Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Performing Information Manoeuvre Through Persistent Engagement

Nick Reynolds

Performing Information Manoeuvre Through Persistent Engagement

Nick Reynolds

RUSI Occasional Paper, June 2020

Royal United Services Institute
for Defence and Security Studies

189 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 189 years.

Published in 2020 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, June 2020. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Executive Summary

INFORMATION HAS ALWAYS been critical to warfare. Today, however, changes to the information domain are forcing militaries to adapt how they operate. With the boundary between peace and conflict becoming increasingly blurred, and with the collapse of the distinction between domestic and foreign affairs due to connectivity and globalisation, the British Army is now called upon to persistently compete against a diversified array of threats both above and below the threshold of warfighting.

A new concept is therefore necessary, and pertinent existing and emerging technologies such as artificial intelligence require a robust conceptual framework to guide their adoption and use. Primarily, the ever-increasing volume of data that typifies the information environment poses an insurmountable challenge to management approaches involving centralisation.

Information Manoeuvre is particularly relevant across the 'Protect', 'Engage' and 'Constrain' stages of the PECF framework as laid out in the Integrated Operating Concept (IOpC), as it is there that the preconditions for the 'Fight' are set.[1] Information Manoeuvre is dependent upon persistent engagement to provide the human relationships and situational awareness that are vital to understanding the environment, other actors, events and trends. First and foremost, Information Manoeuvre is about people, and what they need to know to operate effectively.

This paper seeks to identify the key changes in the operating environment, and their implications for established military concepts. It has reached the following conclusions:

- Operating in the information domain equates to more than just the application of virtual fires to achieve effect. The British Army will operate in a densely connected and contested information environment. It will not be able to consistently assure its own networks, and will be reliant on plugging its C4ISTAR capabilities into civilian infrastructure, either because the civilian population is critical to the desired operational outcomes, or because the UK must operate with coalition or multinational partners with varying levels of capability. Doctrine should therefore emphasise that British forces must manoeuvre through this virtual environment.
- It is necessary to include informational aspects to schemes of manoeuvre. As information and networks cannot be assured, and because of the requirement to integrate into wider information infrastructure to send and receive data, commanders must be prepared to define and fight for the information they need, so that priorities in assurance become lines of effort. This both dictates the technical requirements of the force and necessitates

1. Army Concepts Branch, 'British Army Operating Concept: What it Means for the British Army, Draft v2', , 11 September 2019, pp. 2–5.

the adoption of a planning cycle and battle rhythm that recognises when particular information is needed.

- Information Manoeuvre must be brought into collective training, and collective training must be conducted within a contested electromagnetic spectrum (EMS). The British Army must train with units and capabilities being denied to the force. Unlike hypothetical capabilities being brought in, which is difficult to simulate, being subject to denial and therefore having capabilities removed can be implemented immediately. Training within a contested EMS is the only way to build the desired culture and level of trust within and between units and the systems that they will depend upon.
- Defence requires a resilient and flexible bearer network that can circumvent outages and blockages and allow different elements and echelons of the force to communicate under degraded conditions. Operational communications that allow units to reach back to higher headquarters should be integrated with the tactical network, to avoid intermediate headquarters being relied on to manually mediate what data is routed and how. Users should be able to use the bearer network to access and draw upon stored data from different formations and echelons. The network must also be able to integrate into the Combined, Joint, Intra-Governmental, Inter-Agency and Multinational (CJIIM) environment, while imposing a high degree of security on specific components. Commanders must define where and when they prioritise connectivity over security, and vice versa.
- Information Manoeuvre requires the deployment of teams who will be exposed to risk. The concept must therefore be supported by the requisite permissions and authorities. Furthermore, permissions cannot simply be held at higher echelons, since this makes the force vulnerable to decapitation or paralysis as tactical actions are pushed to operational and strategic decision-makers. The British Army must have pre-emptive permissions that enable its practitioners to employ their skills while persistently engaged.
- Judging when to apply effects is a critical output of Information Manoeuvre and is best enabled through persistent engagement. Militaries often judge the effectiveness of information activity in terms of the speed of decision-making it enables. Although speed brings advantages on the battlefield, it is not decisive. Instead, the force should prioritise applying effects with carefully judged timing to maximise their impact.
- The measurement of effects in Information Manoeuvre is complex because numerous audiences are affected. As with timing, there is a tendency for influence to be pursued relentlessly, enemy networks attacked or degraded wherever possible, and adversary narratives challenged, because these activities seem important. The Manoeuvrist Approach, however, demands that effects are delivered to achieve cognitive effect. Thus, Information Manoeuvre should consider how information activities shape an adversary system, rather than simply confronting adversary systems symmetrically.
- Effects-based assessments of operations are essential at the interface between physical and informational effects. Killing the wrong person at the wrong time can have disastrous consequences. Conversely, the discrete application of violence beneath the threshold of warfighting can send a clear and unambiguous message, which – if connected to appropriate influence activity – can have decisive cognitive effects in the service of deterrence and avoiding war.

Introduction

ON 3 JANUARY 2020, Major General Qassem Soleimani – commander of Iran's Quds Force – was targeted and killed in an airstrike by the US.[1] It was an unexpected and remarkable escalation in the ongoing contest between the US and Iran. The short-term impact was far greater than anything US sanctions or rhetoric had been able to produce. Iran's response to the targeted strike included an ineffectual series of missile attacks on coalition troops based on Iraqi soil[2] and the tragic shooting down of a civilian passenger aircraft,[3] seriously damaging the mythos that Iran had built around itself of being a competent unconventional adversary.

Several months on, the legal justification for the strike remains in dispute, and it is unclear what long-term effect it will have on US–Iran and US–Iraq relations. The critical takeaway from this operation is that whether it proves to be a success or a failure will be determined not by the event itself, but by how the physical effect is leveraged to communicate intentions, thresholds and political resolve. In and of itself, the action may be meaningless, or it may be exploited by the US's adversaries. With improperly calibrated justifications, it may prove to be counterproductive or damaging to the US's goals in the region. If the right messaging and diplomacy are adopted, it could either impose limitations on malign Iranian activity, advantageously shape the relationship between the US and Iran, or force the two countries to the negotiating table. What can be clearly derived from the killing of Soleimani is that kinetic action and messaging, when disaggregated, are of limited potency. It is through the coordinated application of these mechanisms that the greatest and most nuanced effects may be produced.

The current international security environment has been variously characterised as being in a state of 'durable disorder'[4] or 'constant competition'.[5] States no longer declare war on each other, as the consequences, costs and particularly the constraints and legal obligations associated with doing so are judged to be too expensive.[6] Most armed conflicts are small- and medium-scale cases of endemic instability conducted largely through proxies or a partnered component.[7] This general description of the current state of affairs is not new, and has received

1. *BBC News*, 'Qasem Soleimani: US Kills Top Iranian General in Baghdad Air Strike', 3 January 2020.
2. *BBC News*, 'Iran Attack: US Troops Targeted with Ballistic Missiles', 8 January 2020.
3. *BBC News*, 'Iran Plane Crash: Tor-M1 Missiles Fired at Ukraine Jet', 21 January 2020.
4. Sean McFate, *Goliath: Why the West Doesn't Win Wars. And What We Need To Do About It* (London: Michael Joseph, 2019), p. 8.
5. Ministry of Defence (MoD), Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18: Information Advantage', 2018, p. 4.
6. Tanisha M Fazal, 'Why States No Longer Declare War', *Security Studies* (Vol. 21, No. 4, 2012), pp. 557–58.
7. Amos C Fox, 'In Pursuit of a General Theory of Proxy Warfare', Land Warfare Paper 123, Institute of Land Warfare, February 2019, p. 1.

detailed academic attention.[8] What is most relevant to the British Army is that the decisiveness of military activity is determined as much in the information domain as by purely kinetic activity. Synergising informational and physical capabilities has never been more important. Information is also becoming increasingly integrated. Psychological operations, intelligence, electronic warfare, counterintelligence, and command and control (C2) have hitherto largely existed in disparate silos. Today, the systems supporting these activities are merging. Because the targets of psychological operations are also information producers, they are equally targets for intelligence collection. Intelligence gathered from scraping this information must be stored and transmitted to inform command decisions, and it is therefore both a target for electronic warfare and a priority for assurance by security systems.

A second important change in the information operating environment is the much greater population density that permeates the modern battlefield, both physically and virtually. The Army Operating Concept states that 'the Army is decisive on Land, where people live',[9] and given the urban nature of most societies, a focus on the urban space and population centres is implied. Since the physical population will record and disseminate content, localised physical activity can have a disproportionate impact in shaping the attitudes of the wider population, and therefore can turn a permissive environment hostile, or vice versa. As an illustration of the extent of this phenomenon, the combined length of all video footage taken in Syria of the conflict and shared online since 2011 is several times greater than the length of the war in real time.[10] Armies must therefore be able to integrate and operate between face-to-face and virtual relationships. Navigating human terrain – and the information that flows between people – is increasingly critical to achieving the Manoeuvrist Approach: the British doctrinal variation of manoeuvre theory aimed at exploiting unexpected and unorthodox opportunities to achieve cognitive effects upon adversaries and thereby achieve objectives without the need to physically destroy the enemy.

In seeking to conceptualise how to navigate, operate and gain advantage in this information domain, the British Army has developed the Information Manoeuvre concept.[11] British Army operations possessing an informational element are not new. The need for a new concept stems from an international environment in which traditional military activity, though still important in imposing thresholds, is feared to be of increasingly limited utility in addressing threats

8. John Arquilla, *Insurgents, Raiders, and Bandits: How Masters of Irregular Warfare Have Shaped Our World* (Chicago, IL: Ivan R Dee, 2011), pp. 267–80; Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Westport, CT: Praeger, 2009); David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2009).
9. Army Concepts Branch, 'British Army Operating Concept: What it Means for UK Security, Draft v7', 11 September 2019, p. 1.
10. Andy Greenberg, 'Google's New YouTube Analysis App Crowdsources War Reporting', *Wired,* 20 April 2016.
11. Headquarters Force Troops Command, *Force Troops Command Handbook* (Upavon: Headquarters Force Troops Command, 2017), pp. 10–11.

outside the conventional warfighting space. These limitations will be compounded if military activity cannot be coordinated effectively with messaging and political direction. Furthermore, if technological change is not assimilated correctly, the result could be disastrous. In the First World War, the telegram and telephone appeared to be a revolutionary force multiplier for those who were able to integrate these new forms of communications into their forces. However, the enthusiastically adopted technology served to separate generals from their armies, and the already critical tactical and operational issues created by the new paradigm of industrialised warfare were rendered incomprehensible to distant commanders, despite their improved ability to communicate with their subordinates. Under these conditions, 'operations degenerated into indecisive stagnation'.[12]

The need for a new concept is also driven by the need to maintain parity with adversaries and competitors. Superior ISR, C2, and data management have been at the heart of Western military operations for decades. Advantage in the information domain, however, cannot be assured. Where totalitarian regimes of the 20th century sought to lock down, isolate and deny information, new and old competitors are becoming more nuanced at managing and exploiting data. The Chinese government, for instance, allows criticism on online social media platforms, as this is a key means for them to gauge public sentiment, only censoring discussions that generate collective action.[13] While the British Army has often been limited in its activity within the information domain, particularly online and via social media, adversaries have incorporated it into their levers of national power and integrated it with military effects, granting them the capacity to punch above their weight.[14] The cyber element of Russian thinking on information warfare has long emphasised the psychological impact that cyber operations can have on their adversaries, and is well-integrated into overall Russian strategy.[15] As Clint Watts notes, 'Russians are brilliant at [information warfare] because they don't see it as a subcomponent of warfare, it is warfare'.[16] Australian General Angus Campbell defined the current paradigm as the return

12. Robert Leonhard, *The Principles of War for the Information Age* (New York, NY: Ballantine, 1998), p. 14.
13. Gary King, Jennifer Pan and Margaret E Roberts, 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument', *American Political Science Review* (Vol. 111, No. 3, 2017), pp. 484–501.
14. Tom T, 'CARD ECHO; The Value of a Quick Guide', *Wavell Room*, 6 February 2020, <https://wavellroom.com/2020/02/06/card-echo-the-value-of-a-quick-guide/>, accessed 27 May 2020; Frank Ledwidge, *Losing Small Wars: British Military Failure in Iraq and Afghanistan* (New Haven, CT: Yale University Press, 2011), pp. 210–39; Stuart Crawford, 'Military Struggles with Social Media – An Analysis', *UK Defence Journal*, 21 February 2020.
15. Timothy L Thomas, 'Russian Views on Information-Based Warfare', *Airpower Journal* (Vol. 10, 1996), p. 26.
16. Clint Watts, cited in Nick Brunetti-Lihach, 'Information Warfare Past, Present, and Future', *Strategy Bridge*, 14 November 2018, <https://thestrategybridge.org/the-bridge/2018/11/14/information-warfare-past-present-and-future>, accessed 2 December 2019.

of an updated form of political warfare.[17] By contrast, the British Army has untapped potential that it has yet to leverage through coordinating physical activity and information in operations. Information also provides avenues and vectors for offensive action against which the British Army and the UK as a whole may be vulnerable. That existing capabilities are deficient has been demonstrated in Afghanistan and Iraq, where it has been argued that it was the insurgents who truly practised the Manoeuvrist Approach through initiative, surprise and the leveraging of their superior information about the local terrain and population to undermine Western credibility and dominate the narrative.[18] Effective information operations therefore require intelligence and targeting functions to include a deep contextual understanding of the environment, necessitating persistent engagement throughout the world's expanding human terrain. Rapid societal and political change driven by advancing technology has meant that permissions, authorities and regulatory frameworks lag behind the reality of the current and future information domain.[19]

This paper is an independent assessment of the character of the future information operating environment, and the capabilities and conceptual frameworks that the British Army requires to effectively operate within it. In 2019, RUSI was commissioned by the British Army's Directorate of Information to examine how the information domain is evolving, and the impact on established military concepts of manoeuvre. In addressing these issues, RUSI engaged in six months of consultations with military officers, civilian officials and security industry practitioners from countries including the UK, the US, France, Israel and Ukraine. The author also conducted a focused review of the extensive developing literature on the information domain, encompassing past doctrine and methods, to assess the relevance of established concepts to the contemporary battlefield. The paper is largely theoretical and is not based on empirical research or field work. Consultations with practitioners currently conducting operations in the information domain and with those developing the Information Manoeuvre concept aimed to complement the data gathered from the review of the literature. A conceptual approach was taken, rather than focusing on the operational or tactical levels, but reference is made to numerous practical examples to best illustrate lessons learned and highlight good practice.

This paper does not attempt to describe the British Army's Information Manoeuvre concept, or to prescribe what it must be. Instead, it seeks to demonstrate why a concept that encompasses military activity in the information domain and physical military manoeuvre is necessary if militaries are to remain competitive in the future operating environment. The paper seeks also to reach conclusions that may inform those developing the Information Manoeuvre concept. The paper primarily intends to unpack how changes in the information domain are reshaping concepts at the heart of traditional military activity, and vice versa. For example, it explores persistent engagement as a critical function in enabling information manoeuvre, by ensuring situational awareness in the human environment. With the latest available figures indicating

17. Brendan Nicholson, 'ADF Chief: West Faces a New Threat from "Political Warfare"', *The Strategist*, 14 June 2019.
18. Ernest Y Wong, 'Leveraging Science in the Manoeuvrist Approach to Counterinsurgency Operations', *AUSA Land Warfare Papers* (No. 80, October 2010), p. v.
19. MoD, Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18', p. 21.

that there are now less than 75,000 full-time and fully-trained British Army personnel,[20] persistent engagement is recognised as a difficult task given the Army's small size, to the point that it has been described in the Army Operating Concept as 'expensive and politically sensitive'.[21] This paper cannot resolve this issue, but does highlight some of the considerations that must be balanced.

The paper is divided into three chapters. The first explores the drivers for change arising from the information operating environment. The second examines the components of a force optimised to manoeuvre within the information domain. The third outlines the different conceptual frameworks that are nested within Information Manoeuvre, which must be understood for the components to function correctly.

20. *BBC News*, 'Strength of British Military Falls for Ninth Year', 16 August 2019; British Army, 'The Army in Numbers', <https://www.army.mod.uk/umbraco/Surface/Download/Get/7999>, accessed 14 May 2020.
21. Army Concepts Branch, 'British Army Operating Concept: What it Means for the British Army, Draft v2', 11 September 2019, p. 2.

I. The Future Information Operating Environment

MANY ELEMENTS OF the information domain are not new, and have a long literature that need not be re-examined here.[22] However, there are several elements of the information domain that are undergoing fundamental changes which must affect military operations. The three foremost changes in the information operating environment are: the shift in computing from net processors to net producers of information; the emergence of artificial intelligence (AI); and the scope and scale of contestation throughout the information domain. This chapter unpacks each of these and their implications for the British Army.

Processing and Producing

The fundamental issue which defines the information age is that the computer today 'is not simply a *processor* of information; it is also a *producer*'.[23] Therefore, while computers may promise to process information more effectively, the amount of information that they produce makes the processing of information more demanding. Today, information operations are propagated at a new speed and scale across an instantly responsive network that integrates the majority of the global population and has drastically reduced the costs of entry, allowing individuals and small groups – sometimes with very little funding – to generate high volumes of content, messaging and random data.[24] Production of information is not only vastly greater, but is also conducted by an increasingly diffuse array of actors who can be difficult to identify en masse. Whether the computer proves to be a better processor than it is a prolific producer defines the information space. Issues of attack and defence, the ability to infiltrate or protect systems, to find targets and to hide from surveillance – by hiding in the noise or concealing oneself – are evolving dynamics that stem from this question.

---

22. Rid and Hecker, *War 2.0*; John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001); Jon Latimer, *Deception in War: The Art of the Bluff, the Value of Deceit, and the Most Thrilling Episodes of Cunning in Military History, from the Trojan Horse to the Gulf War* (Woodstock, NY: Overlook Press, 2001); David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century* (New York, NY: Basic Books, 2017); P W Singer and Emerson T Brooking, *LikeWar: The Weaponization of Social Media* (Boston, MA: Houghton Mifflin Harcourt, 2018); Richard A Clarke and Robert K Knake, *Cyberwar: The Next Threat to National Security and What to Do About It* (New York, NY: Ecco Press, 2010).
23. Leonhard, *The Principles of War for the Information Age*, p. 17. Emphasis in original.
24. MoD, Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18', p. 3.

It is questionable whether it will be possible to harness computational power to process sufficient information to achieve comprehensive situational awareness – a prerequisite for leveraging that information to one's advantage.[25] Currently, the computer is a far better producer than it is a processor. Sensors and detection are far more capable than they were before,[26] but despite popular fears of the information domain becoming a tool of mass surveillance, the sheer volume of electronic communication is making it increasingly difficult to collect and analyse. This is a growing weakness in signals intelligence (SIGINT).[27] The advent of high-density persistent ISTAR in the form of lower-cost UAVs has changed the threat picture in conflict zones considerably,[28] but this will further increase the processing burden associated with analysis. Psychologist Robert Cialdini hypothesised that, in the information age, comprehensively analysing situations will become more difficult, relegating humans to analysing ever-narrower segments of a problem or relying on heuristics.[29] Creating cognitive effect through influence is therefore easier[30] when the target lacks the tools that might assist in filtering or aggregating information and understanding complex problems.[31] Yet defence is more difficult because of the increased likelihood of strategic surprise.

States governed by authoritarian regimes have resisted their declining ability to monitor their own citizens.[32] Russia currently uses a 'System for Operative Investigative Activities' to track the activity of its citizens online.[33] It is thought to be exporting this to client states as a cheaper model of controlling internal populations than the extensive and expensive Chinese approach of mass surveillance and suppression.[34] Russian companies are not market leaders, and their technology has experienced problems such as the accidental leaking of data.[35] Nevertheless, it has the advantage of being inexpensive and easy to install and use. Export of this technology has primarily been to former Soviet countries, but markets have also been found in Africa, South America and the Middle East.[36] Russian ideas, such as that of a sovereign internet – which aims

25. Leonhard, *The Principles of War for the Information Age*, p. 19.
26. *Ibid.*, pp. 17–18.
27. Richard Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: HarperCollins, 2011), p. 550.
28. David Axe, 'Turkey Has a Drone Air Force. And It Just Went to War in Syria', *National Interest*, 2 March 2020.
29. Robert B Cialdini, *Persuasion: The Psychology of Persuasion* (New York, NY: Harper Collins, 2007), pp. 277–79.
30. *Ibid.*
31. Aldrich, *GCHQ*, p. 550.
32. Mari Ristolainen, 'Should "RuNet 2020" Be Taken Seriously? Contradictory Views About Cyber Security Between Russia and the West', *Journal of Information Warfare* (Vol. 16, No. 4, 2017), pp. 113–14.
33. James Andrew Lewis, 'Reference Note on Russian Communications Surveillance', Commentary, Center for Strategic & International Studies (CSIS), 18 April 2014.
34. Alina Polyakova, 'Russia is Teaching the World to Spy', *New York Times*, 5 December 2019.
35. *Ibid.*
36. *Ibid.*

to create a centrally controlled and heavily restricted national intranet[37] – have been adopted or copied abroad.[38] Iran has copied the Russian practice of interfering with internet access when facing domestic protest,[39] as did Syria in 2011.[40]

This shift from computers being net processors to net producers of information has far-reaching implications for the British Army. During the Second World War, forerunners of computers drastically accelerated the breaking of codes because they could process a vast number of possible combinations at a rate that could not be matched by human codebreakers.[41] Thus, the machine reduced a large quantity of data to a comprehensible and manageable volume of conclusions. This has been the trend in military computer processing ever since. Computers have taken in ever-greater volumes of information and processed it to deliver a useable volume of output. This development arguably reached its height during the Global War on Terror as the US pursued 'total information awareness'.[42] This led to the expansion of targeting cells supporting brigade-sized formations like Task Force Stryker,[43] which comprised hundreds of analysts trained to sift and process the combined imagery intelligence (IMINT), SIGINT, human intelligence (HUMINT), electronic intelligence (ELINT), and open source intelligence (OSINT) collected from the battlespace. This trend may have peaked due to the manpower and infrastructure requirements reaching an unsustainable level while delivering diminishing returns. The size of these targeting cells required large bases in theatre that, against anything but a sub-peer adversary, would have a large signature and be easily targeted. Furthermore, even a single platform – such as an F35 multirole combat aircraft or an Ajax armoured fighting vehicle – has a sensor suite capable of producing far more information than it can safely transmit to a central headquarters. Thus, the notion of a unified central database that commanders and planners can interrogate to draw upon a complete picture of the battlefield is illusory. Instead, individual platforms will need to be highly selective in what they share across limited data bandwidth, providing the centre with a limited picture of the battlespace. If this centralised data is to be useful rather than misleading, and since this requires a precise set of criteria for what data a platform is to share with higher echelons, it follows that the quantitative methods used to leverage big data[44] are increasingly

37. Ristolainen, 'Should "RuNet 2020" Be Taken Seriously?', p. 113; Alena Epifanova, 'Deciphering Russia's "Sovereign Internet Law"', *DGAP Analysis*, No. 2, January 2020, p. 2.
38. Polyakova, 'Russia is Teaching the World to Spy'.
39. *Ibid.*
40. Ahmad Shehabat, 'The Social Media Cyber-War: The Unfolding Events in the Syrian Revolution 2011', *Global Media Journal* (Vol. 6, No. 2, 2012), p. 2; Bryan Lee, 'The Impact of Cyber Capabilities in the Syrian Civil War', *Small Wars Journal*, 26 April 2016.
41. Max Hastings, *The Secret War: Spies, Codes and Guerrillas, 1939–1945* (London: William Collins, 2015).
42. Sharon Weinberger, *The Imagineers of War: The Untold Story of DARPA, the Pentagon Agency that Changed the World* (New York, NY: Alfred A Knopf, 2017), p. 303.
43. Harry Tunnell, 'Task Force Stryker Network-Centric Operations in Afghanistan', Center for Technology and National Security Policy, National Defense University, October 2011, p. 2.
44. Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (London: John Murray, 2013).

in need of direction. This must be informed by qualitative analysis as to what data from a given operating environment is critical. Therein lies the importance of persistent engagement, and of integrating those in forward positions managing human relationships with those to the rear tasking computer systems to collect, analyse and contest the information domain. It is only through direct human contact with the human and physical terrain of the operating environment that appropriate qualitative criteria can be established to enable headquarters to determine and thereby leverage the data that is relevant.

Artificial Intelligence and Machine Learning

AI and machine learning (ML) are perhaps the most important technological advancements with which the British Army can engage. If they deliver what some proponents believe they promise,[45] they will herald the beginning of a seismic shift in the information domain. However, there is no consensus about whether this shift will actually occur. Sean McFate is a notable contemporary sceptic, having claimed that '[s]o far, no one has been killed by a cyberweapon', and that AI 'can barely accomplish basic cognitive tasks'.[46] He is partly correct. However, cyberweapons in the form of offensive algorithms have demonstrably killed indirectly by altering human behaviour and degrading systems that are intended to prevent death.[47] Furthermore, in contrast to McFate's scepticism, a study by a prominent team of AI researchers and developers considers the technology, far from being over-hyped, to be passing the point of early experimentation towards a degree of maturity and practicality.[48] The unresolved shortcoming of AI is that it has yet to deliver effect at scale.[49] The value of AI may not be in cognitive tasks, but in automating sub-tasks, allowing humans to become more efficient in conducting operations in the digital space.[50] The proliferation of AI could empower small teams, improving the agility and resilience of headquarters. This is a future scenario, but an imminent one.

Currently, detection is difficult due to the complexity of the environment, but once forces are detected, they are easily destroyed. A revolutionary improvement in processing would result in a comparable revolution in detection and precision targeting. AI and ML may therefore invert the processor–producer dynamic. Robert Leonhard's conceptual contest between information processing and production looks to be decisively determined over the course of the next few years.[51] This has far-reaching implications for kinetic military capabilities.

---

45. *Ibid.*
46. McFate, *Goliath,* p. 15.
47. Anjuli Shere, 'From Cyber Attack to Heart Attack: The Hidden Human Impact of Hospital Hacks', *New Statesman*, 3 December 2019; Sung J Choi, M Eric Johnson and Christoph U Lehmann, 'Data Breach Remediation Efforts and Their Implications for Hospital Quality', *Health Services Research* (Vol. 54, No. 5, 2019), pp. 971–80.
48. Miles Brundage et al., 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation', Future of Humanity Institute, University of Oxford, February 2018, pp. 4, 40.
49. *Ibid.*, p. 40.
50. *Ibid.*, p. 6.
51. Leonhard, *The Principles of War for the Information Age*, p. 17.

Behavioural or predictive analytics, which are likely to leverage AI, also have great potential.[52] Even in jurisdictions where there is a restricted scope to exploit data, such as the EU due to the General Data Protection Regulation (GDPR), social media use will generate sufficient activity to allow for behavioural analytics to be employed for detection, analysis, influence and – in the case of malign actors – manipulation.[53] Currently, behavioural analytics techniques are often unscientific and far less effective than they are made out to be in the popular consciousness, using frameworks such as the Myers-Briggs Type Indicator[54] that have been debunked by clinical psychologists.[55] Despite fears about the consequences of behavioural and predictive analytics, the evidence is mixed with regard to the level of effect that these can have.[56] The question is whether this will change as the technology matures.

The information age has increased complexity. Under the condition of complexity, cause and effect are very difficult to determine except with the benefit of hindsight. As Jim Storr explains:

> Complex problems generate huge amounts of information. That information [which] [sic] can often be dealt with adequately near to the source of complexity, at the risk that the local actor responds inappropriately from a global context. One response to this is to ensure that the actor understands the overall intent. That is, Mission Command once again. The other alternative is to centralise by passing all the information upwards.[57]

Currently, the former solution, that of Mission Command, is preferable.[58] Yet ongoing technological advances have raised a hypothetical question: what if the old estimate-based planning is replaced by truth-based planning through the incorporation of consistently accurate behavioural predictions?[59]

This hypothetical revolution may not come to pass. Realistically, the prospect of AI and ML generating their own vast wave of new data is far more likely than these technologies imposing order on the sheer volume of communications currently and constantly being produced. Nevertheless, it is essential that any progress towards such a paradigm inversion is carefully followed. What is certain is that surveillance and deception are both technical capabilities that, using mature behavioural targeting, will be increasingly effective, and the competition between

52. MoD, Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18', p. 21.
53. Orestis Papakyriakopoulos et al., 'Social Media and Microtargeting: Political Data Processing and the Consequences for Germany', *Big Data & Society* (Vol. 5, No. 2, 2018), pp. 2–10.
54. A theory which hypothesises that people can be divided into 16 distinct personality types.
55. Merve Emre, *What's Your Type? The Strange History of Myers-Briggs and the Birth of Personality Testing* (Glasgow: HarperCollins UK, 2018), pp. 1–18.
56. Angela Chen and Alessandra Potenza, 'Cambridge Analytica's Facebook Data Abuse Shouldn't Get Credit for Trump', *The Verge*, 20 March 2018.
57. Jim Storr, 'A Command Philosophy for the Information Age: The Continuing Relevance of Mission Command', *Defence Studies* (Vol. 3, No. 3, 2003), p. 126.
58. *Ibid.*
59. Leonhard, *The Principles of War for the Information Age*, p. 19.

surveillance and deception will manifest in new ways. 'These concerns are most significant in the context of authoritarian states, but may also undermine the ability of democracies to sustain truthful public debates'.[60] Technically savvy and determined adversaries, aided by advances in electronic warfare such as GPS spoofing,[61] signal that future electronic warfare advances may primarily take the form of improved deception measures rather than tracking. Adversary forces may use these capabilities 'to fade into the *sociopolitical* background';[62] in other words, to hide among the people as insurgents.

The issue of deception highlights the foremost consideration in the introduction of AI to military operations: assurance. If data cannot be pooled centrally – because production continues to outpace processing and bearer capacity – it is most likely that AI will function in support of discrete command processes, drawing on internal data first. For instance, it is conceivable that an AI could draw on consumption and inventory reports, projected consumption rates, known hostile and friendly positions, and route mapping to present unit commanders with alternative courses of action with attached risk estimates for the resupply of their forces. However, where an algorithm would interrogate data using questions authored by its designer, an AI would theoretically develop and subsequently shape its own questions. If a commander felt compelled to check the data underpinning an AI's conclusions at each planning iteration, then the AI would not have produced any efficiency in the unit. Thus, to add value, the AI must be trusted sufficiently that the commander accepts the robustness of its conclusions. This requires confidence not only in the AI's judgement, but also in its resilience in the event that certain data is denied or corrupted. As such, the integration of AI into the force is less a function of whether it is technologically possible to develop such command support tools – they are becoming increasingly prevalent in civilian life – but is instead a function of the extent to which humans are prepared to trust their life and the lives of their subordinates to that system.

This requires a degree of AI literacy among users, and training in realistic environments with a contested electromagnetic spectrum (EMS) where the AI can be seen to function when confronted with the frictions of combat. There is an inherent tension between the need to inform the force about how an AI works, so as to engender trust, and the imperative of protecting its mechanics from observation by adversaries, for if its mechanics can be understood, they can be gamed. By way of example, consider the German artist Simon Weckert, who concentrated a large number of cellular phones on a bridge, causing Google Maps to report a traffic jam.[63] If the Army is to deploy AI, it must build trust between its soldiers and their command support tools.

60. Brundage et al., 'The Malicious Use of Artificial Intelligence', p. 6.
61. Mark Harris, 'Ghost Ships, Crop Circles, and Soft Gold: a GPS Mystery in Shanghai', *MIT Technology Review*, 15 November 2019.
62. Leonhard, *The Principles of War for the Information Age*, p. 20. Emphasis in original.
63. Alex Hern, 'Berlin Artist Uses 99 Phones to Trick Google into Traffic Jam Alert', *The Guardian*, 3 February 2020.

The Contested Information Domain

The information space has rapidly evolved and will continue to do so at pace. The major development is that of the Internet and electronic communications, which now facilitate and mediate a large proportion of human interaction. This has not supplanted the previous generation of communications – such as television, radio and the telephone – which still have a wide audience and user-base and enjoy a great deal of trust. However, the current system of the Internet, smartphones and social media differs from traditional communications sources in that it interactively links individuals into a near-universal network which is instantaneously responsive to new information, constantly channels personalised information to individuals, and occurs at hyper-accentuated speed and scale.[64]

The information domain is contested in two ways. First, it is awash with disinformation, with constant competition for control of narratives being an unavoidable feature. Second, the infrastructure through which information flows is subject to threats through various means.

Disinformation has not created the post-truth information space, but thrives within it, and is funded and supported by several state actors.[65] While a multitude of platforms exist, 'Facebook remains the platform of choice for social media manipulation'.[66] Most online disinformation activity comes from a small selection of countries. Facebook and Twitter attribute the majority of influence operations conducted on their platforms to just seven countries – China, India, Iran, Pakistan, Russia, Saudi Arabia and Venezuela – which either directly or indirectly sponsor networks of fake accounts and a variety of messaging strategies to spread disinformation to influence audiences both domestically and abroad.[67] With its unrivalled manpower and hands-on approach to domestic political messaging, Chinese domestic disinformation is probably the most extensive example, with estimates suggesting that 'a large proportion of [Chinese] government web site comments, and about one out of every 178 social media posts on commercial sites, are fabricated by the government'.[68] While this is a huge amount of messaging output, it still amounts to little more than 0.56% of discussion on commercial Chinese forums, an indication that state disinformation does not necessarily dominate all online discourse. Comprising a low volume relative to the number of genuine online users, disinformation is deployed in a

64. MoD, Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18', p. 3.
65. Stephan Lewandowsky, Ullrich K H Ecker and John Cook, 'Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era', *Journal of Applied Research in Memory and Cognition* (Vol. 6, No. 4, December 2017), p. 353; Robert Chesney and Danielle Citron, 'Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics', *Foreign Affairs* (Vol. 98, No. 1, January/February 2019).
66. Samantha Bradshaw and Philip N Howard, 'The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation', Computational Propaganda Project, Oxford Internet Institute, University of Oxford, 2019, p. i.
67. *Ibid.*, pp. i, 11–13.
68. King, Pan and Roberts, 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument', p. 26.

targeted manner. Some areas of discussion are significantly influenced, with large swathes of online debate left untouched.[69] In terms of tone, it is difficult to distinguish disinformation from normal online discourse, and the way in which content manipulates the audience may be subtle or subjective, for '[d]isinformation is most often simply spin'.[70] This may be done with the aim of burying or hindering political dissent and opposition, or even mere discussion of controversial topics, as well as preventing dissidents and political opponents from connecting with like-minded people.[71] Furthermore, the tone and quantity of much disinformation has the effect of being psychologically exhausting.[72]

New avenues for disinformation are constantly emerging. Ever-improving computing equipment and software has made the means to make deepfakes – convincing but fabricated videos of real people – accessible to non-state actors and individuals. Information warfare has proliferated beyond the state-on-state context, and new disinformation techniques spread quickly if others detect them and consider them useful.[73] Once one actor develops and deploys a particular disinformation technique, it can quickly proliferate and enable other actors to take inspiration and deploy similar techniques, if deemed appropriate for their own goals. The pace at which offensive techniques proliferate makes countering them challenging.

A critical aim of disinformation is to destroy trust in the established system of government and between social groups.[74] The ongoing allegations of Russian interference in the UK's political parties and electoral processes, exacerbated by the recent refusal of the incumbent government to release a report into Russian activity,[75] are damaging to the UK's credibility regardless of the degree to which the allegations are true. The destruction of trust has often taken the form of promoting fake stories about political opponents to induce disgust and resentment of their actions. This can be done both by the creation of artificial political opponents, as well as

69. *Ibid.*
70. Darren Linvill and Patrick Warren, 'That Uplifting Tweet You Just Shared? A Russian Troll Sent It', *Rolling Stone*, 25 November 2019.
71. King, Pan and Roberts, 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument', pp. 1–3; Carl Miller, 'Inside the British Army's Secret Information Warfare Machine', *Wired*, 14 November 2018.
72. Maxim Eristavi, 'Why the US Keeps Losing the Fight Against Disinformation', *Atlantic Council*, 24 July 2017.
73. Simon Paterson, 'Sex, Lies and Videotape', *Edelman*, 13 November 2019, <https://www.edelman.co.uk/insights/sex-lies-and-videotape>, accessed 3 December 2019; Alex Hern, 'Far Right "Use Russian-Style Propaganda to Spread Misinformation"', *The Guardian*, 12 November 2019.
74. Linvill and Warren, 'That Uplifting Tweet You Just Shared?'; Darren Linvill and Patrick L Warren, 'Students Need to Learn How Trolls and Bots Stir up Online Divisions', *Times Higher Education*, 5 September 2019.
75. Dan Sabbagh and Luke Harding, 'PM Accused of Cover-Up Over Report on Russian Meddling in UK Politics', *The Guardian*, 4 November 2019.

creating fake allies, which can then become conduits for disinformation.[76] Adversaries 'know that, in political warfare, disgust is a more powerful tool than anger. Anger drives people to the polls; disgust drives countries apart'.[77] For example, Russian propaganda has often used fake online accounts and outlets to highlight legitimate issues of gender and racial inequality.[78] Disinformation can serve adversary interests by exacerbating existing antagonisms, sowing social division and undermining faith in institutions.[79] Regardless of the efficacy of any given technical tool, creating internal division is the primary cognitive effect that adversaries have sought both to *create* among target populations and *suppress* among their own.

Twentieth-century political warfare was based on 'the exploitation of sociological contrasts'.[80] During the Cold War, the US and the Soviet Union identified social tensions in their adversaries that could be useful points of leverage.[81] These techniques are still prevalent: the US electoral process has been a specific and deliberate target of Russia's Internet Research Agency's (IRA) information operations during the 2016 presidential elections and ever since, with social divisiveness over key issues being the central point of leverage.[82] The most targeted group for IRA disinformation were African Americans.[83] Similar strategies, under names such as 'information control',[84] have long been conducted by authoritarian regimes against their own citizens. However, while pioneered domestically by authoritarian regimes during the Cold War, globalisation from the 1970s onwards has blurred the distinction between foreign and domestic issues.[85] What differs is that these methods now have the potential to be refined and directed abroad, not to mention exported to the partners of authoritarian states.

Combined with micro-targeting, the potential for information campaigns to have significant political effects has become a cultural anxiety. Originally an advertising technique, micro-targeting is commercially lucrative and cheap to deploy, with the IRA targeting American voters in 2016 at a cost of as little as $0.16 for one political advert 'which eventually racked up

76. Linvill and Warren, 'That Uplifting Tweet You Just Shared?'; Linvill and Warren, 'Students Need to Learn How Trolls and Bots Stir Up Online Divisions'.
77. *Ibid.*
78. *Ibid.*
79. *Ibid.*
80. William R Kinter and Joseph Z Kornfeder, *The New Frontier of War: Political Warfare, Present and Future* (Chicago, IL: Frederick Muller, 1963), p. xix.
81. *Ibid.*
82. US Senate, Select Committee on Intelligence, 'Russian Active Measures, Campaigns and Interference in the 2016 US Election: Volume 2: Russia's Use of Social Media with Additional Views', Report 116-XX, pp. 4–6.
83. *Ibid.*
84. King, Pan and Roberts, 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument'.
85. Aldrich, *GCHQ,* p. 344.

16,000 reactions and 95,000 shares'.[86] Yet fears about deliberate political motivation should be tempered by an understanding that emotive, politically extreme disinformation is highly profitable when targeting an audience that is already sympathetic to the messaging being broadcast. Barriers to entry are already low for individuals or groups to engage in these kinds of hostile cyber activities.[87] In particular, far-right social media pages have proven to provide a consistent revenue stream, with many having been set up or co-opted purely for financial gain.[88] In these cases, the resulting political effect is simply an externality. Given the lack of penalties for spreading emotive disinformation, whether for mainstream political actors[89] or individuals, the high-benefit, low-cost proposition incentivises this sort of rhetoric, and it will be a feature of the online information space without new, forceful disincentive measures, sanctions and punishments.

Countering disinformation has proven to be difficult in part because sophisticated disinformation campaigns often come with inbuilt defence mechanisms. The creation of implicit associations between concepts[90] is an effective psychological tool to maintain disinformation. It is utilised by adversary information operations that not only undermine the target but also cause opponents to inadvertently sabotage their own counternarrative. One example is the Russian state's recent strain of propaganda associating support for the LGBTQ+ community with child abuse and foreign influence to undermine Russian society, thus delegitimising pro-LGBTQ+ rights initiatives.[91] Well-meaning, issue-based external support for the LGBTQ+ community unintentionally reinforces the Russian narrative of national victimhood and Western degeneracy. This presents a 'heads I win, tails you lose' scenario of furthering the state's social agenda and building domestic resistance against what is perceived as outside interference.[92] As a technique of influence, implicit association is particularly effective when targets or other supportive actors have poor situational awareness or lack the cultural understanding that prevents them from detecting how it has affected the audience's worldview. Under these circumstances, actors may engage in miscalibrated information operations that fail to challenge or inadvertently reinforce adversary narratives.

The physical infrastructure and EMS upon which the information domain is built is itself contested. Actions, such as cyber attacks on infrastructure in Western democracies, have so far been mostly ineffectual in the grand scheme of events, and have sometimes been dismissed

86. Natasha Singer, '"Weaponized Ad Technology": Facebook's Moneymaker Gets a Critical Eye', *New York Times*, 16 August 2018.
87. HM Government, 'National Security Capabllity Review', March 2018, p. 21.
88. Christopher Knaus et al., 'Inside the Hate Factory: How Facebook Fuels Far-Right Profit', *The Guardian*, 5 December 2019.
89. Casey Newton, 'Facebook's Decision to Allow Lies in Political Ads is Coming Back to Haunt It', *The Verge*, 15 October 2019.
90. Anthony G Greenwald and Mahzarin R Banaji, 'Implicit Social Cognition: Attitudes, Self-Esteem, and Stereotypes', *Psychological Review* (Vol. 102, No. 1, 1995), pp. 4–27.
91. Stephen Ennis, 'Russia's Mixed Messages on LGBT', *BBC News*, 29 April 2016.
92. *Ibid.*

as a phantom threat.[93] However, the Syrian civil war illustrates how a concerted campaign for control of the underlying communications infrastructure throughout a country can have a decisive impact.[94] Ukraine provides an ongoing example of a heavily contested EMS,[95] and there has been some evidence that Western critical infrastructure has a latent vulnerability to sustained attack from powerful adversaries with the capability to inflict catastrophic damage.[96] This highlights the challenge to information assurance.

Another aspect of the contemporary information domain is the widespread use of espionage technologies. These need only have a moderate degree of sophistication, because information moved across the Internet is generally insecure. Even those forms of communication designed to have a high standard of encryption, such as WhatsApp, are being penetrated by surveillance.[97] While the digital footprint that each individual leaves has been seen as a symptom of attempts to monitor or control the population, the various forms of voluntary mass surveillance to which people routinely submit themselves are primarily driven by advertising, and are 'merely symptoms of modernity'.[98] Nevertheless, the threat to information integrity and the difficulty of ensuring information security are pervasive issues.

These factors all have critical implications for both the conduct and need for Information Manoeuvre as a component of military operations. Traditionally, information operations and electronic warfare effects have been considered 'non-lethal fires'.[99] They are effects, applied to the battlefield. Understanding the level of contestation, however, requires a more dynamic appreciation of how the environment can be shaped, denied, secured or contaminated. It therefore becomes a domain within which forces manoeuvre. Shaping effects can be achieved across all three of what the British Army terms 'dimensions in warfare': the physical, virtual and cognitive. In the information contest, the centre of gravity is to a large extent the perceived authority of an adversary versus one's own forces. Shaping functions both affect how adversaries and the human terrain in the battlespace engages with information, and the physical means by which they access it. This can therefore be affected by the assurance, denial or destruction of

93. McFate, *Goliath*, p. 16.
94. Eva Bellin, 'Reconsidering the Robustness of Authoritarianism in the Middle East: Lessons from the Arab Spring', *Comparative Politics* (Vol. 44, No. 2, January 2012), pp. 129–31; Ahmad Shehabat, 'The Social Media Cyber-War', p. 2; Lee, 'The Impact of Cyber Capabilities in the Syrian Civil War'.
95. Liam Collins, 'Russia Gives Lessons in Electronic Warfare', *AUSA*, 26 July 2018.
96. Bruce Schneier, 'Someone Is Learning How to Take Down the Internet', *Lawfare*, 13 September 2016.
97. Stephanie Kirchgaessner, 'Israeli Spyware Allegedly Used to Target Pakistani Officials' Phones', *The Guardian*, 19 December 2019.
98. Aldrich, *GCHQ*, p. 550.
99. Wilson A Shoffner and Christopher D Compton, 'The Future of Fires: Dominating in Large-Scale Combat Operations', in Thomas G Bradbeer (ed.), *Lethal and Non-Lethal Fires: Historical Case Studies of Converging Cross-Domain Fires in Large-Scale Combat Operations* (Fort Leavenworth, KS: Army University Press, 2018), pp. 203–09; Scott D Applegate, 'The Principle of Maneuver in Cyber Operations', 4th International Conference on Cyber Conflict, 2012, pp. 1–13.

physical infrastructure supporting specific channels of communication just as much as by the dissemination of messages. In the event of a major conflict, it is possible to envisage states attempting to seal off the information environments of their populations, while seeking to contest the adversary's information space. The penetration of that sealed environment could involve physical infiltration of malware, or the conduct of standoff offensive cyber operations to open up areas of the information domain for contestation. Similarly, a state that perceives itself to have lost the trust of an audience may seek to contaminate the battlespace by engendering disgust and dejection among its inhabitants. Recognising when this is being achieved may signal advantage, but also demands a shift in approach if the terrain is to be secured, rather than becoming mutually denied. One point for land forces operating in the information domain is that unlike ground holding, control in the information domain is likely to be transitory. Like sea control, it cannot be held absolutely or indefinitely. Thus, the critical question becomes how a force can manoeuvre in the information domain to achieve advantage in the physical or cognitive dimension. It is as a contested environment that information has been elevated to a domain of warfare.

II. Components of Information Manoeuvre

THE DOCTRINAL COMPONENTS of Information Manoeuvre originate from 6th (UK) Division's predecessor, Force Troops Command (FTC), and are comprised of five pillars of capability: Networks; Intelligence; Cyber; Influence; and Security.[100] While valid and useful, these capabilities are strands that run through all military activity, partially reflecting FTC's role as a force-generating pool for combat support and combat service support elements to the whole force. In operationalising FTC into a full division, it is necessary to examine the five pillars indirectly through the components of an operating model. This chapter examines four components of Information Manoeuvre: the *actors* who conduct it; the *audiences* who comprise the *targets* to be affected; the *systems* that deliver these effects; and the *permissions* necessary to enable effective operations.

Actors

The new Integrated Operating Concept (IOpC) divides the operating environment into the separate states of 'Protect', 'Engage', 'Constrain' and 'Fight'. This is sometimes referred to as the PECF framework.[101] The 'Protect' state refers to securing the UK homeland, dependencies and interests. The 'Fight' state refers to the conduct of warfighting. However, the nuance and challenges of the concept largely fall within the 'Engage' and 'Constrain' states, which fall outside of direct protection of the UK homeland and below the threshold of warfighting. Roughly speaking, the 'Engage' state comprises the day-to-day activities that the British armed forces will conduct on the world stage under normal, permissive conditions; those of partner force capacity building, joint exercises and the strengthening of UK partnerships. The 'Constrain' state envisages those contested areas that necessitate deployments to deter – or, if necessary, deny – adversaries' access to a battlespace. Violence may be employed in either state, but to different ends. This is where much of the Army's ongoing operational activity will take place.

The IOpC acknowledges that these conceptual divides are artificial. This causes problems when attempts are made to use the IOpC to formulate a coherent strategy and use the concept to determine a division of labour, because multiple states may coexist in the same environment. For example, Anthony Cordesman argues that the US and its allies do not have a strategy or any clear goals for Iraq after the elimination of the Islamic State's territorial holdings.[102] Yet the

100. Headquarters Force Troops Command, *Force Troops Command Handbook*, pp. 10–11.
101. P R Barnes, 'Director Capability Delivers Keynote Speech on the Future of the British Army', British Army, 21 January 2020.
102. Anthony Cordesman, 'The Real Lessons of Mosul (and Sixteen Years of War in Afghanistan, Iraq, and Syria)', Commentary, CSIS, 19 July 2017.

US in Iraq and Syria, seen through the framework of the IOpC, is in the 'Fight' state against the Islamic State but in the 'Constrain' state against Iran, Russia and the Syrian government. It is also seeking to 'Engage' the Iraqi government. Alternatively, Oliver Major suggests a framework identifying the counter-Islamic State campaign as a highly kinetic combat operation within the broader theatre's 'Constrain' level.[103] In either case, the IOpC is a useful theoretical tool that cannot be oversimplified without losing its utility or becoming misleading. Information Manoeuvre is not synonymous with sub-threshold operations. However, it is within that sub-threshold space that a detailed, nuanced approach to Information Manoeuvre is the most relevant, as it must compensate for the limitations that the threshold of warfighting imposes on the use of kinetic effects.

6th (UK) Division, a new formation intended for capacity building and irregular warfare, is the principal actor which will take over generating forces for and conducting persistent engagement operations in the 'Engage' state. While Information Manoeuvre is relevant to all parts of the British Army and Combined, Joint, Intra-Governmental, Inter-Agency and Multinational (CJIIM)[104] efforts to which the Army will contribute, 6th (UK) Division will build the networks, relationships and information channels through which the foundation of Information Manoeuvre will occur, and into which 16 Air Assault Brigade, 3 Commando Brigade, 3rd or 1st Division can integrate should they be echeloned into theatre when required to conduct 'Constrain' or 'Fight' activities.[105]

6th (UK) Division serves as a bridge between Field Army and both UK Strategic Command – formerly known as Joint Forces Command (JFC) – and the Allied Rapid Reaction Corps (ARRC), and is arguably the initial unit charged with delivering Information Manoeuvre through persistent engagement in areas relevant to the UK's national interest.[106] Nevertheless, other organisations would benefit from adopting the same concept of operations as 6th (UK) Division, so as to best facilitate their potential deployments when 6th (UK) Division is already present. While the Army has previously subcontracted C2 to PJHQ, it is now retaking responsibility for this function and would serve as an intermediate C2 provider should escalation require the deployment of heavier forces.[107] Nevertheless, given its other commitments, 6th (UK) Division should not allow its role of force generation for joint structures to interfere with its delivering capabilities in-house.

In many ways, Special Operations Forces (SOF) provide a model for how the British Army should approach persistent engagement operations. SOF are successful because they are 'deep

103. Oliver Major, 'The Nature of the Fight in the Army Operating Concept: A Strawman for Director Capability', Draft, pp. 1–2.
104. Land Warfare Centre, *AFM Tactics for Stability Operations, Part 1: Counter-Irregular Activity* (Warminster: Land Warfare Centre, 2019), pp. 2–8.
105. Army Concepts Branch, 'British Army Operating Concept: What it Means for the British Army, Draft v2', pp. 1–2.
106. Ivan Jones, 'CFA Intent', presentation given at Land Warfare Centre, Warminster, 19 July 2019.
107. *Ibid.*

generalists'[108] or 'specialized generalists',[109] but many of their capabilities come from leveraging non-military attributes. Many of US SOF Civil Affairs units are reserve units,[110] which allows them to leverage outside expertise from wider society. US SOF also approach special operations in broader terms than UK Special Forces are able to, including a large number of non-combat functions – an approach from which 6th (UK) Division can adopt best practice. This is particularly evident in the realm of partner capacity building: 'Some of the most frequently deployed SOF assets are Civil Affairs (CA) units, which provide experts in every area of civil government to help administer civilian affairs in operational theatres'.[111] It is notable that US SOF also include a large media and psychological operations component, as well as esoteric capabilities such as specialist aviation advisory teams to build and develop partner air forces.[112] Their cultivation and use of a wider skillset and range of expertise within formations is worth emulating.

Persistent engagement with partners should primarily build security and stability; however, a worst case scenario of security deterioration or outside aggression would necessitate persistent engagement and partnering operations provision for conducting successful proxy warfare as a contingency.[113] The establishment of a forward presence is important to ensure that military commitments can be upscaled at short notice if required, and also as a signal of commitment in its own right. It also allows the environment to be understood and influenced, underscoring its relevance to Information Manoeuvre.[114] Since 6th (UK) Division will hold the relevant relationships and be persistently engaged, they will be the liaison element not only with partners, but also with allied formations and the 1st and 3rd Divisions of the British Army. Within the 6th (UK) Division, the transition from a dispersed posture to engage partners, and a concentrated posture to deter and potentially fight adversaries, is managed through the formation of a Divisional Information Manoeuvre Group (DIMG), which brings together dispersed lines of effort into a C2 hub able to support a warfighting formation. It is therefore essential that their C4ISR capabilities be exquisite to ensure that any transition or escalation involving additional forces being committed to theatre can benefit from as seamless a transition as possible in terms of command, control and information capability. However, the improvements and investment in C4ISR and information management technology that this necessitates should not translate into bloated C4ISR structures; it is important that technology be leveraged to allow smaller numbers of people to be as efficient and informed as possible, so that they can produce the best output

108. Jagdish Sheth and Andrew Sobel, *Clients for Life: How Great Professionals Develop Breakthrough Relationships* (London: Simon and Schuster, 2001), pp. 87–90.
109. Eitan Shamir and Eyal Ben-Ari, 'The Rise of Special Operations Forces: Generalized Specialization, Boundary Spanning and Military Autonomy', *Journal of Strategic Studies* (Vol. 41, No. 3, 2018), p. 336.
110. Congressional Research Service, 'U.S. Special Operations Forces (SOF): Background and Issues for Congress', updated 11 March 2020, <https://fas.org/sgp/crs/natsec/RS21048.pdf>, accessed 4 June 2020, pp. 3–4.
111. *Ibid.*, p. 3.
112. *Ibid.*, p. 5.
113. Fox, 'In Pursuit of a General Theory of Proxy Warfare', pp. 1–2.
114. British Army, 'Integrated Operating Concept', 2019, p. 14.

– providing their subordinates with succinct and executable plans, and support in terms of fires and ISR, at the right time. This will require commanders and staff officers to be well trained and well practised.[115] To protect these capabilities, information security and counterintelligence functions must be robust to ensure that these capabilities are able to continue operating when the information domain is contested. Potential approaches to this will be addressed in detail in the subsequent discussion of systems.

Information Advantage, which Information Manoeuvre is designed to deliver, seeks to deliver information as a distinct lever of national power rather than an underpinning element.[116] The use of dedicated formations, such as 77th Brigade, for influence is rational. The reality is that information will still constitute an underpinning element, but having specialist functions dedicated to it at the highest level as if it were a lever is a useful and usable way of structuring informational capabilities. There is a risk that information is stove-piped as a function if it is either improperly integrated or actively marginalised. To prevent this, influence units require enhanced capabilities and permissions to operate effectively, as well as a say in the formulation of strategy to ensure that their expertise and capabilities are reflected in overall planning.

The 77th Brigade consists of only 470 personnel, well below its intended strength.[117] However, the undermanning of the 77th Brigade should be seen in the context of widespread internal disagreements within Western forces about how to get the right cyber personnel in place.[118] The evidence suggests that the 77th Brigade has had comparative success in recruiting highly skilled outside specialists;[119] the brigade's staff includes approximately 100 reservists from senior managerial positions or with deep technical expertise,[120] making the formation well connected and influential in the wider information space.

To return to the five pillars, turning these capabilities into operational actors demands an effective C2 structure. For the UK, this structure is provided by 6th (UK) Division, which may be said to have three postures: provision of its capabilities to support UK forces; dispersed deployment to engage with partners and allies; and concentration into the DIMG to enable warfighting. Thus, one organisation has the requisite components to engage and understand its audience, allowing higher echelons to prioritise and retrieve relevant data from the information domain. It has the access to lay the foundations for human and technical networks to ensure their robustness

115. Jim Storr, 'Ten Years Observing Command and Control', *Journal of Military Operations* (Vol. 3, No. 1, Spring 2015), pp. 28–31.
116. MoD, Development, Concept and Doctrine Centre, 'Joint Concept Note 2/18', pp. 13–14.
117. David Bond, 'UK Army Unease Mounts After Decade of "Underfunding"', *Financial Times*, 14 May 2018.
118. Nina Kollars and Emma Moore, 'Every Marine a Blue-Haired Quasi-Rifleperson?', *War on the Rocks*, 21 August 2019.
119. Mary Hanbury, 'A Twitter Executive is Also a Reservist for the British Army's Information Warfare Unit', *Business Insider*, 1 October 2019.
120. British Army, 'Groups Within 77th Brigade', <https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/groups>, accessed 4 September 2019.

and engender trust under strain. And it has the capacity to contest the information domain in competition or conflict. Given its limited size, however, critical attention must be given to where effort is focused, and on when permissions and posture need to shift through the IOpC states, while acknowledging that they may overlap.

Targets and Audiences

The targets and audiences that Information Manoeuvre is intended to affect are varied. There is a challenge posed by UK partners and allies as explicit targets of Information Manoeuvre. It is important to draw a distinction between persuasion and manipulation, and between information sharing within a collaborative relationship and the intrusive extraction or insertion of information against an adversary or enemy.

With regard to adversaries and enemies, there are issues surrounding how to translate longer-standing and better-understood concepts of physical actions and effects into the digital space. The British Army's offensive cyber capabilities have only officially been directed at Islamist terrorist organisations and networks, though some ministerial rhetoric has indicated that this may extend to other state actors.[121] Writing for *Wired*, Carl Miller quoted an unnamed 77th Brigade officer who alleged that the brigade uses 'grey' or 'black' messaging,[122] referring to messaging or propaganda which is either not obviously attributable, hides the source or origin, or involves an active falsification of the supposed source.[123] According to the officer, this is generally only used in counter-piracy, counterinsurgency and counterterrorism operations.[124] This is likely a reflection of the controversial nature of directing these capabilities at other states – even when they are adversaries – and at the population at large. Caution in using black or grey messaging is sensible, given the negative consequences of being discovered to have been lying or propagating deliberately inaccurate information.[125] The traditional alignment of information operations with 'non-lethal fires', however, has arguably made it an adversary-centric discipline, where the audience and targets for information are not confined to adversaries. This shift in language from fires to Information Manoeuvre is important, because a partner would likely object to fires being applied against their territory, but may grant permission for an ally to manoeuvre across it.

121. Gareth Corfield, 'We'll Hack Back At Russians, Declare UK Ministers in Cyber-Blitz Blitz [sic]', *The Register*, 23 May 2019, <https://www.theregister.co.uk/2019/05/23/uk_will_hack_other_countries_say_ministers/>, accessed 4 September 2019.
122. Miller, 'Inside the British Army's Secret Information Warfare Machine'.
123. Philip M Taylor, *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era*, 3rd Edition (Manchester: Manchester University Press, 2003), p. 225.
124. Miller, 'Inside the British Army's Secret Information Warfare Machine'.
125. Kim Fridkin, Patrick J Kenney and Amanda Wintersieck, 'Liar, Liar, Pants on Fire: How Fact-Checking Influences Citizens' Reactions to Negative Advertising', *Political Communication* (Vol. 32, No. 1, 2015), pp. 127–51.

The importance of differentiating between manoeuvre and fires also holds true for the approach to offensive action against adversary C2 networks, infrastructure and supply chains. The way in which offensive actions are conducted will pose ethical dilemmas. While the risks of offensive activity proving to be disproportionate, indiscriminate or escalatory are low, issues may arise when adversary C4ISTAR and cyber capabilities are inextricably interlinked with civilian infrastructure and supply chains. Denying or degrading these capabilities will inevitably involve civilian infrastructure. Here, Information Manoeuvre provides a conceptual framework for when and how it is appropriate to direct actions against capabilities, infrastructure and supply chains that serve both military and civilian functions. Rather than considering all offensive cyber actions as the employment of digital fires, may be considered a digital form of manoeuvre. The approach to action against military networks embedded in civilian communications infrastructure can be analogous to a military unit's physical manoeuvre through an inhabited civilian settlement in which an enemy has taken up position. This is a useful distinction and can assist with calibrating actions to cause the correct effect in a targeted and discriminate manner.

With regard to allies and partners, the most prominent issues are of establishing interoperable and complementary networks, both physical and digital. How to integrate external allies and partners into the force can be seen as an extension of manoeuvring information within that force. The British Army often works in or with joint and multinational structures such as JFC, ARRC, NATO and Five Eyes (Australia, Canada, New Zealand, the UK and the US), which requires it to integrate and work with peers. Yet the Chief of the General Staff recently noted that the main integration challenge that the UK faces is keeping pace with US forces – a far more difficult prospect than keeping pace with adversaries.[126] Conversely, less capable partners who the British Army routinely works with, such as the Afghan National Security Forces, will be difficult to integrate into British networks given that their own information architecture will be different. This not only poses issues for interoperability, but integration may create vectors for adversaries to attack British information and C4ISTAR systems.[127]

Working with US forces and the Afghan National Security Forces, though very different prospects operationally, are fundamentally the same type of activity requiring the same problems to be solved. These include: how the British Army should persistently engage with another network through integration; and how to move information between them in order to successfully operate together. The IOpC acknowledges this tension.[128] In a multinational coalition context, the British Army should expect to fight at the division level, but in other contexts it will be the Battle Group. Therefore, the UK faces a broad set of tasks within this problem-set that require resolution. These comprise manoeuvring information within the force and with partners, plugging force multipliers (such as C4ISTAR capabilities and targeting data) into those partners, and building relationships.

126. Mark Carleton-Smith, 73rd Kermit Roosevelt Lecture, Fort Leavenworth, 7 March 2019, 01:06:00, <https://www.youtube.com/watch?v=bL3JYU1b2I8>, accessed 15 December 2019.
127. Jack Watling and Daniel Roper, 'European Allies in US Multi-Domain Operations', *RUSI Occasional Papers* (September 2019), p. 16.
128. British Army, 'Integrated Operating Concept'.

In the physical domain, operating alongside allies has more of an operational and deterrent effect than internal routine training,[129] and the hope is that this activity will create networks. A barrier to the effectiveness of the British Army is the difficulty of achieving a balance between a broad enough international footprint to engage in all areas of interest and concern while ensuring that footprint is well resourced and deep enough to achieve effect locally. In response, the IOpC recommends that NATO's international engagement networks be incorporated and leveraged into the UK's persistent engagement strategy.[130] The UK government laid the foundations for this by publishing its International Defence Engagement Strategy in 2013,[131] with the Defence Attaché Network providing an initial point of contact across the globe. While it has limited local capacity due to the small size of most UK embassy defence sections, this network can establish what opportunities are available for relationship building, or which areas of concern require political attention to overcome barriers that might otherwise impede or constrain engagement efforts.

Once the Defence Attaché Network has identified opportunities, the British Army can proceed with engagement operations. The correct political prerequisites, such as top-level buy-in,[132] must be in place for teams tasked with engagement activity to succeed. It is vital for defence sections to identify whether these have been met before engagement teams are deployed, what type of trainers are sent and at what level within partner institutions it would be most useful to deploy them. Given the British interest in increasing engagement with sub-Saharan Africa,[133] lessons from persistent engagement with weak states remain pertinent. Creativity and flexibility are necessary to tailor support to local conditions, not only in what is provided but in what incentive structures should be put in place. Major General Tony Jeapes recalled making a virtue of necessity in Oman, for he had very few weapons with which to supply his *firqat* proxy forces, and made the different units compete for material support by proving that they could conduct offensive action against the enemy.[134] If the correct types of support are provided and the proper incentive structures created, partner forces would be able to better focus on improving their operational capabilities.[135] In order to deliver this aspiration, the combat-focused trainers such as the Specialised Infantry Group require a non-infantry component, not as enablers but

129. Jones, 'CFA Intent'.
130. British Army, 'Integrated Operating Concept', p. 13.
131. James Chandler, *UK International Defence Engagement Strategy: Lessons from Bassingbourn* (London: Chatham House, 2016), p. 4.
132. Jack Watling and Namir Shabibi, 'Defining Remote Warfare: British Training and Assistance Programmes in Yemen, 2004–2015', Briefing No. 4, Oxford Research Group, p. 33.
133. Oxford Research Group, 'Infographics: Fusion Doctrine in Five Steps', 18 November 2019.
134. Tony Jeapes, *SAS Secret War: Operation Storm in the Middle East* (London: Greenhill, 2005), pp. 99–100.
135. Watling and Shabibi, 'Defining Remote Warfare', p. 33.

as combat support and combat services support trainers. They must also be empowered to hold partner forces to account.

While acknowledging that Information Manoeuvre must target audiences that are not inherently hostile, as well as partnered forces, deception of adversaries remains a critical capability in warfare. The planting of false information, distribution of propaganda and misleading material, and psychological operations targeting morale, as well as the penetration, denial or destruction of opponents' information systems, are all components of Information Manoeuvre. One of the challenges that the British Army must address are the rules of engagement underpinning these activities and the process for transition between different rules of engagement. It is becoming increasingly difficult to separate these activities from wider social media and information activities, since the systems supporting these activities are often the same.

It is important at this juncture to emphasise that military electronic warfare and the social media space, while quite separate in some regards, are linked on the modern battlefield. The conflict in eastern Ukraine has seen pioneering integration of the kind that the British Army and UK government at large needs to understand, monitor and periodically utilise. One example was the Ukrainian use of an Android smartphone app which helped artillery crews to process targeting data. The Fancy Bear/APT 28 hacking group, known to have ties with the GRU – Russia's foreign military intelligence – successfully infected the app with malware, and leveraged the information they were able to collect to gather intelligence and coordinate counter-battery fire against Ukrainian artillery units. This went undetected by the Ukrainians for over a year.[136] Intelligence generated from this type of malware has even been used in coordination with psychological operations to achieve cognitive and physical effect on the battlefield. Ukrainian units were warned that they would soon be attacked and Ukrainian parents were messaged and told that their sons had been killed in action, while Russian SIGINT monitored the increased traffic of subsequent messages being sent and received, and used this to determine the location of Ukrainian units and coordinate artillery fires accordingly.[137] This not only highlights the new technical capabilities, but also illustrates what a determined state adversary can achieve when it builds the requisite structural mechanisms to successfully coordinate nominally independent groups of hackers, the intelligence services, proxy militias and the regular military to achieve effect. While the tactics are malicious, it is nevertheless an example of cross-government coordination and moving information through internal structures made possible by technological development in both the military and the broader information domain from which the UK government should learn.

The rules of engagement will remain a challenge. No one, for example, would consider a hypothetical scenario where a deepfake video delivered to German troops before D-Day ordering them to redeploy, as improper. If it proved successful, no doubt such measures would be

136. Dustin Volz, 'Russian Hackers Tracked Ukrainian Artillery Units Using Android Implant: Report', *Reuters*, 22 December 2016.

137. Daniel Brown, 'Russian-Backed Separatists Are Using Terrifying Text Messages to Shock Adversaries — And It's Changing the Face of Warfare', *Business Insider*, 14 August 2018.

incorporated into the positive narrative of the effectiveness of Operation *Overlord*'s supporting deception activity. But today, when armed conflicts are rarely declared and such activity is carried out in the public sphere, where many spectators outside of the area of hostilities may not perceive what is happening to be war, the thresholds of the application of such capabilities must be clearly established and articulated in order to maintain legitimacy. In short, the target audience for information manoeuvre is diverse. The challenge is how to classify and control it.

Systems

In order to be effective, Information Manoeuvre is reliant on the correct systems being available, particularly the technical systems underpinning the British military's C4ISTAR capabilities. Here, it may be useful to provide a basic explanation of bearer networks or multi-bearer communications networks, for they are a mission-critical capability for the British Army – and for defence as a whole – to be able to implement Information Manoeuvre.

Fundamentally, a network is a collection of connected nodes. In this context, a bearer network is a network with the capability and flexibility to carry or bear data between nodes by a variety of different routes that may have different characteristics. Which route is used may be dependent on a variety of factors that include the type of data being transmitted, the size of the data packets, the security requirements associated with the data, and the degree to which access to the network is contested. This supports the efficient transmission of different types of data within an integrated overall system, as well as the overall resilience of the network. An example of a bearer network would be a network that integrates the wider Internet and a bespoke, secure military radio network, and which could flexibly route data packets through either one. Another example might be a bearer network consisting of a tactical very high frequency radio network for company-level units and an operational network transmitting data on high frequency wavelengths, which might be integrated to allow data to pass through either network. The bearer network capabilities required to integrate different forces' C4ISTAR already exist off the shelf, with systems able to integrate disparate radio and communications systems from different manufacturers using different frequencies and means of moving data.[138]

Another aspect within the realm of technical systems are the British Army's data-management capabilities. These are interlinked with the bearer network requirements, which will be the means by which that data will be routed. A multitude of technical solutions exist, whether defence specific, commercial or open source, and there are many possible approaches that could be adopted. What is critical is that whatever technical solution is adopted, it would support the Joint Force and wider UK government by contributing to a common data-management system. This will be a challenge. The British Army alone operates several data-management solutions for different purposes, and these do not necessarily communicate or interface with each other. When factoring in the other services and arms of government, agreeing on solutions that satisfy all parties given their differing requirements, organisational cultures and habitual modes of

138. Cubic, 'Radio Over IP', <https://www.cubic.com/solutions/c4isr/rugged-iot/connectivity-gateways/radio-over-ip>, accessed 10 December 2019.

operation will be a challenge. However, a shared understanding of and commitment to merging into a cohesive system would facilitate cross-government integration – an aspiration that has often proved elusive due to technical and structural constraints. While there is already dialogue across government on this subject, generating agreement and buy-in sufficient to actually adopt such a solution will be a challenge that will determine to what degree Information Manoeuvre fulfils its potential.

In order to best support the force, the minimum requirements for these systems to work are:

- The network must be able to integrate external partners and allies.
- The network must be able to impose a high degree of security on specific components, to assure that data is not intercepted and compromised.
- The network must be resilient and flexible enough to circumvent outages and blockages and allow different elements and echelons of the force to communicate under degraded conditions.
- The network must facilitate tactical peer-to-peer communications so that deployed units are able to communicate and coordinate in real time.
- Operational communications that allow these units to reach back to higher headquarters should be integrated with the tactical network, to avoid a reliance on intermediate headquarters to manually mediate what data is routed and how.
- Different formations and echelons should be able to use the bearer network to access and draw upon stored data that they may require in a flexible manner.

Bearer networks have traditionally been differentiated by the method of transmission. Human operators have often been the element that joins different systems so that the six-digit grid reference provided by a forward observer can be put into an artillery fire control system. However, most concepts of integration supporting modern complex weapons, and the situational awareness expected to optimally support Information Manoeuvre, require the transfer of increasingly complex data that a human operator cannot quickly and effectively translate. This lag in translation between bearer systems accounts for the large targeting staffs that have characterised Western counterterrorism operations. Encryption and translation both take time, so in moving data it is desirable to reduce the number of times it must be encrypted, decrypted and translated. Since the creation of a single connected system is unrealistic – as it is overly vulnerable to penetration from multiple entry points – some translations will be necessary in any bearer network or networks supporting the British Army. However, in reducing the time taken to translate material, and in ensuring the compatibility of systems, it becomes highly desirable for a common defence operating system to support families of separately developed applications. Thus, whether it is possible to develop a common defence operating system should be carefully considered. This would allow new applications to enter the defence ecosystem, which can understand – and interrelate to – those already being utilised, reducing the number of translations of different streams of data across the network.

Permissions

While getting the broader operational considerations right establishes many of the preconditions for success, specific permissions, authorities, freedoms and constraints can allow defence to act proactively or, if set inappropriately, can undermine operations.[139] Jim Storr has raised concerns about information activity requiring mission command being disincentivised in the past by a lack of permissions and legal protections.[140] Combined with the correct capabilities, well-framed, politically supported and sufficiently empowered persistent engagement operations have the potential to provide the requisite global network to support UK national interests. But it cannot be leveraged for advantage if UK forces lack the permissions to manoeuvre in the information domain.

The prerequisite condition for success is situational awareness. Historically, the majority of Britain's intelligence has been SIGINT gathered by GCHQ.[141] Aggregated electronic information and intercepted communications will continue to comprise the bulk of intelligence, but the British Army needs its own organic capacity to gather, process and disseminate this information. 6th (UK) Division's operations should include the leveraging of the passive exploitation of available data, for even commercially available options that aggregate open source information online are useful as they assist Intelligence Corps personnel with sifting through large quantities of data and tracking or monitoring social media in real time for early warning. Platforms that can relieve manpower for more useful analytical functions already exist in the commercial sector and can be readily leveraged.

The British Army, even in the comparatively peaceable 'Engage' state, requires offensive cyber permissions. Degrading the capability of enemies to utilise information or conduct their own operations are essential tasks.[142] There are signs that the US is already moving in this direction. The US cyber strategy now includes 'defending forward' as a deterrence measure, as part of persistent engagement in cyberspace.[143] While the US Department of Defense (DOD) tends to avoid disclosing the exact nature and intent of its cyber operations, there is some evidence that deterrence will in practice be achieved with threats such as offensive malware[144] – an acceptance that such activity has been normalised as a policy tool and is no longer the exclusive purview of covert operations or espionage. This would constitute a notable shift from the Obama-era ideal of creating a safe and open online environment.[145] Adversary capabilities of this kind are routinely directed at the UK itself. The UK government's National Cyber Security

139. MoD, Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18', p. 4.
140. Storr, 'A Command Philosophy for the Information Age', pp. 124–25.
141. Aldrich, *GCHQ*, p. 530.
142. MoD, Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18', pp. 12–13.
143. US Department of Defense, 'Summary: Department of Defense Cyber Strategy 2018', p. 4.
144. Karl Grindal and Karim Farhat, 'Persistent Engagement or Preparing the Battlefield?', *Internet Governance Project*, 24 June 2019.
145. Jacquelyn G Schneider, 'Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy', *Lawfare*, 10 May 2019.

Centre has warned of a wide-ranging and determined campaign by the GRU to target numerous organisations and companies with cyber attacks, asserting that the attacks were seemingly indiscriminate and designed to cause general disruption and confusion.[146] Given that Russia, China, Israel, Iran and the US all conduct this type of activity, to abstain would be to cede a capability for little reason.[147]

Permissions may need to be devolved to lower levels. The US Army has experimented with pre-emptive cyber permissions and authorities of this kind in the *Cyber Blitz* and *Orient Shield* exercises in 2019, where US forces from the new Intelligence, Information, Cyber, Electronic Warfare and Space (I2CEWS) detachment, expecting to be cut off from their commanders, utilised offensive action across the EMS and cyberspace on their own initiative throughout the scenario.[148] This scenario is the most likely case for when lower echelons require offensive permissions. Under other circumstances, operations may be planned centrally. However, in order for the British Army to present a resilient target, devolved permissions and capabilities are beneficial in that they create a problematic target for adversaries and prevent opportunistic attacks.

A simple yet elusive approach is to focus on asymmetric approaches and avoid fixating on enemy strengths or simply projecting one's own weaknesses onto opponents. An example of this trap is a conventional military force focusing only on defeating the conventional military forces of its opponents in battle.[149] Similar approaches have been made in the commercial sector, advocating asymmetry as a means of avoiding a tunnel-vision fixation on obvious rivals.[150] The alternative is to dispassionately identify the true point of leverage, whatever it may be or however it may manifest, and determine the best way of exploiting it. This principle is, of course, easier said than done. All of these are basic and known pitfalls of intelligence work, but they bear consideration. For the military to successfully adopt asymmetric approaches, it requires greater access and permission to operate in the commercial and political sectors where these intersect with the land domain; by having the capability to conduct a wider range of non-kinetic actions, this could establish the preconditions for a change in thinking that more easily accommodates non-kinetic solutions.

Information Manoeuvre needs to address what permissions it has to conduct messaging, particularly in terms of honesty. While the information domain is rife with disinformation and

146. National Cyber Security Centre, 'Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed', 3 October 2018.
147. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017), pp. 116–54; Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', *Strategic Studies Quarterly* (Vol. 12, No. 3, 2018), pp. 98, 112; Kirchgaessner, 'Israeli Spyware Allegedly Used to Target Pakistani Officials' Phones'.
148. Mark Pomerleau, 'What the Army Learned About Multidomain Operations at Cyber Blitz', *C4ISRNET*, 22 October 2019.
149. Leonhard, *The Principles of War for the Information Age,* pp. 226–39.
150. Peter Thiel and Blake Masters, *Zero to One: Notes on Start-Ups, or How to Build the Future* (London: Virgin, 2015), p. 38.

spin, there is a requirement for the British Army, under the right circumstances, to engage in the opposite approach to messaging – blunt, realistic appraisals. In 1958, then Israeli Minister for Foreign Affairs Golda Meir undertook her first official visit to several African countries. In Accra, Ghana, expecting to discuss economic development, she found herself instead questioned by several leaders from different African countries regarding her close security cooperation with France, which at the time was unpopular in Africa for its conduct in Algeria.[151] Her blunt response was an admission that, with powerful military adversaries receiving subsidised Soviet military support, Israel would establish relations with any major power that it could. This effectively contextualised Israel's position for Meir's audience and allowed her to deepen economic and diplomatic ties with several of the states represented, despite their differences.[152] Defence operates an echelon below that of diplomacy between heads of state. However, the ability for Defence to express how it must approach problems with a greater level of candour than it currently does under certain circumstances would be of immense value. Given the highly centralised permissions process for publicising information, the British Army likely needs greater permissions not only to combat – and in certain circumstances deploy – disinformation, but also to disseminate accurate information through trusted and identified human communicators.

The British Army needs to liaise with the wider defence system and with government to develop a better messaging strategy than it currently possesses. Engagement with the media is inevitable.[153] While the British Army has permissions to speak to the media and utilise online platforms on a routine basis, it must release information that acknowledges and better explains why the UK government acts in the way that it does when faced with conflicting imperatives. The permissions need to be pre-emptive, to ensure that UK influence operations can synchronise as best as possible with the near-immediate pace of the information domain. As with all Information Manoeuvre, this needs to be tied to good situational awareness, understanding of both local dynamics and how they fit into the broader international system, and consideration for the concerns of, consent of and coordination with the wider UK government. This need not cause political embarrassment if cross-government coordination is successful. Above all else, the British Army should not habitually engage in spin. This is not to say that the British Army should not engage in deception. Permissions to conduct deception, or obscure the purpose of military activity, are operational necessities. However, clear rules of engagement must be established to bound when and how such activities are pursued. Indeed, permissions to conduct deception operations are also valuable when granted to a well-integrated counterintelligence system, since monitoring the appearance of deliberately contrived information disseminated to a suspect target can be an invaluable method of identifying enemy agents or indiscrete friends.

There is a perception that the granting of pre-emptive permissions is to open up the force to escalation and reputational risk due to the impetuosity or incomplete perspective of the person on the ground. At the same time, restrictive permissions can impose risks to the reputation and

151. Sasha Polakow-Suransky, *The Unspoken Alliance: Israel's Secret Relationship with Apartheid South Africa* (New York, NY: Vintage, 2011), pp. 27–28.

152. *Ibid.*

153. Leonhard, *The Principles of War for the Information Age,* pp. 24–25.

safety of deployed personnel. For example, consider a theoretical British Army team delivering training to a partner force. It comes under fire. Should it have permission to exercise judgement in defending itself? Almost certainly. But suppose, instead, that the team were criticised on local social media by a locally influential person. Should the team leader be allowed to respond, either online or in person? Whereas permissions are available in the first kinetic instance, in the latter it is likely under current MoD policy that the team leader would need to seek centralised approval. To a Major in PJHQ, the incident may appear trifling and may therefore be relegated to a low priority for response, or permission may be declined because this is seen as the risk averse option given a lack of time to properly investigate and assess the balance of the situation. But the long-term consequences of not engaging could be severe. It could allow false or misleading narratives about the trainer's presence to spread, turning the population hostile, and thereby facilitating subsequent kinetic attacks. It could also show British soldiers as indecisive, permission seeking and passive in the eyes of partnered forces, undoing the respect that ensures the effectiveness of training and the security of the team through the willingness of partnered forces to defend them. Ultimately, the team leader is in a better place to decide on a course of action, and so permissions must be in place to enable them to exercise their professional judgement.

An implicit permission necessary to effectively practise Information Manoeuvre is the political buy-in to the importance of these methods. Since at least the 1990s, Western publics have exhibited a low tolerance for friendly casualties, often judging operational success solely on whether significant friendly casualties were suffered.[154] The campaigns in Iraq and Afghanistan constitute the highest level of military casualties that the UK has tolerated in recent years. The value that Western society places on its military personnel can work against it strategically, as casualties, either real or prospective, can cause a decisive loss in political and popular appetite for utilising those people in situations involving physical risk.[155] The aftermath of the Battle of Mogadishu in 1993 is perhaps the archetypal example of this lack of tolerance.[156] However, another contributing factor is that operational outcomes – apart from friendly casualties – are poorly reported and difficult to understand for domestic media commentators and the general public. The key to judging success is in the detail, but if the public is generally disengaged from an issue, then the issue will only be cognitively digested in abstract terms. Another interpretation is that the military and policymakers have so far found it difficult to make the case that individual security issues abroad matter.[157]

Another part of what Information Manoeuvre can offer is a better-informed British Army that is able to understand strategic issues and thus provide relevant advice to policymakers and other parts of government. UK Fusion Doctrine enshrines a coordinated whole-of-government

154. Brunetti-Lihach, 'Information Warfare Past, Present, and Future'.
155. Justin Bronk, 'The Weakness of "People" in Deterrence', *RUSI Commentary*, 18 December 2019.
156. Roger N Sangvic, *Battle of Mogadishu: Anatomy of a Failure* (Fort Leavenworth, KS: United States Army Command and General Staff College, 1999), p. 21.
157. Hew Strachan and Ruth Harris, *The Utility of Military Force and Public Understanding in Today's Britain* (Santa Monica, CA: RAND, 2020).

approach to security matters in UK policy, leveraging security, economic and influence levers of government power in a coordinated manner under the National Security Council (NSC).[158] While Fusion Doctrine considers the primary role of military activity to be providing security so that other government agencies can conduct their operations, the operational reality is acknowledged as requiring land forces to conduct significant influence operations.[159] As a critical component of a coordinated cross-government endeavour, the British Army must address problems in totality, and cannot confine itself to military-specific functions, even if other arms of government take the lead on non-military matters. What must be addressed, however, is what this means in practice in terms of permissions to provide support in the information domain to other departments. To operate effectively in this space, the British Army must divest itself of a blinkered, symmetrical focus on adversaries' equivalent military capabilities, which has in recent years impeded the application of the Manoeuvrist Approach. Information operations are not simply about using information assets to combat those of an adversary or enabling more efficient combat operations. They encompass any aspect of operations where information is influential, and these encompass the physical domains.

If the British Army and the wider UK government do not conduct effective and far-reaching influence operations, this will leave a narrative void which other actors will fill in ways that the UK government will struggle to counter retroactively. The British Army must play a role in proactively contesting this space. Yet the British public is often nervous about the development of these capabilities, fearing that the government intends to conduct influence operations against them. The Scottish Member of Parliament Douglas Chapman went so far as to accuse 77th Brigade of conducting manipulative information operations against Scotland, an erroneous claim which he quickly retracted,[160] that nevertheless highlights a discomfort with and suspicion of government-conducted influence campaigns given the prominence of political manipulation online. Given that the domestic information environment is connected to those in operational theatres, it is important to establish for the public the bounds and legitimacy of the permissions that the British Army wields in conducting Information Manoeuvre. Without this understanding, the political risks of operations must impose a considerable constraint on the effectiveness and responsiveness of operations.

158. HM Government, 'National Security Capability Review', pp. 10–11.
159. Land Warfare Centre, *AFM Tactics for Stability Operations, Part 1*, pp. 4-2, 5-2.
160. George Allison, 'Politician Claims that the British Army's 77th Brigade is "Attacking" Scots Online', *UK Defence Journal*, 23 August 2019.

III. Concepts

HAVING CONSIDERED SOME of the most far-reaching changes in the information operating environment, and the components required for conducting operations within the information domain, the conceptual implications of these for Information Manoeuvre and for established concepts of operations in general will now be addressed. This chapter is divided into four sections. The first is a brief discussion of alternative information concepts and where Information Manoeuvre sits within this debate. This is necessitated by both the appreciable conceptual innovations that have already been formulated and which are relevant to the British Army's own concepts, and the inability of alternative doctrines and approaches to entirely resolve the inherent challenges of addressing the complexity of the information domain. The subsequent sections cover Information Manoeuvre's integral sub-concepts of: speed, tempo and opportunity; how determining and measuring effects should be approached; and C2 in the context of a contested information domain.

Alternative Information Concepts

The Information Age has created the promise of using networked sensors to feed information into resilient and responsive C2 structures, better informing the force and enabling faster decision-making. The contemporary debate has built upon earlier doctrines, many of which are superficially similar and use many of the same component concepts and the same language. Network Centric Warfare, a direct predecessor and contributor to current thinking about information warfare, aimed to better integrate units to share battlefield awareness, allowing units to disperse while still working towards the same intent.[161] The Find, Fix, Finish, Exploit, Analyse, and Disseminate (F3EAD) model of operational decision-making, which was originally developed and utilised within the US Special Forces community, was a permutation of both the intelligence cycle and operational cycle that integrated the two into a single cohesive process.[162] This reflected how Special Forces have long benefited from investment in C4ISR and the ability to perform intelligence functions either in-house or with high levels of support from intelligence services.

The latest iteration of the information operations concept is the US Army's Multi-Domain Operations (MDO), which dictates that the Army needs to integrate capabilities across all

161. David S Alberts, John J Garstka and Frederick P Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Washington, DC: DoD C4ISR Cooperative Research Program, 2000), pp. 88–93.
162. Charles Faint and Michael Harris, 'F3EAD: Ops/Intel Fusion "Feeds" the SOF Targeting Process', *Small Wars Journal*, 31 January 2012.

domains, including space and cyber, in what it terms 'convergence'.[163] This goes beyond an earlier concept – 'synchronisation' – which allowed US and allied forces to fight a coordinated multi-domain campaign in the First Gulf War of 1991, but could only do so with prior coordination and planning. MDO are intended to achieve the same effect, but in a shorter timeframe and using more responsive, decentralised means.[164] In essence, MDO is information-empowered mission command, and is highly relevant to Information Manoeuvre. While the intellectual frameworks are somewhat different, both MDO and Information Manoeuvre are compatible in that they view domains as having collapsed into each other, with information being a unifying strand throughout the operating environment that can be used to identify and exploit vulnerabilities.

Other countries are developing similar concepts to MDO. The Chinese PLA term for modern conflict, as they currently conceive, it is 'systems confrontation'.[165] This aims to leverage exactly the same sorts of capabilities in terms of information, precision fires and strikes, and joint operations to destroy a given opponent's own systems. The systems to be targeted consist of all elements of C4ISR, while concurrent Chinese disruption activity will separately degrade and interfere with information flows between the various elements of the opponent's system.[166] There are two particularly notable elements of Chinese systems confrontation. First, they consider an opponent's fires capabilities to be of the utmost importance due to the threat that they pose, and they are thus worthy of targeting. Second, particular attention is paid to 'disrupting the time sequence and/or tempo of the enemy's operational architecture. This is to degrade and ultimately undermine the operational system's own "reconnaissance-control-attack-evaluation" process'.[167] In Chinese military literature on systems confrontation, 'information dominance is thought to be the core precondition to achieving dominance in other domains'.[168] In PLA academic discourse, information includes both the cyber domain and the electromagnetic spectrum.[169] Dang Chongmin and Zhang Yu outlined a sequential approach to dominance across domains; the information domain should be dominated first and foremost, followed by the air and space domains, with the land and/or sea domains being dominated last. However, there is little evidence that their precise interpretation of the general systems confrontation theory has achieved wider acceptance by other Chinese academics and theorists.[170] It is notable that Dang and Zhang hypothesised that domains are best dominated from fastest to slowest in terms of operational tempo.

163. US Training and Doctrine Command, *The US Army in Multi-Domain Operations, 2028* (Fort Eustis, VA: TRADOC, 2018), p. vi.
164. Watling and Roper, 'European Allies in US Multi-Domain Operations', pp. 14–15.
165. Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND, 2018), p. ix.
166. *Ibid.*, p. x.
167. *Ibid*., pp. x–xi.
168. *Ibid*., p. 12.
169. *Ibid*.
170. *Ibid*.

While different doctrines have focused on different elements of the information space, what they have often had in common is that they attempt to build structures that better integrate information using technology. The criticisms that can be levelled at them generally fall under the same broad themes:

- They either explicitly or implicitly promote centralisation, and the creation of vulnerabilities in terms of centralised C2 nodes; most reference mission command and subordinate empowerment, but the structures that they propose are, in practical terms, different forms of centralisation.
- Military operations are framed as separate from other activities; all attempt to integrate it into the broader information space but are constrained by longstanding structures that prevent this from being achieved.
- Speed and faster decision-making cycles are treated as an inherent means to attain decisive advantage, without integrating this with the question of why and how commanders at different echelons can make the right decisions at the right points.

Usually, information doctrines are created with an awareness of the first two issues and include attempts to solve them. It should be noted that this is a deep-rooted problem. Even Fusion Doctrine has been criticised as centralising decision-making powers with the NSC in a way that creates a single point of vulnerability.[171] The final issue, of speed, is often not perceived to be a problem, though Chinese systems confrontation is astute in its approach to this aspect of information.

These are issues that Information Manoeuvre has an opportunity to fix. If information can be manoeuvred within the British force and through government effectively, the UK's military capabilities will be increasingly credible, which will be critical to effective deterrence.

Speed, Tempo and Opportunity

Perhaps the most important deficit that Information Manoeuvre needs to correct is how the British Army approaches speed. Jim Storr is of the opinion that 'the British Army appears to have forgotten about speed and tempo'.[172] It is not that the Army does not think about speed. However, the framework by which it approaches it is problematic. According to the Army Operating Concept, 'the Army will radiate deterrence by increasing the speed of decision-making relative to the adversary'.[173] This is based on John Richard Boyd's OODA loop theory – that a decision cycle comprises 'Observing', 'Orienting' oneself, 'Deciding' and finally 'Acting'.[174] This is not a problem unique to the British Army, but is deeply ingrained in the Western way of war.

171. Watling and Roper, 'European Allies in US Multi-Domain Operations', p. 18.
172. Jim Storr, *The Human Face of War* (London: A&C Black, 2009), p. 38.
173. Army Concepts Branch, 'British Army Operating Concept: What it Means for UK Security, Draft v7', p. 1.
174. John R Boyd, 'Destruction and Creation', US Army Command and General Staff College, 3 September 1976, p. 1.

The US Army's data strategy, not yet unveiled, is based on ensuring that the US decision-making cycle is faster than that of adversaries, and was described by Lieutenant General Stephen G Fogarty as being 'sense, understand, decide, act and assess'.[175] It is also narrowly employed:

> Generally, the U.S. military gravitates towards the use of information to support kinetic solutions. The emergence of the so-called information revolution in military affairs in the 1990s led the services to use information to strike targets faster and more accurately through concepts such as net-centric warfare and effects-based operations through networking, sensors, computers, and satellites.
>
> … While adversaries comfortably blend political and military operations, the American military tradition studiously avoids political considerations in campaigns. Military success is presumed to lead inexorably to a favorable political outcome overseas. Hence some have concluded 'power and diplomacy to occupy separate spheres'.[176]

A major issue that the OODA loop theory fails to address is that it does little to synchronise domains that run to fundamentally different timetables. Cyber operations, particularly social media and influence operations, are fast, and sometimes deliver effects that are either virtually instantaneous or occur within a matter of minutes. By contrast, the air domain is fast but periodic, while the maritime domain is much slower, and the land domain slower still. When countering irregular warfare or conducting peace support and stabilisation operations, it is very slow indeed. The political domain is often unresponsive to changes occurring in theatre, and slow to assess or reassess failure. While timeframes may on occasion be comparable to those of land operations, the considerations and timetables are likely to be delinked, making coordination difficult.

The counterpoint to this is decentralisation. An example is how 'self-synchronisation – an essential element of Network Centric Warfare'[177] – is essentially identical to ideas of mission command dating back to the 1930s, except that subordinate commanders are empowered with information.[178] Network Centric Warfare's conception of speed was unsophisticated, for the most part simply equating a faster decision cycle to advantage,[179] and leveraging adaptation or mission command when centralised C4ISR systems fail. This binary approach to operating leaves little scope for efficient coordination through an intermediate state of partial communications failure, disruption or denial.

The existing framework should not be entirely dismissed. At a basic level, Boyd's OODA loop model of decision-making has validity, and the principle of maintaining a faster decision-making

175. Mark Pomerleau, 'A New Name – and Focus – for Army Cyber Command?', *C4ISRNET*, 21 August 2019, <https://www.c4isrnet.com/show-reporter/technet-augusta/2019/08/21/a-new-name-and-focus-for-army-cyber-command/>, accessed 28 May 2020.
176. Brunetti-Lihach, 'Information Warfare Past, Present, and Future'.
177. Storr, 'A Command Philosophy for the Information Age'.
178. *Ibid.*
179. Alberts, Garstka and Stein, *Network Centric Warfare,* p. 89.

cycle than adversaries, and thus increasing the credibility of the UK's deterrence posture, is an aspiration of the Army Operating Concept.[180] One example of the importance of decision speed is the collapse of France in the Second World War, a feat of conventional arms that has rarely been matched, let alone surpassed.[181] However, getting inside an adversary's decision cycle by being faster is overly simplistic.

The Vietnam War is one useful case study. North Vietnamese forces were routinely less responsive at the tactical and operational level than their US opponents.[182] Yet the war holds more lessons on speed and timing than the common truism of US tactical superiority. A faster OODA loop and more responsive US forces were rendered irrelevant by North Vietnamese strategic patience, though there were periods when decisive outcomes were possible. In 1965, the North Vietnamese made a credible attempt to invade the South to pre-empt American involvement.[183] They were unable to achieve their aims before the large-scale deployment of US forces, and by 1966 South Vietnamese and US forces had succeeded in putting the North Vietnamese on the defensive. By 1967, South Vietnamese and US forces were aggressively pursuing the North Vietnamese Army and the Viet Cong, causing some North Vietnamese politicians to call for peace talks.[184] Strategic patience was ultimately decisive, but 1965 presented a window of opportunity that both sides responded to aggressively, with the US achieving short-term success in that instance.

The conflict between Israel and Egypt from 1967 until 1973 is another period that deserves scrutiny – in particular, the actions of the Israelis in 1967. This was a brief time window in which there was, though imperfect, an unprecedented and never-repeated level of political unity within the Arab coalition,[185] with prospective support from the Soviet Union. Israel faced a credible existential threat and narrowly avoided a pre-emptive Egyptian strike through careful messaging and disinformation, and then struck once the Egyptians no longer expected it.[186] Then Prime Minister Levi Eshkol's many preceding diplomatic overtures to Egypt, Israel's other Arab neighbours, and the US and Soviet Union were genuine. But the Israeli government rapidly switched from desperate negotiating[187] to a decision by Eshkol and his cabinet to go to war.[188]

180. Army Concepts Branch, 'British Army Operating Concept: What It Means For UK Security, Draft v7', p. 1.
181. Storr, *The Human Face of War*, p. 37.
182. Cecil B Currey, *Victory at Any Cost: The Genius of Viet Nam's Gen. Vo Nguyen Giap* (Dulles, VA: Potomac Books, 2005).
183. H R McMaster, *Dereliction of Duty: Lyndon Johnson, Robert McNamara, the Joint Chiefs of Staff, and the Lies that Led to Vietnam* (New York, NY: HarperCollins, 1997), p. 229.
184. Gregory A Daddis, *Westmoreland's War: Reassessing American Strategy in Vietnam* (New York, NY: Oxford University Press, 2014), pp. 81–86.
185. Avraham Sela, 'The 1973 Arab War Coalition: Aims, Coherence, and Gain-Distribution', *Israel Affairs* (Vol. 6, No. 1, 1999), pp. 36–39; Michael B Oren, *Six Days of War: June 1967 and the Making of the Modern Middle East* (Oxford: Oxford University Press, 2002), p. 163.
186. Oren, *Six Days of War,* pp. 119–26, 159–61, 170–215.
187. *Ibid.*, pp. 61–126.
188. *Ibid.*, pp. 152, 157–58.

Then Defence Minister Moshe Dayan leveraged the earlier atmosphere of uncertainty by giving a press conference immediately before the war with feigned irresolution, making the famous statement that 'it is too late and too early' for military action.[189] The start of operations proper immediately afterwards[190] allowed them to achieve strategic surprise. This was remarkable in that Israel created a window of opportunity which favoured themselves and exploited it under circumstances where they faced multiple temporal constraints. They faced an opponent who already strongly suspected that they would attack[191] and had mobilised their forces for imminent war,[192] while Israel could not themselves sustain a long war.[193] As Eshkol believed, they also had much to fear from a Soviet intervention.[194] From such dire circumstance and with little temporal room within which to manoeuvre, they were able to signal a deceptive intent and then pre-emptively attack with perfect timing to achieve strategic surprise, psychologically paralyse the Egyptian government and maximise their military success.[195]

Israel would later themselves be initially psychologically out-manoeuvred in the October 1973 Yom Kippur War by their adversaries. Aided by a comprehensive deception plan, Egypt achieved strategic surprise when it assaulted and crossed the Suez Canal.[196] Though there was some difference of opinion between the military and political leadership as to what should constitute a favourable military outcome, with officers such as General Saad el-Din el-Shazly and General Mohamed Fawzi taking a more realistic view than then President Anwar Al-Sadat, neither side sought to destroy Israel as had been attempted previously. Instead, Egypt committed to making a favourable peace with some level of domestic legitimacy.[197] Speed is an advantageous characteristic, albeit one that the outmatched Egyptian military did not possess.[198] Trevor Depuy argues that timing was the critical factor in determining the outcome of the war, and that the Egyptians, though they set the conditions for their success, failed to fully capitalise on windows of opportunity that they had created by their successful crossing of the Suez Canal.[199]

Another example that highlights other temporal and decision-cycle dynamics is the 1993 Battle of Mogadishu. Task Force Ranger, the small US SOF task force entrusted with capturing Mohamed Farah Aidid and dismantling the Habar Gidir clan's leadership, had a faster decision-

189. Howard M Sachar, *A History of Israel: From the Rise of Zionism to Our Time* (New York, NY: Alfred A Knopf, 1981), p. 638.
190. Oren, *Six Days of War*, p. 170.
191. *Ibid.*, pp. 158–59.
192. Youssef H Aboul-Enein, *Reconstructing a Shattered Egyptian Army: War Minister Gen. Mahamed Fawzi's Memoirs, 1967–1971* (Annapolis, MD: Naval Institute Press, 2014), p. 111.
193. *Ibid.*
194. Oren, *Six Days of War,* pp. 149–50.
195. *Ibid.*, pp. 170–210.
196. Sela, 'The 1973 Arab War Coalition'.
197. Fouad Ajami, 'The End of Pan-Arabism', *Foreign Affairs* (Vol. 57, Winter 1978/79), p. 358; Aboul-Enein, *Reconstructing a Shattered Egyptian Army,* pp. 166–67.
198. Aboul-Enein, *Reconstructing a Shattered Egyptian Army,* pp. 29–45.
199. *Ibid.*, p. 185.

making cycle than its adversaries, but it was insufficient to deal with irregular fighters operating autonomously. While decisions were made at speed, the exposure of the MH-60's vulnerability to RPG fire from the ground was not adequately incorporated into decision-making for several cycles. In some respects, the speed at which planning could be changed inhibited the ability to factor in new information regarding the greater risk of established concepts of operation. The opportunity to take ad hoc tactical steps to protect the vulnerable helicopters, which were left in orbit of the target area for 40 minutes, were missed, with disastrous results.[200] The C2 system was responsive, but the commanders proved inadequately adaptable to changing circumstances.

With regard to Aidid's Habar Gidir militia, their decentralisation made them formidably responsive combatants and allowed them to quickly counterattack any and all elements of Task Force Ranger as these were committed to the operation, inflicting casualties and damage at every opportunity.[201] However, a lack of overall C4ISR meant that the militia, unaware of the larger picture, overcommitted to battle, fixed themselves by repeatedly attempting to overrun US positions, and suffered unacceptably high casualties. Once the cost of the battle became apparent, Aidid and the Habar Gidir clan's will to fight was broken, causing them to call for a ceasefire, though the Clinton administration failed to capitalise on this opportunity.[202]

Such pivotal windows of opportunity are rare, and for them to be identified and capitalised on is rarer still. A conclusion one can draw is that the speed – or time-based – aspect of Information Manoeuvre has two elements. The first is tactical, and relatively easy to achieve: roughly analogous to Boyd's OODA loop, it is to enable UK forces to operate at sufficient speed to not be habitually outpaced by adversaries. This is unlikely to provide decisive advantage, for adversaries will adapt,[203] but it will ensure that UK forces are resilient and competitive. The second is operational and strategic. Information Manoeuvre should be utilised to disrupt adversary windows of opportunity, open windows of opportunity for friendly forces and to assure the British Army's information operations – not to outpace adversaries, but to ensure that land forces remain responsive and are not paralysed by disruption.

A fait accompli scenario – where an adversary's seizure of a small area of territory inflicts disproportionate damage to the victim's credibility by changing the facts on the ground faster than an opponent can respond – presents the UK and NATO with strategic dilemmas that are difficult to solve if adversaries achieve strategic surprise. Here, the use of strategic information operations to either detect or have sufficient situational awareness to accurately interpret the relevant tactical and atmospheric information can prevent adversaries from achieving strategic surprise and executing a fait accompli operation. This is very similar to the 'left of bang',[204] a tactical theory of combat emphasising dominance through pre-emption. If relations

200. Sangvic, *Battle of Mogadishu*, pp. 24–30.
201. *Ibid.*, pp. 13–19.
202. *Ibid.*, pp. 20–21.
203. Leonhard, *The Principles of War for the Information Age*, pp. 210–11.
204. Patrick Van Horne and Jason A Riley, *Left of Bang: How the Marine Corps' Combat Hunter Program Can Save Your Life* (New York, NY: Black Irish, 2014), pp. 15–17.

between the UK and an adversary were to deteriorate, a response could be to leverage the UK's information capability to disrupt adversary decision-making, create doubt or impose delays that close windows of opportunity, and thereby have a decisive strategic effect. It is critical that this capability and approach is developed within 6th (UK) Division operations. Moreover, the effective functioning of 6th (UK) Division's intelligence apparatus is essential to preventing strategic surprise. Strategic estimates are large and complex, therefore requiring in-depth study, which in turn results in a longer intelligence cycle. However, if long-planned aggression goes undetected at the strategic level or the evidence and conclusions are otherwise unclear, short-term tactical warning is vital.[205] The 6th (UK) Division and persistent engagement can serve to prevent strategic surprise through providing just such early warning, if the correct relationships and capabilities are put in place and developed.

Timing is also relevant in influence operations. Behavioural analytics and micro-targeting, despite their questionable efficacy, have a far greater potential for effect when deployed at critical moments. Benign advertisements to micro-targeted groups have been used by malign actors to build up pages and profiles with large followings, which then in the immediate prelude to recent elections have deployed disinformation within a short timeframe in which it has proven difficult to detect the disinformation and disseminate a response.[206] This is, in effect, the creation of a one-off impossible decision cycle akin to a surprise offensive action.

Another angle from which this topic may be viewed is that of effect. Effects-Based Operations (EBO) was a joint concept that was primarily sponsored by the US Air Force and proved controversial with Army and Marine Corps commanders. However, it may provide some answers to the question of speed and timing. It was officially (though only temporarily) killed in August 2008 by then commander of JFCOM James Mattis. The debate regarding whether it proved impossible to implement due to the underlying theory being flawed or whether it was the victim of improper implementation continued long afterwards.[207] Though a key detractor of EBO, retired USMC Lieutenant General Paul Van Riper argued that, despite the flaws that he saw with the privileging of strategic air power, the EBO concept was of some value in that it called for attacking systems rather than targets.[208] Effects-Based Approach to Operations (EBAO) lives on in US joint doctrine. It emphasises an understanding that problems are complex and may therefore defy standard solutions; by focusing on the desired effect or intended end-state of operations, EBAO aims to better integrate actions and restore focus on overall strategic goals rather than becoming mired in questions about process or structure.[209] Notably, this focus on

205. Aldrich, *GCHQ*, p. 388.
206. Singer, '"Weaponized Ad Technology"'.
207. John T Correll, 'The Assault on EBO: The Cardinal Sin of Effects-Based Operations Was That It Threatened the Traditional Way of War', *Air Force Magazine*, January 2013, pp. 50–54.
208. *Ibid.*, p. 54.
209. Curtis E Lemay Center, 'The Effects-Based Approach to Operations (EBAO)', last updated 4 November 2016, <https://www.doctrine.af.mil/Portals/61/documents/Annex_3-0/3-0-D06-OPS-EBAO.pdf>, accessed 22 October 2019.

effects and the disrupting of systems is similar to the Chinese systems confrontation doctrine,[210] and can be seen in the way that Chinese domestic social media disinformation is used in short, well-timed bursts at critical points in the calendar.[211] This does not provide a better model of speed and timing, but may contribute to an intellectual framework that avoids the pitfalls that a focus on achieving a faster decision cycle might lead to. It can be done by emphasising how adversaries should be dislocated and disrupted through Information Manoeuvre at critical points in time, and how decisive solutions should be sought over those which are merely incremental or attritional.

Standard decision-making processes (examples include the aforementioned OODA loop and F3EAD, the American BACMIS team-leading method, or the intelligence cycle) can result in *paralysis by analysis* or, worse, *information overload* if they are inappropriately time consuming for the situation at hand. Heuristics and Mission Command are and will remain essential to decision-making even in the Information Age.[212] Recent UK operations have slowed and suffered from coordination issues by improper use of technology to expand staff numbers and introduce additional process, driven by a lack of understanding of what output was needed.[213] Even if decision-making cycles outpace those of adversaries, some situations do not allow tactical decision advantage to be leveraged into broader operational or strategic advantages.

The evidence suggests that these lessons have not been interpreted correctly by Western forces. The Mosul Study Group lamented that US–Iraqi information operations were too slow to keep pace with the changing battlefield during operations against the Islamic State, and insufficiently synchronised to mass effects at the correct time and place.[214] The implication from the study was that if US forces could have extracted more speed and precision from targeting then the overall urban fight would not have been attritional. Yet the Iraqi force, backed up by extensive Western C4ISR capabilities, had a competitive OODA loop and better synchronisation of assets than the Islamic State's forces. The problem was not speed – while timing is more relevant as a causal factor, it is most likely to be that urban warfare is inherently slow and muddled, and requires strategic patience. The 'grinding positional siege that manifested itself as an urban, layered defense against a slow, methodical siege' may have been inevitable regardless of how effective the attackers' information management was,[215] and was a rational choice of ground by the Islamic State when faced with a technologically superior foe. Leonhard argues that weapons need to create the correct cognitive effect, otherwise they should be considered useless. His example is that of physical fires. These are not decisive insofar as their cognitive effect on an adversary is generally to compel the enemy to conceal themselves, adapt, deceive,

210. Engstrom, *Systems Confrontation and System Destruction Warfare,* p. ix.
211. King, Pan and Roberts, 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument', pp. 11–13.
212. Van Horne and Riley, *Left of Bang,* pp. 36–40.
213. Storr, 'Ten Years Observing Command and Control', pp. 28–30.
214. Mosul Study Group, 'What the Battle for Mosul Teaches the Force', No. 17-24, US Army Training and Doctrine Command, September 2017, p. 39.
215. Amos Fox, 'What the Mosul Study Group Missed', Modern War Institute, 22 October 2019.

counteract, move into urban terrain and mingle with the population, changing the political context. Physical fires do not necessarily have the cognitive effect of compelling adversaries to capitulate or accept defeat.[216] The rise of attritional urban battle was the consequence of defenders choosing to impose this fight upon the attacker because urban defence acts as a force multiplier. For the Iraqi government, Mosul was a centre of gravity for the local population that they had to seize. This was a strategic issue, not a pacing issue. That it has been framed as one is unfortunate and incorrect.

Information Manoeuvre needs to refine its concept of speed and timing and incorporate this into how units are trained and operate. While militaries that are unable to respond to stimulus in a timely fashion are likely to perform poorly,[217] being faster than one's opponent is not enough to ensure that decisive effects are delivered. Speed no more confers decisive strategic effects than lethality. It is a vital component of achieving decisive effect but is not one in itself.

Determining and Measuring Effects

Given that the information domain is highly contested, it is worth considering the effects that will be applied to British forces by adversaries. An ongoing task for 6th (UK) Division and the rest of the British Army is countering disinformation. While this falls within the remit of other arms of government, the British Army will be the target of disinformation when deployed, will have the best understanding of its own operations and significant ground-level situational awareness. This underscores the value in having an organic capability to counter disinformation as both a defensive measure and to capitalise on opportunities. Much of the output may be channelled through the 77th Brigade, which holds responsibility for media messaging, but disinformation should be the concern of the entire formation, and the British Army's concept of operations should reflect this.

6th (UK) Division engagement operations and 3rd (UK) Division activity in the 'Constrain' state will be met with disinformation designed to either discredit them or create suspicion in the minds of partners and the population at large.[218] British deployments to Estonia have already faced active attempts to discredit them though means such as staged pub brawls.[219] British forces must have pre-established narratives and lines to take to counter this. Detecting disinformation attempts in advance, as has successfully been done in Estonia,[220] is useful in mitigating against the damage, as counternarratives can prime the audience to reject these attempts.

216. Leonhard, *The Principles of War for the Information Age*, pp. 210–11.
217. Storr, *The Human Face of War*, pp. 37–40.
218. Fox, 'In Pursuit of a General Theory of Proxy Warfare', p. 14.
219. Mark Hookham, 'Troops Face New Enemy – Kremlin's Fake News', *Sunday Times*, 19 March 2017.
220. *Ibid.*

It should be understood that traditional countermeasures to disinformation such as 'the threat of legal action'[221] are limited in their effectiveness due to the nature of modern information warfare techniques that leverage subtle biases, false equivalencies or partial truths.[222] Neglecting the establishment of counternarratives would be unwise, but they should be established with the understanding that they are merely a tactical measure to compete within the information domain and will not necessarily grant decisive advantage. When the UK is caught out and surprised by a new strand of messaging, uncoordinated counter-messaging may be counterproductive. Doing nothing is sometimes a valid response to disinformation.[223]

Successful information operations countering hostile narratives have generally not set out to disprove an opposing narrative, but to convincingly make their own case. For example, consider the disinformation surrounding the use of a nerve agent in Salisbury.[224] Although initially difficult to counter, strong negative messaging tied with extensive and conclusive proof of Russian culpability was effective at shifting public opinion, as reflected in social media activity online. 'Only two of the 10 most viral stories in the weeks following the announcement were sympathetic to Russia'.[225] The Russian claim that their two operatives had been in Salisbury on a sightseeing tour was met with widespread ridicule, with several satirical media outlets and platforms cementing the narrative of Russian dishonesty.[226] The Russian Embassy in London's official statement still blames the British security services for manufacturing the incident and 'whipping up an anti-Russian hysteria for the sake of their internal political interests',[227] but this view has been successfully discredited.[228] Despite the success of the messaging campaign, it should be noted that the GRU operation still constituted a failure of deterrence, and Russia's (implausibly) deniable covert action campaign against enemies of the Russian state continues undeterred.[229] But insofar as the UK's messaging was successful, it sold a convincing alternative narrative and allowed the comparative frailty of Russian explanations to discredit themselves, rather than reacting to Russian disinformation products. The lesson to be learned from this is that in the information domain, defence is derived from credibility, and advantage is won through seeking to apply effects rather than mitigate adversary action.

---

221. Simon Paterson, 'Disinformation: The Threats To Trust Are Changing, Are You?', *Edelman*, 16 April 2019, <https://www.edelman.co.uk/insights/disinformation-threats-trust-are-changing-are-you>, accessed 3 December 2019.
222. *Ibid.*
223. *Ibid.*
224. Tom McTague, 'Britain's Secret War With Russia', *The Atlantic*, 3 December 2019.
225. *Ibid.*
226. *Ibid.*
227. Embassy of Russia in London, '85 Weeks Have Passed Since the Salisbury Incident – No Credible Information or Response from the British Authorities', 6 November 2018, <https://rusemb.org.uk/article/530>, accessed 3 December 2019.
228. McTague, 'Britain's Secret War With Russia'.
229. Bojan Pancevski, 'Germany Expels Russian Diplomats Over Murder of Chechen Rebel', *Wall Street Journal*, 4 December 2019.

The other conceptual element of Information Manoeuvre that must be addressed is that of introducing physical effects to complement messaging in such a way as to create the desired cognitive effect. Much of this is simply down to good situational awareness, which enables the correct use of assets, including physical force. History holds many examples of missteps resulting from a lack of understanding of adversaries or a focus on inappropriate channels for effect. The revelation to rank-and-file members of the Taliban that their leader Mullah Mansour had for two years concealed his predecessor Mullah Omar's death – supposedly to maintain morale – caused a deep rift and dissent within the organisation.[230] This internal division was resolved when Mullah Mansour was killed in an airstrike, restoring a functional degree of unity.[231] Mullah Mansour was also arguably a better prospective counterpart to negotiate with than his hardline replacements.[232] A fixation on targeted strikes against the Taliban's hierarchy and a failure to reflect on what was understood about the Taliban prevented the US from utilising the opportunity created by internal Taliban dissent to either change their course of action or come up with a more creative means of exploiting the situation.

Cognitive effect can revolve around the act of killing and physical violence, but it is important to understand where this activity sits, when it should be used and when it is counterproductive. While killing is seen predominantly as an element of warfighting, it frequently occurs in other operations. Oliver Major argues that the Army Operating Concept's 'Constrain' stage of competition may include localised tactical fighting, a reflection of the fact that the distinction between the 'Constrain' and 'Fight' stages is in practice not a clear one.[233] Killing is not dictated by a predetermined entry into the 'Fight' space outside the Army's remit. The reality is that escalation from 'Constrain' to 'Fight' is dependent upon the crossing of thresholds that are imposed in part politically but may also be dictated by events on the ground. Understanding these thresholds has a degree of practical and tactical relevance. Thresholds are defined as such by actors, not only because of physical or objective criteria.[234] The physical or objective reality of events in a given theatre informs and influences whether actors consider thresholds to have been crossed, but the crossing of thresholds is also informed by strategic understanding of the situation in general, political factors, tolerance for localised violence when balanced against the perceived risks of escalation, and other cognitive factors.

A successful example of the achievement of cognitive effect and enforcement of thresholds through the use of force was the Battle of Khasham on 7 February 2018 in Deir ez-Zor Governorate, Syria. Here, US forces destroyed a combined Syrian government and Wagner

230. David Kilcullen, *Blood Year: The Unravelling of Western Counterterrorism* (Oxford: Oxford University Press, 2016), pp. 182–83; Christopher Dickey, 'Trump, Afghanistan, and "The Tweet of Damocles"', *Daily Beast*, 15 December 2019.
231. *Ibid.*
232. Ashraf Ali, 'Mullah Akhtar Mansour: How the CIA's Hit on Taliban Leader Could Unleash Terror Group Hardliners', *ABC*, 30 May 2016; Fazul Rahim, Mushtaq Yusufzai and F Brinley Bruton, 'Analysis: Why Afghanistan Peace Prospects Look Worse After Mansour's Death', *NBC*, 7 June 2016.
233. Oliver Major, 'The Nature of the Fight in the Army Operating Concept', pp. 1–2.
234. Jack Watling, 'We Need to Relearn How to Do Deterrence', *RUSI Commentary*, 5 December 2019.

Group private military force that crossed the mutually agreed Euphrates River deconfliction line in an aggressive advance against the US-backed Syrian Democratic Forces' positions. For a time, Wagner Group was a leading proxy actor for the Russian government. True mercenary organisations or private military companies (PMCs) are technically illegal under Russian law, but seem to be allowed to operate extra-legally without interference under certain circumstances, related to their utility to the Russian state.[235] There is evidence that the Russian military was aware of the Wagner Group action before and throughout the incident.[236] However, before the battle, the Russian military denied that the PMC was under their control, at which point US forces engaged the force. The battle was entirely one-sided, with as many as several hundred Russians killed.[237] After the incident, the Russian Foreign Ministry firmly denied that the Russian nationals were military servicemen.[238]

The longer-term effect was that Russian forces and their proxies respected the deconfliction line.[239] NATO and Western governments have sometimes been described as having 'a lack of long-term vision to do anything other than de-escalate tensions'.[240] The incident between Wagner Group and the US military provides a useful counter-example to fears that tactical combat will inherently prove escalatory. Rather, by having sufficient situational awareness, the relevant channels for information to adversaries, the right military capabilities, a good understanding of the political context, and possessing the will to initiate tactical combat action in accordance with established thresholds and boundaries, lethal military force can be used discriminatingly and precisely to achieve cognitive effects such as deterrence. The implications of this incident for Information Manoeuvre is that higher echelons must appreciate that a message may be best delivered through the threat or application of physical violence, and that this is not necessarily an escalatory measure.

The relationship between physical and information activity is no less important in calibrating attacks against an adversary's C2 infrastructure. Those who measure the pursuit of competitive advantage by the relative speed of friendly as opposed to hostile OODA loops will be inclined to take any and all opportunities to deny opponents access to decision-making tools, data and C2. Just as kinetic strikes against poorly selected targets can have a counterproductive result, so too forcing an opponent to adopt reversionary communications, or enact mission command without access to higher echelons can result in force a losing access to valuable sources of intelligence, or an adversary not being susceptible to cognitive effects via deception, because they have given their orders and can no longer amend them. Thus, electronic warfare, cyber

235. Neil Hauer, 'The Rise and Fall of a Russian Mercenary Army', *Foreign Policy*, 6 October 2019.
236. Ellen Nakashima, Karen DeYoung and Liz Sly, 'Putin Ally Said to Be in Touch with Kremlin, Assad Before His Mercenaries Attacked US Troops', *Washington Post*, 22 February 2018.
237. Alex Lockie, '"They Beat Our A—es": Russian Mercenaries Talk About Humiliating Defeat by US in Reportedly Leaked Audio', *Business Insider*, 26 February 2018.
238. *TASS*, 'Russians Injured in Recent Clash in Syria Were Not Servicemen — Foreign Ministry', 20 February 2018.
239. Watling, 'We Need to Relearn How to do Deterrence'.
240. McTague, 'Britain's Secret War With Russia'.

activities and network contestation must be comparably calibrated with the benefit of effective situational awareness, creating a demand signal for intelligence collection.

Command and Control of Information Manoeuvre

As has already been established, the accuracy and lethality of modern fires and offensive capabilities have driven adversaries to invest in avoiding detection. Even more so than conventional military deception and concealment, the asymmetric survival strategy of choice has repeatedly been fading into the sociopolitical background.[241] This results in the increasing urbanisation of war. This is not just the case for insurgents and irregular forces; conventional militaries may habitually place themselves in urban areas if facing a more capable adversary in 'an attempt to dislocate [Western military] fires … this is an attempt to use political leverage against our military advantages'.[242]

In light of this, urbanisation trends have implications for Information Manoeuvre. Urban environments now involve multiple domains, with cyberspace and the electromagnetic spectrum featuring heavily. Civilian communications infrastructure, networks and nodes in these domains are clustered in the urban space, and if civilian infrastructure cannot be leveraged then military forces face the challenge of overcoming the disruption inherent in tall buildings and electromagnetic congestion interfering with military C4ISR networks.[243] Satellite observation and the denial thereof renders the space domain directly relevant to and interlinked with urban environments, and the air domain is directly overhead.[244] This will not mean that large numbers of light infantry are required; mechanised and combined arms forces have significant advantages over light ones for urban operations. The light infantry urban fight requires mobile protected firepower to be effective.[245] A high level of network integration is therefore essential to connecting these different types of forces, their sensors and capabilities, often between different partners providing different elements of the force. This was done successfully in Mosul, where secure American and insecure Iraqi C4ISR systems were incorporated into the same overall network during the battle down to the company level.[246]

Given that the world's major global powers are effectively committed to a cyber and electronic warfare arms race, C4ISR networks must be built to have resilient characteristics. UK forces must ensure that they can communicate when coordination is integral to operations, and transfer information securely across the force.[247] According to joint doctrine, resilient systems may

241. Leonhard, *The Principles of War for the Information Age*, p. 20.
242. *Ibid.*
243. Jeremiah Rozman, *ILW Spotlight 19-3: Urbanization and Megacities: Implications for the US Army* (Arlington, VA: AUSA, 2019), pp. 3–4.
244. Watling and Roper, *European Allies in US Multi-Domain Operations*, p. 14.
245. Leonhard, *The Principles of War for the Information Age*, p. 20.
246. Mosul Study Group, 'What the Battle for Mosul Teaches the Force', p. 53.
247. Leonhard, *The Principles of War for the Information Age,* pp. 226–39.

disincentivise offensive EMS activity against them,[248] but this is unlikely, and adversaries have invested in and are likely to employ capabilities such as layered wide-area jamming, targeting everything from GPS and radio frequencies to civilian cell networks.[249] In addition to hardening systems, building redundancy and alternative channels and means of utilising and moving information can enable operations to continue in the face of adversary efforts to disrupt or degrade British C4ISR.[250]

Addressing the complexity of the environment and the concurrent level of threat is an area in which technological advances may soon bear fruit. The DoD, by its own admission, lacks a common operating picture for the EMS, but the US Army's Electronic Warfare Planning and Management Tool (EWPMT) aspires to provide a comprehensive system of EMS battle management and is perhaps the best system currently available to the DoD to analyse the EMS in its entirety.[251] The last of the four batches or 'capability drops' of EWPMT are not projected to be delivered until 2021,[252] but these promising capabilities should be explored by 6th (UK) Division, with the understanding that they will not solve the issue of complexity but merely provide a coping mechanism to prevent overload and paralysis. A well-educated and well-trained human component of the force will still be the essential factor determining whether deployed forces can function effectively.

Intelligence support from strategic assets was successfully pushed down to front-line operational units in Iraq, something that has historically been done poorly by the British military and intelligence agencies.[253] Given the impact of political or adversary action on the permissiveness of the urban space, this strategic support will continue to be useful, as the information that they may detect will help contextualise the ground-level tactical intelligence that the force routinely absorbs. Evidence of the importance of 6th (UK) Division's deployed signals units having channels established with both higher military echelons and civilian intelligence agencies can also be found in the Falklands War:

> The most important lesson – soon forgotten, of course – was that local army sigint units often found they were collecting strategic sigint that related to high policy, while strategic sigint collectors using national resources found they were often collecting tactical sigint of more use to those in the front line. The systems were not well designed to move this material in a sophisticated way to the right customers.[254]

248. MoD, Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18', pp. 10–11.
249. Jack Watling and Justin Bronk, 'Strike: From Concept to Force', *RUSI Occasional Papers* (June 2019), p. 29.
250. MoD, Development, Concepts and Doctrine Centre, 'Joint Concept Note 2/18', pp. 10–11.
251. Mark Pomerleau, 'What to Do with an Electronic Warfare Problem Like Syria?', *C4ISRNET*, 29 October 2019, <https://www.c4isrnet.com/electronic-warfare/2019/10/29/what-to-do-with-an-electronic-warfare-problem-like-syria/>, accessed 31 October 2019.
252. *Ibid.*
253. Aldrich, *GCHQ*, pp. 525–26.
254. *Ibid.*, p. 413.

Assuring communications within an operational theatre should be supplemented by maintaining interdepartmental channels for information so that opportunistically gathered information, if of strategic relevance, can be redirected to the relevant destination.

Leonhard sees the urban space as advantageous to Western forces, giving them access to the population and to infrastructure to support the military,[255] though this would be on the condition that they can successfully integrate themselves. This raises the importance of the capability to plug military C4ISR networks not only into partner forces but also into civilian networks. Moving information across the force is critical, and is constrained by bandwidth and speed.[256] Persistent engagement in the information space, plugging into partner networks and maximising the ability to meaningfully interact with the population to ensure that the urban space works *for* rather than *against* the force will all be critical.

The issue of integration into civilian networks will require an acceptance of some level of risk to network security. Within the US Army Signals Corps '[t]here is a running joke … that it is acceptable to fail missions but not a CCORI [Command Cyber Operational Readiness Inspection] (the networks must comply with security standards, but that does not mean that the networks need to work)'.[257] The joke highlights that some elements within the US Army suffer from a longstanding problem in cyber security, that of putting 'the information assurance cart before the mission assurance horse'.[258] Similar issues have been recognised by Ivan Jones, who instructed his division to become less process-driven, and less metrics-driven in the planning process, a cultural change intended to allow a commander to focus on the enemy commander, not on his validators.[259] Yet the signals elements of 6th (UK) Division will be faced by increasing challenges of this kind due to the nature of persistent engagement operations and the inherent requirement to integrate military communications systems with outside networks, both of partners and with the Internet at large. Different digital infrastructures create difficulties when partners and allies need to operate together. Convincing them to integrate is also challenging; one partner's system vulnerabilities may be seen as a vector for threats to the other, and there are also concerns regarding losing control of one's data and of becoming over-dependent.[260] The conflicting imperatives between information assurance and mission assurance will become exacerbated, not lessened, and a culture that is not accountable for mission failures or successes, and is primarily judged on whether processes are adhered to, would compromise the division's effectiveness. 6th (UK) Division requires a permissions and incentives structure that places the mission first.

255. Leonhard, *The Principles of War for the Information Age*, p. 20.
256. *Ibid*.
257. James Torrence and Joseph Pishock, 'The Army Signal Corps Must Change its Culture', *Small Wars Journal*, 6 November 2018.
258. Martin C Libicki, 'Cyberspace Is Not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society* (Vol. 8, No. 2, 2012), p. 330.
259. Jones, 'CFA Intent'.
260. Watling and Roper, 'European Allies in US Multi-Domain Operations', p. 16.

Putting the mission first emphasises the fact that effective C2 for Information Manoeuvre is ultimately about people and their training, before it is about systems. More comprehensive work is being done by Defence Science and Technology Laboratory (Dstl) on improving C2 resilience by the adoption of a less technology-centric model. A critique of the current C2 system is that it lacks survivability and redundancy, with only the primary method of communication being routinely trained and tested. The imperatives that have led to this state of affairs and the complexity of contemporary military communications systems mean that to use them effectively, personnel and signals operators must specialise in their operation, leaving little capacity to develop, train and test alternative means. This is exacerbated by training exercises that draw in multiple participating units. The benefits of practising interoperation have an unfortunate side effect, which is that if the communication system fails then the exercise may be seen as a waste of time for other participants. Combined with an approach to training that still involves a large degree of validation against the functioning of primary processes, this results in the British Army all too often ceding the opportunity to train and test units on their ability to operate without their primary communications. This is efficient, but it leaves the British Army vulnerable to paralysis if its communications are disrupted,[261] or perhaps of even greater concern, allows the Army to be shaped by adversary electronic warfare capabilities into adopting their reversionary communications procedures and so adopting a predictable tempo of operations.

The proposed alternative is a model with multiple channels of communication that can be adjusted to bypass blockages and alter emissions control states while retaining effectiveness. This is less a technological solution, as while different communications systems will need to be integrated, the model is also reliant on changes to the planning cycle, means of issuing orders and concept of operations, and the continuing implementation of Mission Command.[262] Ideas about building resilient, decentralised and adaptable networks are not new,[263] but require cultural change and investment. This has additional utility in that, unlike other models for operational information warfare, it has the potential to avoid the issue of creating vulnerability through centralisation.

Technology should not be used as a replacement for properly training and investing in personnel.[264] Throughout the 20th century, 'poor discipline by the human operators often proved to be the great weakness in otherwise impregnable cypher systems'.[265] Furthermore, even the most exquisite systems will have vulnerabilities or may be degraded or denied. Nevertheless, rather than having an exquisite primary system of C2 and then relying on personnel to improvise, adapt and overcome when it ceases to function correctly, technology and systems should be designed

261. Author interview with senior Defence Science and Technology Laboratory (Dstl) officials, London, October 2019. The C2 Resilience model documentation cannot be released at the time of writing as it is in draft.
262. *Ibid.*
263. Leonhard, *The Principles of War for the Information Age*, pp. 226–39.
264. McFate, *Goliath*, pp. 55–56.
265. Aldrich, *GCHQ*, p. 15.

to bridge the gap between normal and abnormal states of operation, providing the means of maintaining C2 in a graduated way without resorting to entirely decentralised initiative.[266]

If it is accepted that the information domain is contested, then absolute network assurance cannot be guaranteed or expected. It is unreasonable and unrealistic for commanders to treat access to communications as an isolated signals responsibility. Given the volume of data moved around a modern force, the number of networks involved, and the active physical and virtual contestation of those networks by adversaries, systems will be compromised or denied. Commanders therefore must be prepared to articulate what data they must access, when and where. Which connections are vital, which are merely advantageous and which can be put aside during different phases of an operation? On which channels and links is a commander prepared to accept risk? And if a commander does require a specific link to higher echelons, or across an urban space, to what extent are they prepared to adapt their scheme of ground manoeuvre to assure the physical infrastructure upon which those communication links depend? In a contested information domain, C2 demands that officers be prepared to fight for information, and therefore to ruthlessly prioritise what information matters. This underscores once again that though the information domain is highly technical, like all domains of warfare, it is first and foremost human, and technical systems depend upon well-trained and coordinated human operators.

266. Author interview with senior Dstl officials, London, October 2019. The C2 Resilience model documentation cannot be released at the time of writing as it is in draft.

Conclusion

THE GOAL OF Information Manoeuvre is to deliver or assist in the delivery of the correct cognitive effect, which will be achieved through ensuring that physical and virtual means are utilised in concert. Understanding the best way to do this will require a clear understanding of the future operating environment. Urbanised and digitally connected with increasing density, the future battlefield will produce a torrential volume of raw data, and with adversaries and enemies embedded within layers of physical and virtual civilian infrastructure, identification, targeting and rules of engagement will all prove to be difficult.

The challenges of scale, limited resources and adversaries who are both capable and determined to contest this space make the delivery of decisive cognitive effect a challenge. Therefore, it must be determined very clearly at the political level what the UK government wishes to achieve, what the intended cognitive effect on other actors is, and where and when the British Army has the capability to apply the relevant actions to achieve or contribute to the achievement of these effects and outcomes, thus avoiding the misapplication of resources and ensuring a unity of effort. This must include an understanding of the appropriate metrics by which to judge success, and what thresholds and red lines the UK government wishes to impose, so that these can be messaged as such and the correct force posture adopted by the relevant components of the British Army and joint force. Likewise, the British Army must learn to work better outside of the purely military space in order to work well within the information domain. This is necessary for, and will facilitate, the British Army becoming more comfortable with blending non-kinetic capabilities and effects with the well-developed kinetic capabilities and effects that it can already bring to bear.

Within the digital information domain in particular, AI and ML are technologies that will determine the exact shape of the future operating environment. Despite their potential as capabilities to process the vast quantities of data that modern society and human activity now habitually produce, their apparent trajectory indicates that there will be a greater data volume than can be processed. Therefore, selectiveness and qualitative analysis, far from being marginalised, will be more important than ever. If some processing or analytical tasks are handed off to AI and ML, there is a requirement for a high level of trust that can only be built by a widespread understanding by personnel at all echelons of how the architecture of the AI and ML supporting them works. AI and ML will create new dynamics and systems, and as with all dynamics and systems these will be gameable; blind adoption of AI and ML would confer no advantage. The main task associated with bringing these new technologies into the force is about preparing the humans who will be supported by it and getting qualitative issues right. AI and ML, if understood, can be integrated properly without building in weaknesses, and once trusted can transform how a force operates, so as to create efficiencies rather than additional human structures to manage and oversee it.

To keep pace with the current threat environment, the British Army's C2 structures must continue to be modernised. The current tendency to prioritise the maximising of the efficiency of primary C2 networks at the expense of building and developing resilient networks is an organisational propensity that must be changed. While from one perspective this is a technical niche, it will have broad implications for the wider force. Whether the British Army successfully develops better C2 operating practices that can assure that sufficient information can be transmitted for it to operate effectively even when faced with a contested EMS could make or break the British Army's ability to accomplish its mission in the future. It should be understood that the network technology to accomplish this likely already exists; adapting the way that the force trains may determine whether this goal is accomplished.

The network technology that underpins C2 has another set of requirements: these networks must be capable of being plugged into the wider Internet and other networks, of pushing and drawing information from across different echelons, and be accompanied by a data-management solution that eliminates the stovepipes that the force currently endures. The need to work with Five Eyes and NATO as well as with less capable partners presents at best a diverse range of tasks and at worst conflicting imperatives with regard to how the British Army approaches interoperability. Versatile networks constructed with an understanding of this challenge can mitigate against these issues and contradictions, but a bad network solution will amplify them. If procurement simply obtains another incrementally improved military network along the same design approach as previous iterations, the stovepipes and inefficiencies will provide neither the interoperability with other allies and partners nor the capability to engage with the wider information domain that is necessary to make Information Manoeuvre work. Without an appropriate solution, the architecture and content of the future operating environment will present an insurmountable challenge due to the burdens of volume and the requirement for human mediation, whereas it could and should be infrastructure and information that can assist and be utilised by the force.

While improved C2 networks, data management, and AI and ML are important, they are enabling capabilities. They must support digital and physical persistent engagement, which are required in order to provide the situational awareness upon which qualitative assessments as to what data matters must be based. To counter effective adversary and enemy influence and disinformation activity, permissions need to be devolved, otherwise the British Army will be hopelessly slow, and will struggle to shape the information space proactively. The British Army's influence operations are too centralised. While some centralised command and oversight is necessary to ensure coordination and protect against some risks, overemphasis has pushed too many decisions about influence, particularly through messaging, up to a high level where most individual initiatives are trivial and will either be actioned too late or not at all. At scale, this dynamic cedes the information space to adversaries. If the British Army is to not be reactive to adversary and enemy influence activity, and is to be truly competitive in shaping narratives, this is a requisite change.

As persistent effects are difficult to achieve in the digital information space, relationships with partners and allies are critical. As with digital influence operations, physical persistent

engagement requires devolved permissions, in particular the permissions to accompany and build deeper, longer-standing relationships. Without accepting the risks inherent to deploying small teams in a dispersed manner with relatively little support, it will be impossible to achieve persistent engagement through presence. Despite all of the aforementioned issues surrounding the digital information domain, such as processing and volume, humans are still the producers of that information and are still the primary targets. Therefore, human relationships are still key, and the British Army still needs to develop them. For all the importance of standoff capabilities such as computing power, technical networks and algorithms, these cannot be relied on as they are not a substitute for face-to-face relationships and interaction.

Without the right persistent engagement mechanisms, networks and relationships, it will be impossible to collect the right information, or, if it is collected, to identify it as such. If the wrong information is collected, or the wrong conclusions drawn, this intelligence failure will mean that it will be impossible to formulate an informed and coherent strategy. Relationships will be built with the wrong people, and kinetic effects will be applied inappropriately, killing people who should not have been killed. This will alienate the very audiences that the force intended to influence, turning permissive environments into hostile ones, and undermining the UK's reputation, legitimacy and strategic goals. Information Manoeuvre and the Manoeuvrist Approach are intended to facilitate a better outcome; all the factors outlined should be understood as contributing to the synchronisation of relationships, influence and messaging with physical and kinetic actions, rather than replacing the physical and kinetic, to achieve the desired effect – the destruction of the adversary's willingness to fight.

About the Author

Nick Reynolds is the Research Analyst for Land Warfare at RUSI. His research interests include land power, wargaming and simulation. Prior to joining RUSI he worked for Constellis. He holds a BA in War Studies and an MA in Conflict, Security & Development from King's College London. During his time at KCL, he was Head of Operations of the KCL Crisis Team, which organises large-scale crisis simulation events.