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.

> '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.