Expeditions with MCUP

The Disinformation Age

Toward a Net Assessment of the United Kingdom's Cognitive Domain

Paul Ottewell

https://doi.org/10.36304/ExpwMCUP.2022.03

Abstract: This article analyzes the territory in which the battle of strategic narratives is fought—the *cognitive domain*—and the nature of the battle itself—*cognitive warfare*. It exposes three asymmetries between the United Kingdom, Russia and China. These are: (1) the maturity of cognitive warfare doctrine; (2) the ease with which cognitive warfare can be waged vice defended against; and (3) that illiberal states enjoy greater freedom of maneuver in the cognitive domain than their liberal competitors. These asymmetries combine toward a strategic diagnosis that China and Russia are approaching overmatch of the United Kingdom in its cognitive domain, with implications for the latter's security. Scholars and practitioners facing similar challenges elsewhere may benefit from examining the situation in the United Kingdom.

Captain Paul Ottewell is a Royal Navy warfare officer. He holds a bachelor's degree in computer science from the University of Manchester and a master's degree in defence studies from King's College London. His research area of interest is computational disinformation. The views expressed in this article are solely those of the author. They do not necessarily reflect the opinions of Marine Corps University, the U.S. Marine Corps, the Department of the Navy, the U.S. government, or the government of the United Kingdom.

Keywords: disinformation, net assessment, cognitive domain, cognitive warfare, information maneuver, asymmetry

In liberal democracies, the *vox populi* (voice of the people) is a cherished concept, a referent object vital to the proper functioning and accountability of the state. During the past three decades, the cyber domain has accumulated such bandwidth, autonomy, and penetration that it is increasingly plausible that malign actors could now use it to manipulate public opinion. Globally, people have become agents in an "attention economy" enabled by a transnational information network that weaves the internet, personal computing, mobile telephony, and social networking websites into a highly intuitive and ubiquitous machinery of communication.[1] The wisdom of the crowd may be giving way to the deception of the masses. This article examines the growing threat to the sovereignty of public discourse and the associated implications for a society's recognition of security issues and the state emergency activity it leads to.

Manipulation of public opinion is not new. There is evidence of propaganda—defined here as "the forming of texts and opinions in support of particular interests and through media and non-media mediated means with the intention to produce public support and/or relevant action"—at least as far back as Ptolemaic Egypt (305–30 BCE).[2] [3] What is new is the hyperpersonalization and targeting of propaganda made possible by the growth of social media.

The following factors underline the novelty of the situation in 2022:

1. Ubiquity. Social media pervades society.[4]

2. Hyperpersonalization. Through social networking websites, actors can target members of the same household with different messaging, thereby avoiding the scrutiny of the crowd to which mass broadcast propaganda is subjected.[5]
3. Opportunity. Pursuing a propaganda campaign online is both cost-effective and low risk since such activity is sufficiently ambiguous and unattributable to avoid crossing the threshold likely to trigger a security response from the North Atlantic Treaty Organization (NATO).
4. Regulation. Light regulation of social networking websites in comparison to traditional media and the liberal principal of freedom of expression are security vulnerabilities open to exploitation.
5. Efficiency. Even inexpert actors can rapidly create mass effects in the information environment today. The process is exponentially easier and cheaper now than it was before the invention of the social networking websites.

The hypothesis of this study is that the balance of power is currently not in the United Kingdom's favor in the human/cognitive dimension of the information environment, termed here the *cognitive domain*. To test this assertion, this article analyzes strategic asymmetries between the United Kingdom and two of its great power competitors: Russia and China. Both have demonstrated the will and capability to conduct public diplomacy through social media to influence audiences abroad.[6]

From analysis of the strategic asymmetries, the diagnosis emerges that China and Russia are both outmaneuvering the United Kingdom in the cognitive domain to the detriment of the latter's security. This overmatch is

borne of the tension between the democratic principle of freedom of expression and the threat vector for disinformation represented by social media. The implications for liberal democracy and consequently national security strategy are profound: the United Kingdom must confront how to better protect its own cognitive domain.

This article adopts the model proposed by Barry Buzan, Ole Wæver, and Jaap de Wilde in their seminal work on securitization, *Security: A New Framework for Analysis*.[7] Unless otherwise stated, the audience referred to in this work is the population of the United Kingdom and their elected representatives in Parliament.

Value of This Research

To date, cyberwarfare initiatives in the West have focused on scientific and technical measures.[8] However, scholarly research on the weaponization of social media and its implications for security has been scarce by comparison. There is a gap in the literature on the security of the United Kingdom's cognitive domain.

Engaging in or framing responses to cognitive warfare presents legal, moral, and ethical dilemmas to liberal democratic governments. How should the United Kingdom, committed as it is to upholding the rules-based international order, protect its cognitive domain and deter malign activity against it without stooping to the level of its competitors? Answering this question lies in the domain of grand strategy. This article offers a first step toward crafting such a stratagem.

Anchor Definitions

Roger W. Cobb and Charles D. Elder's work on agenda-building is critical to understanding democratic decision-making as involving a series of connected agendas through which issues escalate until they "command the attention and concern of decision makers."[9] Cobb, Jennie-Keith Ross, and Marc Howard Ross introduced the *formal agenda* as "the list of items which decision-makers have formally accepted for serious consideration" and the *public agenda* as "all issues which (1) are the subject of widespread attention or at least awareness; (2) require action, in the view of a sizeable proportion of the public; and (3) are the appropriate concern of some governmental unit, in the perception of community members."[10] Their *outside initiative model* describes the process that a grassroots issue, such as a perceived injustice, must undergo to achieve a place on the public agenda and ascend to the formal agenda. Scholars of the Copenhagen School[11] will recognize parallels with the securitization process.

The United Kingdom's Ministry of Defence recognizes five operating domains: land, maritime, air, space, and cyberspace. However, the contested territory in the court of public opinion lies in a sixth, yet unrecognized, warfighting domain: the *cognitive domain*. The concept of this domain is sufficiently novel that neither academia nor the military has yet settled on its definition. Here, it is defined as consisting of perception and reasoning in which maneuver is achieved by exploiting the information environment to influence interconnected beliefs, values, and cultures of individuals, groups, and/or populations.[12]

Cognitive warfare is competition within the cognitive domain. Existing definitions suffer from a negative bias that ignore the possibility that

cognitive warfare can be waged defensively and constructively as well as offensively and destructively.[13] A neutral definition of cognitive warfare is as follows: maneuvers in the cognitive domain to establish a predetermined perception among a target audience to gain advantage over another party.[14]

This article makes frequent reference to the *rules-based international order*. A collective but contested term for the liberal democratic world order that emerged following World War II, some scholars argue that it grossly simplifies the global situation.[15] However, the term is used frequently in diplomacy and therefore has purchase as a concept. It is used in this article as shorthand for the status quo. The rules-based international order is the sum of the "rules, norms, values, institutions, security agreements, treaties and other mechanisms that foster collaboration and help resolve disputes between states."[16]

The degree to which a state is satisfied or dissatisfied with its place in the rules-based international order and/or with the legitimacy of the order itself is relevant to what follows. Classical realists argue that there are two categories of states. Those whose balance of interests lies in the maintenance of the global order are known as *status quo states*. Those who are unsatiated by the current global order, who "share a common desire to overturn the status quo order—the prestige, resources, and principles of the system," are termed *revisionist states*.[17]

Given the dominance of the media on the information environment, any analysis thereof would be incomplete without examination of the relevant literacies of the audience. This study is concerned principally with *digital literacy*. Allan Martin's definition invokes a broad taxonomy of the

cognitive processes involved in engaging critically with computer-mediated means of communication:

> Digital Literacy is the awareness, attitude and ability of individuals to appropriately use digital tools and facilities to identify, access, manage, integrate, evaluate, analyse and synthesize digital resources, construct new knowledge, create media expressions, and communicate with others, in the context of specific life situations, in order to enable constructive social action; and to reflect upon this process.[18]

Research Methodology: Net Assessment

Net assessment is a framework for analyzing the balance of military power in intractable or persistent states of competition.[19] It is therefore well suited to a study of this nature. The U.S. Department of Defense describes the methodology as the "comparative analysis of military, technological, political, economic, and other factors governing the relative military capability of nations. Its purpose is to identify problems and opportunities that deserve the attention of senior defense officials."[20]

Net assessment does not produce strategy. As Lawrence Freedman puts it, strategy is "the art of creating power."[21] Therefore, an analysis of the relative power balance between parties now and into the future is an essential precursor activity to the formulation of any grand strategy. As an analytical approach, net assessment goes beyond more prosaic, normally quantitative measures of military balance. Net assessment acknowledges that measures of power are only relevant when taken relative to another party. Furthermore, net assessment rises above quantitative measures such

as counts of brigades, warheads, and aircraft to include how less tangible factors such as strategic decision-making processes, geography, politics, and alliances would weigh on each party's ability to deploy a capability decisively.[22]

This article adopts the following characteristics of net assessment:

- It explores instruments of national power beyond the military.
- It identifies long-term trends.
- It examines strategic asymmetries.
- It acknowledges critical differences between states.[23]

Limitations and Potential Problems

Trying to conduct case studies at the state level is fraught with potential for bias since the process of simplifying a complex situation sufficiently to allow comparative analysis requires a heuristic approach. In addition, the available evidence set is so large that it defies definitive quantification, categorization, or comparison. For example, when analyzing a state's foreign policy, it is likely that examples exist of actions that both support and undermine the hypothesis under test, presenting a challenge to a time-poor researcher in remaining objective and thereby a vector for unconscious bias. Similarly, abstract concepts such as advantage and influence present profound difficulties in terms of objective measurement.

Being an exploratory study, the conclusions of this article will lack the greater reliability that would derive from a more comprehensive evidence base.

Analyzing a single operating domain, as the author does here, precludes consideration of the competition between domains and

consequently risks missing key asymmetries. For that reason, all other things being equal, a multidomain net assessment is likely to be inherently more insightful.

Finally, a state's intent to wage cognitive warfare extraterritorially is a tenet of its foreign policy, not a tangible real-world artifact. It can change as quickly as the regime or administration from which it extends. In the case of a rapid transition, such as a coup or revolution, the corresponding case study would be rendered obsolete.

Net Assessment of the United Kingdom's Cognitive Domain[24]

> We resist the invasion of armies; we cannot resist the invasion of ideas.
>
> ~ Victor Hugo[25]

This net assessment proceeds in four stages, beginning with a basic assessment that captures the salient features of the competition. This section discusses the competitive situation as it is today, explores how the balance of power has changed over time, and looks ahead to consider what might happen if the United Kingdom does not change its current policy base.[26]

A founding member of the United Nations (UN) with a permanent seat on the UN Security Council, the United Kingdom is the quintessential status quo state. The nation's ruling party describes its vision of the United Kingdom as "an outward-looking country that is a champion of . . . a rules-based international system."[27] Speaking in January 2020, a parliamentary

undersecretary of state described the rules-based international order as "a system that this country helped to build and one that this Government are determined to defend and strengthen."[28]

In contrast, Russia's strategic goal is to "reorient and disrupt the entire Western-dominated international system" and reassert Russian influence in global affairs.[29] President Vladimir Putin's agenda is intrinsically revisionist. Similarly, President Xi Jinping of China appears set on casting aside Western concepts such as the Westphalian nation-state and instead is "reimagining the world as a single complex network of supply chains and trade arteries" serving China's interests.[30] Xi's vision includes the spread of the Chinese model abroad, given his argument that it "offers a new option for other countries and nations who want to speed up their development while preserving their independence."[31] China's intentions are considered revisionist for this study.

The United Kingdom is in a state of persistent competition in the cognitive domain. Contests in this domain differ from those in the more traditional domains. Taking the initiative or even maintaining a credible deterrent in the cognitive domain is incompatible with the rules-based international order in its current form. The United Kingdom's director general of Joint Force Development describes the situation as such:

> Currently we are being challenged in a "grey-zone" short of armed conflict by agile state and non-state actors—notably Russia—who understand our vulnerabilities and seek to exploit them through multifarious asymmetric approaches and the flouting of rules-based norms.[32]

This is not hyperbole. On 4 March 2018, former Russian spy Sergei V. Skripal and his daughter Yulia were the victims of the first offensive use of nerve agents in mainland Europe since World War II. The attack took place in Salisbury, England. As evidence mounted of Moscow's complicity amid growing international condemnation, Russian diplomats flooded the public narrative with 37 alternative explanations.[33] On 6 May 2019, Facebook deactivated 16 fake accounts that it had traced back to Russia. Analysis would later show that these accounts were part of a sophisticated and international disinformation campaign extending across 30 different social networking websites, involving myriad fake user accounts and nine languages. Named Operation "Secondary Infektion" by the Western researchers analyzing it, the campaign's aim appeared to be "divide, discredit, and distract Western countries."[34]

Separately, China has constructed a machinery of public diplomacy that integrates state media, social networking websites, and both overt and covert commentators to amplify its influence on discourse online. Analysis by the Oxford Internet Institute, a department of Oxford University, found evidence of a network of fake user accounts engaged in the amplification of the social media posts of Chinese diplomats based in the United Kingdom. Many of the associated user profiles masqueraded as belonging to Britons. Together, the network was responsible for nearly half of online engagement with the Chinese ambassador's posts on Twitter.[35] The top 1 percent of so-called "super-spreader" accounts were found to be responsible for half of the posts rebroadcasting (or retweeting) Chinese content.[36]

The COVID-19 epidemic has accelerated China's use of social media to protect the positive image that it seeks to present to the world. Two

examples of this are how Chinese diplomats respond to British Broadcasting Corporation (BBC) reporting on the possible source of COVID-19 and China's treatment of the Uyghur minority in Xinjiang by flooding social media with alternative conspiracy theories.[37]

The United Kingdom, being heavily invested in the status quo, is in active competition with two revisionist great power nations who possess the capability and the intent to subvert the rules-based international order via the cognitive domain.

Figure 1. Tweet by Chinese Consul General @ZhaLiyou suggesting evidence exists that COVID-19 originated in Maine, United States

Courtesy of Marcel Schliebs on Twitter (@m_schliebs), 21 October 2021.

British citizens exist in a state of information overabundance.[38] Through the ubiquity of smartphones and 95-percent internet connectivity, the overwhelming majority of the United Kingdom's electorate can be "tracked, traced, profiled and communicated with" most of the time.[39] Consequently, the electorate is targetable most of the time.

The burden of fact-checking the news in the United Kingdom is shifting from publisher to consumer. Audience share for broadcast news media is falling while younger adults are increasingly using social media as their main source of news.[40] This consumption shift is outpacing the development of digital literacy skills among the general population.[41] Ill-equipped to apply critical thinking to the news they consume, the digitally illiterate are the soft underbelly of the United Kingdom's cognitive domain.

Trust in the mainstream news media is falling. Between 2015 and 2019, the proportion of Britons reporting that they trusted most of the news most of the time fell from 50 to 40 percent.[42] Trust in the Fourth Estate (the press and news media) is a proxy measure of the health of a liberal democracy. If the light that journalism shines on threats cannot reach the electorate, decision-makers may be denied popular support for their emergency actions. The power of investigative journalism to hold the powerful to account is diminishing.

The United Kingdom has fully embraced social media. In 2020, 66 percent of the country's population were users, uploading hundreds of millions of photographs, videos, and audio files to social media networks daily.[43] Though "the camera cannot lie" has never been true, images and especially videos remain powerfully persuasive nevertheless. Advances in machine learning now make possible the production of moving image

disinformation in near real time. The result is known as a *deepfake*. While the average viewer remains just able to distinguish deepfakes from the real thing, this visual disinformation proves sufficiently unsettling as to leave some viewers uncertain of whether what they saw was genuine or not.[44]

Combined, the above factors indicate that the United Kingdom's cognitive domain is highly conducive to the viral propagation of disinformation, with a trend toward further deterioration. A 2019 parliamentary report titled *Disinformation and "Fake News"* diagnosed the United Kingdom as "clearly vulnerable to covert digital influence campaigns."[45]

Left unaddressed, the reasonable worst-case scenario is that a sufficiently organized actor could be successful in influencing the United Kingdom's public and formal agendas and subverting, delaying, or undermining an otherwise democratic decision with security consequences. Consequently, a battle could be lost without a shot being fired. The more likely outcome is that the cognitive domain will become a common—if not the primary—battlefield on which a revanchist Russia and a rising China will pursue their revisionist agendas. Contest there is cheap, deniable, and falls short of the threshold of kinetic warfare likely to trigger a military response from their competitors.

Key Asymmetries

Asymmetries define the balance of power in any domain. This second section of the net assessment explores the underlying causality and examines how the parties are pursuing the competition in the United Kingdom's cognitive domain. This exploratory study will concentrate on

three key asymmetries: doctrinal maturity, the relative ease of waging cognitive warfare compared to defending against it, and freedom of maneuver.

Asymmetry 1: Doctrinal Maturity

Russia and China both have established doctrines for waging cognitive warfare. The United Kingdom does not. Furthermore, institutional reluctance to explore this capability area weighs against its development.

Geoffrey Sloan's concept of doctrine highlights its cognitive connection as the means by which a commander combines their perception of the battlefield with theory to arrive at actionable orders: military doctrine "interprets ideas about war, and how they affect its conduct and its character, by combining strategic theories and operational plans into functional guidelines for action."[46] Of the many available, this definition of military doctrine fits best with the subject of this monograph.

Russia's cognitive warfare doctrine is well documented under various pseudonyms, but the foundational concept is known as *maskirovka*. Maskirovka is the Russian word for military deception, of which Daniel P. Bagge provides a detailed contemporary analysis.[47] Deeply rooted in Soviet strategic culture, the Russian military has updated it for the Information Age. Julian Lindley-French refers to this evolution of the doctrine as "strategic Maskirovka," a coordinated disinformation campaign targeted at NATO member states and the command structure of the alliance itself, with the aim of discrediting and disrupting its functioning.[48]

According to Bagge, strategic maskirovka draws its strength from three sources. The first is the co-option of the internet, in particular social

media, to deceive the target audience at machine speed while preserving plausible deniability.[49] The second source is cybernetics, the science of control and communication in animals, people, and machines.[50] It is through this work that Russia has been able to supercharge the third engine of maskirovka: active measures. The concept of active measures can be traced back to Vladimir Lenin, the first leader of the Soviet Union. Russia has since updated it for the digital age. Today, active measures include overt (white) propaganda through international, state-sponsored media outlets like RT International and covert (black) information warfare through troll farms and botnet factories.

Russian attempts to influence public opinion in the United Kingdom during the 2016 European Union membership referendum and 2017 general election are evidence that the Kremlin is prepared to engage in cognitive warfare.[51] But the threat this poses to democracy is undetermined, and evidence of actual harm is scant. A parliamentary report into Moscow's alleged interference in the politics of the United Kingdom, a redacted version of which Downing Street allowed to be published in July 2020, concluded that there was an absence of evidence of Russian interference in the 2016 referendum.[52] This, however, is not the same as a finding of evidence of absence. The same report found that the government of the United Kingdom did not commission a retrospective assessment of Russian attempts to influence voters in the referendum. An opportunity for the public and security establishment to learn the extent that malign actors were successful in maneuvering in the United Kingdom's cognitive domain—seemingly unopposed—may now be lost.

Maskirovka is the mechanism by which the Kremlin tries to manipulate target audiences. As a doctrine, it explains the general "how" more than it does the specific "what." The latter is the realm of reflexive control theory. This guides the Kremlin's choice of what reality it wishes its target audience to perceive. Like active measures, it has evolved through the decades, with roots in the Soviet Union under Joseph Stalin, but its fruits lie in contemporary Russian thinking. Timothy L. Thomas' definition is rigorous: "Reflexive control is . . . [the] means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[53]

The "reflex" refers to how the opponent's deliberations are steered in such a way as to choose a course of action that (unwittingly) is against their own best interests. At its heart, reflexive control pursues control of the enemy's decision-making processes.[54] The relevant asymmetry is Russia's apparent preparedness to employ this doctrine outside of wartime in the pursuit of its foreign policy ends. Should the Kremlin successfully exercise reflexive control over another state's *vox populi*, however temporarily, this would render acutely vulnerable the collective threat perception and therefore the securitization process that controls the emergency response. To Chinese military theorist Sun Tzu, this is the most skillful strategy of attack: to subdue the enemy without fighting.[55]

China's approach to cognitive warfare is very different, reflecting its more ambitious strategic goal. No single organ of the Chinese state is responsible for what it calls its Grand Overseas Propaganda Campaign.[56] Rather than try to co-opt Western social media to deliver its messaging through subterfuge and brute force as Moscow does, Beijing is taking a

longer-term and more strategic approach in the information environment: the pursuit of systemic advantage.[57]

Shanthi Kalathil points to how, in the past decade, the Communist Party of China has taken influential positions in international media markets, especially in the continental United States, which would in theory allow it to shape reportage and editorial policy to be more sympathetic or positive to Chinese interests.[58] China's involvement in the main media outlets in the United Kingdom has to date been modest. The international satellite news channel China Global Television Network (CGTN) has a regional production hub in London. However, in February 2021, the United Kingdom's communications regulator withdrew CGTN's broadcast license after finding that it was "ultimately controlled by the Chinese Communist Party."[59] China also distributed a monthly pamphlet through *The Daily Telegraph* newspaper from 2010 to 2020. Beijing sponsors Confucius Institutes at British universities, but its most prolific presence is via Twitter from its diplomatic corps. As of yet, there is no compelling evidence that these efforts are achieving salience among the electorate of the United Kingdom.

Across a broad spectrum of activity, the asymmetry that China is exploiting is the lack of reciprocity. In 2020, the World Press Freedom Index of 180 states ranked the United Kingdom at number 45 and China at number 177.[60] Simply put, neither British journalists nor British diplomats enjoy the same freedom to participate in the public discourse in China that liberal democratic principles afford to their Chinese counterparts (and everyone else) in the United Kingdom.

Little is known of the United Kingdom's offensive cognitive warfare capability. London's equity in the rules-based international order limits its

appetite to exploit the cognitive domain, especially offensively. The United Kingdom's ethics of state communication preclude the peacetime use of deception in general and troll farms and/or botnets in particular.[61] Following the end of the Cold War and the rapid growth of the internet, state use of disinformation has become antithetical to liberal democracy. As Thomas Rid puts it, "it is impossible to excel at disinformation and at democracy at the same time."[62] Use of the former undermines trust in the institutions on which the latter depends. However, while deploying a cognitive warfare capability is fraught with difficulty for liberal democracies, this does not render the cognitive domain indefensible by them. In fact, the cognitive domain is vital ground for the correct functioning of democracy itself. So, while the United Kingdom has no published doctrine for the cognitive domain, it has not been idle in exploring its options there.

In February 2018, the United Kingdom's Home Office announced the development of an AI (artificial intelligence) capable of detecting 94 percent of Daesh (Islamic State) propaganda videos with 99.995 percent accuracy.[63] Separately, the United Kingdom's National Security Communications Team was behind a Global Coalition website designed to counter Islamic State disinformation by providing credible open-source information on the situation in the territory it had formerly held.[64] The British Army's 77th Brigade now includes counteradversarial information activity among its capabilities.[65] Furthermore, the government of the United Kingdom has established specialist units to identify false narratives and coordinate a pan-Whitehall response.[66] Admittedly, these are nascent and somewhat disconnected capabilities, lacking the binding principles (such as a doctrine)

that would enable their mutual employment and reinforcement in pursuance of a common strategic end.

In the United Kingdom, information advantage was reconceptualized in a 2018 Joint Concept Note known as JCN 2/18. This document describes the United Kingdom as being threatened in the cognitive domain and sets out actionable steps that the national security enterprise could take in response. The foreword, written by Air Marshal Edward J. Stringer of the Royal Air Force, is a treatise on cognitive warfare, advocating for "a cultural transformation and a conceptual foundation that puts information advantage at the heart of 21st Century deterrence and campaign design."[67] Yet, the first print run of this document was pulped following an objection from the Ministry of Defence's Directorate of Defence Communications about the inclusion of the concept of information maneuver to deceive public audiences.[68] As Robert R. Leonhard wrote, "Ultimately, history will scoff at such [lofty] pretensions just as today we laugh at feudal prejudices against gunpowder."[69]

The United Kingdom published its latest *Integrated Review of Security, Defence, Development and Foreign Policy* in March 2021. Like JCN 2/18, the integrated review acknowledges that weaponized disinformation is a threat to democracy.[70] Government departments, especially the Ministry of Defence, are now programming the capabilities necessary to meet the demands of the integrated review. While the report cited Russia and China's heavy investment in cognitive warfare as a challenge to democratic societies, the government of the United Kingdom has not yet committed to anything beyond "thoughtful investment" in response.[71] Should the integrated review not lead to the development of the thinking and capability

identified in JCN 2/18, it will not be a failure of imagination but a potentially pyrrhic victory of ethos over pathos.

Asymmetry 2: The Relative Ease of Waging Cognitive Warfare Compared to Defending against It

In the long term, cognitive warfare is easier to wage than it is to defend against. The party with the greatest strategic patience has the advantage. This is an asymmetry with two axes. The first relates to audience sensing: defending nations must understand who constitutes their vulnerable audience if a counterdisinformation campaign is to be properly targeted. An aggressor need not be so meticulous and may change strategies at will in the quest for one that delivers results. The second axis relates to tenacity: the defending state must prevail over every attempt to influence its democratic processes while the aggressor can achieve lasting advantage from a single success.

Just as an epidemiologist will look to identify the groups of hosts that are most susceptible to a pathogen, so a defensive strategy for the United Kingdom's cognitive domain would need to identify the audience(s) most inclined to be persuaded by any given disinformation campaign. The common aim is to focus intervention efforts where they will have the most impact on the spreading contagion. Target audience analysis of Chinese and Russian cognitive warfare capabilities is therefore an important step toward a risk assessment and/or mitigation strategy. Given the paucity of open-source analysis of audiences in the United Kingdom, there is value in examining target audiences in the United States to find parallels. Separate studies by the Rand Corporation and the Atlantic Council both identified "the

global ethnic Chinese diaspora [as] a favorable vector of influence for Beijing to leverage," particularly in United States.[72] However, Chinese people account for less than 1 percent (400,000 to 600,000 individuals) of the population of England and Wales.[73] Even in the United States, the proportion of the population estimated to be ethnic Chinese in 2020 was 1.6 percent (5.4 million individuals).[74] Neither group seems large enough to influence the *vox populi* in either state. Therefore, it can be concluded that China must address a broader target audience if it is to ever be successful in influencing the public agenda extraterritorially.

The term *target audience* is not helpful since it presumes the deceptive message is hyper-targeted and that the agent provocateur can be sure by whom their message will be seen and the course that its viral spread will take. This may be so in electoral campaigns that, quite legally, use features like Facebook's lookalike audiences, but Russian methods are more akin to a viral contagion than hyper-personalized medicine. Consequently, it is more important to understand which subset of all the potential recipients of a message will be most susceptible to it than it is to know who the intended target is. The former provides a tangible locus for action to either prevent infection (vaccination) and/or to contain its spread (mitigation). The latter may provide insight into the aggressor's desired outcome, but this may also be unknowable within a relevant timescale. The more significant cohort in cognitive warfare, therefore, is the *vulnerable audience*: those persons most likely to be persuaded by a given disinformation campaign and act upon that persuasion in a way that influences the public agenda.

Fortunately, and as an example of the value of net assessment, the dearth of research on vulnerable audiences in the United Kingdom does not

prevent identification of asymmetries. The aggressor in a cognitive warfare campaign has the relative freedom of measuring, testing, and adjusting the impact of their actions in the open-source media of their target. Conversely, the targeted state cannot afford to wait until the public agenda has shifted, since by then the damage is done. Its challenge of monitoring sentiment and deploying appropriate interventions must be continuous and upstream since the other party need only be successful once in influencing a supposedly democratic decision to effect lasting change. The best form of infection control is to prevent it taking hold in the first place: digital literacy is to cognitive warfare as vaccination is to contagion. Therefore, a whole-of-government defensive strategy in the cognitive domain should include digital literacy as a central tenet.

Digital literacy is nested under "media studies" in the United Kingdom's education curriculum. However, the subject has a reputation for lacking academic rigor among both educational policymakers and parents.[75] As a likely result, the subject is taken by only a small proportion of each cohort—less than 6 percent of the class of 2019.[76] The United Kingdom is missing the opportunity to equip its citizenry for life with digital literacy skills and thereby bolster its resilience to disinformation.

Asymmetry 3: Freedom of Maneuver

Revisionist states enjoy freedom of maneuver in the United Kingdom's cognitive domain that the United Kingdom chooses not to exploit reciprocally. State legislatures must strike a balance between the antithetical ideals of cognitive domain security and the free movement of information and ideas. Hitherto, the government of the United Kingdom has left

internet-mediated communications and social media largely unregulated. China's approach is the polar opposite, featuring tight central control and heavily censorship, while Russia's hybrid model is drifting toward the Chinese example. A combination of technical means and strict regulation of all forms of media protects the Communist Party of China from the galvanizing effect that social networking websites can have when citizens share dissenting opinions or try to coordinate protests online. At the same time, light regulation of social networks and messaging services in the United Kingdom affords Beijing freedom of maneuver in the British cognitive domain that London does not enjoy in mainland China. Whereas Russia is years from achieving the same level of internet sovereignty as China, when compared with the government of the United Kingdom, the Kremlin is relatively unconstrained in the use of disinformation in its public diplomacy.

This asymmetry emanates from the legal frameworks of the protagonist states. The examination of each begins with Russia.[77] While its estimated 91 million users enjoy largely unfettered access to the internet via some 3,500 internet service providers, the Russian state has shifted significantly toward digital authoritarianism since the widespread civil unrest of 2011–13.[78] A free flow of information presents Moscow with two problems. First, the Russian security services lack the technical means of enforcing their laws online, especially when it comes to content served by providers based overseas. Second, the popularity of Western social media services such as YouTube and encrypted messaging services like Telegram among Russians stays the state's hand in simply blocking them for fear of stoking public dissent.[79]

The Russian State Duma legislated to address these shortcomings in 2019.[80] Critics fear that the new laws codify state censorship of the internet. Separately, a series of legislative amendments legalize state monitoring of information flowing across and within Russia's borders and require installation of infrastructure that would theoretically enable the walling-off of Russia from the global internet. If Moscow can implement this legislation successfully, which is by no means certain given the expense and technical challenges involved, the result will be a "centralized management system of the internet by the state authority."[81]

China's laws on disinformation are among the world's strictest.[82] For example, in mainland China it is an imprisonable offence to spread "fake news that seriously disturbs public order through an information network or other media." Furthermore, there is no press freedom; online news providers may only share stories that have been published by the state press agency, Xinhua, or by one of its provincial equivalents.[83]

In addition to its strict regulation of all media, China has designed and constructed its domestic internet infrastructure with information control at its heart. The Golden Shield Project, known colloquially as the "Great Firewall of China," is a tightly integrated system of hardware and software filters that permits a variety of censorship techniques at the national scale.[84] Many foreign websites, including Google, Twitter, and YouTube, are inaccessible to Chinese users, who instead use domestic equivalents such as Baidu (replacing Google) and Sina Weibo (replacing Twitter).[85]

Relative to China and Russia, the United Kingdom currently regulates its domestic internet very lightly. This looks set to change. Parliament is consulting on an Online Safety Bill that, if passed into law, would hand

substantial powers to the United Kingdom's communications regulator, the Office of Communications.[86] The bill would impose many new legal duties on online platforms, including one to protect their users from coming to harm. Contentiously, the bill extends these duties to include protection from content that is legal but might be harmful to adults, such as misinformation on vaccines. Such a move is described by free speech campaigners as "the most significant change in the role of the state over free speech since 1695," a reference to the lapsing of the English government's legal power to censor printed material before publication.[87] The bill seeks to balance new duties toward the individual with new duties toward public goods, in particular its agenda. Social networking websites would be required to protect "the right of users . . . to freedom of expression within the law" and "content of democratic importance."[88] In this latter case, the legislation would protect content that "is or appears to specifically intended to contribute to democratic political debate in the United Kingdom."[89] To give the legislation teeth, the Office of Communications would be empowered to levy fines on social networking websites up to 10 percent of their annual global revenue. In Facebook's case, this would represent a maximum fine of more than $8 billion USD.[90] However, until and unless Parliament passes the bill into law, the United Kingdom's internet will remain largely unregulated space.

Turning to the use of the internet in public diplomacy, international law prohibits the publication of bellicose propaganda or material intended to incite civil disobedience in another state but is silent on the waging of disinformation campaigns with a subthreshold intent to, say, influence democratic processes.[91] One of the principles of liberal democracy—freedom of expression—is being used as a weapon against it.

The United Kingdom's national security community is aware of the growing threat to the cognitive domain. Perhaps understandably given the sensitivity of the subject, the nation's policy and capability toward cognitive warfare is not in the public domain and is therefore beyond the reach of academic analysis here. Certainly, competition in the cognitive domain did not feature in the United Kingdom's most recent *National Cyber Security Strategy* nor has the issue been the subject of a specific inquiry by the House of Commons Defence Select Committee.[92] The single outward demonstration of the United Kingdom's intent to acquire the capability to counter online threats is the announcement of the creation of the National Cyber Force in October 2019.[93] From what is known about this force, it is not clear whether its mandate will extend beyond scientific and technical cyber security and defense into the cognitive domain.

Major Uncertainties

This third section identifies four recognized unknowns in the assessment above that have the potential to significantly impact the conclusions reached should they play out unexpectedly.

First, the reasonable worst-case scenario is highly speculative. The hypothesis that the public agenda could be steered by a foreign power or nonstate actor is unproven. It could be that the threat to national security is misquantified in either direction.

Second, without intervention from the state, the pace at which digital literacy will evolve to naturally regulate the impact of disinformation is unknown. If swift, then this would reduce the salience of cognitive warfare in security terms.

Third, the pace at which social media networks will develop and implement effective frameworks of self-regulation is unknown. If self-regulation can be achieved and sustained such that the networks are substantially less conducive to the viral dissemination of disinformation, this would mark an important development in redressing the asymmetry between liberal and illiberal societies in the cognitive domain.

The final unknown relates to the magnitude of the threat faced by the United Kingdom in the cognitive domain relative to threats in other domains. One international commentator argues that, left unaddressed, the potential damage to the United Kingdom's interests in the cognitive domain will still be less than the damage it is inflicting on its own soft power with its drift toward populism.[94] The priority that the United Kingdom should afford to securing its cognitive domain is therefore deeply uncertain.

Opportunities and Threats

The final step of this net assessment is the identification of opportunities and threats. The former are defined as forthcoming events and/or trends that can be turned to one party's own advantage. The latter are events and/or trends that are likely to be disadvantageous to that same party.

The first opportunity lies in flexing the United Kingdom's considerable soft power to seek consensus among its allies on developing the policy measures necessary to counter state-sponsored disinformation without undermining liberal democratic principles. The United Kingdom sustains a vibrant academic community, a world leading AI research and development capability, and a well-established Development, Concepts and Doctrine Centre.[95] Together, these are the wherewithal necessary to codify a

workable whole-of-government response to the disinformation threat. The draft Online Safety Bill is a tangible example of the United Kingdom providing such thought leadership on regulating internet-mediated communications while also protecting freedom of expression.

A second opportunity is the near certainty that AI will play a pivotal role in identifying deepfakes, inauthentic user profiles, and other hallmarks of disinformation at the speed of relevance. The United Kingdom's edge in AI research and development makes it well-placed to serve this market to the benefit of its prosperity agenda and soft power status.

The first threat is the trend toward declining political support for democratic institutions. As Leila Alieva at the Foreign Policy Centre puts it, "The new generation of politicians and media . . . are balancing a tightrope of risks and dangers of moving farther away from what so far has constituted the identity and core of the democratic states; stable institutions resistant to absolutism, autocratism and illiberalism."[96] If sustained, such political values would be deeply damaging to the United Kingdom's soft power. The consequence would be diminished British convening power, credibility, and political authority on the international stage. With its competitors emboldened, it would become harder for the United Kingdom's diplomats and politicians to defend the status quo of the rules-based international order.

A second threat is the limited supply of academics and software engineers at the leading edge of research into computational disinformation. Here, the public sector is competing against the social networking websites themselves for the talent. As a result, it seems likely that some form of collaboration between public and private sectors will be

essential if liberal states are to maintain a credible and relevant capability in the cognitive domain.

The final threat is time-bound. The internet can amplify and broadcast disinformation across platforms and borders at a pace measured in minutes. The public agenda itself is dynamic and constantly evolving. Yet, current human-driven analysis of the information that flows through social networking websites achieves source attribution, intent determination, and response decisions at a pace measured in days and weeks. In military terms, this suggests a need for a "recognized picture" of the cognitive domain, a processing task so demanding that the use of AI would be essential. Such a live threat picture of the narratives flowing through and between the most popular social networking websites would represent unprecedented state-sponsored surveillance of its citizens' communications. The legislative and ethical barriers to the development of such a capability would be substantial, even if the political appetite existed.

Conclusions

The aim of this study was to identify the competitive dynamics in the United Kingdom's cognitive domain. The three asymmetries exposed can be summarized thus:

1. Doctrinal maturity. Russia and China both have well-established doctrines for waging cognitive warfare. The United Kingdom does not, and institutional reluctance to explore this capability area weighs against its development.
2. Cognitive warfare is easier to wage than it is to defend against. For any counterdisinformation campaign to be maximally effective, the

United Kingdom would need to identify its vulnerable audience, requiring a level of surveillance of its cognitive domain that is at odds with liberal principles of privacy and freedom of expression. An agile and/or patient aggressor faces no such constraints, especially so if their maneuvers go unchallenged.

3. Revisionist states enjoy freedom of maneuver in the United Kingdom's cognitive domain that the United Kingdom chooses not to exploit reciprocally. The United Kingdom's defence of democratic principles such as net neutrality, privacy, transparency, and freedom of expression is laudable and a significant source of British soft power. However, it is difficult to reconcile this with the United Kingdom's apparent reluctance to impose costs on actors that exploit those principles with revisionist intent, since this weighs heavily against the country's national interest. Prevarication in this policy area may represent a pyrrhic victory of ethos over pathos and logos.

In the cognitive domain and beyond, the United Kingdom is facing a strategic situation in relation to China and Russia that is analogous to that which it faced with the Soviet Union in 1946, the beginning of a long Cold War. On one front, the United Kingdom faces a malign, revanchist, and decaying Russia whose opposition to the liberal democratic order is as implacable as it is fundamental. On the other front, it has the rising, revisionist, and techno-authoritarian China, which is intent on reshaping the global order to its lasting strategic advantage. With unipolarity giving way to bipolarity, the great power competition between the global West and China appears to be set for the long term.[97] Russia is a danger to the United

Kingdom's national security because of its weakness; China is a danger because of its strength.[98]

The diagnosis is that, in the cognitive domain specifically, a tenaciously antagonist Russia and a strategically patient China are outmaneuvering the United Kingdom. Both are generating and deploying cognitive warfare capabilities that have no obvious countercapability in the United Kingdom. Through their will to co-opt social networking websites as a delivery method for disinformation, both China and Russia are maneuvering in the United Kingdom's vital territory largely unopposed. Inaction risks ceding an increasingly influential engine of the public agenda and platform for security speech to parties outside the democratic franchise. While social networking websites remain only lightly regulated and concerns about liberal principles preclude development of a countercapability, the United Kingdom's democracy lies exposed to increasing risk of malign foreign influence.

Recommendations

Mitigations for the three asymmetries are likely to be self-reinforcing and interdependent for their success. For doctrinal maturity, reconciliation of the ethics of public diplomacy with the reality of the contemporary security environment will be an important step toward developing a credible capability for information maneuver in the United Kingdom. While pursuit of an offensive cognitive warfare capability is antithetical with liberal democratic ideals, this does not absolve the state of its responsibility to provide security as a public good. As a minimum, the United Kingdom's national security enterprise should establish a doctrine for, and then

acquire, a rigorous defensive and/or surveillance cognitive warfare capability.

The second asymmetry—the inherent advantage of the aggressor—calls for greater resilience to disinformation among the population, since the competition is chronic and persistent. A liberal state must vaccinate its public agenda against illegitimate external influence or risk the sovereignty of its democratic decision-making process. In an age of disinformation, digital literacy should join subjects such as reading, writing, and arithmetic as curriculum priorities for those in full-time education.[99] Investment in such measures will pay dividends over generations. To meet the threat more immediately, an ethical and technical framework is required to define an acceptable role for AI in protecting the public discourse from malign influence without critically undermining liberal principals.

Of the three, the third asymmetry—the regulation conundrum—is the most profound. If tighter regulation of social media in the United Kingdom proves ineffective, then policymakers must explore alternative options to redress the balance. These may lie in other domains or may require new, or new interpretations of, international law, but they should include measures that extend the United Kingdom's deterrence effect over its cognitive domain. Actors that maneuver there against the United Kingdom's interests must face unacceptable costs for doing so. Seemingly, the only reason that the United Kingdom is not pushing back reciprocally in its competitors' own cognitive domains is that it chooses not to. With sufficient technical skill and determination, the former of which the United Kingdom enjoys in abundance, any firewall is permeable. Beyond an illiberal firewall lies an

audience similarly interconnected by social networks and a polity vulnerable to the illuminating light of transparency and freedom of expression.

Final Thoughts

Whether acknowledged as a warfighting domain or not, the cognitive domain is conceptually real. It is the maneuver space for the battle for hearts and minds and the vital ground of democratic decision-making. In securitization terms, it is a referent object in the societal sector. In Clausewitzian terms, its sovereignty is the center of gravity of liberal democracy.

China and Russia are threatening the United Kingdom's cognitive domain. Both have the capability and demonstrated will to distract and confuse public discourse in the United Kingdom. As the United Kingdom's Institute for Statecraft puts it, when "people start to say 'You don't know what to believe' or 'They're all as bad as each other,' the disinformers are winning."[100]

Weapons exist to counter most threats in the more tangible domains of land, maritime, air, space, and cyberspace. Battalions, ships, aircraft, satellites, and server farms are all vulnerable to destruction by counteraction. Threats in the cognitive domain are different. Ideas and narratives, once lodged in a society's hive mind, are tenacious and resilient, like a pathogen resistant to medicine. Therefore, prevention is a better defensive strategy than cure. To protect its democracy, the population of the United Kingdom needs a digital literacy campaign to vaccinate it against the spread of disinformation. More immediately, the country's national security

enterprise requires a credible capability that will deter malign actors from any future interference in British democratic processes.

The vulnerability of the cognitive domain makes it possible that the next war may be won or lost before the vanquished party even recognizes that its interests are threatened. Liberal democracies must now choose whether and how to prepare for that war if they are to be successful in deterring it from ever happening.

---

[1] "Fake News, Free Speech, and Foreign Influence: The Smart Way the United States Can Combat Disinformation," Human Rights First, 8 March 2018.

[2] Florian Zollmann, "Bringing Propaganda Back into News Media Studies," *Critical Sociology* 45, no. 3 (2017): 329–45, https://doi.org/10.1177/0896920517731134.

[3] Alan B. Lloyd, "Nationalist Propaganda in Ptolemaic Egypt," *Historia: Zeitschrift Für Alte Geschichte* 31, no. 1 (1982): 33–55.

[4] Esteban Ortiz-Ospina, "The Rise of Social Media," Our World in Data, 18 September 2019.

[5] Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America* (New York: Random House, 2019), 14–15.

[6] *Assessing Russian Activities and Intentions in Recent US Elections* (Washington, DC: Office of the Director of National Intelligence, 2017); and *Russian Influence and Interference Measures Following the 2017 UK Terrorist Attacks* (Cardiff, Wales: Cardiff University Crime and Security Research Institute, 2017).

[7] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner, 1998).

[8] Daniel P. Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (New York: Defense Press, 2019), 31.

[9] Bryan E. Denham, "Toward Conceptual Consistency in Studies of Agenda-Building Processes: A Scholarly Review," *Review of Communication* 10, no. 4 (2010): 306–23, https://doi.org/10.1080/15358593.2010.502593; and Roger W. Cobb and Charles D. Elder, "The Politics of Agenda-Building: An Alternative Perspective for Modern Democratic Theory," *Journal of Politics* 33, no. 4 (1971): 892–915, https://doi.org/10.2307/2128415.

[10] Roger Cobb, Jennie-Keith Ross, and Marc Howard Ross, "Agenda Building as a Comparative Political Process," *American Political Science Review* 70, no. 1 (1976): 126, https://doi.org/10.2307/1960328.

[11] The Copenhagen School is the body of research founded by international relations theorist Barry G. Buzan. In his seminal work, *Security: A New Framework for Analysis*, written with Ole Wæver and Jaap de Wilde, Buzan theorises the process by which security issues become "securitized" and are thereby dealt with through exceptional measures such as war. See Buzan, Wæver, and de Wilde, *Security*.

[12] Paul Ottewell, "Defining the Cognitive Domain," *Over the Horizon*, 7 December 2020.

[13] Yotam Rosner and David Siman-Tov, "Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion," INSS Insight No. 1031, Institute for National Security Studies, 8 March 2018; and Diana Mackiewicz, "Cognitive Warfare" (conference paper, Institute for National Security Studies Summer Institute, Tel Aviv, Israel, 2018).

[14] Ottewell, "Defining the Cognitive Domain."

[15] Malcolm Chalmers, "Which Rules?: Why There Is No Single 'Rules Based International System' " (occasional paper, Royal United Services Institute, London, 2019).

[16] Michael J. Mazarr et al., *Understanding the Current International Order* (Santa Monica, CA: Rand, 2016), https://doi.org/10.7249/RR1598; and Jonathan McClory, *The Soft Power 30: A Global Ranking of Soft Power, 2019* (London: Portland Communications, 2019), 17.

[17] Randall L. Schweller, "Tripolarity and the Second World War," *International Studies Quarterly* 37, no. 1 (March 1993): 76, https://doi.org/10.2307/2600832.

[18] Allan Martin, "A European Framework for Digital Literacy," *Nordic Journal of Digital Literacy* 1, no. 2 (2006), https://doi.org/10.18261/ISSN1891-943X-2006-02-06.

[19] Andrew F. Krepinevich Jr., "Measures of Power: On the Lasting Value of Net Assessment," *Foreign Affairs*, 19 April 2019.

[20] *Department of Defense Directive 5111.11, Director of Net Assessment* (Washington, DC: Department of Defense, 2001).

[21] Lawrence Freedman, *Strategy: A History* (New York: Oxford University Press, 2013), xii.

[22] Gabriel Elefteriu, *A Question of Power: Towards Better UK Strategy through Net Assessment* (London: Policy Exchange, 2018).

[23] Michael D. Swaine et al., *China's Military & The U.S.-Japan Alliance in 2030: A Strategic Net Assessment* (Washington, DC: Carnegie Endowment for International Peace, 2013).

[24] One of the major challenges for researchers pursuing social network analysis methodology is that "some of the best and most influential are still highly classified." There is no set methodology. See Swaine et al., *China's Military & The U.S.-Japan Alliance in 2030*, 7.

[25] Victor Hugo, *Histoire D'Un Crime* (Paris: Michel Lévy Frères, 1877). Literal translation of the original French.

[26] Andrew F. Krepinevich and Barry D. Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy* (New York: Basic Books, 2015), 107.

[27] *Get Brexit Done, Unleash Britain's Potential: The Conservative and Unionist Party Manifesto 2019* (London: Paragon Customer Communications, 2019), 51.

[28] "Queen's Speech: Volume 801," Hansard, UK Parliament, 7 January 2020.

[29] *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion* (Somerville, MA: Recorded Future, 2019).

[30] Daniel Araya, "China's Grand Strategy," *Forbes*, 14 January 2019.

[31] Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era" (speech, 19th National Congress of the Communist Party of China, Beijing, 18 October 2017).

[32] *Information Advantage*, Joint Concept Note 2/18 (London: UK Ministry of Defence, 2018), iii.

[33] Karen Pierce, "Evidence of Russia's Involvement in Salisbury Attack" (speech, United Nations Security Council, New York, 6 September 2018).

[34] *Operation "Secondary Infektion": A Suspected Russian Intelligence Operation Targeting Europe and the United States* (Washington, DC: Atlantic Council, 2019), 4.

[35] Marcel Schliebs, *China's Inauthentic UK Twitter Diplomacy: A Coordinated Network Amplifying PRC Diplomats* (Oxford, UK: Programme on Democracy & Technology, University of Oxford, 2021).
[36] Marcel Schliebs, *China's Public Diplomacy Operations: Understanding Engagement and Inauthentic Amplification of PRC Diplomats on Facebook and Twitter* (Oxford, UK: Programme on Democracy & Technology, University of Oxford, 2021).
[37] Julia Bergin, "How China Used the Media to Spread Its Covid Narrative—and Win Friends around the World," Conversation, 12 May 2021.
[38] Philipp Lorenz-Spreen et al., "Accelerating Dynamics of Collective Attention," *Nature Communications* 10, no. 1 (2019), https://doi.org/10.1038/s41467-019-09311-w.
[39] *Communications Market Report, 2019* (London: Office of Communications, 2019); and Wylie, *Mindf*ck*, 44.
[40] *News Consumption in the UK: 2019* (London: Office of Communications, 2019), 7.
[41] John B. Horrigan, *Digital Readiness Gaps* (Washington, DC: Pew Research Center, 2016).
[42] Nic Newman, *Reuters Institute Digital News Report* (Oxford, UK: Reuters Institute for the Study of Journalism, 2019), 20.
[43] Bernard Marr, "How Much Data Do We Create Every Day?: The Mind-Blowing Stats Everyone Should Read," *Forbes*, 21 May 2018.
[44] Cristian Vaccari and Andrew Chadwick, "Deepfakes And Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," *Social Media + Society* 6, no. 1 (2020), https://doi.org/10.1177/2056305120903408.
[45] *Disinformation and "Fake News": Final Report* (London: House of Commons, 2019), 71.
[46] Geoffrey Sloan, "Military Doctrine, Command Philosophy and the Generation of Fighting Power: Genesis and Theory," *International Affairs* 88, no. 2 (2012): 244, https://doi.org/10.1111/j.1468-2346.2012.01069.x.
[47] Bagge, *Unmasking Maskirovka*.
[48] Julian Lindley-French, *NATO: Countering Strategic Maskirovka* (Calgary, AB: Canadian Defence & Foreign Affairs Institute, 2015).
[49] Bagge, *Unmasking Maskirovka*.
[50] "What Is Cybernetics?," University of St. Andrews, accessed 15 November 2021.
[51] *Disinformation and "Fake News."*
[52] *Intelligence and Security Committee of Parliament: Russia* (London: House of Commons, 2020).
[53] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237–56, https://doi.org/10.1080/13518040490450529.
[54] Thomas, "Russia's Reflexive Control Theory and the Military."
[55] Sun Tzu, *The Complete Art of War*, trans. Ralph D. Swayer (Boulder, CO: Westview Press, 1996).
[56] Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, 30 January 2018; and Larry Diamond and Orville Schell, eds., *China's Influence and American Interests: Promoting Constructive Vigilance* (Washington, DC: Hoover Institute, 2018).
[57] Stacie Hoffman, Samantha Bradshaw, and Emily Taylor, *Networks and Geopolitics: How Great Power Rivalries Infected 5G* (Oxford, UK: Oxford Information Labs, 2019), 15.
[58] Shanthi Kalathil, *Beyond the Great Firewall: How China Became a Global Information Power* (Washington, DC: Center for International Media Assistance, 2017), 1–6.

[59] "Ofcom Revokes CGTN's Licence to Broadcast in the UK," press release, Office of Communications, 4 February 2021.
[60] "2020 World Press Freedom Index," Reporters Without Borders, accessed 15 November 2021.
[61] AM Edward J. Stringer, CB, CBE, RAF, interview with author, 28 May 2020; hereafter Stringer interview.
[62] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020), 11.
[63] *National Security Capability Review* (London: Her Majesty's Government, 2018).
[64] The Global Coalition against Daesh (website), accessed 15 November 2021.
[65] "77th Brigade: Influence and Outreach," British Army, accessed 15 November 2021.
[66] "Government Cracks Down on Spread of False Coronavirus Information Online," Gov.UK, 30 March 2020.
[67] *Information Advantage*, iii.
[68] Stringer interview.
[69] Robert R. Leonhard, *The Principles of War for the Information Age* (New York: Ballantine Books, 1998), 25.
[70] *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy* (London: Her Majesty's Government, 2021), 27.
[71] *Global Britain in a Competitive Age*, 49.
[72] Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, *Chinese Disinformation Efforts on Social Media* (Santa Monica, CA: Rand, 2021), 120, https://doi.org/10.7249/RR4373.3; and Dexter Roberts, *China's Disinformation Strategy: Its Dimensions and Future* (Washington, DC: Atlantic Council, 2020).
[73] "Chinese Ethnic Group: Facts and Figures," Gov.UK, 27 January 2020; and "Chinese Diaspora," Academy for Cultural Diplomacy, accessed 15 November 2021.
[74] Abby Budiman and Neil G. Ruiz, "Key Facts about Asian Americans, a Diverse and Growing Population," Pew Research Center, 29 April 2021.
[75] Julian McDougall and Julian Sefton-Green, "Media and Information Literacy Policies in the UK" (paper, London School of Economics and Political Science, London, 2014), 4.
[76] *GCSE (Full Course) Results, Summer 2019* (London: Joint Council for Qualifications, 2020).
[77] The author would argue that political appetite is embodied in the national legislative base. In the cases of China and Russia, there is a strong theme of lawfare there. Political appetite is a little too intangible for the author's liking as an analytical concept. The author has deliberately chosen asymmetries that can be measured in some fashion. The author cites similar reasoning for not analyzing psychological asymmetries either.
[78] "Russia: Number of Internet Users, 2015–2022," Statista, 2020; and Lily Hay Newman, "Russia Takes a Big Step toward Internet Isolation," *Wired*, 5 January 2020.
[79] Alena Epifanova, *Deciphering Russia's "Sovereign Internet Law"* (Berlin: German Council on Foreign Relations, 2020).
[80] Gabrielle Tétrault-Farber, "Putin Signs Law Making Russian Apps Mandatory on Smartphones, Computers," Reuters, 2 December 2019; and "Russia's Putin Signs Law Banning Fake News, Insulting the State Online," Reuters, 18 March 2019.
[81] Epifanova, *Deciphering Russia's "Sovereign Internet Law,"* 2.
[82] Daniel Funke and Daniela Flamini, "A Guide to Anti-Misinformation Actions around the World," Poynter, last updated 13 August 2019.

[83] *Initiatives to Counter Fake News in Selected Countries* (Washington, DC: Library of Congress, 2019), 18.
[84] Roya Ensafi et al., "Analyzing the Great Firewall of China over Space and Time," *Proceedings on Privacy Enhancing Technologies* 1 (2015): 61–76, https://doi.org/10.1515/popets-2015-0005.
[85] Sonali Chandel et al., "The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall," *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (2019): 111–19, https://doi.org/10.1109/cyberc.2019.00027.
[86] *Draft Online Safety Bill* (London: Her Majesty's Government, 2021).
[87] *Right to Type: How the "Duty of Care" Model Lacks Evidence and Will Damage Free Speech* (London: Index on Censorship, 2021), 4.
[88] *Draft Online Safety Bill*, 29–31.
[89] *Draft Online Safety Bill*, 12.
[90] "Facebook Reports Fourth Quarter and Full Year 2020 Results," Facebook, 27 January 2021.
[91] Eric De Brabandere, "Propaganda," Oxford Public International Law, last updated August 2019.
[92] *National Cyber Security Strategy, 2016–2021* (London: Her Majesty's Government, 2016); and "Defence Committee," UK Parliament, accessed 15 November 2021.
[93] Ben Wallace, "Address to the NATO Parliamentary Assembly 2019" (speech, Queen Elizabeth II Centre, Westminster, London, 14 October 2019).
[94] Sir Adam Thomson, KCMG, email to author, 19 May 2020.
[95] *Government Artificial Intelligence Readiness Index, 2019* (Malvern, UK: Oxford Insights, 2019).
[96] Leila Alieva, "Brexit in the Context of Democracy under Threat," Foreign Policy Centre, 3 October 2019.
[97] Yuen Foong Khong, "The US, China, and the Cold War Analogy," *China International Strategy Review* 1, no. 2 (2019): 223–37, https://doi.org/10.1007/s42533-020-00034-y.
[98] Julian Lindley-French, interview with author, 26 May 2020.
[99] *Online Harms White Paper* (London: Her Majesty's Government, 2019).
[100] *The Integrity Initiative Guide to Countering Russian Disinformation* (London: Institute for Statecraft, 2018).