Royal United Services Institute
for Defence and Security Studies

Occasional Paper

The Future Conflict Operating Environment Out to 2030

Peter Roberts (Editor)

The Future Conflict Operating Environment Out to 2030

Peter Roberts (Editor)

RUSI Occasional Paper, June 2019

Royal United Services Institute
for Defence and Security Studies

188 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 188 years.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, June 2019. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

Printed in the UK by Stephen Austin and Sons, Ltd

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

Introduction

Peter Roberts

> Perhaps wars weren't won anymore. Maybe they went on forever.[1]

> War used to be easy to define. Once, we could say with confidence whether we were at war or peace. If the former, we could identify with whom we were fighting and where the front was. Americans in particular have for a long time had the good fortune of being able to say that the war—any war—was 'over there'.[2]

THIS COLLECTION OF essays is about contemporary trends in war and warfare,[3] and how they will shape the actions of belligerents in future conflicts. Its conclusions have implications for the force design of Western militaries and signposts the adaptations that will need to be undertaken to meet the challenges of the next decade. Its research seeks to stimulate a conversation about the overly restrictive ways in which Western thinkers consider competition, conflict and combat to broaden the discussion beyond an orthodoxy of military interventions in which combat is something bound by laws, behaviours, conventions, ethics, morals, values, and geography. Its deductions naturally lead to a further research question that examines what an adequate Western response might be.

The traditional taxonomy can be confusing. Historical terms such as 'limited war' have connotations that lead some to infer direct linkage to counterterrorism, counterinsurgency, or stabilisation operations; things once captured under 'Operations Other Than War'. The legacy of post-Cold War thinking leaves limited war as a category of 'wars of choice' rather than existential conflict. But this does not expose its real limits: either the self-imposed restraint or limited means states deploy. As Lawrence Freedman usefully highlights, '[O]ne reason why limited war can be a difficult strategic category is that it is used to refer to conflicts where enough is at stake to demand engagement but not so much as to require total commitment'.[4] Yet in many ways the activities described in this paper are 'limited'. Not in how they are undertaken (small interventions can often be as 'high intensity' as total war to the actors involved), but in the objectives they seek to deliver, whether political, geographic, military resource, or resource based. This distinction is important to understand, but because of issues surrounding Western military taxonomy, the term 'limited war' is not used.

---

1. Ernest Hemingway, *A Farewell to Arms* (New York, NY: Scribner, 1929), p. 118.
2. Zachery Tyson Brown, 'Unmasking War's Changing Character', Modern War Institute, 12 March 2019.
3. War, used in its broadest sense in this paper, being the activity undertaken by states against each other; warfare being the military actions undertaken as part of combat, deterrence, coercion, and suasion between actors.
4. Lawrence Freedman, *Ukraine and the Art of Strategy* (Oxford: Oxford University Press, 2019), p. 35.

Within this paper, authors use the term 'school' or 'way of war'. This applies to the way in which states understand conflict and expect to fight. It is not simply a military theory: it is the fusion of politics, history, foreign and security policy, and culture. As such it usually has a very distinct national identity. However, this paper assumes a Western way (or school) of war.

While the West has historically encompassed different ways of war, since 1945 these schools have merged with US concepts. In Europe, there have been four distinct 'schools of war': French, British, Prussian/German and Russian. None of these have been constant, and whilst there are similarities between them, each differs significantly – from their understanding of the 'principles of war' through to command and control.[5] But since 1945, these individual schools of thought have gradually merged with the American into a single Western way of war – in which wars are expeditionary in nature, with a definite start and end, and are planned and orchestrated using 'ways, means and ends' processes. Increasingly, this school of thinking about conflict has become based on technological determinism (in which technological superiority assures victory) and has demanded ever-greater cross-government involvement to minimise or mitigate the lack of mass and scale of the military instrument. Notably, Russia, China, Iran and North Korea have each retained or indeed developed their own school of military thought.[6]

Western schools of military theory are arguably developing more slowly than ever before. The divergence of thinking demonstrated by key states in leading state doctrines of Multi-Domain Operations (for the US), Strategic Autonomy (for the French), Modernising Defence Programme (for the UK), or indeed the absence of will to provide a coherent NATO-wide concept of operations (for the Alliance) has not helped to establish clear, intellectually led thinking. Instead, it is the non-Western concepts of war and warfare that provide the greatest insights into the future. These schools have driven the greatest evolution in military concepts for over 50 years; they need to be understood in some detail.[7]

Scope and Structure

The paper does not deal with total-war scenarios in which the weapons used (including strategic nuclear weapons), territorial scope, combatants involved, or the objectives pursued, are unrestricted – although the activities examined here may be a precursor to such scenarios, and this paper touches on the use of tactical nuclear weapons as an intrinsic element of escalation dominance by some states. Neither does this paper classify today's character of war as simply a matter of speed ('hyper war') or the blending of older tactics with new technology ('hybrid', 'non-linear', 'fourth-generation', 'next-generation', or even 'contactless' war). For example, in many ways, hybrid warfare is neither new nor a particularly useful observation; even the

5. Jan Armstrong and J J Wigen, *Contemporary Military Theory* (London: Routledge, 2014).
6. Peter Roberts, 'Designing Conceptual Failure in War: The Misguided Path of the West', *RUSI Journal* (Vol. 162, No. 1, 2017), pp. 14–23.
7. The paper does not take into account the Israeli school of war within the research presented here. The Israeli school is indeed significant but has had no impact on the broader Western concepts of war and warfare.

originator of the concept, Frank Hoffman, has backed off the idea. Much of the discussion over 'hybrid' confuses unfamiliarity for novelty: the Viet Cong was a hybrid force according to modern definitions, as were the Boers and LTTE (Tamil Tigers). There are many other examples, yet none of these poses a conceptual problem for us today.

The distraction of fashionable terminology is not a uniquely Western problem. Potential Western adversaries are also using their own terms: 'Trojan horses' and 'fifth-column strategies' have been highlighted by Russian military leaders, as have 'local wars under high-tech conditions' by Chinese leaders. Yet none encompass the highly differentiated nature of war across actors and regions, often relating to their own diverse context and history.

A standard presumption is that preparing for future conflict is a core role of government. The effectiveness of these preparations determines how states are perceived by others, underpinning perceptions about a state's hard, soft, smart and sharp power, including whether a state is seen as a 'safe' place to do business. In many ways, perceptions about the security environment shape trade patterns and impact the prosperity and success of societies.

Designing military forces for the future plays a key role: defence procurement has economic implications, but also underlines the security posture of states. Military force designs therefore require an idea of what equipment is for and what a future conflict may look like – in military parlance, the Future Operating Environment. There have been many documents produced by Western governments, militaries and academics on the future of war and warfare.[8] Many of these have been criticised for not acknowledging the role of other belligerents, being prone to technological determinism and fads, or intellectually lazy.

Whilst there are a variety of methodologies for examining the future of war and warfare, this paper adopts an enemy-centric prism. It acknowledges that the future tends to be a mutated version of the present, and that to understand future conflict one must understand those of the past and the present. As such, this paper takes a baseline of contemporary conflict and key trends and extrapolates from these. The paper goes beyond other similar exercises by incorporating not only a Western perspective, but also interpreting and analysing the activities of competitors and potential enemies.

The paper is not intended to be comprehensive. Given the need for brevity, authors focus on the most relevant factors and evidence across a selection of conflicts and trends. Authors examined the evidence from a five-year period, selecting the key factors and themes during a discussion with leading defence thinkers from around the world. Research included discussions with over

8. See, for example, Australian Ministry of Defence, 'Future Operating Environment 2035', draft document, November 2016, <https://www.cove.org.au/wp-content/uploads/2017/03/Future-Operating-Environment-2035.pdf>, accessed 4 January 2019; UK Ministry of Defence, 'Future Operating Environment 2035', December 2015. There are also non-governmental documents, see, for example, Kimberly Amerson and Spencer B Meredith III, 'The Future Operating Environment 2050: Chaos, Complexity and Competition', *Small Wars Journal*, July 2016.

8,500 political and military figures, at every level, from more than 85 states, and a variety of research trips. The key conflicts examined therefore stem from activities by Russia, China, Iran, and North Korea; the future of terrorism is also included. The paper does not predict that these states will be key belligerents in future. Rather, the way they undertake coercion and warfare is a useful indicator of how other states may aspire to act. As such, an important view held by all authors of this paper is that conceptualising their activities is more important than the platforms they use to undertake them.

While this paper is partly speculative, it is grounded in the reality of policy, properly evidenced, and based on a realistic research question: it is not an excuse to keep admiring the problems around future conflict. Given the need for plausibility and utility, the paper keeps its deductions to the period up to 2030. While it is tempting to state that shorter timeframes lead to more accurate forecasting that longer ones, this is not necessarily true or helpful. Many predictions fail to materialise or are warnings that are not heeded.[9] No Western government foresaw the resurgence of Russia before 2014; after 2014, many Western intelligence agencies predicted that Moscow could not afford to maintain such an aggressive foreign policy stance for more than five years. Similarly, many believed that China's rise would be accompanied by a peaceful and controlled transition from authoritarianism to democracy.

Limiting the timeframe for examination to a decade does, however, allow the paper to discount some of the more unlikely economic and technological trends. It discounts the rise of an unlikely new global military or economic superpower. Technological singularity is deemed unlikely,[10] as is the arrival of strong artificial intelligence.[11] Human biological enhancements, symbiotic neural systems, and transmorsive adaptation[12] are all beyond a 10-year horizon. Instead, the analysis in this paper considers the trends that might shape force design, and the way in which militaries conceive combat, conflict and warfare.

The paper is in four parts. First, it examines the contemporary schools of war: threshold warfare (Russia); proxy warfare (Iran); coercion and economic warfare (China); brinkmanship (North Korea); and terrorism. Second, it examines key influential trends: domestic pressures; societal changes; precision and space; the electro-magnetic spectrum; proliferation of unmanned systems; and technological change. Third, the paper characterises the Western way of war. The conclusion makes deductions from the work as a whole. These essays are not exhaustive conclusions, and the authors acknowledge what has not been considered, including: chemical and biological weapons; ballistic missile defence; urban warfare; and high-intensity near-peer or peer-on-peer combat. Other studies have already covered this ground. While additional sections were considered, extending the scope of the analysis risked distracting from an examination of enemy-centric culture and concepts of war.

9. Laurence Freedman, *The Future of War: A History* (London: Allen Lane, 2017).
10. Anthony Berglas, *When Computers Can Think: The Artificial Intelligence Singularity* (Scotts Valley, CA: CreateSpace, 2015).
11. Peter Roberts, 'Lethal Artificial Intelligence and Autonomy', RUSI Conference Report, December 2018.
12. The ability to shape shift objects and appearance.

Section 1

CONTEMPORARY SCHOOLS OF WAR

Back to the Future? Thresholds, Hybridity and Tolerance Warfare in Russia's Concept of Limited War

Ewan Lawson

IN THE FIRST decades of the 21st century, the West has struggled to cope with a return to complex inter-state competition which does not fit into a simple peace–war dichotomy. Against a background of peerless Western military power after the 1991 liberation of Kuwait, and the military instrument having become the lever of choice for Western governments, the campaigns in Iraq and Afghanistan have sown doubt in the minds of the public and politicians. At the same time, potential adversaries have recognised that one way to counter Western military strength is to ensure that it is not used – as shown by the Obama administration's failure to deter Syrian use of chemical weapons, by Russia's actions in Georgia and Ukraine, and by China's occupation of islands in the South China Sea.

Academics and commentators have come up with a range of labels for this phenomenon, including 'hybrid', 'grey-zone', and even 'tolerance' warfare.[13] This chapter considers the emergence of the phenomenon and its implications for the future operating environment, with a particular focus on the significance of thresholds. It first reviews the problem of taxonomy to provide a simple explanatory framework – recognising that not all will agree. It then focuses on Russian operations in Ukraine, before concluding with potential responses.

Before considering how to address the problem, it is necessary to be clear on what it is. While the concept of hybrid warfare has become vogue in the aftermath of the Russian occupation of Crimea, its potential was identified nearly a decade before those events. Writing in 2006, Frank Hoffman notes how potential adversaries were likely to combine non-conventional forms of warfare – from irregular warfare to terrorism, in sequence or simultaneously – to target the vulnerabilities of those militaries.[14] He cites the success of Hizbullah against Israel in the 2006 Lebanon War as an example; a style of war that was to be repeated in Iraq and Afghanistan.[15]

13. 'Tolerance' warfare was introduced in International Institute for Strategic Studies, *Strategic Survey 2018: The Annual Assessment of Geopolitics* (London: Taylor and Francis, 2018).
14. Frank G Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute, 2007), p. 7.
15. *Ibid.*, p. 8.

In Hoffman's logic, hybrid warfare is the use of a range of techniques to exploit an adversary's vulnerabilities. Where state actors have adopted this approach, it is at least in part to exploit the perceived vulnerability of a democratic opponent that generally requires political approval to employ a military response to a problem. The Information Age, and in particular widespread connectivity and social media, has allowed Western adversaries to use disinformation and obfuscation to subvert political processes,[16] reflecting a desire to ensure the response stays below the threshold of a military response. This has given rise to the concept of threshold warfare.

A RAND report from 2016 emphasises that the various hybrid means are not new in themselves, but they are specifically designed to avoid eliciting a full-scale, conventional military response.[17] Indeed, the study notes how Western governments have themselves made use of such hybrid means, including propaganda and proxies.

Thresholds take a variety of forms and can be defined in one sense as 'a negotiated, declared, or tacitly understood delimiter between measures short of war and high-order conflict (such as full-scale conventional or nuclear war)'.[18] This definition focuses on high-order conflict and thresholds such of NATO Articles 5 and 6, but it can be equally be applied at lower levels of military response, such as the US so-called 'red line' on Syrian chemical weapons use in 2013. There is something of a feedback loop here, as it can be argued that nuclear weapons currently represent the ultimate threshold: states seek to acquire them both to deter adversaries from aggressive action, but also to provide the space under which they can conduct hostile activities of their own. From this, the concept of grey-zone conflict is simply the identification of those activities that take place below the level of a defined or perceived threshold. So far, so conceptual – but what does this mean in practice?

While threshold warfare has been practised by a number of states, the activities of Russia in Crimea and Eastern Ukraine provide an interesting case study of contemporary application, providing a grounding to consider the future operating environment. However, it is important to recognise that the current approach has its roots in earlier Soviet-era thinking about revolutionary warfare. In the 1920s, efforts to take control of countries such as Estonia and Georgia included a combination of supporting proxies, propaganda and subversion that was later reflected elsewhere in inter-war Eastern and Central Europe, and indeed resonates today.[19] These practices were built on the idea of reflexive control – 'a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the

16. Patryk Babaracki, 'Putin's Postmodern War with the West', *Wilson Quarterly* (Winter 2018).
17. Ben Connable, Dan Madden and Jason H Campbell, *Stretching and Exploiting Thresholds for High-Order War: How Russia, China, and Iran are Eroding American Influence Using Time-Tested Measures Short of War* (Santa Monica, CA: RAND Corporation, May 2016), p. viii.
18. *Ibid.*, p. ix.
19. Toomas Hiio, 'An Attempted Communist Coup D'Etat on 1 December 1924', *Estonica.org*, 28 September 2012.

predetermined decision desired by the initiator of the action'.[20] It aims to ensure that Russian actions are not perceived as crossing a given threshold. The intent is to use obfuscation and disinformation to sow doubt in the minds of key decision-makers. As well as conventional military and diplomatic activity, Russia continues to employ 'active measures' which include political influence operations, control or influence of traditional media, blackmail and increasingly the use of social media and cyber operations to achieve its aims.[21]

Post-Soviet Russia has kept an interest in maintaining influence and control in its so-called 'near abroad', including Ukraine. It is not the purpose of this chapter to discuss the conflicts in Crimea and Eastern Ukraine in detail, but rather to see how they might fit the concept of threshold warfare. The first thing to note is that it was always unclear what the threshold for a Western military response might be. Ukraine was not a member of NATO, and therefore Article 5 could not be invoked. However, the Kremlin was sufficiently concerned about the Western response that from the outset it employed tactics and techniques to allow for a degree of plausible deniability, most notably the use of troops without identification (the so-called 'little green men'). In Eastern Ukraine this was developed further. Not only did Russia encourage the formation of local militias as proxies in the early stages of the conflict, it also enabled Russian volunteers and mercenaries to support.

It can be argued that the threshold Russia is trying to avoid lies between civil and inter-state war. While many civil wars involve foreign actors, Russia seeks to avoid being recognised as a party to an inter-state conflict, instead aiming to be seen as a key arbitrator of the peace process.[22] However, alongside its military contribution the Russian effort has used a broad range of tools to both blur its own involvement and undermine the Ukrainian authorities. At the forefront has been an information campaign, supported by offensive cyber activities, that has portrayed the Ukrainian electoral process as corrupt or illegal. This campaign has been targeted beyond Ukraine to potential supporters through the use of troll farms, which seek to cast doubt on the validity of claims of Russian involvement either through efforts to undermine the material or the source. The archetype of this may have been the effort to deny Russian involvement in the shooting down of Malaysian Airlines flight MH17.

Key to an effective campaign staying below the threshold is to target the non-military and the military vulnerabilities of the opponent. In the case of Ukraine, this includes its electrical grid, which is heavily reliant on Russian gas. The Kremlin has been willing to use nominally private enterprises such as Gazprom.[23] Further, it has sought to psychologically exploit this vulnerability through a series of cyber attacks on the electrical distribution system in Kiev. The

20. Timothy L Thomas, 'Russia's Reflexive Control Theory and the Military', *Journal of Slavic Military Studies* (Vol. 17), p. 237.
21. US Department of State Bureau of Public Affairs, 'Soviet "Active Measures": Forgery, Disinformation, Political Operations', Special Report No. 88, October 1981.
22. Taras Kuzio and Paul D'Anieri, 'Annexation and Hybrid Warfare in Crimea and Eastern Ukraine', *E-International Relations*, 25 June 2018.
23. Multinational Capability Development Campaign, 'Understanding Hybrid Warfare', January 2017.

interconnectivity and anonymity provided by the digital age facilitates hybrid methods in the grey zone below the threshold. It is reasonable to conclude that while Western military power still has the potential to be decisive in a conflict, further consolidation of the Information Age will keep this approach an attractive option for potential adversaries.

Although the military plays a significant role, countering threshold warfare uses all levers of national power. This is being increasingly recognised in the West, with the UK developing the Fusion Doctrine and the US developing the Joint Concept for Integrated Campaigning.[24] These efforts at integration are slowly starting to gain traction, although the systems of government in both the UK and the US make this challenging – as shown by the UK's own evolution from the Comprehensive Approach in 2004, through the Integrated Approach and then the Full Spectrum Approach, before arriving at the Fusion Doctrine in 2018. Arguably there are lessons to be learned from some smaller states who recognised the challenge earlier: not only in the Nordic and Baltic states, but also in, for example, Singapore through models of Total Defence.[25] The key military decisions will therefore be identifying the defence contribution to countering threshold warfare. While this will inevitably include traditional warfighting capabilities, the deployment of military assets in support of the civilian authorities outside warfighting may well become increasingly important.

Other chapters in this paper consider hybrid and grey-zone warfare. But they are arguably fundamentally sub-categories of adversary efforts to stay below the threshold of Western military response. The apparent success of these efforts – at least as measured by Russia's de facto annexation of Crimea and the failure to formally recognise it as a participant in the conflict in Eastern Ukraine – would suggest that it is likely to be the modus operandi of the West's adversaries for the foreseeable future. This should frame both defence policy and capability decisions. This process could draw much the experience of others, particularly those who have adopted models of Total Defence.

24. HM Government, 'UK National Security Capability Review', March 2018; US Joint Chiefs of Staff, 'Joint Concept for Integrated Campaigning, 16 March 2018.
25. Singapore Ministry of Defence, 'The 5 Pillars of Total Defence', <https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/about_us/5_Pillars.html>, accessed 1 May 2019.

Proxy Warfare: Iran

Jack Watling

THE US CAMPAIGNED in Iraq for more than 10 years, while operations in Afghanistan have continued for 18 years. Yet despite a considerable force commitment, at vast expense,[26] it is Iran that wields the greatest leverage in Baghdad today, while US attempts to prevent Pakistan's interference in Afghanistan have been an unequivocal failure. In the face of the global superpower, both Iran and Pakistan have asserted their interests by force at minimal expense by means of proxies. The US also employed proxies in these conflicts; but while it won the conventional battles, it lost the proxy war, and arguably the campaign. As General Richard Barrons notes, 'proxy warfare is the most successful kind of political war being waged of our generation'.[27] This chapter aims to define proxy warfare, to understand how it can be waged successfully, and to identify the limitations of what it can achieve.

The term 'proxy' is widely employed to denote a client that receives funding and equipment from, and acts in the interests of, a patron. It is impossible, however – under such a definition – to distinguish capacity building, stabilisation, and alliances on the one hand from sponsorship of terrorist groups or subversion on the other. In attempting to define proxy warfare by building a criteria for proxies, Bertil Duner concludes that 'it is impossible to demonstrate a single example of a state acting as a proxy for some other state … our analytical instruments are defective'.[28] They have scarcely improved over the nearly 40 years since Duner made this observation.[29] Some have sought to escape this definitional challenge by identifying proxy wars, rather than proxies. Andrew Mumford defines proxy wars as 'conflicts in which a third party intervenes indirectly in order to influence the strategic outcome in favour of its preferred faction'.[30] But

26. Leo Shane III, 'Price Tag of the "War on Terror" Will Top $6 Trillion Soon', *Military Times*, 14 November 2018.
27. Richard Barrons, remarks delivered at the conference 'The Warfighter in the Twenty-First Century', RUSI, London, 23 November 2017.
28. Bertil Duner, 'Proxy Intervention in Civil Wars', *Journal of Peace Research* (Vol. 18, No. 4, 1981), p. 359.
29. Even experienced scholars often label US and Saudi operations in Yemen as 'war by proxy', even though it is unclear who is carrying out whose policy, and which is formally an alliance. See, for example, C Anthony Pfaff, 'Strategic Insights: Proxy War Norms', Strategic Studies Institute, 18 December 2017. Legally, a proxy is a group over which a state maintains effective control. This is a very high threshold, enabling denial by obscuring the mechanism of influence. See Ruth Jamieson and Kieran McEvoy, 'State Crime by Proxy and Judicial Othering', *British Journal of Criminology* (Vol. 45, No. 4, 2005), pp. 504–27.
30. Andrew Mumford, 'Proxy Warfare and the Future of Conflict', *RUSI Journal* (Vol. 152, No. 2, 2013), p. 40.

few wars fail to fit this definition; under this rubric the UK was a US proxy during the opening years of the Second World War. Moreover, proxy activity does not only take place during actual fighting; consider Hizbullah's operations in West Africa and South America.[31]

The obsession with establishing a proxy identity for groups is far less analytically helpful than understanding the strategic objectives for which states establish proxies. Focusing on proxy warfare as a strategy, as David Sterman observes, 'would allow us to zoom in on features like secrecy, plausible deniability, and the ambiguity of command responsibility that make a proxy warfare strategy meaningfully distinct from other forms of warfare.'[32] The essence of proxy warfare is to implement one's policy through others. There are several reasons for adopting a proxy strategy. A state may want to implement a policy that, if pursued openly, would bring about retaliation – such as Pakistan's use of Lashkar-e-Taiba against India.[33] A state may develop proxies to compensate for its own risk aversion or lack of mass. Casualties among a proxy force are less likely to have political ramifications at home: the US use of the Kurdish militia Yekîneyên Parastina Gel (YPG) in Syria is a prime example.[34] In the context of a failed state or feral city,[35] a state may use proxies to safeguard its interests without incurring the domestic backlash and local opposition that deploying sovereign forces would entail: for example, the UAE's mobilisation of local groups to hold contested ground in Yemen.[36]

Conceptualising proxy warfare as a strategy provides a more robust methodology for identifying proxies. Proxies are the organisations beyond its own forces through which a patron seeks to implement its policy. A proxy may consider itself to be a deniable asset of a patron, like the GATIA in Mali,[37] or not, as in the Counter Terrorism Service (CTS) in Iraq.[38] It may be an alliance of convenience, as with the Mujahideen-e-Khalq's cooperation with Mossad to kill Iranian

31. Ronen Bergman (translated by Ronnie Hope), *The Secret War with Iran: The 30-Year Clandestine Struggle Against the World's Most Dangerous Terrorist Power* (New York, NY: Simon and Schuster, 2008), pp. 169–84.
32. David Sterman, 'How Do We Move Beyond "Proxy" Paralysis?', New America Foundation, 7 March 2019.
33. Steve Coll, *Directorate S: The CIA and America's Secret Wars in Afghanistan and Pakistan, 2001–2016* (London: Allen Lane, 2018), pp. 341–48.
34. Sana Hussein, 'What is Behind the US Support for the YPG', *Middle East Monitor*, 30 January 2018.
35. 'Feral cities' are urban spaces with very limited institutional control, managed by informal governance structures, armed groups and criminal organisations: Basra and Mogadishu are prime examples.
36. Adam Baron, 'The Gulf Country That Will Shape the Future of Yemen', *The Atlantic*, 22 September 2018.
37. Author observations, northern Mali, June 2015. Following ceasefire violations by Tuareg separatists, the government would respond with counter-violations via GATIA, while stressing the need to uphold the agreement.
38. Given the close working relationship between US forces and the CTS, Iraqi and Iranian officials complained to the author that they are like an 'American proxy'. Some American officials concede that there are merits to the allegation. However, the CTS does not. See Michael Knights and Alex Mello, 'The Best Thing America Built in Iraq: Iraq's Counter Terrorism Service and the Long War Against Militancy', *War on the Rocks*, 19 July 2017.

nuclear scientists.[39] It may not realise that it is serving a patron's interests. The proxy may be coerced into cooperating, as Jabat Al-Nusra did with several Free Syrian Army groups in Syria.[40] In most cases, organisations being used to implement a proxy strategy by a patron will not define themselves as a proxy, but will have their own objectives.[41]

Proxy warfare is not new; consider competing state support for governments and opposition movements during the era of imperial competition.[42] There are good reasons for expecting its prevalence to increase over the next decade, however.[43] As international supply chains and reliance on exquisite systems increase the costs of conventional war, states will aim to compete below the threshold of direct conflict. This is demonstrated in Syria, where, despite direct competition between major powers with significant interests in the outcome, external actors have primarily worked through partners on the ground.[44] As information from the front line becomes increasingly accessible to citizens via social media, and trust in government erodes, the political cost of deploying sovereign forces will remain high.[45] As urban areas expand – with portions of urban centres turning feral – there is likely to be a growing number of contested spaces in which external states can take advantage of weak governance to pursue their interests.[46] Finally, as information about proxy warfare is more widely available, the concept has been normalised to the extent it is often advocated openly,[47] rather than waged in secret.[48]

Proxy warfare has become increasingly common, but it has been pursued with varying degrees of success. Perhaps the most successful user of proxy warfare is Iran. Iran does not simply employ proxies for operational convenience; they are integral to Iran's national security strategy. The

39. Ronen Bergman, *Rise and Kill First: The Secret History of Israel's Targeted Assassinations* (New York, NY: Random House, 2018), pp. 589–609.
40. Jabat Al-Nusra focused on governance, issuing identification and setting up courts, and thereby started to hold other Syrian groups accountable to its rules – forcing them to operate under its leadership, or disband. See Oliver Holmes and Alexander Dziadosz, 'Special Report: Syria's Islamists Seize Control as Moderates Dither', *Reuters*, 19 June 2013.
41. The reasons for becoming a proxy are diverse. See Daniel L Byman, 'Why be a Pawn of a State? Proxy Wars from a Proxy's Perspective', Order From Chaos blog, Brookings Institution, 22 May 2018.
42. National Archives, FO 800/70: Cecil Spring Rice to Edward Grey, 28 March 1907.
43. Candace Rondeaux and David Sterman, 'Twenty First Century Proxy Warfare: A Briefing Document', New America Foundation, November 2018.
44. Jeffrey Martini, Erin York and William Young, *Syria as an Arena of Strategic Competition* (Washington, DC: RAND Corporation, 2013).
45. Edelman, 'Edelman Trust Barometer 2018: Global Report', January 2018.
46. David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York, NY: Oxford University Press, 2015), pp. 232–62.
47. John McCain, Joseph Lieberman and Lindsey Graham, 'The Risks of Inaction in Syria', *Washington Post*, 5 August 2012.
48. Richard Aldrich and Rory Cormac, *The Black Door: Spies, Secret Intelligence and British Prime Ministers* (London: William Collins, 2016), pp. 247–54.

successes Iran has achieved through its proxies have caused other states to seek to replicate their methods.[49]

The Iranian government perceives the US as its greatest threat, as the only country capable and inclined to attempt its overthrow. Moreover, the Iranian government is under no illusions as to the outcome. Although Iran's air defences may impose a cost on the US gaining air supremacy[50] and prohibit limited strikes on strategic facilities,[51] Iranian forces would invariably be outmatched by the US in a conventional confrontation. Iran's defence policy is therefore one of deterrence, using missiles,[52] its navy[53] and proxy forces to inflict sufficient damage in a regional 'deep battle' to make war with Iran too costly an undertaking. If deterrence fails, Iran does not expect the US to conduct a comprehensive ground invasion, but rather to try and foster internal uprisings.[54] The Iranian government expects that because of the strength of Iranian nationalism, and determination to defend religious sites, domestic opposition would fail to topple the government.[55] Iran would use its proxies to inflict casualties on the US and its regional allies, with the aim of driving its adversaries to negotiate.

Hizbullah is the linchpin of Iran's deterrence strategy. Loyal to Ayatollah Khamenei, Hizbullah will coordinate strategically with Tehran. Although Hizbullah does not currently seek a war with Israel, and has many domestic interests in Lebanon that are distinct from Iran's, Tehran would have little difficulty in forcing Hizbullah to strike.[56] Hizbullah's stockpile of rocket artillery, and its growing arsenal of medium-range missiles, would likely force Israel to undertake a ground invasion of Lebanon in the event of wider escalation, and thence engage in costly fighting with Hizbullah's 35,000 trained forces in mountainous terrain and the urban littoral.[57] The damage to Israel would be considerably greater than the 2006 war. There is also the possibility – given

49. The author has, on several occasions, been asked by officials in other states to discuss what can be learned from the Iranian approach.
50. Robert Ashley, 'Statement for the Record: Worldwide Threat Assessment', testimony before the Senate Armed Services Committee, <http://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/1457815/statement-for-the-record-worldwide-threat-assessment/>, accessed 1 October 2018.
51. Iran's fleet of 43 F-14 Tomcats would make a limited strike costly. See International Institute of Strategic Studies, *The Military Balance 2018* (London: Routledge, 2018), p. 336.
52. Steven Hildreth and Cyrus Jabbari, 'Iran's Ballistic Missile and Space Launch Programs', In Focus, Congressional Research Service, 2018.
53. Berenice Baker, 'Iran's Fast Attack Craft Fleet: Behind the Hyperbole', *Naval Technology*, 16 January 2013.
54. An assessment consistent with the policy line advocated in Washington. See Najmeh Bozorgmehr and Katrina Manson, 'John Bolton Support for Iranian Opposition Spooks Tehran', *Financial Times*, 2 April 2018.
55. A judgement with historical precedent. See Patrick Clawson, 'Iran's Economy: Between Crisis and Collapse', *MERIP Reports* (No. 98, 1981), pp. 11–15.
56. Jack Watling, 'Iran's Objectives and Capabilities: Deterrence and Subversion', *RUSI Occasional Papers* (February 2019), pp. 17–18.
57. *Ibid*., pp. 19–20.

past practice – that Hizbullah would kidnap the nationals of states opposing Iran to weaken a political coalition.

Iran also retains relationships with Hamas and Palestinian Islamic Jihad (PIJ) in Gaza, and the Houthis in Yemen. Unlike Hizbullah, these are organisations with entirely independent political objectives, and Iran has a minimal capacity to shape their actions or coordinate with them.[58] However, by providing them with minimal support, Iran significantly reduces the diplomatic space for these groups to negotiate, and protracts the conflict – fixing Israel, and Saudi Arabia and the UAE, respectively, in politically costly battles. The objective is different with each group. The aim in Palestine is to ensure that Hamas maintains its armed struggle against Israel[59] with PIJ acting as a spoiler in ongoing ceasefire negotiations,[60] because progress in the Israel–Palestine peace process would undermine the legitimacy of Iran's strategic deterrent. In Yemen, by contrast, Iran supplies some technical assistance, including IED components, and carries out symbolic attacks – such as a missile strike on Riyadh[61] – to retaliate against the Saudi kingdom for its actions against Iranian interests in Syria. Beyond direct harm to Israel, Saudi Arabia and the UAE, both of these ongoing conflicts cause diplomatic problems for Iran's adversaries.[62]

Whereas the Israeli-Palestinian conflict and Yemeni Civil War impose a greater cost on Iran's adversaries, Syria is perceived to be a non-discretionary yet costly war for Iran. Syria had been a valuable ally – bolstering Iran's deterrence against Israel – but today is a dependent, with Iran spending considerable sums to maintain proxy forces over which it has limited control.[63] Nor has the war seen a meaningful expansion of Iranian leverage in Syria, with Russia blocking Iranian access to military facilities, and President Bashar Al-Assad unwilling to make himself subservient through economic concessions.

Iran has had much greater success in Iraq, although here too it is important to recognise the limits of Iranian influence. On the one hand, the centrality of the Badr Organization to the Iraqi state – managing the Ministry of Interior and with a sizeable standing army within Iraq's

58. *Ibid*., pp. 21–26.
59. Sayed Ali Khamenei, 'Imam Khamenei's Response to Hamas Leader's Letter on Arab States' Betraying Palestine', *Khamenei.ir*, 4 April 2018, <http://english.khamenei.ir/news/5578/Imam-Khamenei-s-response-to-Hamas-leader-s-letter-on-Arab-states>, accessed 29 January 2018.
60. Isabel Kershner, 'Israel Accuses Iran of Ordering Palestinian Rocket Fire from Gaza', *New York Times*, 27 October 2018.
61. Michael Knights, 'The Houthi War Machine: From Guerrilla War to State Capture', *CTC Sentinel* (Vol. 11, No. 8, 2018).
62. On the withdrawal of technical assistance for aircraft, see Bruno Waterfield, 'UK and France Denounce German Ban on Saudi Arms Sales', *The Times*, 24 February 2019. On mounting hostility in Congress, see Catie Edmondson and Charlie Savage, 'House Votes to Halt Aid for Saudi Arabia's War in Yemen', *New York Times*, 13 February 2019.
63. Consider the struggle for control between Iran, Russia and Damascus. See Charles Lister and Dominic Nelson, 'All the President's Militias: Assad's Militiafication of Syria', Middle East Institute, 14 December 2017.

security apparatus – ensures that Iraq will retain strong economic links with Iran and facilitates the transfer of personnel and materiel through Iraqi territory. Ultimately, Iran aims to stabilise Iraq as a market for Iranian goods.[64] Meanwhile, through paramilitary groups, including Khateib Hizbullah and Asaibh Ahl Al-Haq (AAH), Iran maintains the ability to strike US forces should they seek to establish a large and permanent presence in Iraq. Iran exercises limited control over AAH, while the Badr Organization is not dependent on Tehran and therefore works as a partner rather than a subordinate. Iranian policy in Iraq is also constrained by Iraqi sensitivities over Persian domination, so that if Iran is too direct in asserting its influence it faces significant backlash from the Iraqi population.

Iran's proxy strategy imposes multiple dilemmas on its adversaries. Direct retaliation against Iran for its proxy strategy would likely be seen as an unacceptable escalation by many other states. Decisive retaliation against the proxy itself is liable to be seen as the suppression of internal opposition, and therefore to incur a diplomatic cost. Admittedly, many of the groups Iran is sponsoring operate beyond the law, and regional collaboration to catch and prosecute money launderers and weapons smugglers could have an effect on constraining Iran's interference in the domestic affairs of its neighbours. The problem is that most of Iran's adversaries also employ proxies, although more often at the operational rather than the strategic level. Iran may have been remarkably successful in employing proxies, but that success is liable to inspire the wider employment of comparable tactics. The challenge presented by Iran today is therefore one that is liable to become a recurring concern.

Iran's proxy activity in Iraq is instructive of what makes for an effective proxy strategy. Tehran has provided support to a range of groups over a long period of time, keeping the same individuals as points of contact to foster mutual trust. In return, Tehran's demands have been narrow. Fighting US forces was an activity Iran's proxies wanted to do in any case; Iran simply provided some of the means. By supporting multiple groups, and adjusting its levels of support, Iran is able to avoid becoming dependent upon a single ally. However, varying levels of support are justified to partners in terms of available resources and priorities, not as a punishment. It is lazy to assume that Iran's success is purely the result of cultural familiarity; it has successfully developed partnerships with forces that are not ideologically aligned with Tehran, including Al-Qa'ida[65] and Hamas. The crucial point is that Tehran builds long-term relationships and is clear about a narrow set of interests that define the relationship.

In countering a proxy strategy, it must be decided whether to deter it, by holding the patron directly accountable for their interference in other states, or counter it by engaging in comparable tactics.

64. Iranian officials claim that Iraq is the destination for approximately 70% of the country's non-oil exports.

65. Cathy Scott-Clark and Adrian Levy, *The Exile: The Flight of Osama Bin Laden* (London: Bloomsbury, 2014), p. 146.

Defeating a proxy strategy that has been declared illegitimate requires that no distinction be drawn between the conduct of the proxy and its patron. This approach has been used by the US to deter AAH and Khateib Hizbullah in Iraq to some effect.[66] Alternatively, a state may argue that if a patron will not acknowledge a proxy, then the proxy will not be protected. Again the US demonstrated the effectiveness of this approach when it defeated Russian mercenaries in the Euphrates Valley.[67] The use of law enforcement to constrain proxy activity can also prove highly effective; Hizbullah's attempts to rebuild its international terrorist capabilities after the assassination of its operations chief Imad Moughniyah were frustrated in a highly alert counterterrorist environment.[68]

If the decision is instead to compete within the proxy arena, there are an array of policy options available. The first is the training and development of a counter-proxy, constraining the effectiveness of the enemy. The use of the CTS in Iraq by the US as a flagship unit in countering Daesh (also known as the Islamic State of Iraq and Syria, ISIS) was highly effective in undermining the narrative that Iraq's defeat of Daesh was exclusively the work of Iran. Alternatively, proxies can be co-opted, as Assad has started to do with the YPG in Syria.[69] Finally, there is defeating proxy forces in detail, since the patron may struggle to offer meaningful protection. The proxy can either be given a path out by breaking links with its patron, or be forced to become dependent on the patron, in which case it may be possible to impose an escalating cost on the patron in retaining the proxy. In Iran's case, the financial strain of international sanctions has constrained its capabilities,[70] forcing the state to argue publicly that its foreign policy advances Iranian interests, even while this alienates its proxies who do not see themselves as subservient to Iran.

Ultimately, in responding to proxy warfare the West faces a choice. Western policymakers are increasingly talking about contesting the 'grey zone' between peace and war.[71] It is important to note that the decision to contest the grey zone should be a conscious choice. The alternative is to not recognise grey-zone activity, and to prosecute those who act in it as criminals, or attack them as terrorists – calling the bluff of those who believe that the ambiguous relations of a group to a patron state should offer that group protection. Such an approach requires careful study of escalation management, as recently demonstrated by escalating hostilities in Kashmir following an attack by a Pakistani proxy.[72] If it is decided to contest the grey zone – a path that

66. White House, 'Statement by the Press Secretary', 11 September 2018.
67. Thomas Gibbons-Neff, 'How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria', *New York Times*, 24 May 2018.
68. Matthew Levitt, *Hezbollah: The Global Footprint of Lebanon's Party of God* (Washington, DC: Georgetown University Press, 2013), pp. 75–116.
69. Roy Gutman, 'America's Dirty Secret in Syria: A De Facto Alliance with Assad', *Daily Beast*, 27 February 2018.
70. Following the re-imposition of sanctions, there has been an estimated 50% reduction in Iranian financial support to Hamas. Author interview with an expert in terrorist financing in the Levant, London, February 2019.
71. Gavin Williamson, 'Defence in Global Britain', speech at RUSI, London, 11 February 2019.
72. *BBC News*, 'India Pakistan: Kashmir Fighting Sees Indian Aircraft Downed', 27 February 2019.

Western states have pursued many times before – it is critical to treat that activity as both a whole-of-government and secret effort. The UK's approach to the Dhofar Rebellion in Oman may be seen as a highly successful example of such an operation.[73] Many subsequent attempts to contest the grey zone, failing to accept the moral ambiguity necessary to act effectively in this space, have arguably led Western states to be consistently outmanoeuvred and outmatched. Even in Afghanistan during the Soviet invasion, the CIA's reluctance to cross certain lines ceded considerable long-term influence to Pakistan.[74] Therefore, if the West is unwilling to accept the political and moral compromises involved, then it is better to deter and defeat grey-zone activity rather than engage in it.

73. John Akehurst, *We Won a War: The Campaign in Oman, 1965–1975* (Salisbury: Michael Russell Publishing, 1982).
74. Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan and Bin Laden* (New York, NY: Penguin, 2005).

Coercion and Economic Warfare: China

Sidharth Kaushal

A STRIKING PROPAGANDA POSTER published in Germany just before the First World War depicted Britain as a gigantic octopus straddling the globe. For all its crudeness, the poster captured the essence of 'structural power': the ability of a country to control the flows of goods, services and information through a globalised system. This achieves strategic results by redirecting transactions – either shutting opponents out of globalised networks or channelling flows to privileged allies and partners.[75] Trade reliant sea-powers have realised – as early as the Athenian leader Pericles – that avoiding costly engagements on land, using their financial strengths to purchase the loyalties of allies and financially strangle their adversaries, and raiding to erode the fibre of an opponent's economy, represented a more effective means of achieving strategic outcomes than head-on clashes.[76]

A historical example of this structural power occurs in the Age of Imperialism in which German commentators viewed the UK's power with trepidation. Not long after the war began, telegraph lines to Berlin's colonial outposts were shut, and the navigation certificate system with which the UK identified contraband provided it with the information needed to curtail Germany's trade. A more recent example of structural power in action is the closure of the SWIFT banking system to Iranian financial institutions by the US as part of its wider programme of economic coercion to curtail the Iranian nuclear programme. This fits into a wider pattern of the use of the US's extra-territorial reach to curtail its rivals' financial freedom of action – a case in point being the recent secondary sanctions on Iran extending financial penalties both to actors that do business with Tehran and a wide swathe of actors that in turn do business with these companies.

Challengers to such states have historically relied on two means of riposte. First, some states have attempted to emulate and then supplant the network centrality of the maritime hegemon by building parallel networks. This has typically been the approach of semi-open states who have trade-based economies. Initially, this course of action relies on commerce with the central power to build up stocks of capital. Subsequently they embark on a process of using their greater centralisation to consciously reorient the system towards themselves, first in increments and then openly. In 16th-century England, for example, the English relied (as competitors) on capital from the Dutch Republic to build its economy before effectively reorienting global commerce

75. Susan Strange, 'The Persistent Myth of Lost Hegemony', *International Organization* (Vol. 41, No. 4, 1987), pp. 551–74.

76. Andrew Lambert, *Seapower States: Maritime Culture, Continental Empires and the Conflict that Made the Modern World* (New Haven, CT: Yale University Press, 2018).

from the Dutch Republic towards itself, eventually passing legislation dictating that commerce being brought to England or its colonies would be carried exclusively in English ships.[77] Having gained network centrality, challengers can use their newfound structural power to coerce rivals and purchase political loyalties by means short of war. Selectively granting other states market access, exerting control over financial flows, and other economic inducements, augment military instruments in such a state's toolkit.

Other challengers have attempted to break the trading system of the hegemon by corroding the system itself by attacking the nodes and connective tissue of such systems (for example, global trading norms and standards) upon which the pre-eminent power relies for its power. This approach has typically, but not exclusively, been the strategy of choice for closed, often autocratic societies with less to lose from a systemic collapse than their opponents. The guiding principle of the French Jeune École school of strategic thought at the turn of the 20th century, for example, was that Britain's dependence on overseas food and resource lifelines left it uniquely vulnerable to a *guerre de course* against its economic life lines which – even if it disrupted global trading systems more generally – represented France's best hope of securing a decisive advantage. The same openness that confers centrality on open societies paradoxically leaves them much more vulnerable to disruption than their closed opponents.[78]

As the current century unfolds, the core strategic dynamic of a quiet competition to either build or disrupt structural power against the backdrop of the more violent, visible competition of open war is likely to continue in a manner similar to past eras. The changes that are likely to be seen are to the grammar and not the logic of this competition, as new avenues for the transfer of material and information such as cyberspace and space emerge.

China: A Network in its Image

As mentioned above, rising economic powers often opt for a form of symmetry in their approach to creating structural power whereby they seek to emulate existing power structures but with a mercantilist twist. Using their often-greater levels of centralisation, mercantilist states generate network power by fiat – meaning that the economic fidelity of the networks they preside over can sometimes be sacrificed in the name of political interest. Using incentives such as selective access to credit for politically loyal companies, these states can convince their companies to sacrifice economic benefit for political necessity when needed. This is not usually the case in more liberalised markets, where controlling the flow of goods and services through tools such as sanctions requires a more ponderous, formalised legal process.

Similar to England in the build-up to the Anglo-Dutch Wars, the economic component of China's competitive strategy has proceeded in three stages. First, China attempted to open itself to capital flows from the developed world, while retaining the capacity to occasionally leverage

77. Graham Allison, *Destined for War: Can America and China Escape the Thucydides Trap?* (Victoria: Scribe Publications, 2015), pp. 45–47.
78. Andreas Roksund, *The Jeune Ecole: The Strategy of the Weak* (Leiden: Brill, 2007).

the dependencies that these flows created to build a constituency for itself in the West. For example, when the administration of US President Bill Clinton considered linking China's most-favoured-nation status to clauses regarding human rights in the 1990s, China actively and successfully lobbied Western companies such as Boeing to campaign against this move. To underscore the fact that it had alternatives, China hosted representatives from competitors (such as Airbus) in other countries in the build-up to the Congressional debate surrounding the clauses.[79]

This approach gave way to a period of hedging, in which a more confident China created a network of free-trade agreements (FTAs) both regionally (such as the China–ASEAN FTA) and extra-regionally that were predicated on a 'no strings attached' model of trade that would not be predicated on structural reforms. This was not a challenge to the Western economic order per se, but it did insulate China from pressure to reform its own economy by cultivating a coalition of like-minded actors. It was also in this period that China began a process of buying up entire supply chains of critical resources with its state-owned enterprises in anticipation of growing resource competition.[80]

Under President Xi Jinping, China has moved to consolidate this patchwork of agreements into a coherent network. In the form of initiatives such as the One Belt One Road project, the New Maritime Silk Road and the Asian Infrastructure Investment Bank, China is becoming the centre of a web of economic relationships in which it secures privileged access for its companies through favourable loans, political protection, and a series of other side payments to debtor states. Similar to England's exclusive maritime shipping network, China is now shaping its own more coordinated form of network centrality.

When converting this network centrality into coercive power, China has adopted a two-track approach that can be grouped into the categories of denial and command. Congruent with its military posture, China's use of coercive leverage on external great powers such as the US does not aim to materially compel them, but rather to prolong their decision-making process and undercut their capacity for a timely crisis response. Several People's Liberation Army (PLA) publications have pointed out that a core vulnerability of the US is the fact that going to war requires a domestic consensus of multiple stakeholders.[81] To prolong this consensus-building process, China does not need to target the US economy writ large, only those sectors and political actors that depend most on Chinese trade. Moreover, the object of coercion is not to seriously damage these sectors but to demonstrate that China can do so – perhaps by making an example of selected companies. This, in conjunction with a media offensive to give an economically beholden 'peace faction' a narrative to rally around is the first, invisible,

79. James Mann, *About Face: A History of America's Curious Relationship with China, from Nixon to Clinton* (New York, NY: Knopf, 1999), pp. 292–93.
80. Aaron L Friedberg, 'Globalisation and Chinese Grand Strategy', *Survival* (Vol. 60, No. 1, 2018), pp. 7–40.
81. Roger Cliff et al., *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States* (Santa Monica, CA: RAND Corporation, 2007).

layer of China's anti-access strategy.[82] This complements the military threat posed by China's anti-access network of shore-based missiles which, by posing physical risk, will give even players who are not economically beholden to China reason for pause. Both the military and economic components of the denial approach rely on tacit threats, not the actual use of coercive military and economic tools which might do enough damage to galvanise an adversary's public. Crucially, China does not need to coerce the US into changing its policies: merely prolonging the domestic discussion about the merits of intervention in the US is enough. In the meantime, as per its local-war doctrine, China expects to have settled the issue on its periphery militarily with a short, sharp campaign. Thus, even if a domestic consensus to intervene does eventually crystallise, it will be too late. This is unlike traditional economic coercion which inflicts economic pain for a specific political concession. Rather, like the anti-access strategy it complements, it is a strategy of delay. Much of the coercion is likely to take the form of tacit threats as opposed to explicit punitive actions given that the object is not to inflict pain but to use the fear of economic costs to delay action.

By contrast, China's coercion of near powers is more direct and expansive in its ambition. As illustrated by its embargo of agricultural products from the Philippines in 2012 and its 2010 embargo of rare-earth exports to Japan, China is comfortable using explicit coercion in the form of sanctions and embargoes to get what it wants on its immediate periphery. This complements its strategy of waging short, sharp local wars in its close vicinity.[83]

Effectively, then, China's economic statecraft follows the contours of its military doctrine. Near China's shores both China's military posture and its use of economic coercion aim towards short, sharp displays of power to secure limited ends in localised conflicts. Moving further from China's shores, its economic coercion takes the form of tacit threats aimed to give an opponent pause, while its military posture aims to deter rather than defeat an intervention by an outside power. This twin-pronged approach which Chinese strategists call counter-intervention is effectively a strategy of deterrence – or at least delay – aimed at keeping local clashes local.

Russia: The Autarkic Disruptor

If rising wealthy quasi-centralised economies pose one strategic challenge, they are joined by another type of state – one both weaker and more dangerous. Autarkic or quasi-autarkic states are simultaneously more resilient to global disruptions and cognizant of their opponent's susceptibility to it. Their approach to economic coercion is thus more overt, aggressive and potentially disruptive than that of mercantilist states and crosses the boundary into open warfare. A case in point is Russia which, as Foreign Minister Sergei Lavrov described it, is a 'minority stakeholder in globalization'.[84] The Russian economy is not truly autarkic, to be sure –

82. William Norris, *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control* (Ithaca, NY: Cornell University Press, 2018).
83. Dan Blumenthal, 'Economic Coercion as a Tool in China's Grand Strategy', statement before the Senate Committee on Foreign Relations, 24 July 2018.
84. Christopher Coker, *Future War* (Cambridge: Polity Press, 2015), p. 91.

exports of oil account for roughly 16% of its GDP – but it is increasingly reliant, in the absence of foreign capital, on an internal state-led system for financing projects and a national information infrastructure (including an emerging nationally bounded internet). Russia thus has less to lose from economic fluctuations than more interconnected powers.[85]

While commerce disruption is hardly new, the avenues by which it might be prosecuted, and its efficiency within an international trading system dependent on a handful of infrastructural and information bottlenecks, have increased drastically. As articulated by General Valery Gerasimov in his now famous article on hybrid warfare, the use of kinetic force now depends on its effective coordination with non-kinetic means including economic suasion and political disruption.

Thus, for example, Russia has demonstrated its willingness to target the financial sinews of rivals through means such as cyber attacks – for example, shutting down the cash machines in nearby Estonia for a day in 2007 following the removal of a Soviet-era monument in Tallinn. Similarly, the Russian war with Georgia in 2008 was accompanied by large-scale denial-of-service attacks against key financial institutions in Georgia.[86]

More recently, the Russian navy has unveiled the deep-diving submarine *Losharik*, capable of interfering with the transatlantic communication cables that underpin the internet. This capability, along with Russia's development of its own smaller-scale internal version of the internet, is in a way a continuation of what William C Fuller dubbed Russia's strategic habit of leveraging the 'advantages of backwardness'.[87] The very complexity that renders countries economically sophisticated also renders them vulnerable in ways that closed, hierarchical societies that have less to lose from mass disruptions to a rules-based order are not.

Conclusions

While economic coercion is a strategic tool, it has ramifications for the military operating environment. Militaries contemplating power projection cannot assume they will be able to generate an agile response to contingencies in regions such as East Asia for political rather than operational reasons. Allies of Chinese adversaries, facing the prospect of economic coercion by China, may choose to exercise their sovereign right to withhold military access – as Turkey did to the US with Incirlik Air Base before the Iraq War, albeit for different reasons. As such, building partner capacity to hold the line for the initial period of a conflict until a political consensus to intervene has crystallised will be vital. Investing in the anti-access capabilities of small entities such as Taiwan and Vietnam and focusing on less politically contentious tasks – such as providing these states with intelligence, surveillance and reconnaissance capabilities – will be key. While Western military intervention may prove decisive in the long run, the capacity for economic coercion and military deterrence to delay this intervention in the early stages of

85. Silvana Malle, 'Economic Sovereignty: An Agenda for Militant Russia', *Russian Journal of Economics* (Vol. 2, No. 2, 2016), pp. 111–28.
86. Allison Lawler Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press).
87. William C Fuller, *Strategy and Power in Russia 1600–1914* (New York, NY: The Free Press, 1988).

a conflict will mean that the capacity for local forces to hold on in the initial stages of a conflict will be a cornerstone of deterrence.

Regarding autarkic states, a different challenge emerges. Securing critical physical infrastructure such as undersea cables and building societal resilience in cyberspace will be key to effectively confronting states willing to use the threat of mass system disruption as a coercive lever. The counter to such activities will require greater military integration into the civil responsibilities of protection of critical national infrastructure: an extension of civilian military cooperation beyond that with which democracies have historically been comfortable.

Brinkmanship and Warfare in North Korea

Justin Bronk

THE CONFRONTATION BETWEEN the US and North Korea has continually held world attention over several decades. States large and small have been treated to a real-world demonstration of how a concerted campaign of aggressive military brinkmanship by a comparatively weak power has successfully deterred the world's sole superpower.

It is striking that despite a large disparity between North Korea and its international foes, it has managed to successfully attain its overriding goals. Through threats of military action, actual aggression in limited contexts, and use of extreme official language, it has bought time to develop the strategic nuclear arsenal which its leader Kim Jong-un views as essential for the long-term defence of his rule, but which the world's only superpower has long warned is both unacceptable and a potential *causus belli*. This is no mean achievement, especially given the fates of other rogue states since the end of the Cold War. Brinkmanship is a key part of why North Korea has been able to leverage its few military advantages to, at least thus far, successfully deter US and South Korean armed interventions, despite repeated provocations and an active nuclear programme.

Developed under a decades-long arms embargo and sanctions regimes, the Korean People's Army (KPA) externally resembles the massed forces of the mid-Cold War Warsaw Pact far more than modern Western-pattern manoeuvre and information-centric forces. The ground forces are composed of 82 divisions with a heavy reliance on both fixed and mobile air-defence systems, tanks (over 4,300), massed infantry and above all artillery – with 8,600 heavy artillery pieces over 76.2mm calibre and more than 5,000 multiple launch rocket artillery systems.[88] The KPA can also count on over 7 million reservists. Despite its impressive mass and firepower, the KPA relies on outdated equipment and is at face value precisely the sort of force the Western military machine was designed to defeat. However, among its conventional assets, the KPA has developed extensive special operations forces, and chemical and biological agents to augment its artillery and rocket firepower and sophisticated cyber-warfare capabilities, plus its more publicly visible nuclear weapons programme.[89] The special forces and cyber capabilities in particular give North Korea deniable, or at least low-profile, options to conduct coercive

88. South Korean Ministry of National Defense, *2016 Defense White Paper* (Seoul: Youngsan-gu, 2016), p. 268.
89. Eleanor Albert, 'North Korea's Military Capabilities', Council on Foreign Relations, 6 June 2018; Cristina Varriale, 'North Korea's Other Weapons of Mass Destruction', *Arms Control Today* (Vol. 48, No. 7, September 2018), pp. 6–10.

escalation against South Korea during periods of tension or to force a renewal of crisis talks, while the chemical and biological weapons add an additional level of terror to the prospect of a North Korean artillery bombardment on the northern districts of Seoul and the many military and civilian assets within range of the demilitarised zone (DMZ).

The threat of massed artillery bombardment has long served as Pyongyang's deterrent force during North Korea's long road to nuclear statehood – with thousands of heavy tube and rocket artillery pieces able to rain destruction down on densely populated parts of one of the world's largest cities, with or without including chemical and biological warheads. While this threat is sometimes overstated – North Korea could not flatten all of Seoul – it is still a mass-casualty and hugely destructive scenario for South Korea to contemplate.[90] Although the US and probably even South Korea alone do possess the means to destroy the North's artillery assets, the sheer number of targets and their well dug-in and fortified positions in mountainous terrain means that the task would take days without resort to tactical nuclear weapons. Combat-air assets attempting to pinpoint and neutralise artillery positions north of the DMZ would also have to deal with pop-up air defence and possibly even hostile air threats even after the initial suppression/destruction of the enemy air defences campaign – which itself would take time to prepare and prosecute. All the while, the other signature KPA tactic of massed, formation-level infiltration and disruption would make force protection and coordination even south of the DMZ extremely difficult for South Korean and US commanders.[91]

Without the ability to construct and maintain defensive military capabilities sufficient to confidently repulse even an all-out attack by South Korean military forces, let alone those of the US, North Korea has instead pursued a military strategy which emphasises the amount of offensive damage which can be inflicted before the regime would inevitably be defeated. In many ways this resembles many Cold War nuclear deterrence constructs in focusing on maintaining the ability to inflict unacceptable damage rather than win a war. However, where North Korea arguably differs from Cold War deterrence postures is in the extent to which it actually uses its offensive capabilities – albeit in carefully calibrated and limited situations – to control the tenor of relations and the shape of negotiations with the outside world. North Korea, both under Kim Jong-il and Kim Jong-un, has repeatedly shown it is willing to step to the apparent brink of armed conflict to further its foreign-policy objectives. In effect it has taken the approach outlined by the famous deterrence scholar Thomas Schelling, in which openly accepting vulnerability and self-deprivation of options for avoiding a suicidal confrontation enhances rather than detracts from the ability to maintain escalation control in a crisis.[92]

There have been multiple armed and often bloody encounters between North and South Korea, including: guerrilla actions in the aftermath of the North Korean spy submarine grounding at

90. Roger Cavazos, 'Mind the Gap Between Rhetoric and Reality', NAPSNet Special Reports, 26 June 2012.
91. See US military comments in Michael Peck, 'North Korea Plans to Defeat the U.S. Army in a War. Here's How', *National Interest*, 12 January 2018.
92. See game theory essays collected in Thomas C Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 2003).

Gangneung in 1996; the First Battle of Yeonpyeong in 1999; the sinking of the ROKS *Cheonan*; and the shelling of Yeonpyeong in 2010. They form part of a decades-long North Korean approach to keeping South Korea on the defensive and using small-scale armed incursions and direct attacks on isolated assets and bases. More recently, a pattern has developed of a drumbeat of nuclear-weapons tests and increasingly long-range ballistic missile test firings. In particular, in 2017, with global fears running high of a war sparked by a pre-emptive strike by President Donald Trump's administration against North Korea's nascent nuclear ICBM capabilities, Pyongyang doubled down. In August and September, it fired missiles over Japan and far into the Pacific and detonated what it claimed was a miniaturised thermonuclear warhead.[93] An even-longer-ranged missile test followed in November, fuelling fears of war in the event of a US strike operation to enforce the red line, set by multiple administrations, of a nuclear ICBM capability, which the November test seemed to put well within reach for Pyongyang. However, even for a relatively bellicose US administration, the potential damage, both physical and diplomatic, that would have resulted from a full-scale North Korean counterattack against the south meant that a limited strike was ultimately not attempted.

The US-led suppression of an enemy air defences operation, which would have been required to conduct a strike against North Korean missile and nuclear facilities with reasonable chances of success, risked convincing the leadership in Pyongyang that a full-scale invasion or decapitation attempt was underway. Since extremely aggressive and hyperbolic language has become the norm for North Korea's statements – especially on foreign armed interventions – it has long been very difficult to separate Kim Jong-un's actual red lines and willingness to use force from bluster. The periodic uses of military force against South Korean targets over decades have successfully reinforced extreme language, secretive decision-making structures, and ambiguous nuclear, biological and chemical weapons' capabilities to create an image of North Korea as not only a rogue state but one potentially willing to inflict catastrophic damage on a hair trigger – despite the clearly suicidal outcome of such an attack.

Following North Korea's display of brinkmanship in 2017, the first half of 2018 saw an intra-Korean summit in April leading to the signing of the Panmunjom Declaration, and subsequently the extraordinary summit between Kim Jong-un and Donald Trump in Singapore in June. While vague common declarations towards total denuclearisation of the Korean Peninsula were included in the outcomes of both summits, there are no concrete measures or any inspection regime being imposed on Pyongyang in return for rapid de-escalation. In other words, from a position of hopeless overall military (and economic) weakness, Pyongyang's brinkmanship, through careful use of military aggression at critical junctures while denying the US or South Korea any possibility of retaliation or disarming strikes without catastrophic consequences, have delivered a win for Kim Jong-un.

Despite the overtly self-destructive nature of any large-scale North Korean strike on South Korea, let alone Japan or US bases in Guam or elsewhere, its threats to inflict devastating damage on Seoul and the wider region were essentially believed. Kim Jon-un has developed

93. *BBC News*, 'North Korea Fires Second Ballistic Missile over Japan', 5 September 2017.

a semi-credible nuclear intercontinental ballistic missile capability and remained in power without armed intervention against his regime or weapons programmes, in direct contrast to the stated policy objectives and red lines of the US. In so doing, it has proven not only the value of perceived political irrationality in deterrent relationships, but also of an overtly offensive military posture and a ruthless attitude to using force and resorting to brinkmanship, whatever the stakes. There is a strong argument to be made that a critical part of the reason why North Korea's brinkmanship succeeded is bound up in the specific geography of the Korean Peninsula, and more specifically the regime's complex but crucial relationship with China. Both have complicated the calculations of successive US and South Korean administrations to Pyongyang's advantage. However, it does not follow that other would-be rogue states will not be tempted to try and replicate this strategy, especially if they were at least tacitly shielded by a geopolitical alignment with other major powers such as China or Russia. This would potentially increase not only the risk of nuclear proliferation, but also the demand for long-range conventional weaponry and the political aggression required to successfully deter interventions through heavily armed, apparently self-destructive brinkmanship. It may also increase the pressure on Western leaders to 'call the bluff', leading to destabilising and costly wars that neither side really wants.

The Future of Terrorism

Adam Maisel

IN THIS CHAPTER, 'terrorism' is defined as the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political ends. As such, the concept of terrorism, by its very nature, runs counter to Western military orthodoxies. Whereas a Western military is an instrument of national power (and thereby accountable to a higher national authority), terrorists lack sovereign territory (or a governing body to be beholden to) and the rigid leadership associated with traditional martial power. Further, while a conventional military is often used for deterrence and defence, terrorist organisations capitalise on the use or threat of violence to exact political outcomes. Bruce Hoffman elaborates further, stipulating that terrorism

> is specifically designed to have far-reaching psychological effects beyond the immediate victim(s) or object of the terrorist attack. It is meant to instil fear within, and thereby intimidate, a wider 'target audience,' or public opinion in general. Terrorism is designed to create power where there is none or to consolidate power where there is very little. Through the publicity generated by their violence, terrorists seek to obtain the leverage, influence, and power they otherwise lack to effect political change on either a local or an international scale.[94]

Using this definition, this chapter primarily focuses on terrorism conducted by Al-Qa'ida, Daesh and their respective affiliates. It explores the current trends and favoured attack techniques, and analyses how terrorism will endure in the future operating environment. Particular attention is paid to Al-Qa'ida and Daesh because of their intent and ability to conduct terrorist attacks within the West and against Western interests. Their selection does not discount the many other terrorist organisations; rather their capability to conduct operations regionally and globally makes them good case studies for terrorism in the future operating environment.

This chapter excludes Daesh's attempts to establish a Caliphate in Iraq and Syria. This manifestation of the group is more akin to an insurgency or pseudo-state, and cannot be classified as a terrorist organisation in the classic sense.[95] This paper does not dispute the notion of 'people's war' espoused by Mao Zedong, or its post-Mao manifestations (in which terrorism can be viewed as a phase preceding military mobile operations).[96] Daesh will here be examined in the context of terrorist activities it has attempted and executed, specifically against targets within the West. Further, groups such as Hamas, Hizbullah and Houthi rebels bear more

94. Bruce Hoffman, *Inside Terrorism* (New York, NY: Columbia University Press, 2006), pp. 40–41.
95. Audrey Kurth Cronin, 'ISIS is Not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat', *Foreign Affairs*, March/April 2015.
96. Thomas A Marks and Paul B Rich, 'Back to the Future – People's War in the 21st Century', *Small Wars and Insurgencies* (Vol. 28, No. 3, 2017), pp. 422–23.

resemblance to proxy or non-state armed groups; proxies are examined in this paper in Jack Watling's chapter 'Proxy Warfare: Iran'.

Although the number of terrorist attacks has increased globally during the 21st century, they are concentrated in a few countries – Afghanistan, Iraq and Pakistan – and do not pose an existential threat to any Western state. From 2001 to 2015, the Global Terrorism Database recorded more than 85,000 incidents of terrorism, averaging to over 5,000 incidents annually. Although the annual average of attacks is much higher than previous decades (amounting to 3,000 in the 1980s and 1990s), much of this is due to better reporting in developing countries and the classification of terrorism as a separate form of violence, even during war.[97] Nonetheless, terrorism must be considered a persistent threat to the West, and moreover a driver of instability in several states in the Middle East, Southwest Asia and Africa. This instability can potentially lead to existential threats for Western interests (for example, the impact it could have on oil and gas supplies).

Recent trends in terrorism in Europe have shown an increase in relatively unsophisticated means of attack. Of the 10 fatal jihadi terrorist attacks that occurred in the EU in 2017, eight involved vehicle-ramming, stabbing or a combination of both. The remaining two employed a suicide bomber and gunmen, respectively.[98] The use of large SUVs and commercial vehicles for the purpose of ramming public gatherings and large clusters of pedestrians has also seen an uptick globally, with five or fewer such attacks annually between 1990 and 2014, doubling in 2014, and increasing to 35 in 2015 alone.[99] Data beyond that is not yet available, preventing an analysis of whether this is a continuing trend or simply a spike accounted for by methodology.

The proliferation of unsophisticated attacks, both in Europe and globally, demonstrate the durability of simpler attack methods. The weaponisation of easily accessible and generally unrestricted items (such as commercially available vehicles and knives) is a trend that will likely continue, although the nature of attacks will change based on security measures implemented to deter such efforts. Although terrorists favour spectacle, opportunism will continue to factor heavily in the calculus of future attacks, particularly in countries with stronger counterterrorism measures in place. Moreover, spectacle and opportunism should not be conflated as mutually exclusive. In the theatre of the mind, the possibility of being run over at a Christmas market or stabbed on a daily commute can achieve similar psychological and political effects as an armed siege or series of bombings, with notably less risk of interdiction.[100]

A further evolution can be seen in the relationship between terrorist organisations and state actors. Terrorist organisations, wittingly or not, find themselves employed in the strategies of nation states. The use of terrorist groups as proxies can be particularly effective in negating

97. Brian M Jenkins, 'Middle East Turmoil and the Continuing Terrorist Threat – Still No Easy Solutions', testimony before the Committee on Armed Services, US House of Representatives, 14 February 2017.
98. Europol, *European Union Terrorism Situation and Trend Report 2018* (The Hague: Europol, 2018).
99. Cameron Reed, 'Taking Stock: What the US is Learning from Europe's Spate of Urban Truck Attacks', *Small Wars Journal*, November 2018.
100. Yuval Noah Harari, 'The Theater of Terror', *The Guardian,* 31 January 2015.

conventional and nuclear military imbalances between states. Pakistan has illustrated this since the late 1990s, demonstrating an emboldened use of proxy terrorist groups since it developed nuclear weapons.[101] More recently, it has employed Leshkar-e-Taiba to challenge India without escalating to conventional war, culminating in the coordinated Mumbai attacks of 2008. These attacks allowed Pakistan to mount military operations (in the guise of a terrorist proxy and with a veneer of deniability) against India, without escalating to conventional or nuclear conflict.[102] As states find themselves in scenarios where conventional military force provides too great a risk over reward, more will turn to the use of proxy groups (and often, terrorist organisations with shared values and grievances) as a means to implement national strategy. While this sits uneasily with the general assumption of a return to great power competition in the international security environment, it is an important claim: major power competition does not mean non-major power conflict will not occur. The examination of Iran's use of proxies and terrorist groups by Jack Watling in this paper provides sound evidence to support this deduction.

Historically, terrorist organisations have shown not just their resilience, but also their amorphous and flexible organisational architecture. The ubiquitous cell structure, resistant to penetration and dismantlement by law enforcement and counterterrorism forces, has been made ever-more resilient by the availability of end-to-end encrypted messaging platforms such as Telegraph, WhatsApp and iMessage. As RAND analysts Seth Jones and Martin Libicki observe, clandestine cellular networks are most vulnerable at their hubs (at the level of, for example, cell leader, mid-level leadership, and mid-level to senior leadership); and a network can be degraded to the point of non-operability if enough nodes are destroyed.[103] The prevalence of encrypted communications effectively hardens these hubs, complicating counterterrorism efforts, a problem aggravated by the unwillingness of tech giants to disclose keys or methods to defeat encryption.

Terrorist organisations have also shown a keen understanding of the cyber domain, including as a tool to bypass communication susceptible to interception; propagate their values and narrative; and recruit and train aspirants. Anwar Al-Awlaki of Al-Qa'ida pioneered the 'digital caliphate', publishing tens of thousands of sermons on YouTube, lacing reflections on Islamic jurisprudence with propaganda and calls for attacks against the West.[104] Daesh expanded on Al-Qa'ida's forays into exploiting the internet, using it as a means to inspire, coordinate and fund terrorist attacks.[105]

To date, the cyber attacks conducted by terrorist organisations remain simplistic, focusing principally on distributed denial-of-service attacks on government websites and hacking of

101. Kilcullen, *Out of the Mountains,* p. 103.
102. *Ibid*.
103. Seth G Jones and Martin C Libicki, *How Terrorist Groups End: Lessons from Countering al Qa'ida* (Santa Monica, CA: RAND Corporation, 2008).
104. Scott Shane, 'The Lessons of Anwar al-Awlaki', *New York Times*, 27 August 2015.
105. David P Fidler, 'Terrorism, the Internet, and the Islamic State's Defeat: It's Over, But It's Not Over', Council on Foreign Relations blog, 28 November 2017.

websites to disseminate sympathetic messaging.[106] However, terrorist organisations such as Daesh have shown aspirations to enhance their capabilities in cyberspace. In 2015, Ardit Ferizi, an ethnic Albanian hacker with connections to Daesh, accessed a US online retailer to steal the credit-card information of more than 100,000 customers. Ferizi extracted the details of customers registered with government and military emails, passing along a 'kill list' of over 1,300 individuals to Daesh, which in turn publicly released them on Twitter.[107] Going beyond traditional attempts to inspire individual attacks, Ferizi enabled Daesh to disseminate clearer targeting information for would-be attackers, and offered a harbinger of how terrorists will hone their cyber capabilities.

Former US Justice Department official John Carlin classified terrorism in two categories: 'Terrorism 1.0' used the West's tools and vulnerabilities against it (Al-Qa'ida's weaponisation of commercial airliners for the 9/11 attacks). 'Terrorism 2.0' further built on exploiting these vulnerabilities, but has effectively embraced the digital environment to recruit, propagate, target, and in some cases attack Western interests.[108] How then will 'Terrorism 3.0' manifest itself in the future operating environment?

Like its previous iterations, Terrorism 3.0 will not pose an existential threat to the West but will remain a persistent and significant concern. Further, terrorist groups will have the potential to severely threaten Western interests by posing a security risk for partner states, principally in the Middle East, Africa and Southwest Asia. Moreover, the use of terrorist organisations by states to further their own ends will continue, especially for those that suffer from an adverse military balance with their rivals. Terrorists will seek to exploit opportunities and vulnerabilities, altering their methods based on effectiveness and in response to counterterrorist measures. As the world continues to become more interconnected, and sophisticated technology is increasingly accessible to the general population, terrorists will grow their capabilities in these areas. The cyber domain will become more contested by terrorist actors, and the possibility of offensive cyber operations mounted by terrorist groups will become a reality. Simultaneously, terrorists will continue to employ methods that mark a return to the primitive;[109] using easily accessible commodities such as commercial vehicles and knives to inflict carnage and instil fear. Practitioners of warfare and national security must remain wary of these trends, despite the desire to address conventional conflict more thoroughly.

Military forces have historically had the role of protecting the people (depending on the legal frameworks of individual states): several leaders of European states have used their armies to

106. *The Telegraph*, 'Australian Airport Website Hacked by Islamic State', 13 April 2015.
107. John P Carlin, 'Inside the Hunt for the World's Most Dangerous Terrorist', *Politico*, 21 November 2018.
108. Jen Patja Howell, 'The Lawfare Podcast: John Carlin on "Dawn of the Code War"', Lawfare podcast, 24 November 2018, <https://www.lawfareblog.com/lawfare-podcast-john-carlin-dawn-code-war>, accessed 1 May 2019.
109. Brian Michael Jenkins, 'Fifteen Years on, Where are we in the "War on Terror"?', RAND Blog, 7 September 2016, <https://www.rand.org/blog/2016/09/fifteen-years-on-where-are-we-in-the-war-on-terror.html>, accessed 7 May 2019.

provide protection, deterrence and reassurance to their people in the aftermath of terrorist incidents. While it seems the presence of armed soldiers, sailors, marines and aviators has achieved the desired impact, sustaining such commitments at scale and over time has had an impact on the training and readiness of those forces for the great-power, high-intensity conflict. A more sustainable solution could be in the use of smaller, more dispersed military bases to provide persistent military presence and reassurance in a greater number of locations – much like a counterinsurgency 'ink-spot' theory, which requires deep and persistent local presence and contact with the population to retain their support, develop local intelligence and prevent other actors from occupying the space.

But employing militaries for sustained counterterrorism missions raises the unpleasant question again: should militaries prepare for war or constabulary duties? Because of the training requirements for each mission, and the much-reduced scale of Western militaries today, these are mutually exclusive roles.

Section 2

INFLUENTIAL TRENDS

Domestic Pressures: Threats to the Homeland

Elisabeth Braw

IN JULY 2018, posters started appearing around the Latvian capital of Riga, warning residents of spiders on the loose. 'Attention! Poisonous spiders!', the official-looking posters warned, advising residents to call the health authorities if they spotted any of the spiders. Latvians were predictably alarmed, many calling the authorities and many more telling their friends about the poisonous-spider invasion.

There were no spiders: the posters turned out to be a hoax.[110] But although the absence of a spider invasion on the streets of Riga was undeniably good news, the prank brutally illustrated the vulnerability of free and open societies. Produced at low cost, possibly by one person, the posters efficiently achieved three goals: sowing panic among residents; wasting the time and money of the authorities in addressing the fake spider invasion; and making Latvians doubt the ability of their institutions to keep the country safe. Although spider posters may seem to have nothing in common with tanks, today they occupy the same sphere as tools of aggression. Like soldiers and military hardware, spiders, computer attacks, and disinformation campaigns can be used to efficiently undermine societies.

Compared to invasion and occupation, non-kinetic tools of aggression are merely an irritant. Given the small monetary investment and risk involved with such forms of aggression, they can, however, be even more effective than the traditional military kind: they are harder to spot and define, and they fall below the threshold of aggression used by most Western states, including for potential NATO Article 5 commitments.

The reality is thus that malign influence and disruption of civilian life constitute an easy form of aggression. In addition to being relatively inexpensive, they can sow chaos in daily life, and they are hard to detect and punish. Most Western countries now import a large percentage of food and other daily necessities, and retailers increasingly operate using the just-in-time model, which limits stocks to a minimum and thus reduces costs. Such commercial efficiencies, however, harbour vulnerabilities. A hack on the IT systems of food retailers could quickly lead to empty store shelves. Critical national infrastructure, in turn, is in many cases part no longer owned by the government but by private companies, often foreign-based. Hacks of the power grid or transportation networks could quickly bring cities and countries to a standstill. Longer disruption could cause devastating cumulative damage. Lloyd's Insurance reports that a cyber attack on 50 suppliers to the grid covering the northeastern US would immediately leave 93

110. *LSM.lv*, 'Invasion of the Fake News Spiders!', 30 July 2018.

million people without power, with it only fully restored after two weeks. Phone systems, internet access, television and radio, street lights, traffic signals, and other services would be shut down. Lloyd's offer an assessment:

> Although only a few people are hurt in the initial incident, the long power outage does take its toll in human deaths and injury. There are many accidents resulting from the blackout, including road traffic and industrial accidents. There are people hurt in riots, looting and arson attacks. As the power cuts continue through the hot summer months, heat stress affects older and infirm people, with a rash of deaths reported in nursing homes. Backup generator failures in hospitals result in treatment equipment failing. People are reported sick from eating food that has defrosted or not been properly cooked.[111]

Enormous devastation, and yet it is not a military attack.

In an era of social media and internet news consumption, meanwhile, malign influence – 'fake news', disinformation campaigns, influence operations – knows no borders. As Russia's use of fake Facebook accounts in swing states during the 2016 US presidential election showed, malign influence can reach the population without ever intersecting the government. Indeed, old-fashioned methods such as posters can now be combined with social media: without social media and mobile phones, Riga's fake poisonous spiders would have gained far less traction.

That is precisely why traditional defence and deterrence are so ineffective against these new, non-military threats. Indeed, the digital revolution, combined with globalisation, has dramatically increased the vulnerability of Western societies to severe disruptions. This has put new pressure on the homeland, which has for the past quarter-century mostly been shielded from national security concerns. Indeed, in countries located at a distance from potential Cold War conflicts – the US, Canada, Australia and New Zealand but also Europe west of the Rhine – there must now come the realisation that for the first time in two generations the homeland faces palpable threats.

A number of governments are beginning to act, albeit only through small steps. The governments of Australia and New Zealand have blocked Huawei, the Chinese company that is the world's largest supplier of 5G networking equipment, from supplying the country's new 5G mobile network, citing 'a significant network security risk'[112] – the risk that the network could be shut down or its structure altered without the knowledge of the host country. Given the extreme reliance of modern societies on mobile telecommunications, disruptions of mobile telephony could wreak havoc on daily life and cause anger among the population towards the governments.

---

111. Lloyd's, 'Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid', Emerging Risk Report, 2015.
112. Jasper Jolly, 'New Zealand Blocks Huawei Imports Over "Significant Security Risk"', *The Guardian*, 28 November 2018; Finbarr Bermingham, 'Australia's Huawei 5G Ban is a "Hedge" Against Future Chinese Aggression, Says Former Prime Minister Malcolm Turnbull', *South China Morning Post*, 29 March 2019.

Related to such fears, the US Congress in 2018 banned Huawei and its fellow Chinese mobile telecoms provider ZTE from supplying the US government and government contractors.[113]

Perhaps predictably, however, several countries located near Russia are taking the lead in exploring solutions, partly by resurrecting their Cold War Total Defence models. During the Cold War, Sweden, Finland, Denmark and Norway maintained highly sophisticated Total Defence plans based on the notion that any territorial defence of the homeland involved not just the armed forces but all of society. The policy was partly based on the self-evident reality that the respective countries had miniscule armed forces compared to those of the Soviet Union and would – with the exception of Norway, a member of NATO – struggle to defend their countries against Soviet forces for any extended period of time. Total Defence planning, as led by the government, thus aimed to use all available means to delay the advance of hostile forces: deterrence by collective denial. In addition, Total Defence created conditions to ensure society – government and citizens' daily life – would be able to function without crippling disruption in case of war or other national crises. Today, the results of post-Cold War privatisation make it even more important for governments to work in close cooperation with the private sector, particularly in critical national infrastructure. Denmark's 2017 Foreign and Security Policy Strategy states that the Danish government should 'reach out and strengthen Denmark in collaboration with civil society organisations, the business community, universities and think tanks'.[114] Indeed, the country's Ministry of Defence has increased its crisis preparedness coordination with leading companies. Both Denmark and Estonia have a centrally placed official who acts as the respective country's Total Defence coordinator. Sweden, in turn, has significantly increased the funding and competencies of its Civil Contingencies Agency, which recently published the brochure *If Crisis or War Comes*,[115] with easy-to-understand instructions for the population, sent to every household in the country. Latvia is introducing a resilience curriculum currently being rolled out at secondary schools.

While such steps are commendable, and should be adopted by other Western states, the seamless nature of hybrid, threshold or grey-zone warfare means the West must counter it with equally seamless defence (and thus deterrence). Indeed, two major steps are required: societal resilience must be added to the political agenda, and its components clearly identified and combined to a comprehensive policy and then implemented. Some of these steps may require legislation, some merely cultural changes; responsibilities have to be assigned, but not duplicated, among government departments and ministries. Companies and the wider population must be incentivised to participate in national security. Such decisions, too, are part of implementing and improving societal resilience. Societal resilience – resilience as part of deterrence by denial – must then be paired with traditional military defence to form a unified

113. Jacob Kastrenakes, 'Trump Signs Bill Banning Government Use of Huawei and ZTE Tech', *The Verge*, 13 August 2018.
114. Mika Aaltola et al., *Societal Security in the Baltic Sea Region: Expertise Mapping and Raising Policy Relevance* (Riga: Latvian Institute of International Affairs, 2018), p. 18.
115. Swedish Civil Contingencies Agency, *If Crisis or War Comes* (Stockholm: Swedish Civil Contingencies Agency, 2018).

defence package. The phrase 'whole of society' is often mindlessly thrown about. In national security, however, it is for the most part a new field. As a result of emerging forms of warfare, not even countries that perfected Cold War Total Defence can simply dust off their old plans.

It may be depressing to note that all this needs to happen even as hybrid, threshold and grey-zone warfare are already targeting the West. In 2007, following the removal of a Soviet-era statue in Tallinn, Estonia was hit by a massive cyber attack that disrupted banks, government agencies and news media outlets.[116] Today the world is even more dependent on technology than in 2007; indeed, in 2017 NotPetya – malware created by the GRU-affiliated Russian hacker collective Sandworm, which had previously been deployed against Ukrainian government agencies and companies – hit Maersk, the world's largest container shipping company.[117] It crippled the company's IT network, causing losses of some $300 million. In addition, FedEx lost some $400 million as a result of the attack; the French construction conglomerate Saint-Gobain lost a similar amount; and Cadbury owner Mondelēz lost $188 million.[118] Consumers around the world were left without their daily goods.

Social media-fuelled fake news, meanwhile, is creating a dangerously unstable environment that can be exacerbated and exploited by an adversary. In the UK, for example, only 2% of children and young people possess the skills necessary to tell whether a news story is real or fake.[119] Put another way, the non-military aspects of hybrid, threshold, or grey-zone warfare are already harming the homeland to such an extent that increasing resilience – and thus deterrence – is imperative.

116. Damien McGuinness, 'How a Cyber Attack Transformed Estonia', *BBC News*, 27 April 2017.
117. Mike McQuade, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August 2018.
118. *Ibid*.
119. National Literacy Trust, 'Fake News and Critical Literacy: The Final Report of the Commission on Fake News and the Teaching of Critical Literacy in Schools', 2018.

Politics and Demographics in the 21st Century: Networks and Neo-Feudalism?

Sidharth Kaushal

A GREAT DEAL WAS written at the turn of the millennium that the world had entered a post-state era. In this view, the forces of the Information Age and globalisation had created an era of neo-feudalism in which the Westphalian state would be one actor among many in a field cluttered with private entities, transnational organisations and localised ethnic groups.[120] This environment, it was said, would usher in an era of post-Clausewitzian conflict in which the trinity of the people, the army and the state was no longer an effective framework with which to analyse conflict: warfare would take on a form in many regards difficult to distinguish from crime.[121]

The central flaw in this analysis was not that the trends that it identified were not real, but rather that the inferences it drew from these trends were inappropriate. The era of globalisation is not, as some have suggested, a post-Clausewitzian era in which states have been supplanted by armed bands and private organisations,[122] but one in which the nature of the state has altered to something resembling its pre-Westphalian form. The European states of the 15th century were coalition-managers who needed the support of the clergy, mercenary companies, and proxies across their borders to project power effectively. Movement towards a somewhat analogous state of affairs can now be seen across the world. As a result, states are faced with both constraints and opportunities. On the one hand, generating the resources and political will to sustain large-scale protracted conflict is likely to be more difficult than at any time since the Napoleonic era. Simultaneously, however, states can both substitute their own forces for non-state proxies, and also find allies beyond their borders more easily than might have been the case in a less information-rich environment characterised by stronger, hierarchical states. States can build supporting coalitions including both smaller states and a growing array of non-state actors, including insurgents, criminal groups and non-state political actors (for example, NGOs which, as former US Secretary of State Colin Powell noted, can act as 'force multipliers' by supporting a given state's narrative).

This has ramifications for where great powers can project force, against whom, and how. Against rival great powers, the conduct of direct operations on a large scale is likely to become

120. Kenichi Ohmae, *Managing a Borderless World* (New York, NY: HarperCollins, 1989).
121. Martin Van Creveld, *The Transformation of War* (New York, NY: The Free Press, 1991).
122. *Ibid*.

increasingly infeasible for states that will, as shown below, see their capacity to sustain such action erode. Rather, the most common form of competition is likely to be indirect, supporting rival networks of proxies in fragile states throughout the Global South.

When states do clash directly, they will have incentives to localise conflicts and, by extension, to form tacit or explicit agreements to limit their use of force. This logic of limited war may extend to cyberspace, despite the technical feasibility of all-out cyber war against an opponent's homeland. For example, Chinese strategists explicitly insist that cyber warfare must be operational (targeting military facilities) and not target an opponent's homeland because this would preclude the rapid de-escalation they hope for and bring reprisals in kind to China's own vulnerable networks.[123]

A deduction from the previous two propositions is that mobility and flexibility are likely to matter more than power. If powerful states are mutually deterred from escalating competition above certain levels, then the characteristics critical to strategic success are the ability to deploy forces rapidly to win a localised clash and the ability to provide niche capabilities (air support, for example) to networks of allies who will act as a state's primary tool of influence on the ground. The sort of approach outlined here is particularly amenable to liberal maritime powers, accustomed as they are to conceptualising strategy in precisely these terms.

The Changing Nature of the State

States have been joined in the economic, political and, to a degree the military domain by a plethora of non-state actors. In economic terms, the ability of corporations to shift their activities from one state to another has seen states (and, in some cases, local administrative units within states) compete for their presence – for example, altering their regulatory frameworks to attract investment.[124] Similarly, the provision of public services is increasingly through contracted private actors. By way of an example, in 1997 the UK introduced private finance initiatives which stipulated that contractors should take on a substantial portion of the capital costs for public projects in which they were involved, in return for responsibility for a wider array of tasks – with some tasks such as IT-modernisation identified as being beyond the capacity of the state to capitalise or research, and thus contracted out entirely.[125] The post-modern state has shifted from the business of government (the direct provision of goods and services) to governance (managing coalitions of actors to play this role).

In the security sector, this trend has manifested itself in the increasing reliance of states on private sector research and development. As the recent controversy regarding the collaboration

123. David C Gompert and Martin Libicki, 'Cyber Warfare and Sino-American Crisis Instability', *Survival* (Vol. 56, No. 4, 2014), pp. 7–22.
124. Leonard Seabrooke and Duncan Wigan, 'Global Wealth Chains in the International Political Economy', *Review of International Political Economy* (Vol. 21, No. 1, 2014), pp. 257–63.
125. Patrick Dunleavy et al., *Digital Era Governance: IT Corporations, the State, and e-Government* (Oxford: Oxford University Press, 2008), p. 197.

of Google with the US Department of Defense illustrates, private actors not wholly reliant on government orders, like the specialised arms firms of old, retain their autonomy.[126] Moreover, private actors are increasingly at the tip of the spear. Military contractors have become a ubiquitous feature of modern warfare and, in areas such as the cyber domain, states have for some time been almost wholly reliant on the private sector – with one expert noting that information warfare may well be a mercenaries' field.[127]

The structural devolution of state functions to other actors in the Information Age has been accompanied by challenges to the state and citizen identity. The late 20th century saw local and transnational identities both rise to compete with national identity. Polls from across the developed world over the past two decades indicate a steady decline in the number of people who state that their national identity is a primary identity, as opposed to either a transnational value-based community (for example, a pacifist or an environmentalist) or a parochial local identity.[128] The degree to which citizens will, in this context, sacrifice either blood or treasure for a state that no longer is a source of primary identity might then be questioned.

Of course, we should not overstate the retreat of the state in the developed world – state revenues as a percentage of GDP are significantly higher than they were in the early to mid-20th century, and states are still the single most powerful actor in interactions with smaller partners. Indeed, public–private partnerships may have enhanced the state's efficiency by eliminating wasteful redundancies in their systems. However, reliance on a multiplicity of actors, many of which are gaining greater agency in their interactions with the state and do not concede its primacy in all matters, means that what Clausewitz dubbed as 'friction' – the numerous impediments to the use of force in a direct and overwhelming manner – is now more prevalent in the minds of policymakers than ever before.

In parts of the developing world, the state is being hollowed out in an altogether different manner. The most common form of conflict since the end of the Cold War has been intra-state conflict in the developing world. This absolute and relative increase has multifarious causes. These include the withdrawal of Cold War superpower patronage; the need to alter the state's economic role to attract foreign investment, which has removed old patronage networks that sustained local economies; and the Information Age, which has reinvigorated ethnic and localised sub-state or transnational identities that had lain (for the most part) dormant while the nation state had a

126. Frank Hoffman, 'The Hypocrisy of the Techno-Moralists in the Coming Age of Autonomy', *War on the Rocks*, 6 March 2019.
127. Thomas Adams, 'The New Mercenaries and the Privatization of Conflict', *Parameters* (Vol. 29, No. 2, 1999), p. 103.
128. Pippa Norris, 'Global Governance and Cosmopolitan Citizens', in Joseph S Nye Jr and Elaine Kamarck, *Globalization and Governance* (Washington, DC: Brookings Institution Press), p. 177; Franco Zappettini and Ruxandra Comanaru, 'Bottom-up Perspectives on Multilingual Ideologies in the EU: The Case of a Transnational NGO', *Journal of Contemporary European Research* (Vol. 10, No. 4, 2014), pp. 402–22.

relative monopoly on information.[129] The salient point is that this trend is likely to both intensify and take new forms as it interacts with great-power competition. Urbanisation will concentrate populations in mega-cities, which are predicted to contain over half the Earth's population under 30 years of age by 2035, potentially straining the infrastructure of the developing world's urban centres and exceeding the capacity of public services to respond. Within these circumstances, if history is any guide, the likely providers of the public goods that national authorities cannot provide will often be criminals, warlords and strongmen ruling over localised fiefdoms.[130] The services of these actors, though they may be more criminal than political, will be invaluable to actors looking to generate influence in wartime. By way of an example, Al-Qa'ida in Iraq outsourced the task of kidnappings to local criminal gangs to generate revenue. In a similar vein, it is not unlikely that a great power looking to project power will rely on such actors to provide their forces with information and supplies and to garrison and control areas that they are already familiar with – a point noted by Russian strategists such as Vladislav Surkov and Valery Gerasimov.[131] The idea that forces should cooperate with local allies is not a new one, but the array of non-state partners, the fluidity of transactional relationships formed, and the limited aims that kinetic force will serve in this context are worthy of note.

Domestic Polarisation

The second trend that has emerged and then intensified because of globalisation is the gap between those capable of adapting to the 21st century and those left behind. As the pace of change within societies erodes or eliminates traditional ways of generating income, huge swathes of societies will be left unmoored and directionless, which will fuel polarisation. This matters because a society's capacity to maintain a political consensus determines its capacity to project force credibly. As Harry Summers notes in his analysis of the Vietnam War, military action in the absence of this cohesion is simply unsustainable in the long term.[132] While political polarisation is hardly new (the Vietnam example is an old one, after all), it is likely to intensify in an age of economic displacement and reification of political views caused by new technology. Moreover, as mentioned above, the salience of national identity has declined substantially. As such, the challenges that Summers identified will likely be more salient than ever.

This presents a challenge at the grand-strategic level. The pace of technological change has challenged one of the key underpinnings of the liberal world order, in what John Ruggie called

129. Peter Singer, 'Corporate Warriors: The Rise and Ramifications of the Privatized Military Industry', *International Security* (Vol. 26, No. 3, Winter 2001–02), pp. 186–220.
130. Christopher Coker, *Future War* (Cambridge: Polity Press, 2015).
131. Peter Pomerantsev, 'How Putin is Reinventing War', *Foreign Policy*, 5 May 2014; Kier Giles, 'Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power', Research Paper, Chatham House, London, 2016.
132. Harry Summers, *On Strategy: A Critical Analysis of the Vietnam War* (New York, NY: Random House, 1995).

its 'embeddedness in local politics'.[133] In 1950 the average American had an incentive to care about what happened in Europe, for example, because exports to Europe constituted their own bread and butter. Moreover, expansive welfare states and institutions such as trade unions created a compromise between market forces and societies that was relatively stable. Grand ideological narratives, such as the Washington Consensus, were viable precisely because they were well aligned with the local interests of people who cared little for the long arc of history. As the current century progresses, however, this is increasingly untrue for significant proportions of many societies.

Those segments of a society that are dependent on and benefit from a viable globalised economy, such as the well educated, still have a stake in the order that underpins it. However, many people see globalisation as having eroded rather than enhanced their own lives. This represents not a failure of the liberal world order per se, but an oversight of the key fact that as economies technologically innovate, they become less dependent on the labour of most citizens to function – such is the nature of efficiency itself. For example, a study by McKinsey estimates that by 2030, 35% of manufacturing jobs in the developed world will be lost to automation.[134] In an age of polarisation it will be more difficult to convince sceptical publics that are largely concerned with parochial issues to support the expenditures that accompany a strategic effort. If exploited by opponents skilled in information warfare, social divisions could be an even greater impediment to force projection and the maintenance of a coherent and stable grand strategy.

Challenges and Opportunities for Great Powers

The diffusion of power to a multiplicity of actors has thus both enhanced and weakened powerful states. Powerful states are the only entities that can coordinate large coalitions of disparate actors and use the loyalties of proxies and private actors to project power cheaply. On the other hand, the challenges of securing the transient loyalties of these players, and the managerial challenge posed by the need to leverage increasingly complex domestic coalitions, means that the capacity of the state to wage long, drawn-out conflict has eroded relative to the 20th century.

A caveat might be added here. In a 2018 publication, the US Department of Defense identified a category of state that it dubbed 'digital authoritarian states' that might actually have their power enhanced by the digital age.[135] The technologies that abet fragmentation in either an open or a weak society can enhance the control of a strong centralised state capable of centrally directing managing information flows. Big data, artificial intelligence, and increasingly ubiquitous surveillance of nationally controlled information ecosystems could reinforce the power of such

133. John G Ruggie, 'Embedded Liberalism and the Postwar Economic Order', *International Organization* (Vol. 36, No. 2, 1982), pp. 379–415.
134. James Manyika et al., 'Jobs Lost Jobs Gained: Workforce Transitions in a Time of Automation', McKinsey Global Institute, December 2017.
135. Nicholas D Wright (ed.), 'AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives', White Paper, US Department of Defense Joint Staff, 2019, pp. 20–35.

states. However, such states – although more capable of securing the political quiescence needed for decisive action than either of their post-modern or developing counterparts – have their own barriers to resource extraction for military ends. For example, as Michael Beckley points out, estimating the power of states such as China using GDP excludes the input costs of generating output in an inefficient centralised context, the rising costs of human welfare, and the costs of maintaining internal security (especially in an authoritarian context).[136] As such, Beckley argues, the capacity of a centralised state to rapidly generate and sustain the income needed for war-making for expansive ends against a rival great power is questionable. As such, then, centralised states are as constrained as their post-modern counterparts – albeit for different reasons. The emphasis of Chinese strategists on fighting local, limited wars would seem to validate this point.[137]

The Future of War

Does this mean that great-power competition is impractical, then? Arguably not. Rather, if an analogous period is any guide, we are likely to see long-running competition between states that is characterised by limited direct conflict for limited stakes; indirect feuding through proxies; and relatively fluid networks of state and non-state actors forming kaleidoscopic alliances. As the feudal era progressed, those states capable of securing internal cohesion – such as France under Louis XIV and Sweden under Charles XII – were able to command networks based on loyalties such as religion or ethnicity alongside purely transactional relationships with mercenaries and warlords in the more fragile, less united parts of Europe such as Germany and Italy. Developments such as the printing press – and with it a deluge of easily accessible, often inflammatory, religious and political literature – made weaker societies more volatile and created narratives that allowed segments of their populations to be co-opted by great powers. As such, easy access to information, and the social fragmentation it wrought, made the indirect use of force an appealing option to states that were too internally constrained to use direct force for anything but the most limited ends. Of course, any analogy has its limits, and there are many contextual differences between the late feudal era and today. However, potential futures can be usefully identified by way of an analogy with another period in which states existed alongside multiple sub-state actors (including guilds, mercenaries and the clergy) and could not readily draw on their publics to sacrifice themselves en masse in the name of an overarching identity, and had to cope with an information revolution.

Social changes thus point to an increasing emphasis on the sort of indirect, limited conflict seen in the pre-Westphalian era. States which cannot use force for large-scale, direct conflict without eroding their own domestic consensus will have to rely on the use of proxies and private actors such as mercenaries to compete for influence over fragile, divided societies which lack a strong state. When force is used directly, it will likely be in limited offensives in support of proxies

136. Michael Beckley, *Unrivaled: Why America Will Remain the World's Sole Superpower* (Ithaca, NY: Cornell University Press, 2018), pp. 55–60.

137. M Taylor Fravel, 'China's New Military Strategy: "Winning Informationized Local Wars"', *China Brief* (Vol. 5, No. 13, July 2015).

and private actors in competition with another great power and its own network of proxies. The jockeying between multiple great powers and their respective proxies in Syria is a case in point. Unlike proxy conflicts of the Cold War, moreover, the stake is not control of the state but select portions of it (the Russian and Syrian offensive focused exclusively on consolidating the regime's control of parts of Syria, for example). Absent the Cold War's overarching ideological narratives, alliances are relatively fluid and liable to change – consider, for example, the Iraqi Kurdish leadership's willingness to work with both the US and Iran at different junctures. What is unlikely to be seen, however, is direct high-intensity conflict between states. To the extent that the forces of great powers clash directly, it will be in limited skirmishes. Even in potential theatres of great-power war, such as the Western Pacific, strategists plan for short, sharp engagements followed by de-escalation. Indeed, the PLA explicitly builds de-escalation into its war planning at all levels when considering conflict with the US. Thus, for example, the fact that the DF-21D anti-ship ballistic missile can achieve a mission kill without sinking a carrier is cited as a major advantage for its 'counterintervention' role: it can cripple a response while not doing so much damage, and so make rapid deconfliction possible.[138] This is partially due to the inherent risks of great-power war, but also because few great powers can guarantee the level of societal cohesion and resources needed to prosecute a protracted conflict in the modern era.

Conclusion: The Era of Transactions, Flexibility and Agility

These changes are likely to give rise to an order which, like the pre-Westphalian order, is one of persistent low-level conflict between state-led networks. Crucially, low-level conflict is not bloodless – protracted competition can kill more people over a long time than wars of decisive battles. Proxies or smaller states may well switch flexibly between these networks based on situational needs. In a context where no clear ideology exists to either delineate permanent friends or enemies, or to galvanise publics to support long-term commitments, the conduct of warfare is likely to revolve around the use of indirect means and very limited direct force in the fragile states of the developing world.

Given that, for great powers at least, the kinetic phase of conflict will by necessity be brief and the object of military force will be to support a coalition of proxies and private actors, mobility rather than raw power is of the essence. Being able to deliver decisive support to key allies for limited periods of time – as Russia's Caspian flotilla did in support of Bashar Al-Assad's regime during the siege of Aleppo – will be more important than mobilising for protracted conflict with peer competitors. To the extent that the forces of great powers do clash, it will likely be in localised contexts in which each party restricts its use of force and duration. As such, the mobility needed to generate favourable local force balances will matter more than the aggregate balance of power between states. Forces will likely need to be structured accordingly, with rapid-deployment forces and maritime power projection playing a particularly critical role in a state's force posture.

138. Andrew S Erickson, *Chinese Anti-Ship Ballistic Missile (ASBM) Development: Drivers, Trajectories and Strategic Implications* (Washington, DC: Jamestown Foundation, 2013), p. 45.

In some senses, this is a form of warfare familiar to maritime powers accustomed to eschewing cumbersome armies for forces that could be rapidly deployed to a conflict at a critical juncture or a vital location.

Space, Strategic Advantage and Control of the Military High Ground

Alexandra Stickings

'IF YOU CONTROL space, you can also control the land and the sea': these words, spoken by the commander of the People's Liberation Army Air Force,[139] highlight the recognition of the role of space in military operations. It also reflects a sense of space as the 'new' high ground to be contested in future conflicts. How space, and space power, are conceptualised as orbital activities continue to evolve will have ramifications for future conflicts. This is an important consideration for the West as its potential adversaries increase their space and counter-space capabilities.

Since the launch of the Sputnik satellite in 1957, space has become increasingly militarised.[140] Throughout the Cold War and the space race, the US and the USSR led the way in exploiting space for military purposes. Recognising the potential for space to be used for destructive purposes, the 1967 Outer Space Treaty banned the placement of nuclear weapons or other weapons of mass destruction in space and stated in Article 1 that activities in space 'shall be carried out for the benefit and in the interests of all countries'. However, compliance with this provision has been a somewhat grey area. Satellites support military communications and intelligence, surveillance and reconnaissance (ISR), and weather satellites provide crucial operational information. Global Navigation Satellite Systems, such as the US Air Force-operated Global Positioning System (GPS), provide precise signals that are used for, among other things, maritime navigation, missile targeting, and autonomous systems, and are essential for propagating the precision upon which Western warfighting is based.[141] It is evident, therefore, that space has become almost completely integrated into all military activities. Space, or more importantly the information it provides, is now the force multiplier with perhaps the greatest impact.

---

139. Alan Dowd, 'Defending the High Ground', American Security Council Foundation, November 2012, <https://ascfusa.org/defending-the-high-ground/>, accessed 24 January 2019.
140. For the purposes of this chapter, 'militarisation' is taken to mean the use of space for military purposes and the positioning in space of military assets. Militarisation can also be defined as 'the build-up to a state of war, including any activity in pursuit of this'. See, for example, Joseph Noronha, 'Seizing the Ultimate High Ground: The Growing Military Exploitation of Space', *Indian Defence Review* (Vol. 33, No. 1, January–March 2018).
141. Paul Barnes and Alexandra Stickings, 'The Death of Precision in Warfare?', *War on the Rocks*, 27 November 2018.

Space: The Ultimate High Ground?

The high ground, a position of advantage or superiority, has long been an aspect of military strategy. But what constitutes the high ground has changed throughout history. Sun Tzu in the *Art of War* and other thinkers, particularly those before powered flight, described it in a literal sense, with higher ground offering the advantage over enemies attacking from below. With the beginnings of air power, there were moves to declare this as the new high ground[142] – although its limitations were evidenced by its supposed failures to decisively determine campaigns in the Second World War, Korea, Vietnam, and Iraq.[143]

It may seem obvious, then, that this argument would move to space. In what ways, therefore, can space be seen as the 'new' high ground? Space is sometimes declared as the 'ultimate high ground' without any underlying discussion of what this means and how it has been conceptualised. The concept of high ground needs to be understood in terms of strategic advantage. In this sense, space provides communication for command and control, enabling joint communications and the distribution of orders to the field.[144] Satellites provide arguably the most important enabler in modern war: real-time, on-demand information;[145] and space systems allow for global communication and information access unhindered by geographic and political boundaries.[146] This sets it apart from air power and means it does not face the same limitations. Space as the high ground is about its role as an enabler of operations – rather than acting operationally in and of itself – and acts in support of land, air and sea forces.

Yet there are still questions over how this idea of a new high ground affects military planning and doctrine. Specifically, if space is indeed the ultimate high ground, it is both an operational and strategic asset cutting equally across land, air and sea; yet the way in which military space activities are conceptualised does not entirely reflect this reality.

Space: Domain or Enabler?

The understanding of the central role that space plays across all military activities has manifested itself in the consensus in the West, following the lead of US doctrine, that space is a domain or environment of warfare alongside the traditional domains of land, sea and air. Perhaps the most direct interpretation of this is the proposal in the US to create a Space Force as a

142. David K Edmonds, 'In Search of High Ground: The Airpower Trinity and the Decisive Potential of Airpower', *Air and Space Power Journal* (Spring 1998).
143. William J Astore, 'Air Power is Unlikely to Solve America's Problems', *The Nation*, 21 June 2016; Daryl G Press, 'The Myth of Air Power in the Persian Gulf War and the Future of Warfare', *International Security* (Vol. 26, No. 2, Fall 2001), pp. 5–44.
144. A J Bosker, 'Space is the Ultimate High Ground', *Air Force Print News*, 27 May 2003, <https://www.af.mil/News/Article-Display/Article/139149/space-is-ultimate-high-ground/>, accessed 24 January 2019.
145. Dowd, 'Defending the High Ground'.
146. Bill Posey, 'Space: The Ultimate High Ground', *SpaceNews*, 24 February 2014.

separate armed service,[147] taking the majority of space activities from their current home in the US Air Force. The UK regards space as a domain that requires a level of strategy, planning and personnel concomitant with its national ambition as a global power: yet currently there is no suggestion that responsibility for military actions in space require a new and separate organisational structure.

Decision-makers in the US continue to wrangle over the optimal solution to the Space Force conundrum, where much debate has led to the current proposal for a Space Force that would sit within the Department of the Air Force, which has yet to pass Congress, the two other military space powers of Russia and China continue to move forward with organisational changes that place space in the larger framework of information, and importantly, within the concept of information dominance. Rather than a discrete domain, space is one element of information, alongside cyber and propaganda, that cuts across the three traditional domains of land, sea and air. An example of this thinking can be seen in the 2016 reorganisation of the PLA with the creation of the Strategic Support Force, under which sits the majority of space capabilities, alongside cyber and electronic warfare.[148]

In trying to assess the nature of space in defence there is a tendency towards technological determinism. Although technological development has impacted every area of warfighting, it is perhaps most apparent with space. Access to and operating within space at all is not possible without a relatively rare level of technological capability. Similarly, there is in part a focus on those who assess space conflict on new developments, of either civilian or military origin, tending towards analysis that emphasises what actors can do, rather than what certain actions would actually mean.

All of this points to a central weakness in how militarised space is conceptualised and, consequently, how space power and the nature of conflict in space are defined. The idea of space as a 'global commons' leads to obvious comparisons with the sea and attempts to both define space power and understand international norms and agreements through the same lens. However, this concept has been challenged, in part because of the difficulty in applying terrestrial legal norms to space.[149] One possible answer is to approach space not from within the framework of international-relations theory, but through theories of war. By looking at space within the broader concept of war it will be easier to interpret the actions and intentions of states and assess whether these actions are hostile in nature. This is particularly relevant as the major states move towards non-kinetic capabilities that near the threshold of what is

147. *BBC News*, 'Trump Space Force: US to Set up Sixth Military Branch', 18 June 2018.
148. Kevin L Pollpeter, Michael S Chase and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation, 2017).
149. Marcia Smith, 'Pace Outlines Trump Administration's Approach to Space Development and Law', *Space Policy Online*, 13 December 2017, <https://spacepolicyonline.com/news/pace-outlines-trump-administrations-approach-to-space-development-and-law/>, accessed 22 April 2019.

considered to be a space weapon. Understanding this debate is essential for analysing how war will play out in space in the medium to long run.

Threats and Vulnerabilities

Whatever the outcome of the 'space as a warfighting domain' debate, reliance on space, both for military purposes and for the other national-security and civilian purposes which it supports, is unlikely to decrease. Yet space systems face a variety of threats and hazards which could affect the access to and use of space. The unique environment of near-Earth orbit presents a number of challenges. For example, space weather – solar activity and the associated radiation and high-energy particles it emits – can cause damage both to satellites and the ground stations on which their operation depends.

Space has also become more democratised. As more actors have started space operations, whether civilian or military, orbits – particularly low Earth orbit (LEO) – have become more congested. It is estimated that, on top of the nearly 2,000 functioning satellites, there are over 170 million pieces of debris larger than 1mm, any of which can cause damage.[150] This is a problem which affects each user of space equally: no satellite would be immune to the effects of a chain reaction of collisions.

As states look to ensure their continued access to space, they also recognise the benefits of denying this access to their adversaries, particularly in times of crisis or conflict. Anti-satellite missiles were tested by the US and the USSR during the Cold War,[151] and China and India[152] have since demonstrated missile capabilities. However, the means of attacking satellites have diversified, and now include cyber attacks, high-powered lasers, and electronic warfare that could all disable or disrupt a satellite.[153]

In short, space assets are vulnerable. Understanding their importance is vital to ensure their resilience and to put in place mitigation in the event of their loss. The reliance on such assets also highlights the issue of trust by those who use these assets – both in the information provided by a system and in the ability of the system to continue to operate. Placing trust in vulnerable, interconnected systems to provide strategic advantage is a potential weakness.

---

150. On satellite numbers, see, Timothy Maclay, Walt Everetts and Doug Engelhardt, 'Responsible Satellite Operations in the Era of Large Constellations', *SpaceNews*, 23 January 2019. On debris, see European Space Agency, 'Space Debris by the Numbers', <https://www.esa.int/Our_Activities/Operations/Space_Debris/Space_debris_by_the_numbers>, accessed 24 January 2019.
151. Brian Weeden and Victoria Samson (eds), 'Global Counterspace Capabilities: An Open Source Assessment', Secure World Foundation, April 2018.
152. Carin Zissis, 'China's Anti-Satellite Test', Council on Foreign Relations, 22 February 2007; Jeff Foust, 'India Tests Anti-Satellite Weapon', *SpaceNews*, 27 March 2019.
153. Todd Harrison, Kaitlyn Johnson and Thomas G Roberts, 'Space Threat Assessment 2018', Center for Strategic and International Studies, 2018.

The Future of Space Warfare

It is a common belief that space will play a central role in future great-power conflict;[154] as militaries increasingly rely on space, and space capabilities proliferate, it is difficult to foresee any conflict in which space does not play a vital role. Yet predicting how conflict in space, whether in concept or in reality, will unfold is inherently uncertain. Questions include how a hostile act in space will be recognised – if indeed it can be, considering the difficulties in attribution within the space environment; and what a response, in space or terrestrially, will look like. Much will depend on how the proposed US Space Force develops and the way in which this affects the keen balance between the military ambitions of the US, Russia and China. While significant international agreement on responsible space activity and preventing 'weaponisation' is unlikely – at least within the current global climate – this is not to say that full-scale conflict in space is inevitable. Should plans for activities such as asteroid mining and on-orbit construction become a reality and pose challenges, and the Outer Space Treaty's provisions on the peaceful use of space are pushed to their limits, the more extreme scenarios of conflict in space should still be discounted.

Although the Outer Space Treaty does not have enforcement mechanisms and allows actors to operate within a rather large grey area, it is unlikely that a claim to, for example, the Moon by a single state is feasible. Sovereignty in space will be confined to satellites and other platforms. The physical nature of any space conflict will not see any substantial change, with states aiming to protect their assets from deliberate and accidental damage while developing methods to deny their adversaries from accessing the information provided by space assets.

Space has become so embedded into global military thinking that any state underestimating this and becoming complacent is likely to be at risk of losing it. Although the US has exercised simulated, GPS-denied environments,[155] these have been limited in scope and only address one of the areas in which space plays a role. Conceptual arguments regarding domains, the high ground and force multipliers may seem unnecessary, but are essential for reaching consensus on what military space activities are needed and how they should be organised within the defence framework to ensure effectiveness of action. It is this that will allow the West to be on the best footing for responding to space-based aggression and conflict in the coming decades.

154. Sarah Knapton, 'Star Wars: How Future World Conflicts Will be Decided in Space', *The Telegraph*, 19 December 2015.
155. Daniel Cebul, 'DoD Jams GPS in Western States for Joint Exercise', *C4ISRNET*, 26 January 2018.

Into the Ether: Considering the Impact of the Electromagnetic Environment and Cyberspace on the Operating Environment

Ewan Lawson

THIS CHAPTER CONSIDERS the potential significance of both the electromagnetic environment (EME) and cyberspace on the operating environment for the UK and other Western militaries. It does not engage with the doctrinal debates about whether the EME and cyberspace are domains of warfare or environments, neither does it explore the precise relationship in military organisational terms of cyber- and electronic warfare. While there have been efforts at doctrinal and organisation integration in Western militaries as Cyber and Electromagnetic Activities, they are still nascent and contested.

Potential adversaries of the West, however, conceive of both EME and cyber as parts of information warfare. This chapter focuses on the developments of some of those potential adversaries. It assumes, based on other chapters in this paper, that those potential adversaries will seek to stay below the threshold of conventional military conflict in order to counter Western military strength. This is, in part, through the use of information warfare at both the theatre and strategic levels. In this way, the operating environment for the British military can no longer be confined to the theatre but extends to the home base.

This chapter briefly considers the post-Cold War development of electronic and cyber warfare, before assessing developments in Russian approaches – particularly in Crimea and Eastern Ukraine. It then turns to China's capability modernisation and the significance of the EME and cyber as part of an anti-access area-denial (A2AD) strategy, most notably in the South China Sea, before considering a smaller power in the form of Iran.

It is important to first consider the context for Western military force in the nearly three decades since the end of the Cold War. Potential adversaries have noted the potential lethality of Western military force and therefore seek to avoid direct confrontation. But they have also noted the continuing and deepening reliance on the EME and cyberspace for critical operational functions of those forces. Across a range of activities – including the need to gather, analyse and share information quickly, control autonomous systems, and command geographically dispersed

forces – that reliance impacts across the joint force.[156] For much of this post-Cold War period, Western forces have fought in conflicts where the enemy had a limited electronic-warfare capability and therefore many of those capabilities and skills necessary to compete in the EME have atrophied. At the same time, Western societies have become increasingly dependent on the EME and cyberspace for almost all everyday activities – generating huge benefits for society, but also creating a web of potential vulnerabilities.

When considering Russian capabilities, it is important to recognise that, unlike most Western powers, it has a broad understanding of information warfare that avoids the doctrinal separation between information operations, electronic-warfare and cyber operations.[157] On the other hand, in the post-Soviet era, Russia's electronic-warfare capabilities – along with the rest of its military – went into a serious decline. While military modernisation had restarted by 2008, the conflict in Georgia over South Ossetia that year highlighted some of its weaknesses in the EME. Although the Georgian army reportedly suffered massive interference with its radio communications, the Russians were unable to counter its air-defence systems and lost a number of aircraft as a consequence.[158] This campaign was noted as being the first to demonstrate the integration of cyber with conventional military operations: Georgian websites were defaced, or blocked by denial-of-service attacks; and the Georgian government found it near-impossible to communicate with its own citizens and the outside world.[159] Much of this activity was attributed to so-called 'patriotic hackers', although the degree of coordination and the sophisticated tools used point to at least some involvement of the Russian state. This was an early example of the way in which the cyber vulnerabilities of the home base are likely to be exploited.

Lessons from the Georgian experience have impacted on the Russian military modernisation programme, not least in the EME. Some have identified the development of a doctrine of 'radio electronic combat' designed to 'limit, delay or nullify the enemy's use of [their] command and control systems whilst protecting Russian systems through electronic counter measures'.[160] The aim is therefore threefold: to disrupt enemy command, control and communications; to counter their ISR capabilities; and to defend against enemy precision munitions.[161] The aim was to return to Cold War levels of relative power in the EME, with 60% of electronic warfare equipment being upgraded by 2020.[162]

156. US Department of Defense, 'Electromagnetic Spectrum Strategy', 2013.
157. Aaron Brantly and Liam Collins, 'A Bear of a Problem: Russian Tactical Cyber Operations', *ARMY Magazine*, 28 November 2018.
158. Laurie Moe Buckhout, 'Modern Russian Electronic Warfare', *ISITREP* (Q1 2016).
159. David Hollis, 'Cyberwar Case Study: Georgia 2008', *Small Wars Journal*, 6 January 2011.
160. Buckhout, 'Modern Russian Electronic Warfare'.
161. Igor Sutyagin with Justin Bronk, *Russia's New Ground Forces: Capabilities, Limitations and Implications for International Security*, RUSI Whitehall Paper 89 (London: Taylor and Francis, 2017), p. 81.
162. Buckhout, 'Modern Russian Electronic Warfare'.

So, what does this look like in practice? Building on the lessons identified in the Georgian campaign, Russia has had the opportunity to use its campaigns in Ukraine and Syria as the perfect testing ground for its modernising capabilities. During the occupation of Crimea, Russia again launched denial-of-service attacks and defaced government websites, plus a physical attack to break the fibre-optic connection between the peninsula and the rest of Ukraine. It also attacked the telephone system used by officials and ministers, and jammed Ukrainian naval communications.[163] As the campaign in Eastern Ukraine has progressed, there has since been evidence of both UAVs and ground stations being used for EME reconnaissance and jamming of satellite, cellular and radio communications – along with GPS spoofing and electronic-warfare attacks against both Ukrainian and OSCE UAVs. There is also evidence that Russian forces have become adept at identifying Ukrainian locations by their electronic signatures, and then using this for targeted propaganda text messages and cueing destructive fires.[164] While there was reporting in 2016 that the Russian hacker group Fancy Bears had hacked an Android app used by Ukrainian artillery units, causing the destruction of some 80% of its guns, this figure was later reduced to 15–20%.[165] However, this is still a valuable example of the vulnerabilities that are inherent in some software and is a reminder of the importance of cyber defence.

Where Russia has exploited combat opportunities to develop its capabilities in EME and cyber, China has fewer opportunities to test its modernised tactical capabilities. But it does have a military modernisation programme and, like Russia, emphasises the importance of information in warfare. While much of the focus has been on China's modernisation of traditional warfighting capabilities – such as fifth-generation aircraft, aircraft carriers, railguns, and 'carrier killer' ballistic missiles – it has in parallel been establishing a significant electronic-warfare and cyber capability.[166] China has also maintained a significant cyber espionage and intellectual-property-theft effort; indictments issued in 2014 by the US Department of Justice alleged this was led at least in part by soldiers from the 3rd Department of the People's Liberation Army (3 PLA).[167] However, the PLA effort to develop capabilities for the future information battlefield goes further.

While 3 PLA has clearly been given a key role in cyber espionage, cyber warfare is the responsibility of its sister department, 4 PLA. Traditionally 4 PLA was responsible for electronic warfare, but has recently taken on the responsibility for computer-network attacks as part of the adoption

163. Margarita Jaitner, 'Russian Information Warfare: Lessons from Ukraine', in Kenneth Geers (ed.) *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn: NATO CCDCOE, 2015).
164. Brantly and Collins, 'A Bear of a Problem'.
165. Oleksiy Kuzmenko and Pete Cobus, 'Cyber Firm Rewrites Part of Disputed Russian Hacking Report', *Voice of America*, 24 March 2017.
166. James Johnson, 'China's Vision of the Future Networked Battlefield', *The Diplomat*, 26 April 2017.
167. US Department of Justice Office of Public Affairs, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage', press release, 19 May 2014.

of an offensive information warfare doctrine named Integrated Network Electronic Warfare.[168] 4 PLA is authorised to undertake electronic-reconnaissance tasks as well as computer-network exploitation to identify opportunities for disruptive or destructive effects – although it is not clear where the boundaries are between it, 3 PLA, and some civilian agencies. It also has responsibility for some electronic-countermeasure units and also research institutes focused on developing techniques to counter Western command, control and communication, and ISR systems.[169]

A further step in China's capability development has been the establishment of the PLA Strategic Support Force which seeks to bring together the PLA's space troops (recognition and navigation satellites) with cyber-troops (offensive and defensive) and electronic warfare (jamming and disrupting radars and communications).[170] Details of what this means in terms of capability in the field are hard to come by at the time of writing, as are the organisational implications, but there is little doubt that China will have learned from Russia's activities, both successes and failures, in Ukraine and Syria. Given its apparent strategic focus on A2AD capabilities designed to keep Western forces as far from its shores as possible, it is no coincidence that it has developed infrastructure on disputed reefs in the South China Sea, with reports suggesting that along with anti-ship cruise missiles and surface-to-air missiles it has also deployed electronic-warfare equipment.[171] It is as important to deny access to the EME as it is to physical space.

While it is unsurprising that major powers have been developing cyber- and electronic-warfare capabilities, there are similar developments in second-tier states. A combination of the aftermath of the Stuxnet attacks on the Iranian nuclear programme, hostile activity against Iran by Israel Wiper and Flame malware, and an inability to procure conventional capabilities due to sanctions have together meant that Iran has identified offensive cyber operations as a valuable tool.[172] Unlike China and Russia, this effort has been relatively disorganised and moderately funded, which has placed a ceiling on its cyber capabilities and ability to threaten opponents. This has led to the development of an ecosystem of diverse, state-aligned operators, with different capabilities and affiliations – including groups that appear from nowhere and then disappear when identified by cyber-security researchers.[173] While this is clearly a more ad hoc approach, its actors still report to either the Ministry of Intelligence or the Islamic Revolutionary Guard Corps.

Aside from cyber espionage, Iranian efforts have been disruptive or destructive, and although perhaps not visibly dramatic, have succeeded in imposing significant costs. In 2012, Operation

168. Mikk Raud, 'China and Cyber: Attitudes, Strategies, Organisation', NATO Cooperative Cyber Defence Center of Excellence, <https://ccdcoe.org/library/publications/china-and-cyber-attitudes-strategies-organisation/>, accessed 23 April 2019, p. 23.
169. *Ibid*., p. 24.
170. *Ibid*., p. 25.
171. Amanda Macias, 'China is Quietly Conducting Electronic Warfare Tests in the South China Sea', *CNBC*, 5 July 2018.
172. iHLS, 'Iran's Cyber Capabilities Reflect Unique Internal Ecosystem', 7 January 2018.
173. Collin Anderson and Karim Sadjadpour, 'Iran's Cyber Threat: Espionage, Sabotage, and Revenge', Carnegie Endowment for International Peace, 2018, p. 2.

Ababil targeted the US banking system with a long series of denial-of-service attacks, and Shamoon malware caused hundreds of millions of dollars of damage to the oil company Saudi Aramco.[174] Although there was a relative lull in this activity while the US remained party to the Iran nuclear agreement, an attack in 2018 on a Saudi petrochemical facility using Triton malware – apparently designed to be destructive, although it failed – may be evidence of potential cooperation in offensive cyber between Russia and Iran.[175] This may reflect closer links resulting from cooperation during the conflict in Syria, and is also likely to be reflected in military electronic-warfare capabilities. This is an area in which Iran has already demonstrated ability, having brought down a US drone in 2011 apparently through electronic-warfare techniques using Russian-supplied equipment.[176]

It would appear therefore that Western militaries, including the UK, will face challenges in the EME and cyberspace that impact on the ability to prosecute operations across the battlespace from deep, to near, to rear. Concurrent civilian requirements for access to the EME will mean it is increasingly congested, while adversaries will ensure that it is contested. In cyberspace, ethical and legal concerns will also mean that the freedom of operation for the UK and its allies is likely to be constrained in ways that may not apply to those adversaries. These are challenges that the UK must consider as it develops the Joint Force over the next decade and beyond. While some investment in electronic warfare and cyber equipment will be needed, there are a number of other measures that need not be expensive; procedures and practices can help minimise the risks. Such measures were standard during the Cold War and must be again, and they should also be exercised and evaluated regularly.

Finally, there is a need to recognise that the operational theatre and the home are now indivisible. Resilience needs to be built both within the Joint Force and also at home to guard against disinformation of the kind that targeted the families of soldiers in Ukraine.

174. *Ibid*., pp. 23 and 33.
175. David E Sanger, 'Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute', *New York Times*, 23 October 2018.
176. Scott Peterson, 'Downed US Drone: How Iran Caught the "Beast"', *Christian Science Monitor*, 9 December 2011.

Technological Trends

Justin Bronk

THE CLOSE INTERRELATION between the practice of warfare and the technology of the day is as old as warfare itself. This chapter examines the most influential trends that the author believes will differentiate the future operating environment of the mid-to-late 2020s from the present. It cannot be comprehensive or definitive. There are many technologies not tackled – including strong AI-enabled weapons systems, human bio/genetic enhancement, and nanotechnology – predominantly because it judges that the large-scale deployment of such technologies within mainstream military forces sits in the 2030s timeframe rather than the 2020s.

Sensors and Post-Processing

The first and perhaps most dominant technology trend which is likely to define the mid-to-late 2020s battlespace is the proliferation, increasing sophistication, and multi-spectral nature of sensors in all domains and on both sides of state-on-state and even asymmetric conflicts. This trend – already evident and accelerating – is driven not only by advances in sensor technology, but also the enormous increases in processing power, data-storage capacity, and network bandwidth, all of which have enabled post-processing of sensor data and multi-spectral sensor fusion to become common practice.

Examples include the use by fighter aircraft of infra-red scan and track (IRST) sensors for reliable beyond-visual-range acquisition, target identification, and engagement, and the use of ground-based multi-static passive radars by Russia (among others).[177] IRST uses super-cooled lenses to search for and classify incredibly faint heat sources at long range while passive radars use echoes in the background electromagnetic 'noise' of mobile-phone, television and radio transmissions (among others) to track aircraft without needing a primary radar emitter. For both these techniques, the extremely faint nature of the signals which are being tracked and huge number of false-positive readings and background clutter of one sort or another means that their practicality as operational tools is linked directly to the post-processing hardware and software available to refine the raw sensor data into a usable picture. With modern computing power and availability, many sensor techniques previously considered impractical are becoming usable and, in some cases, increasingly significant threats for assets such as stealth aircraft,

177. For IRST detail for example of Eurofighter Typhoon, see Justin Bronk, 'Maximising European Combat Air Power', *RUSI Whitehall Report* 1-15 (2015), pp. 5–6. For detail on Russian passive multi-static radar techniques, see J R Wilson, 'New Frontiers in Passive Radar and Sonar', *Military and Aerospace Electronics*, 8 February 2016.

and potentially even submarines, which rely on remaining hard to detect for survivability. As available computing power continues to increase, so will this trend.

Many such exotic detection technologies – such as wake-vortex tracking, quantum radar, three-dimensional metre- and decimetre-wavelength AESA radars and LEO infra-red scan-and-track techniques – have serious limitations when used as primary sensors as they have limited capacity to generate target-grade weapon cueing data. However, they offer advantages in detecting threats which are difficult to track using standard X- and Ku-band radars and can be extremely useful for cueing in other higher-resolution sensors if adequately integrated into a common system or picture. At present it remains difficult to successfully fuse and cross-reference sensor data from multiple different arrays, especially if they are operating across different parts of the electromagnetic spectrum. The F-35 fifth-generation fighter aircraft is one of the first assets designed to be capable of cross referencing and internally analysing data gathered by multiple sensors in real time before presenting a single coherent picture to the operator. However, in future this approach will undoubtedly become standard practice for many high-end military forces around the world – especially in naval and land applications less constrained than air platforms by limitations of space, weight and power/cooling capacity.

Advances in sensor resolution, post-processing and multispectral fusion techniques, coupled with a growing variety of large and small platforms in all four domains which can act as ISR nodes, suggests that survivability through evasion alone will become an increasingly risky proposition for assets throughout the battlespace. However, it also means that those assets are themselves likely to have greater situational awareness than ever before. If all players on the battlefield are in possession of far greater situational awareness than today, the competitive advantage to be gained from superior situational awareness may be less decisive in future high-end engagements. In effect, the current 'see first, shoot first' characteristic of much of modern warfare may become less decisive – which in turn will increase the emphasis on having a mix of capabilities from weapons performance, to active protection systems, evasion capabilities and platform hardening.

Edge Processing and Electromagnetic Isolation

The second major technological trend is being driven in part by the sensor advances already outlined and the adversary reactions to the information-centric warfare practiced by NATO and its partner countries since the late Cold War. China and in particular Russia have devoted substantial resources to the development of a wide range of electronic-warfare capabilities intended to blind, degrade and spoof Western sensors, and frustrate network-centric warfare through denial of datalink and satellite-uplink connectivity.[178] The US also has formidable electronic-warfare capabilities, especially in the air environment. High-end systems such as the Russian Krashuka-4 electronic warfare platform are openly marketed for export and are relatively inexpensive for near-peer states looking to enhance their self-defence and/or regional

178. For more detail on Russian electronic-warfare modernisation efforts, see Sutyagin with Bronk, *Russia's New Ground Forces*, pp. 80–82.

disruption capabilities.[179] In future conflict scenarios against near-peer, let alone peer threats, the level of electronic-warfare capabilities on both sides is likely to be far higher than in recent conflicts. Even in operations against asymmetric forces that are short of high-intensity conflict, the presence of rival peer forces in the same operational area – as in Syria today – means these systems will disrupt sensor and datalink performance.[180] Even without the presence of an adversary's high-end electronic-warfare technology, the future operating environment will see worsening problems of electromagnetic 'fratricide' due to intense competition for the bandwidth available across the military electromagnetic spectrum within a given theatre.

Bandwidth bottlenecks and electronic-warfare threats from adversary and (fratricidal) friendly systems will drive the second of the major technology trends in the future operating environment – increasing employment of advanced autonomy in systems to facilitate edge processing of data wherever possible. Put simply, the more processing, analysis and prioritisation of sensor data that can be done by the platform (and operator) at point of collection, the lower the bandwidth and processing, evaluation and dissemination (PED) requirements are. In the best case, capacity and bandwidth can be saved by only transmitting relevant, high-confidence data offboard rather than huge volumes of raw data, and in the worst case the platform collecting the data can make maximum use out of it if communication links are denied. However, this requires significant levels of automation and processing power to be designed into platforms at an early stage. It also implies increasing the degree to which operators and commanders become reliant on and must trust analysis conducted by automated processes beyond what many are comfortable with. Of course, the operator of a modern fast jet or naval weapons system is already exercising meaningful human control based on data which has already been pre-sorted, selected and presented through automated processes. However, edge processing as a standard means of working implies moving human oversight further away from the point of raw-data collection and initial processing on a systemic level.

While edge processing offers advantages and is likely to become common, it implies significant delegation of responsibility to both human operators and automated systems in the battlespace. It assumes assets must be capable of operating in the face of (at least periodic) electromagnetic isolation from their peers. This issue may boil down to a return to 'mission command' in the case of crewed assets, but unmanned lethal assets such as unmanned combat aerial vehicles (UCAVs) used in conditions of connectivity denial/disruption raise serious legal and ethical questions. Many states, including the US, Russia and China are actively developing, testing and using lethal unmanned vehicles on land, air and sea. While the majority are designed for operations in permissive environments and are remotely controlled rather than possessing high levels of autonomy, projects such as X-45, X-47B and Dark Sword suggest this is unlikely to

179. For examples of Russian electronic-warfare products openly advertised, see *TASS*, 'Russia's Cutting-Edge Weaponry Capable of "Blinding" Enemy's Army', 19 April 2017.

180. For Russian electronic-warfare capabilities in Syria, see remarks by Ben Hodges in Paul Mcleary, 'Russia's Winning the Electronic War', *Foreign Policy*, 21 October 2015.

remain the case.[181] Any unmanned system designed to deliver lethal effects will have to be at least capable of performing its mission without real-time human control if it is to be credible in high-intensity warfare scenarios in the future operating environment. This requires significant use of edge-processing techniques, high-level automation and delegated lethal authorities at the tactical level.

Offensive Overmatch at Range

A slew of steadily maturing technologies look set to disrupt the current balance between offensive and defensive capabilities in the future battlespace, as well as extending engagement ranges and decreasing available reaction times. Hypersonic and directed energy weapons are particularly worthy of scrutiny in this regard.

Hypersonic missiles – whether cruise missiles (with projected speeds of Mach 3–5) or hypersonic glide vehicles types, lofted by ballistic-missile boost stages (re-entry speeds of Mach 10–25) – pose significant challenges to existing missile-defence systems. Greatly reduced reaction times, tracking challenges and the hypersonic velocities required for interception mean that hypersonic missiles overmatch both current and most projected defences systems. As a result, efforts to mitigate such emerging threats as the Chinese DF-21D hypersonic anti-ship ballistic missile and the Russian 3M22 Zircon hypersonic manoeuvring cruise missile tend to focus on destruction of the launch platforms, or disrupting the kill chain to prevent accurate targeting of the missile, rather than directly intercepting the missile in flight. Hypersonic missiles also tend to be larger and significantly more expensive, as well as shorter ranged than traditional sub- or supersonic equivalents, which will somewhat limit numbers and proliferation beyond major powers. Nonetheless, they represent a shift back towards offensive advantage after many years of defensive advances in ballistic missile defence and close-in weapons system technology.

Directed-energy weapons such as high-energy laser weapons and electromagnetic railguns have long been almost synonymous with futuristic visions of warfare. However, with the field testing of prototype railguns ashore and even in shipborne trials in China in recent years, and multiple point-defence and selective-kinetic-effects prototype laser weapons systems trialled in the same timeframe on naval and aerial platforms, many believe that the transformative mass introduction of such weapons is finally within sight.[182] Directed energy weapons certainly offer the potential to change the balance between attack and defence at the tactical level in multiple domains. They can strike targets faster than conventional defence systems or manoeuvres can

181. For further discussion of UCAVs and autonomy in the future combat air environment, see Justin Bronk, 'Next-Generation Combat Aircraft', *RUSI Occasional Papers* (November 2018), pp. 2–3, 29–34.

182. See, for example, Franz-Stefan Gady, 'US Navy Tests World's First Drone-Killing Laser Weapons System', *The Diplomat*, 19 July 2017; Graham Warwick, 'General Atomics: Third-Gen Electric Laser Weapon Now Ready', *Aviation Week and Space Technology*, 20 April 2015; and Justin Bronk, 'Potential Chinese Railgun Testing Illustrates the US Navy's Biggest Long-Term Challenge', *RUSI Defence Systems*, 1 February 2018.

counter and offer the potential for rapid and sustained follow-up strikes. At the same time, their limited range (line of sight for lasers, and around 150km for railguns) means that they may have a greater effect improving the self-defence capabilities of large platforms and installations against more conventional incoming threats such as missiles and UAVs.

Lasers and high-powered microwave weapons give sustainment and cost benefits over conventional 'gun' systems since ammunition capacity is simply a matter of available power and cooling. Railguns also offer the advantages of cost-effectiveness and more available rounds, since they do not require complex guidance systems on each round, nor propellant charges. However, all directed-energy weapons are limited in their potential applications by power and coolant constraints, which, barring a revolution in power systems and capacitor energy density, limits their ability to do more than complement existing systems, except on very large specialised platforms, in the short to medium term.

There is, however, a significant adoption bonus for emerging powers over established militaries in the realm of directed-energy weapons. Since available power generation, storage and cooling architecture determine the potential range and destructive capabilities of directed energy weapons in defensive and offensive roles, there is a limit to what can be added to existing platforms not designed accordingly from the outset. For example, naval railguns cannot be retrofitted to a US Navy *Arleigh Burke*-class guided-missile destroyer without gutting the ship and rebuilding it from power-train up. However, for China looking to prove the technology while also constructing a blue-water fleet almost from scratch, the capacity to take full advantage of the potential of directed energy weapons can be built into the force from the outset.

Once in the field, railguns could allow even single destroyer-sized surface combatant to hold something as traditionally well defended as a US Navy supercarrier at risk within 150km, since, before being destroyed, it could potentially fire tens of hypersonic rounds that the carrier's task group could not intercept. What this might mean for freedom-of-navigation operations and wider deterrence patrols is worth considering.

All told, the maturation of missile, railgun and directed-energy weapons capable of overmatching defensive systems will enhance the importance of dispersion, signature minimisation, damage control, resilience, and redundancy; at the force level and for individual assets.

Conclusion

Three significant trends will shape the future operating environment out to the late-2020s, including growth in sensor capability and post-processing; the requirement for edge processing in the face of electromagnetic isolation; and offensive overmatch at range. These will significantly alter the ways in which militaries must fight. The ability of individual platforms and small formations to build a high degree of situational awareness will be offset by inadequate bandwidth and contested access to communications and the rest of the electromagnetic spectrum. This will likely enhance the importance of mission command and training, while penalising reliance on centralised command-and-control architectures. It will also most likely

reinforce the importance of platform hardening, evasion capabilities and defensive aids suites, since remaining undetected will no longer be enough to ensure survivability alone. Furthermore, dispersal and emission control will be critical to remaining survivable as a new generation of weapons make it possible to target and destroy key assets even when heavily defended.

Section 3

THE WESTERN WAY OF WAR

The West: A Unified Concept of War?

Paul Barnes

THERE IS, ACCORDING to Victor Davis Hanson, a golden thread running through the Western conception of war, reaching from the heroic era of the Greek phalanx to the modern day.[183] Its key aspects can be unwoven: decisive outcomes; a rules-based structure; and a distaste for deception. If Hanson is correct, then an analysis of developing threats and the putative changing character of warfare might suggest that 'the Western way of war' is threatened.

A proponent of this thesis would doubtless point to indecisive campaigns in Afghanistan, Iraq and Lebanon; the illegal annexation of Crimea; Chinese terraforming in the South China Sea; global state-sponsored cyber attacks; and the disruption of Western democratic processes by disinformation as evidence of an unprecedented threat to the Western tradition. But while the characteristics of events are different, the Western way of war has overcome threats before.[184] There is little evidence that military force has lost its utility: it remains the *ultima ratio regum*. Rules-based structures remain overwhelmingly supported, at least in the developed world. And deceit in international relations is no more palatable today than it was to the West's Hellenic forebears.

And yet, while the nature of war remains immutable and the key tenets of the Western way of war remain fundamentally intact, the pre-eminence of Western *warfare* may be fading. Its current form was developed in the 1970s and 1980s as a response to overwhelming Soviet mass. From 1973, a Pentagon analysis of contemporary conflicts in Southeast Asia and the Middle East, together with a resurgence of interest in the German and Soviet operational art of the Eastern Front, led after nine years to the production of a doctrine – AirLand Battle – which aimed to exploit the inherent weaknesses of Warsaw Pact forces.[185] Soviet doctrine favoured the use of mass formations of armour, commanded in a rigid and directive manner, to destroy an opponent; AirLand Battle sought to counter this asymmetrically by close operational coordination of air and ground forces deployed to dislocate and decapitate Soviet centralised

183. Victor Davis Hanson, *The Western Way of War: Infantry Battle in Classical Greece*, 2nd Edition (Berkeley, CA: University of California Press, 2009).
184. John France, *Perilous Glory: The Rise of Western Military Power* (New Haven, CT: Yale University Press, 2011), pp. 305–57.
185. Richard Lock-Pullan, ''An Inward-Looking Time': The United States Army, 1973-76', *Journal of Military History* (Vol. 69, No. 2, April 2003), pp. 498–99.

command-and-control systems, neutralise numerical advantage with precision munitions, and hence facilitate a collapse in morale, ultimately leading to conventional defeat.[186]

In reaction to this doctrinal change, Western militaries, although retaining a degree of adaptability, were reconfigured for precision, combined-arms warfare which, in conventional terms, gave those who adopted it substantial military superiority over any similar sized and shaped adversary. Arguably, however, this tactical superiority has been transient; just as the West unhinged the Soviet model of warfare in the 1980s with tactics designed to dislocate command and control, so the West's opponents have, over the last 25 years, found asymmetries to negate its conventional advantage. Since the mid-1990s, by refusing to fight symmetrically, conducting war among the people, and operating in the grey zone between war and peace, the West's opponents have effectively exploited deficiencies in its fighting methodology.[187] In addition, by directly threatening fragile Western societies and exploiting weaknesses in their democratic nature, opponents have created divergent security priorities, predominantly in the grey zone, most notably cyber, which have both reduced resources available for traditional defence and created an intellectual distraction. And yet the dominance of precision combined-arms warfare remains unchallenged in conventional terms; challenges to the West are peripheral, in wars of choice and activities in the grey zone. For Western militaries, the key question demanding an urgent answer is whether the changing character of warfare is permanent or transient; if permanent, the West's fixation with expensive precision-enabled conventional war may prove to have been misplaced.

Politics, Globalisation and Digitisation

The threats facing the Western way of warfare are not only military. Political factors, such as the perceived rise of populism and concomitant loss of faith in political institutions, are widely believed to have encouraged a timidity towards the use of force.[188] This reticence is arguably the result of indecisive and costly interventions and reinforced by a perception, in the political classes at least, of a lack of public appetite for military action. In response, politicians and militaries have encouraged the growth of 'remote warfare'.[189] This type of warfare, largely and perhaps wrongly understood as being without risk, favours the use of intelligence, surveillance, targeting, and reconnaissance capabilities and precision-guided munitions rather than 'boots on the ground', with ground-based intervention limited to the use of proxies, special forces, training, and specialist information units.

186. Michael Evans, 'The Primacy of Doctrine: The United States Army and Military Innovation and Reforms, 1945–1995', Army Occasional Paper No.1, Canberra Directorate of Army Research and Analysis, Department of Defence, August 1996, p. 20.
187. Stephen Metz and Douglas Johnson, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts* (Carlisle, PA: US Army Strategic Studies Institute, 2001), p. 8.
188. Emily Knowles and Abigail Watson, 'Remote Warfare: Lessons Learned from Contemporary Theatres', Oxford Research Group, London, 2018.
189. *Ibid*.

Remote warfare allows Western states to intervene where their forces have greatest use and advantage, using expensive platforms and weapon systems designed for precision, combined-arms warfare to support local forces. This trend is observable throughout Africa and the Middle East and is the response of choice for interventionists. Paradoxically, however, remote warfare diverts assets from conventional military capability and weakens the case for the type of warfare whence remote warfare derives its advantage. This is problematic because, as with the American experience post-Vietnam, political aversion to military intervention may prove to be comparatively short-lived (the US was willing to intervene again within 10 years of the end of the Vietnam War, notably in Grenada in 1983 and later in Panama) and militaries may need to fall back on atrophied resources and experience. Drones, for example, may have been developed for a conventional purpose, but their ubiquity and apparent success in remote warfare may inform future procurement choices and undermine the ability to prosecute wars in which drones are not the whole solution. Remote warfare thus takes its toll, not only in the battlespace, but on the ability of Western militaries to fight conventional wars against peer powers.

Technology

Western dependence on expensive technological solutions to deliver precision effects is also problematic. Technological advance has enhanced military lethality and enabled precision, but at enormous financial cost. In an attempt to spread limited budgets, defence solutions have become increasingly multi-functional, with more roles incorporated into fewer, bespoke platforms. Although these platforms are highly capable, their cost and complexity limit production, and in turn redundancy, resilience and regeneration.[190] Exquisite platforms are also highly dependent on vulnerable networked information, particularly delivered by satellite, for everything from communications, navigation and even propulsion; denial of satellite connectivity would have catastrophic consequences for precision warfare.[191] A consequence of the increasing cost of technological advantage is the requirement to make compensating savings in other areas. In many cases, this has led to reductions in personnel numbers and a growth in contracting, with potentially serious ramifications for deployability and capability in a denied environment.[192]

The Changing Character of Warfare

The fundaments of mass and precision effects are antithetical. A force predicated upon mass requires large numbers to deliver sufficient weight at a critical point to physically destroy an opponent. Conversely, precision aims to neutralise or dislocate an adversary using not weight of numbers but precise effects.[193] Technology has decisively enabled a precision advantage since

190. Barnes and Stickings, 'The Death of Precision in Warfare?'.
191. *Ibid*.
192. Ben Farmer, 'Royal Navy "Needs 4,000 Extra Sailors or Cannot Man the Fleet"', *Daily Telegraph*, 13 October 2015; Jay Edwards, 'Contractorisation of UK Defence: Developing a Defence-Wide Contractorisation Strategy and Improving Implementation', *RUSI Occasional Papers* (June 2018).
193. Robert R Leonhard, *The Principles of War for the Information Age* (New York, NY: Ballantine, 1998), pp. 94–123.

1918. Although the futility of mass effect against mass effect was amply demonstrated in the First World War, it was primarily won by the adoption of precision effects in artillery. Despite the wider adoption of precision techniques in its wake, it took until well after the Second World War for precision to become dominant.[194] Today, while the pre-eminence of precision combined-arms warfare remains unchallenged in the context of peer-to-peer and near-peer conventional warfare, some commentators believe that the changing character of war may have made that paradigm redundant.[195]

The evidence is, however, far from conclusive, based as it is on a mixture of untested theory and empirical observations on the periphery of conventional warfare, most notably in counterinsurgency operations. Proponents point to the successful use of asymmetrical techniques against Western forces as evidence of a permanent change to the character of warfare; indeed some claim that the very nature of war has changed.[196] But the degree to which the observed changes are wholly novel, rather than merely a repackaging, is moot.[197] While techniques may be new, conceptual innovation and adaptation are a natural and traditional reaction to military superiority; the development of Air Land warfare itself represented such an evolution. A small and poorly equipped David slew a large and heavily-armed Goliath with a sling and stone: asymmetry is thus a characteristic of war, not a new paradigm of post-modern warfare.

Proponents of the Revolution in Military Affairs (RMA) such as Andrew Krepinovitch claimed that the networked computer would have a revolutionising effect on warfare. But while computerisation promised a revolution – and has arguably provided an evolution – opponents argue that the flaw in the RMA thesis was exposed by the campaigns in Iraq and Afghanistan.[198] While claims for a revolution were perhaps ambitious, the claims were made for precision combined-arms warfare, not counterinsurgency. Information technology is bringing change to the battlefield by enhancing precision effects, but it is not fundamentally changing the character of warfare.

The Western Way of War 2025–30

It is unlikely that the Western way of war will change appreciably over the next 10 years. Its three key tenets – belief in decisive outcomes, a rules-based system, and distaste for deception in foreign policy – will, although challenged, remain dominant. Although highly dependent on the degree to which policymakers believe that the paradigm remains relevant, it is plausible to assume a combination of spiralling technology costs and pressured defence budgets will see

194. *Ibid*.
195. Herfried Munkler, *The New Wars* (Cambridge: Polity, 2005); Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (London: Allen Lane, 2005); Mary Kaldor, *New and Old Wars: Organised Violence in a Global Era*, 3rd Edition (Cambridge: Polity, 2012).
196. Kaldor, *New and Old Wars,* 2012.
197. Colin S Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld and Nicholson, 2005), pp. 218–26.
198. *Ibid*., pp. 105–28.

militaries face two policy choices. First – and the most likely choice of the two in the timeline here – is to continue with a broadly reductionist policy, downsizing and concentrating effects in smaller but increasingly lethal forces. Second, to accept that the paradigm is unsustainable and seek alternatives which preserve the concept of precision at lower cost while contiguously embracing the changing character of warfare – for example, by adopting a more polymorphous force with units dedicated to specific tasks. The benefits of such a force, with a core trained and equipped specifically for traditional conventional warfare and specialised elements specifically configured to fight with greater agility, would be twofold: budgetary, in that the specialised element would be cheaper to equip and thus save money from straightened budgets; and organisational, in that specialisation would create greater expertise, while encouraging conceptual cross-pollination and effectiveness. Such a reconfiguration of forces would allow deployment of elements prepared for precision combined-arms warfare, but also those ready for other, less intensive and archetypical, forms of warfare.

Conclusions and Deductions

Peter Roberts

THERE IS LITTLE evidence that political and military leaders ever seek to start a full-scale global conflict; and in the aftermath of both world wars and other smaller conflicts since, leaders have increasingly tried to use non-military means to meet their national and ideological ambitions. Yet for non-Western states since 2001, economic, diplomatic and political solutions have not achieved their desired ends. As the evidence presented here points out, these actors are increasingly turning to military action, combined with other levers of power, to meet their own requirements against the threats they perceive to emanate from the West. Western states, meanwhile, have continued to place greater emphasis on non-military means and their vision of a benign international system. Stung by failures in Afghanistan, Iraq and Syria (among others), the West increasingly turned away from military solutions, resulting in a generation of political leaders and decision-makers who do not understand the utility of the military instrument: either their own or that of their competitors.

The analysis in this paper is clear: Western adversaries are acting in ways and through technological capabilities designed to avoid a full-scale conflict. Western competitors are selecting strategies and approaches to competition that do not match Western expectations and presumptions. Foundational thinking in Russia, China and Iran acknowledges that national objectives cannot be achieved in a conventional force-on-force contest with Western counterparts – if warfare is waged in accordance with Western expectations and plans. It seems unlikely that potential adversaries are preparing for major war. But this does not preclude shorter, high-intensity engagements; or longer, lower-intensity ones. Indeed, the increasing use of military force is evident in all the approaches highlighted – not simply for deterrence and coercion, but as the core lever in furthering national ambitions. This should not be a surprise to Western military leaders, but peculiarly it does not seem to have been reflected in Western thinking about force design, concepts of warfare or the planning and construction of contemporary campaigns.

The paper has made a series of observations: about behaviours in contemporary conflict; the strategies and approaches being used by others – whether threshold warfare and brinkmanship; the significance of proxies; economic coercion; the vulnerability of the homeland; the need to factor in space more centrally; and the changes that direct energy weapons could have in the offence/defence equation. Its analysis does not conclude that total war or major conflict between current competitors is pre-ordained, nor that those currently undertaking these actions will be protagonists in future. Rather, the aim of each chapter is to expose the strategies and themes that will shape war and warfare over the next decade. It is certainly possible, for example, that other states might use brinkmanship having seen the success gained by North Korea in using this approach, but without nuclear weapons capability being the key to their action. They might choose to use space, for example, as their leverage. The same might be

said of threshold warfare, economic coercion or proxy strategies. Neither does the analysis claim that any of these approaches are new: there are similarities to Western strategies of the past – and in that, there are plentiful examples of their shortcomings and how they might be defeated. Policymakers should be wary of critiquing adversarial strategies as somehow immoral or unethical: to do so would be hypocritical. Rather, Western policymakers might instead delve into their own historical experiences to reveal the countermeasures that unpicked their own strategies.

The approaches examined in this paper are not necessarily exclusive, but neither are they necessarily complementary: and there is no finding that a response against one will work as a response against another. Each study of the challenge presented by adversaries recognises the differentiation between approaches, based on the context and identity of the state from which they originate. As such, the trends diverge from each other rather than towards a homogenous form of warfare. This is exacerbated by the fact that evolution in military thinking and concepts of how adversaries will fight are not linear. Each school of war is developing in different ways, based on a mix of experience, intelligence, thinking, and technology.

There are many factors and trends that could be analysed further, but the selection of themes above does provide a compelling case for four significant deductions to be made.

First, the West's adversaries seem to perceive a greater link between political objectives and military adventurism and an increasing willingness to use military force when other levers have been less successful. National ambition for change remains high, or threats are perceived to be existential. In preparing to counter Western power, they have acknowledged their own vulnerabilities and have sought to bypass them rather than seeking to invest in strengthening them. It is worth reiterating that accepting vulnerabilities enhances the ability of a belligerent to control escalation in crises.

Second, competitors and adversaries view Western command and control – and the centralisation of information, resources and enablers – to be a vulnerability to exploit. They also observe that the Western trend of elevating responsibilities and authorities to higher levels of command, and in requiring cross-government decision-making, has made Western systems slower and less agile. While adversaries might also acknowledge that the reversal of previously swift and responsive Western command and control helps them, they are also aware that this is due to political rather than military or operational reasons. Western political and military actions are now themselves attractive targets for decapitation strategies – an ironic reversal of Western doctrine since the 1980s.

Third, adversaries see less continuity in Western military action: specifically, the kinds of things that once might have elicited a considerable Western military response. The use of chemical weapons in Syria was the first time many Western analysts noted this issue and began warning of the dangers of signalling 'red lines' but failing to enforce them. In fact, Western adversaries had already noted the muted response to cyber attacks in France, Germany and Ukraine (for example, against TV5Monde and the German and Ukrainian power grids). Previously, Western

adversaries might have believed that actions in contravention of international norms would have elicited a response – but the lack of response to various recent challenges may have emboldened the competitors, belligerents and adversaries of the West.

Fourth, the divergence between the Western and other schools of war (and warfare). There is a noteworthy contrast between the first three conclusions and evolving Western policy and doctrine. It is not clear that adversaries have radically departed from their historical behaviours, strategies and approaches to conflict. Instead, it is the change in Western societies, expectations and attitude to risk, interest and values that has departed from historical norms – and this change has been found wanting. If one believes that Western responses to contemporary security challenges are no longer effective, could this be because the West does not have the stomach for actions that previously worked? Perhaps, then, one might deduce that the way Western militaries and policymakers have been considering war and warfare needs to be refocused: in this, specific focus on analysis of Western trends is worthy since current policy is based on flawed contemporary assumptions and may rely too much on technology to solve problems. In this regard, it is worth highlighting related conclusions from other recent research:

- Adversaries are not observing the same rules and standards as the West.[199]
- Campaigns designed around political or military decapitation are less effective against today's adversaries than the orthodoxy holds. Rather, if applied against Western militaries – whose linear progression of centralisation continues unchallenged – it might be strikingly effective.[200]
- Technological superiority rarely plays a dominant factor in determining military success, nor has it historically been the Western way of warfare pre-Cold War. Force design with technology as the driving force has less probability of success than is currently imagined.[201]
- The electronic environment – in many ways the connective tissue of the Western military machine – cannot be assumed to be merely contested: it may be effectively denied. Contesting electronic dominance to achieve agility will become a whole-force driving factor, with increasing resource implications.[202]
- Information, automated decision-making and data science have not delivered the expected or assumed decisive edge; indeed, currently they add stress to established and proven decision cycles – and can hand the adversary an advantage.
- Combat continues to provide lessons that training cannot simulate. Live training has similar advantages over simulated training. Testing structures against realistic enemy

199. Ewan Lawson and Richard Barrons, 'Warfare in the Information Age: Time for a Change?', *RUSI Journal* (Vol. 161, No. 5, October/November 2016); Peter Roberts, 'Designing Conceptual Failure in War: The Misguided Path of the West', *RUSI Journal* (Vol. 162, No. 1, February/March 2017).
200. Sutyagin with Bronk, *Russia's New Ground Forces*.
201. Jim Storr, *The Hall of Mirrors: War and Warfare in the Twentieth Century* (London: Helion and Company, 2018).
202. Andrew Payne and Peter Roberts, 'Intelligence, Surveillance, and Reconnaissance in 2035 and Beyond', *RUSI Occasional Papers* (February 2016).

> tactics is critical if exercises are to have real value. Testing realistic timescales for decisions, and working against tactics, techniques, and procedures of the enemy are all critical in exposing realities of contemporary fighting rather than fictionalising success to satisfy false metrics of success.[203]

Such deductions lend themselves to further examination against historical precedent. In this case, the conduct of war and warfare remains a distinctly human endeavour, both physical and intellectual. Drawing from wisdom from a longer arc of history, including the conceptual frameworks of Themistocles, Sun Tzu, Carl von Clausewitz, Marcus Aurelius, and Mao Zedong (among others), can have great use in overcoming skewed assumptions of current military and political thinking.[204] Both former US Secretary of Defense James Mattis and future Chairman of the US Joint Chiefs of Staff, Mark Milley, have commented that there is a danger in acting with the 'conceit of the present', believing that our challenges are uniquely difficult, living in a world that is changing faster than ever. The evidence, as cited by Mattis and Milley, debunks these myths and instead challenges this generation to live up to the values and performance of previous generations who faced far greater challenges.[205]

Combining historical wisdom with contemporary conflict, this paper observes additional lessons for military and political leaders:

- A defence policy that views deterrence as a solely reactive posture is not effective in meeting the challenges of an evolving and dynamic security environment. A proactive, dynamic approach to strategy, and to classical concepts such as coercion, deterrence and denial, is required.
- Modern warfare does not manifest the geographic boundaries of historical, post-Cold War expeditionary interventions where the homeland could be assumed to be safe and secure. The homeland has re-emerged as one of the critical battlegrounds for the military and society.
- Late adopters of capabilities are less likely to abide by the rules and conventions that early adopters established.[206]
- A unified theory of warfare (such as multi-domain operations) is likely to be less effective as a binding framework. As scholars have noted previously – and RUSI researchers demonstrate in this paper – counter-Western strategies differ depending on the context, means, ways, and ground. These are dynamic and evolving and are not given to following

203. Non-attributable discussion with Indian army officers at RUSI on 4 March 2018, after the border clashes with Chinese PLA forces in December 2017.
204. Bleddyn Bowen, 'It's About Reaching the Decision, Not Victory: Strategic Theory and the Difficulty of Taking Action', Defence-in-Depth blog, King's College London Department of Defence Studies, 23 November 2016.
205. Robert J Gordon, *The Rise and Fall of American Growth: The U.S. Standard of Living Since the Civil War* (Princeton, NJ: Princeton University Press, 2016).
206. Paul Barnes, 'Enhancing Adaptability', conference paper delivered at the Finabel conference for heads of European armies, April 2019.

a linear path of development in the way that Western militaries experienced (drone development of up-and-coming states has made generational leaps in the same way that non-Western states have evolved their use of ISR).[207]

- Time and space are returning as critical considerations and linking points in war and warfare. Faster (in all things) does not mean better – but when linked to political will and desired exit strategies speed might help states be more decisive.
- Command and control – political as well as military – needs to adapt, relearn lessons, and test itself rigorously.[208]
- Thinking that is bound within rigid frameworks – such as 'domains', 'environments', 'OODA' or 'PED' cycles, 'last safe moment decision-making', 'start' and 'finish' lines, and 'FEBA' – will be unhelpful. Structuring political and military thinking about conflict and combat in these ways will not lead to a competitive edge or success. Rather, the development of 'anti-fragile thinkers' – those that thrive in chaos rather than seeking to bring order to it – will be more effective.[209]

These conclusions expose the stark divergence between the Western school of war and warfare and those of others. It suggests that Western militaries and policymakers need to change how they consider war and warfare.

In this, it is worth emphasising the pivotal role of human decision-makers in conflict. While people might have linear thought-processes, act in rational ways, employ critical thinking and aspire to avoid full-scale conventional war, they are also prone to errors in action, interpretation and perception. So even if the overarching aim of all actors is to avoid full-scale war, errors in judgement might lead them into it.

Critically, the way that Western leaders and populations continue to regard states of hostility and competition as either at 'war' or in a period of 'peace' now appears to be unfit for the contemporary security environment. During ancient and medieval times, the nation state existed more in a state of semi-permanent war, and society structured itself for this building in resilience and military force design. It is only in the 18th and 19th centuries that the binary war/peace divide became so marked and pronounced, both in language and action. This became much more closely defined by 20th-century experiences. Today, war and peace have returned to a situation more like ancient times: conflict and competition appear likely to remain interwoven states that are continuous and contiguous. The failure to understand this, the evolution of warfare itself, and the failure to establish more robust responses to the actions of adversaries, indicates an increasing number of interactions, interventions and conflicts. The real risk is that the West misidentifies these as simply more 'wars of choice' to which limited responses are sufficient, when in fact some might quickly evolve into existential threats, but perhaps not in the way we currently perceive existential wars to emerge or identify themselves.

---

207. Colin S Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld and Nicholson, 2005).
208. Peter Roberts, 'Virtuous Decision-Making in War: "The Good Operation"', *RUSI Newsbrief* (Vol. 38, No. 1, February 2018).
209. Nassim Nicholas Taleb, *Antifragile: Things that Gain from Disorder* (London: Penguin, 2013).

Developing a concept of war and warfare that matches the challenges of the next decade might seem too large a challenge. There are no short-term solutions, and political and military leaders show few signs of accepting a challenge to their baseline assumptions. If change is required soon, driven by events and adversaries, the West might be stuck with inflexible leaders rather than adaptable ones. In which case, defeat looms on the horizon. Provided such defeats are not in existential conflicts, perhaps Western leaders should accept that losses in blood and treasure are inevitable but not too concerning (although soldiers, sailors, aviators, and marines might have different ideas). But this assumption leaves no space for error: and even though no-one wants a full-scale war (a moot point in itself), they can still occur in the event of political and military misunderstanding and miscalculation. The margin for errors has disappeared.

About the Authors

Peter Roberts is Director of Military Sciences at RUSI, having been the Senior Research Fellow for Sea Power and C4ISR since 2014. He researches and publishes on a range of subjects from strategy and philosophy, contemporary war, military doctrine and thinking, command and control, naval warfare, ISR, professional military education, and disruptive warfare techniques. He lectures, speaks and writes on these topics as well as regularly providing advice for both UK and foreign governments. Previously, Peter was a career Warfare Officer in the Royal Navy, serving as both a Commanding Officer, National Military Representative and in a variety of roles with all three branches of the British Armed forces, the US Coast Guard, US Navy, US Marine Corps and intelligence services from a variety of other nations. He served as chairman for several NATO working groups and 5 Eyes Maritime tactics symposia. His military career included service in Hong Kong, the Baltic, Kenya, the Former Republic of Yugoslavia, Iraq, South Africa, Pakistan, and Oman, interspersed with deployments in the GIUK gap and the Persian Gulf. Peter has a Masters degree in Defence Studies and a Doctorate in Politics and Modern History. He is a Visiting Professor of Modern War at the French Military Academy.

Ewan Lawson is Senior Research Fellow for Military Influence at RUSI. He researches a range of subjects including strategy and cross-government working, military influence and information operations, law of armed conflict and war crimes, conflict in Africa, and cybersecurity. He also oversees conferences, meetings and lectures in these areas. He was previously a Royal Air Force officer, initially as a policing and security specialist but in more recent years in a range of joint warfare appointments. Since graduating from the UK Advanced Command and Staff Course, his experience has included tours as a joint operational planner, as the commanding officer of the UK Psychological Operations Group, as military faculty at both the UK and Kuwait Staff Colleges and as the first Defence Attaché at the British Embassy in South Sudan. His most recent experience was within Joint Forces Command with responsibility for the development of cyber-warfare capabilities.

Jack Watling is a Research Fellow at RUSI, responsible for the study of Land Warfare. His interests include overseas capacity building, counterterrorism operations in complex environments, civil war dynamics, and the balancing of near-peer and non-peer threats. He recently completed a detailed study of British training and assistance programmes in Yemen between 2004 and 2015. His PhD examined the evolution of Britain's policy responses to civil war in the early 20th century. As a Hobsbawm Scholar, he completed an MA in Contemporary History and Politics with Distinction, and a BA in History, at Birkbeck College, University of London. In 2018 he co-convened a conference on Irish Rebellion and Militancy in Transnational Perspective. Prior to joining RUSI, he worked as a journalist, contributing to *Reuters*, *The Atlantic*, *Foreign Policy*, *The Guardian*, *Jane's Intelligence Review*, *Haaretz*, and others. He has worked in Iraq, Mali, Rwanda, Brunei, and further afield, has embedded with Iraq's Popular Mobilisation Forces, and the Burkina

Faso Army. Jack was shortlisted for the European Press Prize Distinguished Writing Award in 2016, and won the Breakaway Award at the International Media Awards in 2017.

Sidharth Kaushal is a Research Fellow in Sea Power at RUSI. His research covers the impact of technology on maritime doctrine in the 21st century and the role of sea power in a state's grand strategy. Sidharth holds a Doctorate in International Relations from the London School of Economics, where his research examined the ways in which strategic culture shapes the contours of a country's grand strategy.

Justin Bronk is a Research Fellow specialising in combat airpower and technology in the Military Sciences team at RUSI. He is also Editor of the *RUSI Defence Systems* online journal. Justin has written on air-power issues for the *RUSI Journal*, *RUSI Defence Systems*, *RUSI Newsbrief*, the *Journal of Strategic Studies* and the *RAF Airpower Journal*, as well as contributing regularly to the international media. He is also a part-time doctoral candidate at the Defence Studies Department of King's College London and holds an MSc in the History of International Relations from the London School of Economics, and a BA (Hons) in History from York University.

Adam Maisel is a former Land Warfare Research Analyst at RUSI. He currently serves as an Operations Officer for the US Army's Mad Scientist Initiative and is a veteran of Operations *Enduring Freedom* and *Freedom's Sentinel*. He has also served as a civilian military intelligence adviser to US, NATO and other allied forces. Adam holds a BA in History, Government, and Law from Lafayette College and an MA with Distinction in National Security Studies from King's College London. Adam is a frequent contributor to the Modern War Institute at West Point, the Strategy Bridge, and *War on the Rocks*.

Elisabeth Braw is an Associate Fellow at RUSI. She directs the Institute's Modern Deterrence project, which focuses on how governments, business and civil society can work together to strengthen deterrence of existing and emerging threats. She was previously a non-resident Senior Fellow at the Atlantic Council following a career as a journalist, reporting from the US, Germany, Italy and other countries. She remains a contributor to *The Wall Street Journal*, the *Financial Times*, *Foreign Policy*, and the *Frankfurter Allgemeine Zeitung*, focusing on European defence and security, and frequently speaks at conferences. Elisabeth has also been a Visiting Fellow at the University of Oxford. A native of Sweden, she attended university in Germany, finishing her Magister Artium degree in Political Science and German Literature with a dissertation on nuclear weapons reduction in Europe.

Alexandra Stickings is a Research Fellow for Space Policy and Security within the Military Sciences team at RUSI. Her research interests include military space, space warfare, counterspace capabilities, and international space programmes. She has published on space topics for *RUSI Newsbrief*, *RUSI Defence Systems* and *RUSI Commentary*, and regularly contributes to the media, including the BBC, Channel 4, ITV and Deutsche Welle. Alexandra holds an MSc in International Security and Global Governance from Birkbeck College, University of London, a BA(Hons) in International Studies from the Open University, and a BSc(Hons) in Physics with Astronomy from

Nottingham University. Prior to joining RUSI Alexandra worked in a variety of fields including central and local government, as well as the private sector.

Paul Barnes is the British Army Visiting Fellow at RUSI. A Warrant Officer in the Regular Army, he has served on operations in the Former Yugoslavia, Northern Ireland, Iraq, and Afghanistan. He is the first non-commissioned serviceman to hold an Army Fellowship at RUSI and holds a Chief of the Air Staff's Fellowship. In 2014 he won the Henry Probert Bursary of the Royal Air Force Historical Society and in 2018 he was the recipient of the RAF's Salmond Prize. He holds an MA in Military History from the University of Birmingham and is currently writing a Joint Concept Note entitled 'Enhancing Adaptability' for the Development, Concepts and Doctrine Centre. The focus of his research is military innovation and adaptation, particularly its diffusion in contact. He is the Organiser of the British Military Book of the Year Prize 2018 and the founder of the 'War Talks' series which aims to bring informal professional military education to the Armed Forces.