much room for cooperation and alliances. However, the '…reality of the space age has been that space activities have been characterised by an enormous amount of international cooperation.'[144] The opening quote to this section perhaps best describes how and why certain alliances and partnerships come about with regard to space cooperation: read any US Space Strategy and it is interlaced with a reminder that Russia and China do not behave well in space, from the US perspective. Yet for many years, the US was dependent upon Russian launch capability to get their astronauts to the International Space Station (ISS); with ISS being an excellent example of international collaboration proving to be successful in space.[145] All partnerships, however, are not created equal. Russia, for example, 'does not have the same definition as Europe of what cooperation is,'[146] as it also tends to include sales of technology and data exchange within their approach to international cooperation in space. Viewed through the lens of constructivism, 'states create each other as enemies, rivals or partners, and proceed to share their interpretations of their respective identities,'[147] they also tend to behave as the other expects. Constructivists, according to Nye, 'emphasise the importance of ideas and culture in shaping both the reality and the discourse of international politics.'[148]

The motivations for nations to engage in partnerships and alliances in space are many and varied, and the 'relationships among different networks have become more important,'[149] particularly as the space domain becomes more competitive. Dependent upon a nation's geographic location, or until technology such as Virgin Orbit[150] provides a fully viable launch alternative, there will always be a need for national agreements with those that are well placed for equatorial or polar orbital launch sites, for example. In addition, the sheer expense of being involved in space launches as well as the often substantial cost of satellites is a prohibitive

factor for some; many nations have already seen the economic and power benefits of entering into alliances or cooperation with others. It was early bilateral space cooperation between several European countries, '…which finally led to the formation of the European Space Agency in 1975.'[151] Dolman argues that cooperation regards exploration of space is a popular vision, that it captures public attention, but there is a requirement for continued competition or 'future growth in outer-space exploration is likely to be stunted.'[152]

The incentives behind space related cooperations are not, however, purely driven by financial or launch related factors; select alliances send messages to other actors in the same way that a press conference from a state leader might. Many of those space alliances might be considered as an extension of normal terrestrial business, though some such as the link-up between France and China to cooperate on 'climate actions and space exploration'[153] may be considered more unusual. Through the French Space Agency, France has also taken on a number of 'diverse cooperative steps with foreign authorities'[154] such as Australia, Ethiopia, Germany, India, Saudi Arabia and the UAE. Gray suggests that for these alliances to work, 'communities require ethical codes, formal or informal, because their survival requires predictability in behaviour.'[155] Those ethical codes would have been messaged in some manner, and would likely have needed to be consistent in content, or evidenced by consistent action, to have encouraged another to enter into an alliance: is that actor, for example, speaking the same language regards use of space: do the narratives match or align? Or are they similar enough to make a necessary partnership or alliance more palatable, such as for those nations that need assistance in gaining access to space in the first place via launch capability, for example.[156] There is a continued dichotomy of 'competition and cooperation'[157] in space alliances that is not always evident in terrestrial activity, and suggests greater political significance 'in relation to … foreign policy interests in space activity.'[158]

The previous section of this paper considered the importance of narrative; Miskimmon et al suggest that when individual narratives appear to be in alignment, it is possible for two or more parties to be in agreement on an issue, because '… they understand [it] in the same terms.'[159] This seems straight forward enough, provided it is considered alongside Meyer's work on cultural communication scales: '… what matters is not the absolute position of either culture on the scale, but rather the relative position of the two cultures.'[160] This might go some way to explaining how the US approach[161] to communicating about space can feel very different to the Russian and Chinese narratives; the Chinese in particular reiterating 'the need for nations to work together, rather than against each other, in space.'[162] Meyer's understanding of the cultural differences on communications proposes that all nationalities can be placed on a scale of low context to high context requirements. A low context nation would consider good communication to be precise, simple and clear where any messaging is clearly expressed and understood at face value, whereas a high context nation is seeking more sophisticated, nuanced and layered communication that comes from reading between the lines.[163] Using Meyer's scale, the US is at the far end of low context while Russia and China are towards the higher context end. If, therefore, national policies and

strategies and international treaties are to avoid causing concern and misunderstandings then it is imperative these differences are taken into account when engaging with different audiences. Without it, there will always be a significant gulf between the three major space faring nations, which means the likelihood of significant partnerships between them, or agreements on international treaties, remains slim. This has been recognised by Johnson-Freese, who notes that while the US has said 'it is interested in working with China as a global partner … actions have not matched words when in functional areas such as space.'[164] It reads as a repetition of the US relationship with the Soviet Union during the Cold War: viewing anything and everything that came from the 'other' side with suspicion and distrust.[165]

Dawson proposes that 'the future will be an interesting mix of government and private enterprise ventures into space,'[166] so careful consideration and selection of alliances and partnerships is considered to be one method of increasing levels of power, be that perceived or real power. Gray argues that power has a value of its own, 'as well as for its instrumental worth in aid of interests that are ever open to subjective evaluation as being defensive or offensive,'[167] such as that of space power. Goswami suggests that the Chinese understand this very well, and that 'with power comes influence,'[168] and given the director general of the European Space Agency (ESA) has noted the strategic importance of future cooperation with China,[169] President Xi Jinping is likely to see China's geopolitical and astropolitical influence grow and enable the nation to 'become more of an equal partner in future space operations.'[170] While the US is currently still considered to be the largest space power at play today, it too has created a network of space alliances and partnerships. This is not purely an economic decision as Ziarnick highlights '… the paradox of space power in the early 21st century: the most dominant space power in the world is in crippling fear of being dethroned by a program far smaller.'[171] These alliances and relationships are the basis of constructivism when it comes to space. Wendt suggests there are two basic tenets to this:

1. The structures of human association are determined by shared ideas;
2. Identities and interests of various actors are constructed by these shared ideas.[172]

There is also strength in numbers, and for those countries that cannot compete on the size and scale of the US space programmes, it makes sense to take a collegiate approach. The founding of the European Space Agency (ESA), for example, can be traced back to the early days of the Space Race when there wasn't a single European country that could match the levels of technical capability that both the Soviet Union and the US had at the time.[173] Russia has used space alliances as a foreign policy tool, 'to strengthen political ties with selected countries or to affirm the country's regained power and influence over those countries,'[174] as has the US with the creation of Operation Olympic Defender (OOD). OOD links the US with several of its key defence alliances, most notably the UK which was the first nation to sign up to the agreement in December 2018. This effectively allows the signed nations to share space capability that might not ordinarily be available: it also sends the message that

certain defence relationships that are strong within the terrestrial environment, are growing outside of Earth's atmosphere. Johnson-Freese suggests that inclusion, such as within the aforementioned alliances and agreements, 'is symbolic of acceptance into the international family of space faring nations.'[175] It is unclear how a similar alliance of other militaries outside of OOD membership would be construed by the US: a proactive defensive stance could easily be interpreted as an offensive stance in this example, potentially leading to a downward spiral into a security dilemma.

All relationships and alliances are generally based on some level of trust, and Meyer suggests that there is a trusting scale, with countries leaning towards either task based or relationship based agreements that help build trust between them.[176] Countries such as the US, Australia and the UK can be found at the task end of the scale; that is, building trust through practical and functional type activities, while Japan, Russia, China and Saudi Arabia are at the relationship end; choosing a slower work up and deeper emotional connections to any alliances.[177] Considered against Meyer's communications scale differences that were mentioned in Part Three, the US and many of the traditional Five Eye communities, are consistently at the opposing end of the scales to Russia and China. Given those disparities in both trust and communication, there is work to be done on all sides regards the language and narrative of space if the domain is to remain conflict free, albeit as an area of strategic competition vice a global common, for 'what we perceive space to be shapes our views on how it should be exploited.'[178]

## Part Five: To Infinity and Beyond!

> *'Strategic leadership and dominance in space is not an American birthright, despite the widespread belief that the orderly march into the future is part and parcel of America's destiny.'*[179]
>
> Jim Malachowski

The UK is not the only nation in recent years to have stated an intent to develop its space presence. Hoerber and Sigalas argue that this is because, 'space endeavours are known to generate public appeal and act as a demonstration of societal prowess.'[180] This has all happened within the last century; prior to 1957 and the launch of Sputnik, space was essentially a blank page. It was only after the first satellite was launched that space, 'became an ontological reality directly experienced by mankind.'[181] In that time, the reliance on space enabled technology for both peaceful and military purposes has grown exponentially, as has the level of competition between nation states and private companies in accessing space in the first place.

The UK, despite standing up both a 2* led Space Directorate and Space Command since 2020, does not yet have an approved, updated National Space Strategy.[182] It is therefore also lacking a Defence Space Strategy, and as noted by Lonsdale and Kane, 'military strategy must be integrated within a coherent grand strategy that is itself guided by the common

good.'[183] Sadeh suggests that this is a broader problem, arguing that: 'Spacefaring states do not suffer from a lack of space policy … they do suffer from a lack of explicit space strategies.'[184] Moltz adds that any space strategy needs to consider the reaction of other actors, with communication of the intent behind those strategies aimed to minimise any negative reaction[185], and reduce the possibility of causing future security dilemmas. This is harder to do when considering China, for example, because their 'strategic insights are inferred, rather than extensively laid out,'[186] which highlights again the need to understand how various actors communicate their intent. Strategy, 'links power to purpose, serves and fulfils policy, and provides a means for maintaining advantages for states.'[187] For the UK, while the newly formed Space Command is designed with a military or defence focus in mind, and will have a natural desire to preserve the UK ability to access space, the Space Directorate represents an organisation that looks to link military, cross Government and industry approach to a national space strategy.

Communications and messaging regards space endeavours have ebbed and flowed over the decades. At its peak of human interest, as the race to the Moon came to a conclusion, 'over 528 million people around the world watched a live television broadcast of the mission.'[188] Those communications were facilitated by space enabled technology, which is even more prevalent today than it was in 1969. So, as discussed in Part Three, messaging is about what is said and done, but also what is not said and done, and there is always an audience watching and listening. The tone that national policy documents take will set the scene for how other actors construe the intent, therefore the language chosen should be carefully selected. Johnson-Freese notes that there are many other countries that consider space as a strategic asset, 'though the phrase assumes an entirely different meaning'[189] dependent upon the nation state. From the US perspective, for example, the term *strategic* has become more and more equated with a military approach.[190]

With a growing number of space actors, Klein suggests that those 'with the most active presence and participation in space have a commensurate ability to promote their interests and influence the international legal basis for accessing and utilising space.'[191] The US has not been in the position of having a near peer competitor in space for some time, and China is rapidly proving themselves to be a significant space actor. Fabian suggests that the emergence of China, 'demands actor-specific considerations;'[192] which the current US defence space narrative does not seem to consider. Current levels of mistrust between the two nation states would suggest that it is unlikely anything will change if, as Mahnken states: 'there has been as yet no attempt to understand Chinese strategic culture, decision-making, strategy, operational art, and science and technology,'[193] to the same effort that was made to understand the Soviet Union over six decades ago. Without an amended approach to communications between the two states, particularly around the use of space, it would be easy to see how strategic competition could lead to inadvertent conflict. Zheng suggests that 'in manipulating the language to form and display … distinctive political identities, while portraying the other side as an 'out-group' … [they] are sometimes trapped in the world they construct.'[194] There is,

perhaps, room for the UK and other nation states to act as interlocutors, or space diplomats, between the two nation states given their opposing position on Meyer's communication context scale.[195]

There can be no doubt that there has always been, and will likely continue to be, an element of competition towards achievement within the space domain. Malachowski argues that 'space is a unique domain of all modern human activities, but humanity has a long history of conflict over resources.'[196] With the increasing plans to mine the Moon and passing asteroids, the first nation to be able to do so and return the goods to Earth will reap the benefits. However, effective space mining operations 'could have disruptive effects on the global … precious metal economies, especially if that supply is controlled by a single state.'[197] The US concern is very much that the single state will be China and the US narrative reflects that, portraying China as an irresponsible space user: this is perhaps designed to discourage other nation states from entering into partnerships with them. Huntington refers to this as separate codes that 'govern behaviour towards those who are "like us" and the "barbarians" who are not.'[198] The US has not hesitated to criticise those 'states that have dared even express an interest in engaging with Beijing,'[199] and in doing so they look as if they are constructing the very same bi-polar argument or competition as they had with the Soviet Union in the 1950s and 60s.

Space continues to be filled with opportunity and potential, for both achievement and competition, even when some suggest there has been a 'lack of space development over the last 50 years.'[200] Ziarnick proposes three metrics to measure that development: 'the number of people who have visited space, the distances humans have travelled in space, and the cost of sending a pound of payload into orbit.'[201] Written in 2015, the publication suggests that space has not developed as fast as many believed it would after the rapidly occurring achievements of the early space age: it was written before Elon Musk and SpaceX changed many fundamentals of what was believed possible for rocket launch with reusable boosters, and he has made no secret of his intent to start a human colony on Mars via his Starship launch vehicle.[202] This is another example of commercial enterprise adding to the levels of strategic competition within the domain: there could be potential for the next race to be the one that puts a human on Mars.

Rhetoric, narrative and actions confirm or change a space actor's standing or balance of power: the increasingly open and often antagonistic levels of language used could lead to sufficient friction for a security dilemma to build into conflict. Silverstein and Panda suggest that 'states can pursue mutual benefits in areas considered great commons even under competitive conditions,'[203] but that is very much reliant on gaining a consensus on space being a commons in the first place. Therefore the work that is being undertaken to get nations to sign up to responsible behaviours in space will be vital in creating the norms of behaviour that will encourage actors in treating space as a commons: and this is an area in which the UK could lead.

## Conclusion

*'Space is too important as a strategic asset to leave its fate to inertia, apathy or a few individuals.'*[204]

Joan Johnson-Freese

Space, consciously or not, has become an ingrained part of daily life for a significant portion of the human race. It enables a large part of daily life and maintaining secure access to space enabled capabilities is of vital importance: so much so the UK has listed access to the timing element of GPS as a Tier 1 Risk to its Critical National Infrastructure.[205] It is also only going to get busier, both with the number of active satellites on orbit and with crewed missions to the ISS, the Moon and onwards to Mars, if Elon Musk's dreams become reality.

Given all that has been discussed in this paper, and the geopolitics at the terrestrial level, it would not be wholly unexpected to see the space domain '… replicating the same dynamics that have historically driven security competition on Earth.'[206] Some analysts argue that the current geopolitical frictions between the US, China and Russia have been caused by US policies;[207] by extension those geopolitical issues have extended to the astropolitik arena as described by Dolman.[208] In 1959 Lt Gen James Gavin was convinced that by 1965 the USAF would have men in orbit capable of conducting combat operations in space;[209] in 2005, Gray proposed that 'future warfare will include war in space and cyberspace.'[210] Thankfully neither scenario has come to pass as yet, but it is feasible that increased levels of competition for limited resource such as orbital slots, lack of accepted international commitment to norms of behaviour and responsible space use, little control over commercial satellite constellations and an increase in rhetoric between the bigger space faring nations, could cause enough friction for a security dilemma to arise.

In Part One of this paper, consideration was made to the paradox of space and whether it can truly be considered a global commons, or if the competitive nature of the space actors involved in the environment has always been such that it can only be a domain of strategic competition. Competition does not necessarily have to lead to conflict, but it relies on clear and transparent communications between all entities to ensure there is no misunderstanding regards intent. Fabian has argued that current treaties were 'designed to preserve a status quo favourable to the United States and Soviet Union, and maintain deterrent stability among the great powers during the Cold War.'[211] That status quo is no longer valid, and even the US has shown inconsistencies in referring to space as a global common, with Malachowski suggesting that 'space is no longer a sanctuary for peaceful exploration … [and] is leaning towards a direct clash.'[212]

Part Two discussed the various space actors, and how they have increased from the original two nation states of the US and Soviet Union, to over 80 spacefaring nations and an increasing number of significant commercial players. The language and narrative of space were discussed in Part Three, with comparison made between several states, particularly in relation to national

and defence space strategies. The challenge here is that different audiences require different messaging – there is a need to tell any potential adversary that sovereign space enabled capabilities will be protected; a nation state's politicians need to understand that space is important enough to require consistent and constant investment; the public population need to understand why access to space is a facet of daily life that needs to be protected and if need be, defended. It is simply not possible to get all of that across, to all audiences, with one message, on a single medium. Therefore, how space is spoken about is important, as each nation constructs a reality from what is understood. If it is portrayed as a domain for warfighting and distrust, then it likely becomes it. The relationships between spacefaring nations and those within commercial enterprise were considered in Part Four, along with the role of international treaties in setting the norms of behaviour for responsible space users. There is a potential role in space diplomacy for the UK in this area as many nations 'are beginning to realise how much of their vital national infrastructure depends on space,'[213] and are therefore looking for norms that guide behaviour. Finally, in Part Five the paper considered what might come next in terms of future treaty work and the challenges for maintaining space as a domain without conflict even while recognising its growing importance as an area of strategic competition.

With the UK already assigning itself as a Tier Two, or secondary space power,[214] consideration should be made regards the role it can play to remain of significance to the Tier One space powers of the US, Russia and China and the other space actors. It is highly likely that there will be a requirement for a space interlocutor between the US and China in future, to help alleviate cultural communication misunderstandings and allow for mutually respectful dialogue on future space endeavours to avoid creating further security dilemmas that only add to the level of strategic competition in the domain. Given the work the UK has already done to garner majority consensus on responsible behaviours in space, this is an area that could be further developed for the UK.

In conclusion, nearly sixty-five years ago space was a domain that had not been violated by human presence and was sold as a global commons for all. Prior to that there had not been the levels of competition to drive achievement of the many firsts that followed in the years after, and there was little suggestion that space would become such a significant stage for strategic competition. It was, until the launch of Sputnik, a domain that remained out of reach, available only in the imagination. A lot has changed in those six or seven decades; it has become a domain that is described consistently as contested, congested and competitive, that has more and more actors participating within the environment, and a human population on Earth that grows increasingly dependent on space enabled technology. With growing competition, there are ever increasing levels of friction some of which is driven by escalatory narratives, even while there is more cooperation in place than there has ever been. It would be too easy for that friction to worsen due to a significant change in an actor's space narrative, or for a communication to be misinterpreted.

## Notes

[1] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 81.
[2] Neil deGrasse Tyson and Avis Lang, *Accessory to War* (New York: W. W. Norton & Company, Inc., 2018), 38.
[3] Jules Verne, *From Earth to the Moon* (New York: A. L. Burt, Publisher, 1889), 19.
[4] Throughout this essay there will be reference to the nation state of the USSR, the Soviet Union and Russia. This will vary according to the time period in question and will reference the state as it was known, and referred to, in that particular period.
[5] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 53.
[6] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 1.
[7] Linda Dawson, *War in Space* (Switzerland: Springer, 2018), 13.
[8] David J. Lonsdale and Thomas M. Kane, *Understanding Contemporary Strategy* (Abingdon: Routledge, 2020), 233.
[9] Ibid., 216.
[10] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 5.
[11] For the purposes of this paper, conflict could be considered to be either terrestrially based today or orbitally based in the future.
[12] In the context of this paper the word 'actor' is taken to mean those with a vested interested in the space environment, for example, a commercial company, a nation state or a military force.
[13] Ken Booth and Nicholas Wheeler, *The Security Dilemma* (Basingstoke: Palgrave Macmillan, 2008), 5.
[14] Mark V. Kauppi and Paul R. Viotti, *International Relations Theory* (Lanham: Rowman & Littlefield, 2020), 143.
[15] Vendulka Kubalkova, *Foreign Policy in a Constructed World* (Abingdon: Routledge, 2015), 23.
[16] Language use throughout the essay remains true to the original content, i.e. manned and crewed space flight, and variations in spelling dependent on type of English used in the original document.
[17] In this context, not purely Western based discourse.
[18] Lt Gen James Gavin, *War & Peace in the Space Age* (London: Hutchinson & Co. Ltd., 1959), 212.
[19] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 16.
[20] Eligar Sadeh, *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 54.
[21] Benjamin Silverstein and Ankit Panda, 'Space is a Great Commons. It's time to treat it as such.' *Carnegie Endowment for International Peace*. https://carnegieendowment.org (accessed March 12, 2021).
[22] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 6.
[23] Ibid., 2.
[24] Ibid., 18.
[25] Thomas C. Hoerber and Emmanuel Sigalas, *Theorizing European Space Policy* (Lanham: Lexington Books, 2017), 94.
[26] Linda Dawson, *War in Space* (Switzerland: Springer, 2018), 90.

[27] Andrew Monaghan, *The New Politics of Russia* (Manchester: Manchester University Press, 2016), 9.
[28] Ibid.
[29] United Kingdom. Development, Concepts and Doctrine Centre. *Global Strategic Trends*. 6th ed. (Shrivenham: DCDC, 2018), 53.
[30] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 16.
[31] United Kingdom. Development, Concepts and Doctrine Centre. *UK Air and Space Power*. 2nd ed. (Shrivenham: DCDC, 2017), 72.
[32] Benjamin Silverstein and Ankit Panda, 'Space is a Great Commons. It's Time to treat it as such.' *Carnegie Endowment for International Peace*. https://carnegieendowment.org (accessed March 12, 2021).
[33] There are examples of the UK also sending mixed messaging in this regard, which will be covered in Part 3.
[34] Eligar Sadeh, *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 55.
[35] Everett C. Dolman, *Astropolitik* (Abingdon: Frank Cass Publishers, 2002), 5.
[36] John Andreas Olsen, *A History of Air Warfare* (Washington DC: Potomac Books Inc., 2010), 384.
[37] Micheal Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 5.
[38] Colin S. Gray, *Another Bloody Century* (London: Phoenix, 2005), 292.
[39] Eligar Sadeh, *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 59.
[40] Anthony Cuthbertson, 'Elon Musk Now Controls Over A Quarter Of All Active Satellites As SpaceX Prepares To Launch 1,000th Starlink,' The Independent (2 February 2021), https://www.independent.co.uk (accessed March 15, 2021).
[41] Brent Ziarnick, *Developing National Power in Space: A Theoretical Model* (Jefferson: McFarland & Company, Inc., 2015), 91.
[42] Everett C. Dolman, *Astropolitik* (Abingdon: Frank Cass Publishers, 2002), 70.
[43] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 26.
[44] NATO. Reflection Group. *NATO 2030: United for a New Era*. Belgium: NATO, 2020, 47.
[45] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014), 9.
[46] Andrew Monaghan, *The New Politics of Russia* (Manchester: Manchester University Press, 2016), 4.
[47] Brent Ziarnick, *Developing National Power in Space: A Theoretical Model* (Jefferson: McFarland & Company, Inc., 2015), 2.
[48] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 3.
[49] Lt Gen James Gavin, *War & Peace In The Space Age* (London: Hutchinson & Co. Ltd., 1959), 26.
[50] Thomas C. Hoerber and Emmanuel Sigalas, *Theorizing European Space Policy* (Lanham: Lexington Books, 2017), 127.
[51] Jim Malachowski, 'Don't Gamble on the Next Space Race: Win in the Orbital Gray Zone Now' *Space Force Journal* 1, (2021): 2, https://www.spaceforcejournal.org (accessed February 8, 2021).
[52] Marco Aliberti and Ksenia Lisitsyna, *Russia's Posture in Space* (Switzerland: Springer, 2019), 51.
[53] Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2013), 11.
[54] Marco Aliberti and Ksenia Lisitsyna, *Russia's Posture in Space* (Switzerland: Springer, 2019), 1.

[55] 12 April 1961, only four years after the launch of Sputnik. It would be another eight years before the US landed on the moon.
[56] Harrison H. Schmitt, *Return to the Moon* (New York: Praxis Publishing Ltd., 2006), 16.
[57] Thomas C. Hoerber and Emmanuel Sigalas, *Theorizing European Space Policy* (Lanham: Lexington Books, 2017), 135.
[58] Brent Ziarnick, *Developing National Power in Space: A Theoretical Model* (Jefferson: McFarland & Company, Inc., 2015), 77.
[59] Andrew Monaghan, *The New Politics of Russia* (Manchester: Manchester University Press, 2016), 1.
[60] Britannica. 'Space Exploration – Major Milestones,' Britannica Encyclopaedia, https://www.britannica.com/science/space-exploration/major-milestones (accessed April 13, 2021).
[61] United Kingdom, DCDC, *JDP 0-30: Air and Space Power* (Shrivenham: DCDC, 2017), 72.
[62] James Clay Moltz, 'The Changing Dynamics of Twenty-First-Century Space Power,' *Strategic Studies Quarterly* 13, no. 1 (2019): 66.
[63] Brent Ziarnick, *Developing National Power in Space: A Theoretical Model* (Jefferson: McFarland & Company, Inc., 2015), 12.
[64] Edward Burger and Giulia Bordacchini, *Yearbook on Space Policy 2017* (Switzerland: Springer, 2019), 55.
[65] Office of the Secretary of the Air Force. Twitter Post. May 28, 2021, 21:41 PM. https://twitter.com/secafofficial/status/1398378810874159118?s=24 (accessed May 29, 2021).
[66] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 107.
[67] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 107.
[68] Bleddyn E. Bowen, 'The RAF and Space Doctrine,' *The RUSI Journal* 0, No.0 (2018): 5.
[69] Air Chief Marshal Sir Mike Wigston. 'Speech – Day One.' Defence Space Conference 2020, Virtual Conference November 17-18, 2020. https://www.airpower.org.uk/defence-space-2020/programme/ (accessed November 17, 2020).
[70] David J. Lonsdale and Thomas M. Kane, *Understanding Contemporary Strategy* (Abingdon: Routledge, 2020), 233.
[71] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 20.
[72] The Chinese terminology for an astronaut.
[73] James Clay Moltz, 'The Changing Dynamics of Twenty-First-Century Space Power,' *Strategic Studies Quarterly* 13, no. 1 (2019): 76.
[74] Mark Hilborne, 'China's space programme: A rising star, a rising challenge,' *Lau China Institute Policy Series 2020* 02, (2020): 5.
[75] His Highness Sheikh Mohammed. Twitter Post. April 10, 2021, 10:54 AM, https://twitter.com/hhshkmohd/status/1380821550304223234?s=24 (accessed April 12, 2021).
[76] Mark V. Kauppi and Paul R. Viotti, *International Relations Theory* (Lanham: Rowman & Littlefield, 2020), 157.
[77] Marco Aliberti and Ksenia Lisitsyna, *Russia's Posture in Space* (Switzerland: Springer, 2019), 84.
[78] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 60.
[79] Ibid., 61.

[80] Samuel P. Huntington, *The Clash of Civilizations* (London: Simon & Schuster UK Ltd., 1997), 21.
[81] SpaceX. 'Mission,' SpaceX, https://www.spacex.com/mission/ (accessed May 29, 2021).
[82] SpaceX. 'Dragon,' SpaceX, https://www.spacex.com/vehicles/dragon/ (accessed May 29, 2021).
[83] Christian Davenport, *The Space Barons* (New York: Public Affairs, 2018), 4.
[84] Blue Origin, 'New Shepard,' Blue Origin, https://www.blueorigin.com/new-shepard (accessed May 29, 2021).
[85] Nicholas Onuf, *Foreign Policy in a Constructed World* (Abingdon: Routledge, 2015), 78.
[86] Alister Miskimmon, Ben O'Loughlin and Laura Roselle, *Strategic Narratives* (New York: Routledge, 2013), 176.
[87] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 133.
[88] Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2013), 143.
[89] Ibid., 54.
[90] Alister Miskimmon, Ben O'Loughlin and Laura Roselle, *Strategic Narratives* (New York: Routledge, 2013), 12.
[91] Ibid., 5.
[92] Vendulka Kubalkova, *Foreign Policy in a Constructed World* (Abingdon: Routledge, 2015), 66.
[93] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 215.
[94] Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2013), ix.
[95] Mark V. Kauppi and Paul R. Viotti, *International Relations Theory* (Lanham: Rowman & Littlefield, 2020), 144.
[96] United Nations. United Nations General Assembly. *Resolution 75/36*. (New York: UNGA, 2020).
[97] United Nations. 'Voting Record,' United Nations General Assembly, https://digitallibrary.un.org/record/3893851 (accessed May 29, 2021).
[98] Ibid.
[99] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 20.
[100] Alister Miskimmon, Ben O'Loughlin and Laura Roselle, *Strategic Narratives* (New York: Routledge, 2013), 5.
[101] Brian Weeden, 'Norms of Behaviour and Potential Conflicts in Space,' in *Outer Space; Earthly Escalation* (Washington DC: DOD, 2018), 49.
[102] Eligar Sadeh, *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 55.
[103] Ken Booth and Nicholas Wheeler, *The Security Dilemma* (Basingstoke: Palgrave Macmillan, 2008), 4.
[104] Mark V. Kauppi and Paul R. Viotti, *International Relations Theory* (Lanham: Rowman & Littlefield, 2020), 151.
[105] United States. Department of Defense. *Defense Space Strategy Summary*. (Washington DC: DOD, 2020), 1.
[106] United States. Department of Defense. *Defense Space Strategy Fact Sheet*. (Washington DC: DOD, 2020), 1.
[107] The UK MOD, and other Allied Departments of Defence, have also seized on this vocabulary for describing the space domain.

[108] Nancy Gallagher in *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 52.
[109] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 18.
[110] NATO. Joint Air Power Competence Centre. *Space: NATO's Newest Operational Domain*. (Germany: JAPCC, 2020), 1.
[111] Opening speeches, *Defence Space 2020*, 17-18 November 2020, https://www.AirPower.org.uk/defence-space-2020/programme/ (accessed November 18, 2020).
[112] Bleddyn E. Bowen, 'The RAF and Space Doctrine,' *The RUSI Journal* 0, no.0 (2018), 2.
[113] United Kingdom. Development, Concepts and Doctrine Centre. *Global Strategic Trends*. 6th ed. (Shrivenham: DCDC, 2018), 53.
[114] David Silverman, *Qualitative Research* (London: SAGE Publications Ltd., 2011), 84.
[115] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014), 50.
[116] Samuel P. Huntington, *The Clash of Civilisations* (London: Simon & Schuster UK Ltd., 1997), 59.
[117] David J. Lonsdale and Thomas M. Kane, *Understanding Contemporary Strategy* (Abingdon: Routledge, 2020), 229.
[118] Peter Frankopan, *The New Silk Roads* (London: Bloomsbury Publishing Plc., 2018), 269.
[119] Brent Ziarnick, *Developing National Power in Space: A Theoretical Model* (Jefferson: McFarland & Company, Inc., 2015), 1.
[120] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 94.
[121] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University, 2007), 2.
[122] United States. DOD. *Defense Space Strategy Fact Sheet*. Washington DC: DOD, 2020.
[123] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 197.
[124] Edward Burger and Giulia Bordacchini, *Yearbook on Space Policy 2017* (Switzerland: Springer, 2019), 51.
[125] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 197.
[126] Edward Burger and Giulia Bordacchini, *Yearbook on Space Policy 2017* (Switzerland: Springer, 2019), 158.
[127] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014), 39.
[128] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 215.
[129] Ibid.
[130] Alister Miskimmon, Ben O'Loughlin and Laura Roselle, *Strategic Narratives* (New York: Routledge, 2013), 113.
[131] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014).
[132] Linda Dawson, *War in Space* (Switzerland: Springer, 2018), 18.
[133] Joshua P. Carlson, *Spacepower Ascendant* (Great Britain: Amazon, 2020), 88.
[134] Namrata Goswami, 'Explaining China's space ambitions and goals through the lens of strategic culture,' *The Space Review*, 18 May 2020. https://www.thespacereview.com (accessed April 12, 2021).
[135] Alister Miskimmon, Ben O'Loughlin and Laura Roselle, *Strategic Narratives* (New York: Routledge, 2013), 104.

[136] Ken Booth and Nicholas Wheeler, *The Security Dilemma* (Basingstoke: Palgrave Macmillan, 2008), 270.
[137] Henry Kissinger, *World Order* (London: Penguin, 2014), 226.
[138] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014), 44.
[139] Theresa Hitchens, 'DoD Faces Tough Decisions On Space Rules,' Breaking Defense, https://breakingdefense.com (accessed February 2, 2021).
[140] Alistair Bunkall, 'Russian satellite test had "characteristics of a weapon",' Sky News (23 July 2020), https://news.sky.com (accessed October 15, 2020).
[141] United Kingdom. Ministry of Defence Twitter. @DefenceHQ (Jul 23, 2020 3:48PM) (accessed October 15, 2020).
[142] Theresa Hitchens, 'DoD Faces Tough Decisions On Space Rules,' Breaking Defense, https://breakingdefense.com (accessed February 2, 2021).
[143] Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), 299.
[144] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 55.
[145] Linda Dawson, *War in Space* (Switzerland: Springer, 2018), 83.
[146] Marco Aliberti and Ksenia Lisitsyna, *Russia's Posture in Space* (Switzerland: Springer, 2019), 58.
[147] Vendulka Kubalkova, *Foreign Policy in a Constructed World* (Abingdon: Routledge, 2015), 34.
[148] Joseph S. Nye Jr., *Understanding International Conflicts: An Introduction to Theory and History* (New York: Pearson Longman, 2007), 7.
[149] Ibid., 207.
[150] Virgin Orbit could provide the opportunity for space launch via a re-purposed Boeing 747. While this could allow for horizontal launch options from almost anywhere in the world, the current limiting factor would be the size of the space craft that could be launched.
[151] Thomas C. Hoerber and Emmanuel Sigalas, T*heorizing European Space Policy* (Lanham: Lexington Books, 2017), 59.
[152] Everett C. Dolman, *Astropolitik* (Abingdon: Frank Cass Publishers, 2002), 86.
[153] Edward Burger and Giulia Bordacchini, *Yearbook on Space Policy 2017* (Switzerland: Springer, 2019), 39.
[154] Ibid.
[155] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 43.
[156] Joshua P. Carlson, *Spacepower Ascendant* (Great Britain: Amazon, 2020), 49.
[157] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 19.
[158] Ibid.
[159] Alister Miskimmon, Ben O'Loughlin and Laura Roselle, *Strategic Narratives* (New York: Routledge, 2013), 129.
[160] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014), 22.
[161] And by extension, generally the Five Eye communities of US, UK, Australia, Canada and New Zealand.
[162] President Xi Jinping cited in Peter Frankopan, *The New Silk Roads* (London: Bloomsbury Publishing Plc., 2018), 275.
[163] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014), 39.

[164] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 201.
[165] Mark V. Kauppi and Paul R.Viotti, *International Relations Theory* (Lanham: Rowman & Littlefield, 2020), 154.
[166] Linda Dawson, *War in Space* (Switzerland: Springer, 2018), 106.
[167] Colin S. Gray, *Perspectives on Strategy* (Oxford: Oxford University Press, 2013), 199.
[168] Namrata Goswami, 'What's Ahead for China's Space Program in 2021?', *The Diplomat* (22 January 2021): 5, https://thediplomat.com (accessed February 5, 2021).
[169] Ibid.
[170] John J. Klein, *Space Warfare* (Abingdon: Routledge, 2006), 40.
[171] Brent Ziarnick, *Developing National Power in Space: A Theoretical Model* (Jefferson: McFarland & Company, Inc., 2015), 2.
[172] Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), 1.
[173] Thomas C. Hoerber and Emmanuel Sigalas, *Theorizing European Space Policy* ((Lanham: Lexington Books, 2017), 112.
[174] Marco Aliberti and Ksenia Lisitsyna, *Russia's Posture in Space* (Switzerland: Springer, 2019), 57.
[175] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 227.
[176] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014), 170.
[177] Ibid.
[178] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 5.
[179] Jim Malachowski, 'Don't Gamble on the Next Space Race: Win in the Orbital Gray Zone Now,' *Space Force Journal* 1 (2021): 2 https://www.spaceforcejournal.org (accessed February 8, 2021).
[180] Thomas C. Hoerber and Emmanuel Sigalas, *Theorizing European Space Policy* (Lanham: Lexington Books, 2017), 105.
[181] Michael Sheehan, *The International Politics of Space* (Abingdon: Routledge, 2007), 6.
[182] This has been in development for almost five years and still has not been republished. At the time of writing this paper it was understood that a UK national space strategy would be released in Summer 2021.
[183] David J. Lonsdale and Thomas M. Kane, *Understanding Contemporary Strategy* (Abingdon: Routledge, 2020), 76.
[184] Eligar Sadeh, *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 2.
[185] James Clay Moltz, in *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 32.
[186] Roger Handberg, in *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 259.
[187] Eligar Sadeh, *Space Strategy in the 21st Century* (Abingdon: Routledge, 2013), 1.
[188] Kenny Grosselin, 'A Beneficial and Striking Success: Diplomatic Spacepower and Communication Satellites in the Early Space Age (1958-1972),' *Space Force Journal* 1, https://www.spaceforcejournal.org (accessed February 8, 2021), 12.
[189] Joan Johnson-Freese, *Space As A Strategic Asset* (New York: Columbia University Press, 2007), 6.
[190] Ibid.

[191] John J. Klein, *Space Warfare* (Abingdon: Routledge, 2006), 62.
[192] Christopher Fabian, 'Psychology of Deterrence in Sino-US Space Relations,' *Space Force Journal* 1, (2021): 2, https://www.spaceforcejournal.org (accessed February 8, 2021).
[193] Thomas Mahnken, 'Thinking About Competitive Strategies,' in *Competitive Strategies for the 21st Century: Theory History and Practice* (Stanford: Stanford University Press, 2012), 6.
[194] Shiping Zheng, in *Foreign Policy in a Constructed World* (Abingdon: Routledge, 2015), 217.
[195] Erin Meyer, *The Culture Map* (New York: Public Affairs, 2014), 39.
[196] Jim Malachowski, 'Don't Gamble on the Next Space Race: Win in the Orbital Gray Zone Now,' *Space Force Journal* 0, No.0, (2021): 14.
[197] Christopher Fabian, 'Psychology of Deterrence in Sino-US Space Relations,' *Space Force Journal* 0, No.0, (2021): 5.
[198] Samuel P. Huntington, *The Clash of Civilizations* (London: Simon & Schuster UK Ltd., 1997), 129.
[199] Peter Frankopan, *The New Silk Roads* (London: Bloomsbury Publishing Plc., 2018), 285.
[200] Brent Ziarnick, *Developing National Power in Space* (Jefferson: McFarland & Company Inc., 2015), 75.
[201] Ibid.
[202] SpaceX. 'Missions – Mars,' SpaceX, https://www.spacex.com/human-space flight/mars/index.html (accessed May 30, 2021).
[203] Benjamin Silverstein and Ankit Panda, 'Space is a Great Commons. It's Time to treat it as such.' *Carnegie Endowment for International Peace*. https://carnegieendowment.org (accessed March 12, 2021).
[204] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 5.
[205] United Kingdom. Government Office for Science. *Satellite-derived Time and Position: A Study of Critical Dependencies* (London: Government Office for Science, 2018), 7.
[206] Ken Booth and Nicholas Wheeler, *The Security Dilemma* (Basingstoke: Palgrave Macmillan, 2008), 279.
[207] Paul J. Bolt and Sharyl N. Cross, *China, Russia and 21st Century Global Geopolitics* (Oxford: Oxford University Press, 2018), 130.
[208] Everett C. Dolman, *Astropolitik* (Abingdon: Frank Cass Publishers, 2002), 1.
[209] James Gavin, *War & Peace in the Space Age* (London: Hutchinson & Co. Ltd., 1959), 260.
[210] Colin S. Gray, *Another Bloody Century* (London: Phoenix, 2005), 291.
[211] Christopher Fabian, 'Psychology of Deterrence in Sino-US Space Relations,' *Space Force Journal* 1, (2021): 5, https://www.spaceforcejournal.org (accessed February 8, 2021).
[212] Jim Malachowski, 'Don't Gamble on the Next Space Race: Win in the Orbital Gray Zone Now,' *Space Force Journal* 1 (2021): 1-2, https://www.spaceforcejournal.org (accessed February 8, 2021).
[213] James Landale, 'Can space diplomacy bring order to the final frontier?', *BBC News*, 26 September 2020, https://www.bbc.co.uk/news/uk-54296015 (accessed January 25, 2021).
[214] Bleddyn E Bowen, 'The RAF and Space Doctrine,' *The RUSI Journal* 0, no.0 (2018):5.

Viewpoint

# The Seam between Chaos and Order

By Group Captain Emma Keith

**Biography:** Group Captain Emma Keith is the Commandant of the Tedder Academy of Leadership with responsibility for setting the direction of leadership and command training across the RAF. The Academy is also the Headquarters for coaching and mentoring. The first female to run RAF Officer training, the College won its first triple outstanding from OFSTED during her tenure. Emma received a national award as an Agent of Change for her inclusive approach. Group Captain Keith has a Master's in Leadership and a level 8 diploma in Strategic Direction. With a passion for helping people to achieve their full potential, Group Captain Keith also has a Diploma in Coaching, is an experienced Mediator and is a qualified practitioner in several self-awareness tools.

**Abstract:** As a military organisation we are required to tread the line between chaos and order. This viewpoint considers how leadership can be used to navigate this inevitable tension to exploit opportunity, navigate risk and to ensure that the Royal Air Force (RAF) retains a competitive edge now and in the future operating environment. This viewpoint considers how personal accountability is essential and that leaders at all levels must take responsibility for their own environment.

**Disclaimer:** The views expressed are those of the authors concerned, not necessarily the MOD. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without prior permission in writing from the Editor.

## Introduction

The world in which the RAF operates is increasingly complex, faced with fresh challenges, enabled by advancing technology and an enemy's willingness and ability to adapt and fight in diverse ways. It is imperative that as a Service we continue to force ourselves to consider what mindset, leadership and command skills will be required to meet these encounters with confidence and ability. As a military organisation, constantly confronting unknown and ever evolving challenges, we are required to tread the line between chaos and order, balancing the freedom, creativity, and necessity of operating in chaos with the discipline and structure required in many elements of our day-to-day work. This seam between chaos and order, where opportunity and risk, and success and failure collide is a fascinating environment to explore. Clinical Psychologist, Jordan Peterson describes chaos as 'the unexplored territory', he states:

> 'Chaos is what extends, eternally and without limit, beyond the boundaries of all states, all ideas, and all disciplines… Chaos is where we are when we do not know where we are, and what we are doing when we do not know what we are doing. It is, in short, all those things and situations we neither know nor understand.'[1]

He continues to expand that chaos can generate fantastic freedom but that it can also be a dreadful freedom as chaos is unbounded. Whilst chaos can often be heralded as a mechanism for sparking creativity and opportunity, it must be acknowledged it also carries real risk of carnage and disorder. We need the skills and adaptability to tiptoe this fragile line.

In comparison, order is described by Peterson as the explored territory;

> 'The hundreds-of-millions-of-years-old hierarchy of place, position, and authority. That is the structure of society…order is tribe, religion, hearth, home, and country… it is the flag of the nation. It is the value of currency. Order is the floor beneath your feet, and your plan for the day.'

He extrapolates by stating that order is where our expectations are met, where things turn out as we assume that they will. We have a plan, we execute it, and we return confident in our abilities and knowledge. As a warning he states, 'order is sometimes tyranny and stultification, as well, when the demand for certainty and uniform and purity becomes too one-sided.'

## The Seam

This tension in the seam between order and chaos is arguably where competitive edge lies. An organisation that can maintain essential structures whilst not allowing itself to become rigid; an organisation that can ebb and flow into chaos without losing control can conceivably garner the advantage in a fluid and changing environment. The requirement for rapid adaptability to a multi-faceted changing scenario has been apparent in the war in Ukraine with a constantly evolving threat requiring a myriad of shifting responses. The Ukrainian's methods

have swiftly evolved in response to Russian tactics to target their Critical National Infrastructure. The Ukrainians have shifted from having limited Air Defence ability pre-war in the form of Russian Integrated Air Defence System (IADS) to intercepting most missiles via multiple means. Their defence has been reinforced by Man Portable Air Defence Systems (MANPADS) and a limited number of gifted Surface-to-Air Missiles (SAMs), but they have also used technology and the strength of national feeling to their advantage by creating an app that allows the public to report incoming missiles, where the missiles are and what direction they are heading in. They have harnessed power and information in new and novel ways. Thrown into chaos, they have, out of necessity, reacted at pace to the evolving conditions. There is much to admire as they have truly embraced rapid innovation, moving capabilities from concept to combat in weeks vice years. They have not achieved this alone; the support of allies has been imperative, highlighting the power and influence of international relationships. The Ukrainian's have become comfortable with failing fast but failing forward, taking the lessons, experimenting, and improving at a speed of relevance as their existence depends on it. A catastrophic event which decimated any sense of order has necessitated a transformational and heroic response. It is imperative that we ask ourselves what would our response be? How would we cope thrown from order into chaos with high intensity warfighting against a near-peer adversary? We must challenge ourselves to improve our reaction times and move concept to capability at a faster rate. For example, are we being ambitious enough with projects such as Agile Combat Employment (ACE)? Is this really new doctrine or old doctrine re-branded? How do we create the atmospherics of a burning platform prior to it becoming a reality to ignite necessary action and prevent organisational stagnation? We have long held a philosophy of train hard, fight easy but we must acknowledge that the training need has adjusted and must keep pace with the context or else we will be forced to fight hard.

The Ukranian President, Volodymyr Zelenskyy was sworn into office on 20 May 2019. His election caused headlines due to his previous career in TV and specifically as a comedian. He founded 'The League of Laughter' non-government organisation, produced ten feature length movies, won more than 30 awards at the National Television awards in Ukraine and is a prize-winner of numerous international film festivals and media forums. His is not the usual career back story for a leading politician. As the COVID crisis took hold in 2020 he could be forgiven for assuming this would be the major challenge of his Presidency. Following the outbreak of hostilities in Donbas he transitioned overnight to a war time leader with the sovereignty of his country under substantial threat. I opine that his unconventional background has been a major advantage for President Zelenskyy at a time where warfare is influenced by social media and online communication just as it is by traditional military battles. The President's ability to exert influence and impact the battle space via media content has been outstanding. His use of tone, rhetoric, and cadence in his addresses have all born the hallmarks of a seasoned actor who knows how to connect to his audience. Little is accidental, streaming footage from central Kyiv is an intentional message of defiance to the enemy and solidarity with his soldiers, his continual wearing of combat clothes portrays the vision of a war time leader who is prepared to fight, these decisions have been incisive and powerful. His actions make it clear that whilst

he may be utilising acting skills to his advantage, he is not faking his part. By remaining in the country, and amid the fighting, despite the significant risk to his, and his families lives, he has demonstrated the willingness to make sacrifices to hold his ground and to fight for what he believed in. Leadership in the RAF is defined as, 'the projection of character, principles and behaviours that inspire people to succeed.'[2] He has used technology to incredible effect to aid the projection of his character, maximised his natural ability to connect with an audience and built this on a foundation of someone who has principles and will live by them via their behaviours. He presents as confident in the chaos. It is clear to see that his leadership has been pivotal to the national response. What lessons can we as a Service take from the leadership that we are witnessing?

As we operate in a constantly evolving world, arguably in a period of chronic chaos – war, pandemics, climate crisis, energy and food insecurity and financial instability, what skills do we need our leaders to demonstrate and how do we inculcate this? We must take context into account. What type of leader is required in war time versus peace? Is peace clear cut? Whilst not at war I describe our current context as a period of chronic chaos. Do these contrasting environments demand distinct characteristics? Can a leader thrive in both chaos and order or is it the right leader at the right time? The RAF has an illustrious history, shaped by leadership at all levels, but how can we use leadership in the future to continue to enhance and maximise our position in navigating this tight rope between chaos and order? Leadership has a critical role in ensuring that the organisation continues to accumulate the cultural ability to flex and shift as the context dictates. The RAF will continue to require world-class leadership skills at every level to meet the current and future operating context.

It is imperative to recognise that an individual does not need to have an official position of authority to influence the behaviour of others, and to lead. In a military hierarchical organisation with seniority on display, it can be extremely easy to look upwards for leadership and thus to abdicate your own personal accountability for the environment around you. This is not to say that we should not have high expectations of our seniors, of course we should. It is vital that an individual in a position of authority recognises the impact that they can have, and their role in setting the command climate within their area of responsibility. I propose that as a person with positional authority, the shadow they cast is enhanced. If the Boss is in a difficult mood, it can have a disproportionate impact on members of the team. It should be noted that this influence can also be used to positive effect, casting sunlight with positive behaviours. The relevant point though is that just because we have a Boss it does not relinquish us of our own accountability to lead.

The RAF requires a culture that maximises the full intellectual and physical capacity of every person; quite simply success cannot be achieved by the leadership of one person at the top or by a senior team. It is not easy to remain engaged, particularly against fiscal constraints and infrastructure challenges, however, it is all too simple to blame the context and to let our

own standards slide. *AP7001* advocates the importance of *Leading Yourself*. We must gain full self-awareness of our own strengths and weaknesses. No one person can cover all angles, we all need to understand the key strengths we bring to a team and where we need others to mitigate our weaknesses. Observing and acknowledging other strengths is also an opportunity for our own self-development and increased self-knowledge. Self-awareness, however, is not the holy grail of leadership that many uphold it to be as on its own it is contestably pointless. Consider the Boss who states, 'I know I can be a bit aggressive but that is just who I am.' The individual has great self-awareness, but this is not having any discernible difference on those experiencing their behaviour! The second essential part to leading yourself is self-management, changing behaviour because of the new-found awareness. Only when we have both elements in harmony, we can really claim to be Leading Ourselves.

How often do we truly reflect on our own responsibility and accountability in a situation as opposed to discussing the answerability of those around us? An important part of the *Lead Yourself* narrative is that the standard you walk past is the standard that you accept. This is a familiar phrase in training, but in real life, it is easy to ignore bad behaviour, accept a poor piece of work or simply to fail to report an infrastructure issue. These seemingly trivial details impact our pride, sense of purpose and the professionalism of the environment around us. There is a clear correlation between the lowering of standards and deficient performance on operations, ownership of our environment and personal conduct matter. Instilling these habits and standards whilst in the calm of order will mean they are habitual when required to provide stability in chaos.

Whilst it is a fully accepted academic term, I dislike the phrase 'followers,' it is not active enough as a label. If used, I believe the term requires a word in front of it, such as 'engaged follower' or a 'responsible follower.' I lean to the view of David Marquet, author of *Turn the Ship Around: A True Story of turning Followers into Leaders*. Marquet talks about the positive impact and intellectual capacity generated by turning his followers into leaders when he transitioned the USS (US ship) Santa Fe from the worst to the highest performing submarine in the fleet.[3] I propose that whilst followership skills are essential, we do not wish our people to be a 'follower' we wish them to be an engaged and active leader who utilises followership skills at appropriate times and pertinent to the current operating context. This may sound like a subtle difference, but it is an important distinction. In high performing teams you do not have a leader and a team of followers, you require leadership at all levels.

As Stephen Covey Snr points out, spending time and energy on factors which are outside of our control can lead to feelings of inadequacy and helplessness. Many people can get trapped in this space using all their energy on things they cannot change. He refers to this as our circle of concern; too much time focussing in this area can lead to a downward cycle of motivation and energy. This behaviour could be particularly harmful amid chaos where many elements will be outside of personal control and operating in ambiguity is vital. It can also, unfortunately, lead to people blaming and shaming others thus creating a toxic environment.

Instead, Covey recommends that we become mindful of our circle of influence. He proposes that if we focus our attention on our circle of influence then the circle will naturally expand allowing us to extend our area of impact.[4] If we operate in this space where we can enact change and influence, then our motivation and energy naturally increase and we, and our team, start to move into a positive flow and to provide discretionary effort; another key factor in high performing teams. We can start to influence and control the elements close to us and to bring elements of order to chaos.

Our own military doctrine supports the view of leadership at all levels. Mission command is the basis of our command philosophy and the need to delegate decisions down to the appropriate level is well versed. Doctrine clearly explains that this is to ensure timely decision making thus capitalising on opportunities, and mitigating risks, within a situation. Care must be taken in the re-writing of doctrine; I posit that often the change required is an investment of our time to ensure that we are enacting the good doctrine that we already have versus re-writing.

It would be easy to rest on the laurels of the RAF's past successes as a Service and to advocate that the key tenets of leadership never change. We must be honest that we have also had failures and a rapidly evolving context demands us to question what leadership could look like in the future, for example, what does leadership and command look like in the space and cyber operating environments? It is true that there are core leadership principles that hold true, such as the requirement to communicate, but the way we enact the principles has evolved with the advent of advanced technology and virtual and dispersed workforces. Is communication also now enough? In *AP7001*, the Tedder Academy changed the word 'Communication' to 'Connection'. You can put a great deal of effort into communication but if it has not landed with the intended audience then it has been a waste of time and effort. Consider the earlier reflections of Zelenskyy's leadership and the critical element of a connection with the intended audience and a strengthening of a shared purpose. Leadership is the critical enabler to optimise the RAF's capability across multiple domains, to ensure that through connection we gain discretionary effort from our people to allow us to retain a competitive edge. We require teams that generate diversity of thought, that as a collective can operate in the seam between chaos and order carving and directing the way for success.

Finally, we must consider what behaviours are required to lead a multi-generational work force. Generations are grouped as follows:

- Baby Boomers – born 1946-1964
- Generation X – born 1965-1980
- Millennials – born 1981-1996
- Generation Z – born 1996-2010
- Generation A – born 2010-2024

The oldest members of Generation Z will now be in their mid 20's operating on the front line and in training roles throughout the organisation. In five years, we will have individuals from Generation Alpha joining the organisation. We still have members of Baby Boomers in the organisation for the next few years. There is much discussion about how we must ensure the organisation pivots to be attractive to the younger generations to entice and recruit talent, this is clearly vital particularly against the national landscape with a shortage of skills in areas such as engineering. This is in my view overly simplistic as we must also retain the amazing talent we already have from across the generations, it requires a multi-faceted approach. The younger generations must absolutely be listened to as they positively shape and influence the work environment, but I propose that they must also listen. The older generations can be referenced as outdated in the media but to me this is a dangerous approach. The older generations have experience and accumulated knowledge some learnt via hard lessons. It would be dangerous and naïve to dismiss these perspectives, as ever, in a truly inclusive organisation all people must contribute and only via honest and sometimes challenging debate can the real crux of an issue be identified, and the nuances of a situation be unpicked. If we are to operate decisively in the seam between chaos and order, we must organisationally consider what must alter but of equal importance what must be embedded and retained.

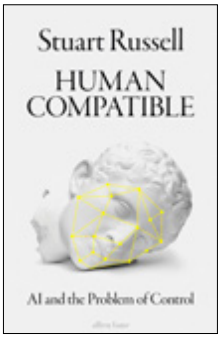
As the RAF's Training Requirements Standard Authority (TRSA) for Leadership and Command the Tedder Academy leads the direction and development of world class, through-career, air-minded Leadership and Command education and training, as such, the Academy sets the strategic direction for leadership in the RAF. The Academy is also the Headquarters for coaching and mentoring. Via input to formal training and informal initiatives such as, conferences, webinars and podcasts the Tedder Academy aims to start important conversations and to make individuals and teams reflect on how they can improve their individual and collective performance. High performing teams do not make excuses, they are not naïve, and they do not shy away from the realities of complexity, they aspire to overcome the issues rather than using them as an excuse.

The Tedder Academy's challenge to every person in Defence is to evoke a sense of pride and ownership in your organisation. The RAF will not succeed due to one brilliant person, it will succeed if we rise together as one team ensuring quality and professionalism and a bedrock of strong leadership is at its heart. Whatever rank, grade, or profession, you have an important part to play in ensuring that the United Kingdom's interests are defended at home and abroad. As a member of the RAF Whole Force, you are the RAF. Be the change that you want to see.

## Notes

[1] Jordan B.Peterson, *12 Rules for Life* (UK: Penguin Random House, 2018), 35-36.
[2] *AP7001* brochure edition 1 June 2020, Tedder Academy of Leadership.
[3] L.David Marquet, *Turn the Ship Around!: A True Story of Turning Followers into Leaders* (London: Penguin, 2015).
[4] Stephen Covey, *The 7 Habits of Highly Effective People* (London: Simon & Schuster UK Ltd, 2013), 88-89.

Book Review




# Human Compatible: AI and the Problem of Control

Author: Stuart Russell

**Publisher:** Allen Lane; 1st edition (8 Oct. 2019) (**ISBN:** 978-0241335208), 352 pages

Reviewed by Group Captain Emma Keith

## Introduction

*Human Compatible* considers the interface between humans and machines and asks the question of how we ensure that the AI we are creating is compatible with the world that humans want to live in. The author, Stuart Russell, is a professor of Computer Science at UC Berkeley, a published author on this topic and a recognised leading expert in artificial intelligence and machine learning. He is not an outside alarmist, he is at the very heart of AI and machine research and presents his concerns in an intelligent, persuasive, and logical way. The book is accessible to a general audience and provides a brilliant introduction to some of the more strategic issues associated with the rapid development and global investment in AI. It will equally appeal to the AI specialist to challenge them to view AI in alternate ways.

In clear and compelling language, Stuart Russell provides a unique perspective on the interaction between humans and machines, he draws on the past, present and the future to present a holistic and balanced view. The book is divided into three main sections, the first, explores ideas of intelligence in humans and in machines and it unpicks the definition of intelligence by questioning what we mean by intelligence? One comment that stood out was, 'Humans are intelligent to the extent that our actions can be expected to achieve our objectives. Machines are intelligent to the extent that their actions can be expected to achieve their objectives (p. 9).' Stuart Russell explores the concept that the vital component is in defining what the objectives are – for example, giving a machine the objective of saving the planet, might mean that it decides to delete the biggest risk to the planet – i.e. the human race.

Clearly highly knowledgeable in this area the author presents the content in easily accessible language and there is no technical knowledge required. I did, however, find the added appendix beneficial for when I wanted to understand a concept in greater depth.

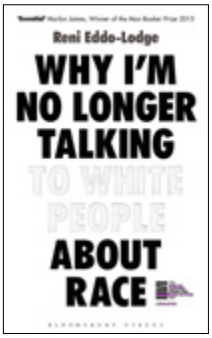
The second section is a fascinating look at some of the problems arising from imbuing machines with intelligence with a particular focus on the issue of control: retaining absolute power over machines that are more powerful than us. Comments such as, 'we have to face the fact that we are planning to make entities that are far more powerful than humans. How do we ensure that they never, ever have power over us? (p. 8)', certainly got my attention. This whole section really captured my imagination as the content cleverly weaved between technical detail and philosophical approaches to life and reinforced how we must consider if what we currently wish for from machines will turn out to be what we really want? It was fascinating to read the authors thoughts on how an intelligent machine may ensure it cannot be turned off as part of its desire to achieve its objective. This was not something I had previously considered, always assuming that an 'off' switch was a way out. The book also reflects on the amount of damage currently caused by basic algorithms nudging human behaviour via social media, for example, and ponders what truly highly intelligent AI could do?

The book concludes with a final section that suggests a new way to think about AI to ensure that machines remain beneficial to humans, forever. Stuart Russell summarises, 'Everything civilization has to offer is the product of our intelligence; gaining access to considerably greater intelligence would be the biggest event in human history. The purpose of the book is to explain why it might be the last event in human history and how to make sure that it is not (Preface).'

I found this a captivating read and regularly read sections out to those around me as the points made were profound and thought provoking. It really made me stop and think. The book does a brilliant job of making a technical and serious topic accessible, easy to engage with, and genuinely gripping. I also enjoyed his dry sense of humour and witty side comments that had the ability to make you laugh whilst simultaneously cleverly reinforcing a point. I highly recommend it to anyone who wishes to engage and understand the world in which we live in, arguably, it is essential reading for anyone who cares about our future.

Book Review

# Why I'm No Longer Talking To White People About Race




Author: Reni Eddo-Lodge

**Publisher:** Bloomsbury Circus; 1st edition (1 Jun. 2017) (**ISBN:** 978-1408870556), 304 pages

Reviewed by Flight Lieutenant Sabrina Sheikh

## Introduction

*Why I'm No Longer Talking To White People About Race* is a Sunday Times and New York Times Best Seller and the first book written by a black British author to top the British book charts. A 2018 Academic Book Week poll named it the most influential book written by a woman. In 2014, Reni Eddo-Lodge made the declaration that she had 'had enough' of talking to some types of people about race, in an attempt at self-preservation, which then catalysed the authoring of this book.

Reni Eddo-Lodge is an award-winning journalist, author and podcaster, listed as one of the best of 2018 by Apple Podcasts, whose involvement in feminist activism began whilst studying English literature. Listed in the Top 100 of the most influential people in the UK of African/African-Caribbean descent according to the Powerlist 2020 and 2021, Reni Eddo-Lodge continues to work on multiple platforms as an influential public voice.

In this self-declared paradoxical continuation of her conversation with white people, Reni Eddo-Lodge discusses Britain's relationship with Race and Racism. At a time when sensitivity around language such as, 'white people' and 'privilege' exists, *Why I'm No Longer Talking to White People About Race* convincingly calls out defiance, complacency and denial, with zero attempt to make the ugly content palatable.

Over a series of chapters, the book provides a distressing and important narrative of Britain's history that penetrates the present environment. Reni Eddo-Lodge analyses overt racism

through the centuries including the World Wars and the decades since, whilst also illustrating the links to present day with the addition of covert racism infiltrating all aspects of our environments and the enduring impact on the life chances of people of colour.

This book explores Britain's integral role in the exponential growth of the Slave Trade and persistent belief that people of colour are lesser, as witnessed in the contemporary treatment of black families, through multiple socioeconomic examples and case studies, including analysis of the Steven Lawrence investigation, education system, policing, social housing, and the weaponising of rhetoric.

This book explains 'White Privilege' and structural inequality. It also confronts the phenomena of racism in feminism over history and the disparities in gender equality work in practice -that primarily benefits white women- and does not live up to the inclusive intentions of feminist theory striving for equality across multiple issues beyond gender alone.

Reni Eddo Lodge explains that 'it is not all white people' and that she does not want to prompt 'White Guilt', but instead calls on white people to speak with other white people to help them recognise the prevalence of racism, accept their privilege, and leverage it to advocate for non-white causes. She provides a clear call to action, challenging those who want to contribute to race equality, to do it incrementally, privately in everyday actions and not for short term public acclaim, accepting that it is a long haul, it is messy -not binary- and it is uncomfortable.

RAF personnel are adept at stepping into unfamiliar and uncomfortable territory. However, this challenge does not wear the soles of our boots, but rather test our agility in the conceptual and moral components as a matter of leadership and resilience at every level, all genders, and all social and educational backgrounds. The subject matter challenges us to reflect on our blind spots, recognise normalised behaviours and an organisations' vulnerability to systemic inequality. Reni Eddo-Lodge unapologetically lifts the veil and helps the reader understand what structural racism is and where it is spawned from.

> 'Structural' is often the only way to capture what goes unnoticed…the implicit biases, snap judgements made on perceptions of competency... it is not just about personal prejudice, but the collective effects of bias'. (p. 65)

Resistance to acknowledging structural racism is commented on with recognition that her audience may not wish to be alerted to a system that benefits them at the expense of others.

Serving in the military is not to live in a vacuum immune to the issues discussed in this book. It may be useful to acknowledge that we continue to be influenced and influential within our work environments as well as our domestic and social circles.

The Wigston Report 2019 was a useful step toward recognising the disparities that exist within our Service. There is a level of discipline and integrity required to wear a uniform, and to an RAF audience the challenge of Racism can be viewed as an opportunity to once again step up to a task that others may feel is *just a bit too difficult*. There is a consensus in race equality literature that it is no longer enough to be 'not racist', we must be 'anti-racist'. In a 2020 address to the RAF BAME Network Air Chief Marshal Sir Mike Wigston, Chief of Air Staff stated that:

> 'It isn't just about zero tolerance of the perpetrator of inappropriate and illegal behaviour, it's also about zero tolerance for bystanders and it starts with us and the cultures we work in'.
>
> Air Chief Marshal Sir Mike Wigston, Chief of Air Staff 2020

This book will help inform the readers reflections on why the lived experience of people of colour is different and not equal to white people. In the wake of the Wigston Report there has been greater attention toward the sharing of lived experience to improve understanding of the issues and develop empathy for those who feel the effects, from those who do not. Throughout the text Reni Eddo-Lodge expertly navigates the multiple roles: as insider researcher critiquing the data, translating history and illustrating her own lived experience. She states that:

> 'Amid every conversation about nice white people feeling silenced by conversations about race, there is a sort of ironic and glaring lack of empathy' (p. xi)

She goes on to describe how she is asked by white people as how to fix it and non-white people how to cope. Acknowledging that racism is exhausting, Reni Eddo-Lodge empathises with the desperation of non-white people seeking change, and the difficulty and discomfort to think about how 'whiteness has silently aided' people in life (p. 221).

Empathy is not only important in leadership, but a useful ingredient to reaching understanding and acceptance that change is needed. Change management theory teaches us that there is an element of grieving involved in the journey toward change, and that grief includes feelings of anger, disbelief, and denial, which are themes consistently visited throughout the book.

Reni Eddo-Lodge comments on 'White Denial', by people who are defiant and those who have been taught not to acknowledge colour, describing the bewilderment and impatience to talk, rather than listen to the person of colour. In chapter 3 she describes a scenario conversing with her friend's French white girlfriend, and the shared beliefs that swiftly turned to differences anger and defensiveness 'like every word I've ever heard before' and then an assessment of the social implications of being accused of causing an atmosphere, being a 'reverse racist' and no longer welcome (p. 90-91). She talks about an emotional disconnect & communication gap between white people and people of colour and convincingly illustrates that they do not enter

conversations about race from equal positions, stating that for people of colour 'it is truly a lifetime of self-censorship' (p. xii).

> 'Entering the conversation with a defiant white person is frankly a dangerous task for me...I have to tread incredibly carefully, because if I express frustration, anger or exasperation at their refusal to understand, they will tap into their pre-subscribed racist tropes about angry black people... it's likely that their white friends will rally around them…trying to engage with them and navigate their racism is not worth that'. (p. xi)

This is the most important book you will read, whether you are interested in diversity & inclusion, confused by it, angered by it, or have any other feelings about Britain's relationship with racism - read this book. It will lift the veil of mystery for those who are struggling to see the issues and/or what to do about them. It puts into words what many seeking equality struggle to express and calls readers to action.

Book Review

# The Weaponisation of Everything

Author: Mark Galeotti

**Publisher:** Yale University Press (14 Feb. 2023) (**ISBN:** 978-0300253443), 248 pages

Reviewed by Squadron Leader Beth Lindley

## Introduction

Published a month prior to the Russian invasion of Ukraine 24 February 2022, Mark Galeotti's *The Weaponisation of Everything: A Field Guide to the New Way of War* is nevertheless relevant and important reading for those studying how to fight hybrid warfare. Galeotti, as the inadvertent inventor of the phrase 'Gerasimov Doctrine', is keen that this book is not seen as advocacy for *the* new way of war, but rather a guide to *a* way of war that is increasingly playing out on the global stage. You may know it as 'Grey Zone Warfare. Asymmetric War. Tolerance Warfare. Unrestricted War. Non-Linear Warfare.' (p. 14) Or, in current military parlance, sub-threshold conflict.

'It is early on the morning of 23 February 2014' the first of many case studies, historical or hypothetical, that Galeotti artfully uses to illustrate his point and open every chapter. The Russian invasion of Crimea on that day is described as 'the first true "hybrid war" conquest'. Galeotti highlights Russia's use of 'deception and treachery', that is to say, 'little green men' and cyberattacks, in a 'ruse [that] is pretty transparent, but it gives Kyiv and the West some pause.' A pause long enough for the peninsula to be, at least for now, irrevocably taken. Case studies include an attack on the National Grid, biohazards in the water supply (a true story from 1570), and 'fake news' about Catherina Medici. This 'new way of warfare' is not new. It's not just Russia, either: Galeotti outlines how 'they' accuse 'us' in the West of the same and call it *gibridnaya voina*. (pp. 12-14)

We learn that the term 'hybrid war' was so-called by Frank Hoffman, in reference to the militant group Hezbollah's battle against the state military of Israel. Now an umbrella term for unconventional warfare, the Western Centre of Excellence in Finland includes state actor activity in the definition of hybrid war, meaning any combination of 'overt and covert military and non-military means'. (p. 15) In other words, everything.

The idea of the 'weaponization of everything' isn't new, either, having been in general use since 2017 and '[reflects] a kind of nostalgic amnesia for a lost world that never really existed' (p. 15) in which civilians were not involved in conflict, as though the Russians themselves didn't use rape and murder as a weapon of war against Europe in the 20th century.

The 'unprecedented interconnectivity of the modern world' (p. 16) enables new methods of warfare, through cyber, space, and the electromagnetic spectrum, as Galeotti demonstrates throughout the book, yet examples of hybrid warfare can be found everywhere throughout history.

Globalisation is viewed as the cause of this perceived shift – 'interconnectivity' – but really that means having a better understanding of wars that happen far away. Civilian casualties are nearly impossible to hide in the age of social media and mobile phones. 'By definition everything becomes public; the only question is how quickly and with what spin.' (p. 33) For Western democracies, public opinions count when it comes to wars. It also means the potential for information exploitation has exponentially increased.

Sub-threshold activity is that which subverts an enemy's expectations or freezes their ability to react, whether through confusion/deniability or attack, which we see in Russia in 2022 and in Rome in the third century BC. It is just the means which have changed.

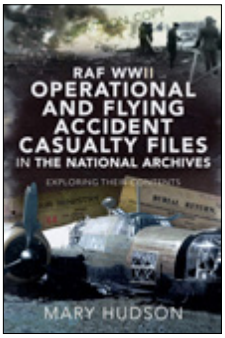
Importantly, *The Weaponisation of Everything* is not 'apocalyptic', as Galeotti describes most other work on this emerging form of conflict. Instead, he offers lessons and examples of previous hybrid warfare, described in plain language. Galeotti's pithy journalistic style makes for easy reading, if a little Hollywood, as he declares 'Nothing, after all, is more powerful when weaponised than intellect and imagination.' (p. 10)

Each chapter ends with a reading list under the heading 'Want to know more?' Here Galeotti provides a diverse selection of further reading, accompanied by his comments. For military theorists, academics, and planners, this complements the traditional understanding from doctrine such as the recent Integrated Operating Concept or the Joint Concept Notes for Multi-Domain Integration and Information Advantage.

*The Weaponisation of Everything* should be recommended to all air power professionals, regardless of Profession, but especially those involved in planning multi-domain operations. The problem with hybrid warfare is that the West treats it as new and dangerous. Galeotti

proves how this form of warfare is as ancient as war itself. One example that is not mentioned in the text is the Trojan Horse: deception is an ancient art. It does, however, require a risk appetite we are currently unfamiliar with, and an ability to conduct unconventional or ungentlemanly activity, else we risk being outpaced by our adversaries.

Book Review




# RAF WWII Operational and Flying Accident Casualty Files in the National Archives – Exploring their Contents

Author: Mary Hudson

**Publisher:** Air World (29 Oct. 2020) (**ISBN:** 978-1526783523), 256 pages

Reviewed by Flight Lieutenant Lilie Weaver

## Introduction

In writing this text, Mary Hudson draws on a long experience with the RAF, first as the spouse of a serving pilot, then as an officer in the WRAF, and later RAF, herself. Finally, after having achieved an MA in War Studies with King's College London whilst still serving, she worked for 14 years for the Air Historical Branch, dealing day-to-day with enquiries concerning the subject of this book – RAF casualty files.

She writes, therefore, with an explicit focus on the technical aspects of exploring such files, and as a guide to those who wish to conduct academic (or personal) research into those who lost their lives during WW2 serving with, or alongside, the RAF. Nonetheless, she is able to weave together the stories told by these documents into a compelling read. Whilst there is no narrative arc per se, Hudson uses examples of particular crews, reproducing the contents of their casualty files split across the sections of the book to give some insight into the chronological process of a crew who did not return from a sortie, the evidence sought as to their fate, kinforming, and onwards through to their eventual (sometimes post-war) identification, burial and commemoration.

The text is split into three sections, the first tracing the casualty handling process from occurrence and first notification through to confirmation, burial rites in the UK and overseas then to how those who went missing on duty were handled. The second focusses on the Missing Research and Enquiry Section (MRES) describing the extraordinary efforts both during and post- WW2 to identify the missing and accord respect and a suitable final resting place for all those who lost their lives serving with the RAF and Dominion (later Commonwealth) Air Forces. It neatly illustrates the ambivalence with which enemy aerial combatants were treated, both at home and in occupied Europe – much of the information on casualties during WW2 came from the German authorities through the International Committee for the Red Cross (ICRC) and this was reciprocated by the British. One of the more jarring photographs included shows the funeral (in Britain) of a Luftwaffe crew, their coffins draped in Nazi flags, with military and civilians alike according respect to the deceased, and similar certainly occurred for Allied casualties in Europe, whilst on the other hand there are cases described of downed airmen being summarily executed by the Gestapo.

It is this section in particular which is illustrated with the stories of the dead and missing through the MRES' files, and Hudson deserves credit for bringing colour to what is, necessarily at times, a morbid and unforgiving subject. She amply demonstrates the enormous lengths the Air Ministry went to both during and after the war to locate and identify aircrew (and others) lost in remote areas, often far from the front lines, and the determination of the Imperial (now Commonwealth) War Graves Commission to make sure that every single combatant who lost their lives in Allied service is commemorated by name.

The final section addresses more directly the involvement of the next-of-kin, describing the nature of correspondence both sent and received – letters received varied from effusive thanks for the efforts to provide timely news of a missing husband or son, to bitter complaints about too little, and even too much information being provided.

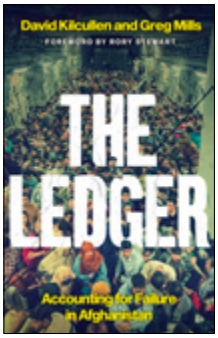
Richly illustrated throughout with contemporaneous photographs and copies of casualty files and related documents, Hudson deserves credit for including enough detail about each crew or casualty to contextualise their story, without the book becoming a series of anecdotes. She handles this sensitive subject unflinchingly, but with tact and clear sympathy for those affected by the loss and grief of losing a loved one to war.

The prose is necessarily precise, at times pedantic, but provides an invaluable and detailed resource for anyone attempting to tackle the byzantine and enormous administrative puzzle that is military bureaucracy. Patiently explaining each reference, department and function, Hudson draws on her considerable experience with archival research to provide a very detailed reference guide. In other hands, this could mean that the text is dry, but to her credit, Hudson has succeeded in producing a very readable account of the process of recording, storing and communicating casualty information during the chaos, and in the aftermath of WW2. Required reading for anyone considering tackling casualty files in the National Archives, and

a fascinating insight into both the bureaucracy and the personal stories surrounding a very human desire – to give loved-ones certainty and the reassurance of a final resting place in the face of losing their nearest and dearest in conflict.

Book Review

# The Ledger: Accounting for Failure in Afghanistan




Author: David Kilcullen and Greg Mills

**Publisher:** C Hurst & Co Publishers Ltd (9 Dec. 2021) (**ISBN:** 978-1787386952), 368 pages

Reviewed by Squadron Leader Chloé Bridge

## Introduction

Operation Pitting was a success story for the RAF with nineteen aircraft evacuating 15,000 eligible people from Afghanistan's capital Kabul in August 2021. Unfortunately, tactical military successes sometimes do not translate into strategic victory, which is one of the core themes of Kilcullen and Mills' book titled, *The Ledger: Accounting for Failure in Afghanistan*. Based on years of experience advising senior leaders and academic research, the authors provide a detailed analysis of what went wrong during the twenty-year Western intervention. This book is logical, balanced and, although frustrating at times, will appeal to all readers of geopolitical studies and especially for the thousands who served in Afghanistan.

The authors present their credibility from the beginning by detailing their military, academic, and literary credentials. A former Australian infantry officer turned Professor, Kilcullen is an expert on counter-insurgency, who has advised General Petraeus and authored several books on warfare. Mills, originally from South Africa, has advised the North Atlantic Treaty Organisation (NATO) and is an accomplished author specialising in African international relations. There is no doubt that both authors have extensive experience, serving not only in Afghanistan but also advising on and researching into the multifaceted nature of the wider geopolitical environment. Their aim for the book was to attempt to make sense of the chaos that erupted with the hasty withdrawal from Kabul. *The Ledger* does this by providing a good

introduction to the complexity and issues surrounding history, culture, and politics in and around Afghanistan, all strengthened by twenty pages of endnotes.

*The Ledger* is also well structured with its subtitle setting the tone from the start. Arranged over five chapters and nearly 300 pages, the authors use a combination of historical precedents and personal experiences to clinically analyse what went wrong before providing a ledger of dos and don'ts for future international missions.

The first two chapters detail the stories of two significant interventions, Vietnam by the United States and Afghanistan by the Soviet Union, with which the authors draw significant comparisons albeit with some differences. The inference is clear that lessons from previous interventions should have been learnt and implemented post-9/11. The authors argue that the West's failure to recognise that Afghanistan was different in terms of culture, politics, and economics was its biggest blind spot. In the third chapter, the authors provide detailed analysis of key reasons for the failures of the intervention. The themes of diplomacy, governance and development, and their respective failures continue through the fourth chapter where events leading to the evacuation in August 2021 are explained. From the inevitable finger-pointing of US politics to the collapse of the Afghan Military, there is plenty of criticism which may disappoint readers that opportunities were missed. The last chapter offers a more strategic picture of the impact of Afghanistan. Examples such as in Africa, specifically Mali and Somalia, are used as comparators to the challenges experienced in Afghanistan. With the notion of 'African solutions for African problems', the authors also provide strategic lessons for governments experiencing similar security instabilities.
The conclusion then details ten key factors for the failed intervention and translates these onto a slightly oversimplified ledger of dos and don'ts for the future. The authors argue that the most important need for interventions is that of a long-term political strategy, which was absent during the entire twenty years in Afghanistan. The book ends bleakly with a question of whether it was worth it, with the authors perhaps disappointingly concluding that it's too early to tell.

Throughout there are familiar references relatable for readers who have served within Afghanistan. These include TGI Fridays on the boardwalk at Kandahar Airfield and Camp Bastion as the largest British overseas base built since the Second World War. However, familiarity is likely to be replaced with frustration as the book repeatedly informs readers of failures on all sides amidst countless lives lost. The authors argue that nothing was inevitable with Afghanistan which makes for difficult reading. Nonetheless, *The Ledger* does attempt to rationalise the complex twenty-year intervention to ensure the West can better understand itself for the future.

Published in December 2021, the ink was barely dry on *The Ledger* before the next geopolitical crisis occurred namely Russia's illegal invasion of Ukraine in February 2022. As a result, some predictions within the narrative may have evolved including the authors' opinion that NATO

would be weakened by the intervention in Afghanistan. NATO's resolve and support to Ukraine may have just reversed that outlook but this is reflective of how quickly geopolitical situations can transform international relations and lessons from the past can be easily forgotten. Therefore, *The Ledger* is an important book for all military leaders and policy makers and with twenty years' worth of subject matter and many lessons to be understood, this book is highly recommended.

The Chief of the Air Staff's Fellowship Scheme provides a fantastic opportunity for RAF personnel of all ranks to undertake sponsored full and part-time postgraduate study at masters and doctoral level. There are a range of Fellowships available including an online part-time MA in Air, Space and Cyber Power, a full-time MA in Security and Strategy and an MPhil in International Relations at Cambridge. Further details, including eligibility criteria, are available in the DIN (2022DIN07-086) but if you or a member of your team are interested in applying then please contact the Directorate of Defence Studies team: CAS-ASDefenceStudies@mod.gov.uk

*https://www.raf.mod.uk/rafcasps*

https://www.facebook.com/RAFCASPS/

https://medium.com/RAF-CAPS

Produced by Air Media Centre, HQ Air Command. 4035_22AJ
UK Ministry of Defence © Crown Copyright, 2023

Sponsor Role email address: CAS-ASDefenceStudies@mod.gov.uk

ROYAL AIR FORCE
Centre for Air and Space Power Studies