

JOINT SPECIAL OPERATIONS UNIVERSITY
DEPARTMENT OF STRATEGIC STUDIES



Information Age Proxy Warfare

by Andrew Maher

JSOU PRESS
OCCASIONAL PAPER
AUGUST 2019

On the cover: Members of the Syrian Democratic Forces stand in formation during a Victory announcement ceremony over the defeat of Daesh's so-called physical caliphate on 23 March 2019 at Omar Academy, Deir ez-Zor, Syria. The Global Coalition will continue addressing the threat Daesh poses to partner nations and allies, while preventing any return or resurgence in liberated areas. PHOTO BY U.S. ARMY STAFF SGT. RAY BOYINGTON

The views expressed in this publication are entirely those of the author and do not necessarily reflect the views, policy, or position of the United States Government, Department of Defense, United States Special Operations Command, or the Joint Special Operations University.

This work was cleared for public release; distribution is unlimited.

**JSOU Press Publications are available for download at:
<http://jsou.libguides.com/jsoupublications>.**

ISSN 2572-9020 (print)

ISSN 2572-9039 (online)

ABOUT THE AUTHOR

Major Andrew Maher is an Australian infantry officer with particular interest in operations conducted by, with, and through foreign forces. He has operational experience over multiple rotations in both Afghanistan and Iraq. Major Maher earned a master's degree in defense studies, has commanded at platoon and company levels, and is currently serving as a military fellow, lecturer, and doctoral candidate at the University of New South Wales, Canberra. His doctoral thesis will examine the topic of information age proxy warfare.



INFORMATION AGE PROXY WARFARE

The utility of employing proxies to achieve strategic ends has increased with the arrival of the information age. Akin to the “classic” nuclear deterrence theory of the Cold War era, the costs of major conventional warfare (to all parties) have encouraged the use of virtually-supported proxy forces to limit the likelihood and costs of escalation in future conflicts. Conversely, the opportunities inherent in information age access, reach and penetration to proxy forces overcome certain conventional force deterrence effects. The author describes these outcomes as being achieved through weapons of mass mobilization, subversion, instruction, and surveillance. This paper explains why such proxy options appeal to government, and how proxy warfare considerations might influence Western military strategy.

I. Introduction

Western nations have arguably struggled to generate effective strategic outcomes for military interventions over the past thirty years. Furthermore, this challenge is seemingly exacerbated by certain nations’ employment of “grey zone” methods of warfare.¹ This assertion is evidenced by examining the Western intention to employ “maneuver warfare”—a concept of operations that leads to a “rapidly deteriorating situation with which the enemy cannot cope.”² It is questionable if Western nations have contrived any “rapidly deteriorating situation” through its strategic actions in recent history. Certainly, the Russians did in Crimea and the Islamic State did in Iraq during 2014. Indeed, the assertion of poor strategic competence is becoming more evident.³ Improving Western strategic competence begins with an expanded understanding of how strategic ends might be achieved and is an essential component to remaining competitive.

The future international environment will be increasingly multipolar, demonstrating “an escalation of interstate competition between a resurgent Russia, a rising China, and the United States and intensifying sectarian divides and regional rivalries between client states.”⁴

Within the next decade, Australia needs to anticipate greater economic, political, and military competition in the Indo-Pacific. China will continue its rise, as will India, Indonesia, and Vietnam. A shifting power balance will challenge the Australian Defence Force’s ability to maintain the

1. “From a national to an individual level, both home and away, we are being outmaneuvered in a ‘grey zone’ short of armed conflict by actors unconstrained by previously accepted norms. Central to this strategic contest is an information battle, where we increasingly lack the initiative.” U.K. Ministry of Defence, *Joint Concept Note 2/18 Information Advantage* (Wiltshire, United Kingdom: Development, Concepts and Doctrine Centre: September 2018), 2.

2. *Land Warfare Doctrine 1: The Fundamentals of Land Power* (Commonwealth of Australia: Australian Army, 2014), 41.

3. Linda Robinson, Paul Miller, John Gordon IV, Jeffrey Decker, Michael Schuille and Raphael Cohen, *Improving Strategic Competence: Lessons from 13 years of War* (Santa Monica: RAND, 2014), xi, www.rand.org; Public Administration Select Committee, *Who Does UK National Strategy?* (London: House of Commons, 28 January 2011).

4. Candace Rondeaux and David Sterman, *Brief: Twenty-First Century Proxy Warfare* (Washington, D.C., New America, 9 November 2018), <https://www.newamerica.org/international-security/reports/twenty-first-century-proxy-warfare/>.

regional technological advantage it maintained during the Cold War. The high-technology, high-lethality, high-cost, conventional war-fighting platforms that Australia is currently acquiring will be of decreasing utility due to their corresponding increasing risk in the event of loss. The more advanced the technology, the greater the risk inherent in operational employment, and paradoxically, the less flexibly the capability provides options to government. Such platforms are thus bordering upon being too costly to use.

The increasing urbanized littoral will exacerbate this challenge because the ability of Western military forces to undertake unilateral kinetic operations due to collateral damage concerns will increase. Likewise, Western political appetite for the risk of casualties is a constraining influence further decreasing the likelihood of certain conventional war-fighting capabilities being liberally employed. Unilateral action using conventional war-fighting platforms is becoming a less attractive option for governments. Operating in this congested urban terrain to apply targeted force requires influence with local forces, as has been learned in the urban centers of Ramadi, Mosul, Ar-Raqqah and Al-Qaim in recent years.

These factors make proxy conflict more likely. Proxy conflict is herein defined as conflict which is perpetrated by others—either knowingly or unknowingly—on behalf of a third party to promote its own interests. This will typically manifest as a major power working through a lesser power. The author does not mean with this definition to include remotely-controlled machines—a consideration which is included within the term surrogate warfare. Furthermore, unlike special warfare, the author

Unilateral action using conventional war-fighting platforms is becoming a less attractive option for governments.

excludes overt capacity-building efforts, as are undertaken daily under international engagement activities. Thus, proxy warfare will generally obscure and separate the patron from the client, and thereby limit attribution of the effects generated. For propaganda purposes, the inverse may also occur. The patron, as a component of strategic signaling, overtly claims the actions by the client.

Recent military operations in Syria and Iraq illustrate the patron-client challenge of proxy warfare. This conflict demonstrates the broader multipolar strategic environment, in which external actors are reluctant to engage in hostilities (with the exception of Iran), and the fickle realities are evident in employing a proxy strategy.⁵ The United States, Australia, the United Kingdom⁶ and other Western partners have all adopted a strategy

5. Syria is a “prototype of ‘new-generation warfare.’ Its main feature is that the state enemies of Syria are conducting covert, insubstantial operations without being drawn into direct military conflict.” Valery Gerasimov, “Russian General Staff Chief Valery Gerasimov’s 2018 Presentation to the General Staff Academy: Thoughts on Future Military Conflict—March 2018,” *Military Review Online Exclusive* (January 2019): 5, <https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/2019/Gerasimov-2019.pdf>.

6. “Remote warfare ... sees the UK and its allies playing a supporting role—providing air support, training, equipment, and intelligence to local and regional actors who do the bulk of frontline fighting against terrorist groups in places like Yemen, Somalia, Iraq, Syria, and Libya.” Abigail Watson, “The Perils of Remote Warfare: Finding a Political Settlement with Counter-Terrorism in the Driving Seat,” *The Strategy Bridge* (5 December 2018), <https://thestrategybridge.org/the-bridge/2018/12/5/the-perils-of-remote-warfare-finding-a-political-settlement-with-counter-terrorism-in-the-driving-seat>.

employing proxies. The strategic and political appeal of embracing a proxy strategy is only likely to be greater in future military contingencies.

2. The Strategic Implications of Today's Information Age

The information age in which we now live is an environment of increasing electronic connectivity, unknown social connections, and instantaneous engagement—which leads to faster decision-making, innovations, and adaptation.⁷ This environment has been described as volatile, uncertain, complex, and ambiguous, but the implications of this environment upon strategy are not clear. Indeed, this complexity contributes to our contemporary challenge in formulating strategy with any longevity. The recent release of the Australian Chief of Army's *Accelerated Warfare* concept responds to this environmental challenge by articulating how an accelerating rate of change in warfare influences warfighting.⁸ A short review of the evolving character of war over the past 350 years highlights this change.

The Environmental Context of an Accelerating Rate of Change in Warfare

The Westphalian System. In 1648, the Treaty of Westphalia resolved the Eighty Years War between the Spanish and the Dutch, and the German phase of the Thirty Years War. It recognized the territorial sovereignty of nation-states, established a norm against interference with another nation's affairs, and established a balance of power to enforce such norms that underwrite today's international order. Proxy warfare was theoretically constrained by this treaty piloting a new age of political civility.

The First Industrial Revolution and the Napoleonic Age. When the Napoleonic Wars ended two centuries later in 1815, the dawn of industrial age warfare ushered in the laying of our Clausewitzian doctrinal foundation in what has been described as First Generation Warfare.⁹ Throughout the Peninsular War, a French Corps (Marshal) commanded between 8 and 20 thousand men and used muskets, cavalry, cannon, and baggage trains to a direct fire range of up to 1.8 kilometers.¹⁰ Cavalry daily rate of movement enabled an influence over approximately 11,000 square kilometers. In this era, warfare saw the birth of operational art and cavalry was a decisive arm.

The call to *Liberté, égalité, fraternité* (translated means liberty, equality, fraternity) that enabled Napoleon's mass mobilization unsurprisingly led to different conceptions of what liberty may mean. Despite Napoleon's obvious ability to seize control of territory decisively, the unleashed potential of the population in Nationalist propaganda challenged his ability to hold said territories, exemplified

7. This adaptation is well discussed by the Boyd Cycle or OODA (Observe-Orientate-Decide-Act) loop.

8. *Accelerated Warfare: Futures Statement for an Army in Motion* (Commonwealth of Australia: Australian Army, August 2018), 41, <https://www.army.gov.au/our-work/from-the-chief-of-army/accelerated-warfare>.

9. William S. Lind, Colonel Keith Nightengale, Captain John F. Schmitt, Colonel Joseph W. Sutton, and Lieutenant Colonel Gary I. Wilson, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette*, October 1989.

10. Michael Glover, *The Peninsular War, 1807-1814: A Concise Military History* (Exeter, U.K.: David and Charles, 1974).

by the emergence of guerrilla warfare in the Iberian Peninsula. At this time, Westphalian norms were ignored by Wellington's support to the Spanish and Portuguese guerrilla, French support to American Revolutionaries, and British support to the French aristocracy and insurgencies in Spain, Naples, and Malta.

It was during this era that the Industrial Revolution set conditions for mass discontent with machines replacing manual labor. This discontent reached a climax with the European Spring of 1848, demonstrating the power of the commune to rise in revolution against oppressive monarchies—a zeitgeist captured by Marx and Engels.¹¹ The Industrial Revolution generated the mass production of weapons for mass armies, but also the printing press, the weapon of choice for the nascent Communist and Anarchist movements.

The Second Industrial Revolution and the World Wars. A century after the Napoleonic Wars, in 1915, World War I armies had mobilized under Nationalist causes, for what was meant to be a short, decisive war, but which instead unleashed 30 years of violence.¹² Western nations fought to a standstill as Napoleonic General staff used operational art to seek decision through superior mobilization using railroad, telegraph, and subsequently radio. Cavalry became irrelevant as rifles, machine guns, obstacles, and artillery “industrialized” killing at the height of second generation warfare. An Australian Infantry Corps (Lieutenant General) commanded between 50 and 100 thousand men and could fire massed artillery to a range of 7-10 kilometers. With the invention of aircraft, the Corps could organically affect approximately 321,000 square kilometers. In this era, combined arms operations were born.

The era of total war corrupted totally. The invention of the submarine expanded the concept of maritime blockade to that of deliberately targeting civilians and merchantmen as a legitimate action—even those declared “neutral.”¹³ The invention of long-range bombers likewise invented “strategic bombing doctrine” thus legitimizing the targeting of civilians. On land, the answer to any question of strategic planning—be it generating manpower, firepower or mechanized vehicles—was simply, more. Such concepts helped contribute to the unprecedented civilian casualties of World War II, culminating in the employment of atomic weapons. Through these dawning technologies,

11. Karl Marx and Frederick Engels, *Manifesto of the Communist Party* (New York: International Publishers Co., February 1848).

12. The conception of World War I neatly fitting into 1914-1918 and World War II into 1939-1945 is too simplistic when examining the political precursors to violence and the influence of technology therein. The oft-quoted trigger in the assassination of Archduke Ferdinand had its roots in the earlier Balkan Wars on 1912-13 and the broader Anarchist movement of the late 19th century. The toll of World War I catalysed the Bolshevik Revolution in 1917 leading to the Russian civil war, and up to twenty-seven revolutions, civil wars and insurrections throughout Eastern Europe and the Middle East. The rise of Fascism in Germany and Italy in the 1920s, and the Spanish Civil War also clearly had their roots in the damage to the social fabric caused by total war. Likewise, the Japanese invasion of Manchuria in 1931, the Italian invasion of Ethiopia in 1935 and the German Anschluss of Austria in 1938, clearly influenced Allied decision-making during the period 1939-1942, and thus cannot be discretely excised.

13. “Germany saw U-boats as a legitimate response to British surface superiority: the problem was that they couldn’t easily search ships, take prizes, or determine passengers’ nationality, all standard practices in earlier blockades ... Wilson almost went to war when 128 Americans perished, in May 1915, on the torpedoed British liner *Lusitania*.” John Lewis Gaddis, *On Grand Strategy* (New York: Penguin Press, 2018), 268-269.

civilian targeting unsurprisingly led to a civilian response, voiced through unprecedented popular mobilization, and the birth of an industrial scale of guerrilla warfare in the Soviet states, the Balkans, France, Burma, China, the Philippines, and Southeast Asia.

The Dawn of Nuclear Deterrence. Fifty years from the outbreak of World War I in 1965, the effects of Eisenhower’s need to counter Soviet conventional superiority via the First Offset Strategy yielded an air force that had evolved to become the dominant arm of the U.S. military. Industrial warfare, however, had matured with the lessons of blitzkrieg into the height of third generation Warfare, despite being constrained by the nuclear stability/instability paradox.¹⁴ The nuclear deterrence of total war ironically encouraged the proxy wars of colonial revolution as the post-World War II lessons of insurrection matured. In 1965, in Vietnam, an American Division (Major General) commanded between 10 and 20 thousand men and could fire 155mm artillery to a range of 14 kilometers. Through nascent airmobile concepts, a division could affect approximately 785,000 square kilometers within hours.

The well-oiled combined arms killing machine of the U.S. military was however, strategically outmaneuvered by different political systems. Giap’s “Peoples War” could weather tactical losses while still achieving political outcomes.¹⁵ Similarly, Soviet propaganda and subversive efforts matured with “Active Measures” to leverage proxies to undermine the national social fabric, particularly within Chile, El Salvador, and India.¹⁶ Crises sparked by the Hungarian Revolution of 1956, the Cuban Revolution of 1959, and the Soviet invasion of Czechoslovakia in 1968, demonstrated how seemingly minor irregular wars could influence the Cold War balance of power. In this era, French, American, and Australian armies fought to adapt their respective cultural and doctrinal concepts of “Counter-Revolutionary Warfare” to varying degrees.¹⁷

Crises sparked by the Hungarian Revolution of 1956, the Cuban Revolution of 1959, and the Soviet invasion of Czechoslovakia in 1968, demonstrated how seemingly minor irregular wars could influence the Cold War balance of power.

The Third Industrial Revolution (The Computer Age). In 1991, 25 years after U.S. entry escalation in Vietnam, the end of history had arrived with the end of the

14. S. Paul Kapur, *The SAGE Encyclopedia of Political Behaviour: Stability-Instability Paradox* (Thousand Oaks, California: SAGE Publications, 2017), https://my.nps.edu/documents/105858948/106279825/Kapur_Sage+Encyclopedia_Stability-Instability_OCt17/c7952c37-2f5d-4462-9630-5bff04f6cd8f.

15. Võ Nguyễn Giáp, *People’s War, People’s Army* (Hanoi: Foreign Languages Publishing House, 1961).

16. Christopher Andrew and Vasili Mitrokhin, *The World Was Going Our Way: The KGB and the Battle for the Third World* (New York: Basic Books, 2005).

17. Amongst others, see Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency* (California: Praeger Security International, 1964); Andrew Krepinivich, Jr., *The Army and Vietnam* (MD, John Hopkins University Press, 1988); and M.C.J. Welburn, *The Development of Australian Army Doctrine 1945-1964* (Canberra, Australia: Strategic and Defence Studies Centre, Research School of Pacific and Asian Studies at The Australian National University, 1994), Canberra Papers on Strategy and Defence, no. 108, http://bellschool.anu.edu.au/sites/default/files/publications/attachments/2016-03/108_SDSC-Wellburn.pdf.

Cold War.¹⁸ U.S. Army rejection of counterinsurgency doctrine for the concept of air-land battle coalesced into what was seen as the epitome of operational art, played out with the evisceration of the Iraqi Army.¹⁹ The nuclear advantage of the First Offset Strategy had been neutered by the specter of mutually-assured destruction. The Second Offset Strategy had thus delivered upon its promise to overcome the perceived deficiencies experienced in land wars in Asia and establish conventional technological overmatch against Soviet armored divisions, echeloned from the Fulda Gap. Emerging in this period, an American Brigade Combat Team (Brigadier General) commanded several thousand men and could directly engage to at least 24 kilometers. Within hours, it could affect almost 2 million square kilometers using organic attack aviation.

This epitome of warfighting prowess sat awkwardly as the UN intervention to Somalia in 1992-93, the Rwandan genocide of 1994, and the Balkans war from 1991-2001, demonstrated the limitations of Western tactical magnificence when operating in “Wars amongst the People.”²⁰ These irregular wars saw a confluence with the then-nascent coming together of terrorism with nationalism, evidenced by the First Palestinian Intifada and the rise of Hezbollah.

The 4th Industrial Revolution (The Information Age). Fifteen years on, following the 2006 Israel-Hezbollah War and the height of the insurgency in Iraq, Western adversaries had again disarmed Western tactical overmatch through dispersal and a democratization of violence. The adversary adopted a hybridization of warfare between conventional and unconventional means, in a manner that rendered any distinction as superfluous.²¹ The employment of man-portable lethality in complex urban terrain by Chechen rebels, Lebanese Hezbollah fighters, and Iraqi insurgents codified what has been termed fourth generation warfare.²² This environment forced doctrinal adaptation to support the “Strategic Corporal” fighting the complex “Three Block War.”²³ Persistent, armed, unmanned aerial systems became normal for support to the conduct of brigade to even battle group-level operations, enabled by the joint and interagency community. Thus, a battle group commander, with 700 men could directly engage to 30 kilometers or more and affect over 4 million square kilometers in under an hour.

Eight years hence in 2014, complex hybrid warfare erupted in Crimea, the Donbass, and in northwestern Iraq. With the innovative use of propaganda, non-Western forces attained a near ubiquitous presence of unmanned aerial vehicles in the battlespace, networked with electronic warfare, and precision fires capabilities in what might be described as a reconnaissance-strike

18. Francis Fukuyama, “The End of History?,” *The National Interest*, no. 16 (Summer 1989).

19. Douglas Skinner, *AirLand Battle Doctrine* (Virginia: Centre for Naval Analyses, 1988), <http://www.dtic.mil/dtic/tr/fulltext/u2/a202888.pdf>; and *Gulf War Air Power Survey, Vol II: Operations and Effects and Effectiveness* (Washington, D.C.: U.S. Government Printing Office, 1993), <http://www.dtic.mil/dtic/tr/fulltext/u2/a273996.pdf>.

20. Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Vintage Books, 2008).

21. Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Virginia: Potomac Institute for Policy Studies, 2007), <http://www.potomacinstitute.org/>.

22. Colonel Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (Delhi: Manas Publications, 2005).

23. General Charles C. Krulak, “The Strategic Corporal: Leadership in the Three Block War,” *Marines Magazine*, January 1999, http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm.

complex.²⁴ Armored vehicle-borne improvised explosive devices on volley proved to be an effective poor-man's preparatory fires. Indeed, the precise lethality capable of being directed within the operating environment was demonstrated, "with an intensity and speed of target location heretofore not seen on any battlefield."²⁵

What next? Over the coming decade, the 3rd Offset Strategy might begin yielding technological solutions to today's Anti-Access/Area-Denial (A2/AD) challenges. For the Australian army, the likely

force construct will evolve to that of enabled battle-groups, (currently commanded by lieutenant colonels) that leverage cyber and electronic warfare capabilities, manned-unmanned teaming and assigned joint, interagency capabilities. Australia has procured new capabilities to include (among others) long-range rockets, advanced fight aircraft (F-35A), airborne electronic attack aircraft (EA-18G), maritime patrol and reconnaissance aircraft (P-8), unmanned attack aircraft (MQ-9 Reaper drone), and unmanned reconnaissance aircraft (MQ-4 Triton drone). These capabilities will transform the tactical environment by giving commanders, who employ perhaps only a hundred or so troops, an ability to engage beyond 100 kilometers and influence millions of square kilometers that may contain millions of people living in the crowded, connected, urban littoral.²⁶

These capabilities are expensive. Nations must thus assess their strategic options through the lens of ever-increasing operating costs, maintenance costs, and procurement costs to gain and maintain an asymmetric technological advantage.



Soldiers, believed to be Russian, ride on military armored personnel carriers on a road near the Crimean port city of Sevastopol on 10 March 2014. PHOTO BY REUTERS/BAZ RATNER/FILE PHOTO NEWSCOM

24. Dr. Phillip Karber, *Lessons Learned from the Russo-Ukrainian War: Historical Lessons Learned Workshop* sponsored by John Hopkins Applied Physics Laboratory and U.S. Army Capabilities Center (Virginia: Potomac Centre, 6 July 2015), <https://www.scribd.com/doc/274009061/Lessons-Learned-From-the-Russo-Ukraine-War>.

25. Karber, *Lessons Learned*, 14. A demonstration of this threat was well evidenced "at Zelenopilya, in a combined MLRS fire strike that lasted no more than three minutes, two Ukrainian mechanised battalions were virtually wiped out with the combined effects of top-attack munitions and thermobaric warheads," 18.

26. Department of Defence, *Integrated Investment Program 2016* (Commonwealth of Australia, 2016), <http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-Integrated-Investment-Program.pdf>; "The RAAF to get MALE-Reaper UAS acquisition confirmed," *Australian Aviation*, 16 November 2018, <http://australianaviation.com.au/2018/11/the-raaf-to-get-male-reaper-uas-acquisition-confirmed/>.

In this context, the direction of Western military contingencies in the near future is likely to be low-cost, proxy warfare.²⁷

So what? A number of variables make proxy warfare more likely:

- **Competition.** With each decreasing time period described above, a doctrinal revolution, or generational shift, is evident as the impact of technological change is felt in our tactical concepts. As these tactics are employed, adversaries cycle through their Observe-Orientate-Decide-Act (OODA) loop to adapt novel solutions that account for each doctrinal revolution.²⁸ This OODA loop is, in each generation, informed by improving information connectivity, progressing from wax-sealed message in the age of sail to globalized instantaneous encrypted communication. A significant challenge is expected to maintain a technological asymmetry over potential adversaries given this competitive learning environment.
- **Lethality.** Each generational shift yields increased lethality, increased range and increased responsiveness to our conventional capabilities, whilst devolving authority of respective levels of command from that of their forebears. With each generation, militaries are becoming more lethal. Each generation also demonstrates a closing gap between conventional and unconventional modes of warfare into what is now recognized as hybrid warfare.
- **Access, reach, and penetration.** With each time period examined, the evolution of improved firepower, mobility platforms, and intelligence, surveillance, and reconnaissance (ISR) capabilities, heightens the force projection challenges against a peer or near-peer adversary. Access to the battlespace has become so challenged as to be physically denied. Reach of information systems is both global and instantaneous. Penetration into the adversary political system is now a ubiquitous feature of adversary operating concepts. These aspects of battlespace geometry are, in combination, highly complex.
- **A blind spot for enduring unconventional actors.** Despite this accelerating rate of change, continuities abound. The Napoleonic Wars demonstrated facets that today are termed hybrid. Irregulars fighting Napoleon's Grande Armée in Portugal, Spain, Malta, Naples, Switzerland, the Tyrol, and Russia, demonstrated operational concepts similar to irregular actions in the Crimea, Chechnya, and the Donbass. Clausewitz's trinity, expressed through the "passions of the people" that rose in Andalucía, Galicia, and Catalonia in 1811, likewise made themselves felt two centuries later in rebellions against the Ben Ali, Bashar al-Assad, and Muammar Ghaddafi regimes in 2011. War's enduring nature abounds however, despite this acceleration of change—a clash of wills punctuated with coercive violence. Yet, concepts of proxy warfare are unfamiliar to most uniformed officers because this continuity is not expressed in Western military education.

27. Thomas Waldman, who notes, supports this assertion: "The exorbitant cost and huge scale of public resources that need to be diverted for large-scale missions have become politically intolerable in an era of economic austerity." Thomas Waldman, "Vicarious Warfare: The Counterproductive Consequences of Modern American Military Practice," *Contemporary Security Policy*, Vol. 39, Issue 2 (2018).

28. Grant Hammond, *The Mind of War: John Boyd and American Security* (Washington: Smithsonian Books, 2001).

- **A multipolar security environment.** The recent security environment of the Cold War era demonstrated the “stability/instability paradox.”²⁹ This environment captured how major nuclear powers, rationally seeking to avoid mutually assured destruction, sought to achieve political ends through indirect means. As the environment shifts from unipolar to a bipolar, or multipolar orientation, then we might expect to see an increasing utility in concepts like the stability/instability paradox.

3. The Strategic Implications of the Information Age Environment

The globalized information age affords both fragility and resilience in the face of a multipolar competition. As previously highlighted, the last time we faced such an environment was the Cold War, the result was the birth of deterrence theory and the stability/instability paradox.

Today’s operational environment presents exacerbated consequences of even isolated employment of weapons of mass destruction—perhaps alternately described as weapons of mass disruption—as stock markets, logistics networks, and analysts are instantaneously, globally informed and consequently begin to adjust and adapt to the new situation. The resilience of globally sensitized national economies to a serious disruptive attack is thus highly uncertain and indeed, its downstream effects may be impossible to predict, given global interconnectedness.

In this environment, the prospects of a deterrence strategy might now be expanding due to the increasing cost of high-technology conventional capabilities, coupled with today’s risk-adverse polity. The same instantaneous communications mediums that allow global audiences to adapt, may thus act disproportionately to a large-scale, conventional engagement. We have already seen this effect with the 1973 Yom Kippur War and the Iranian Revolution collectively generating the 1979 oil shock. The political risk inherent within large-scale conventional warfare is likely to be unacceptable given its disruptive effect for all except existential threats.

The same instantaneous communications mediums that allow global audiences to adapt, may thus act disproportionately to a large-scale, conventional engagement.

A deterrence strategy is further empowered through the recognition of a competition in innovation—and therefore the potential implications of not holding a technological advantage.³⁰

29. The logic of the “stability/instability paradox” is described as follows by the CIA declassified report, *CIA, Limited War* (2 December 1960), <https://www.cia.gov/library/readingroom/docs/CIA-RDP89B00552R000100040004-1.pdf>. “The nuclear stalemate has established a deterrent balance with respect to the latter. Paradoxically, however, by reducing the likelihood that either side would risk such an all-out conflict, it may have made limited wars seem less risky to the Bloc in many parts of the world—especially in underdeveloped areas.” Indeed, this CIA report went on to note that “The Communist Bloc is concentrating more and more effort on those areas which are in a state of rapid and at times violent political, economic, and social change which renders them vulnerable to Communist ‘indirect aggression.’” 2.

30. John Stilton and Bryan Clark *What it Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, D.C.: Centre for Strategic and Budgetary Assessments, July 2015), <https://csbaonline.org/research/publications/what-it-takes-to-win-succeeding-in-21st-century-battle-network-competitions>.

Examples include low-cost, anti-ship cruise missile systems that have proliferated widely, including to non-state actors. Russia has supposedly already developed a hypersonic ballistic missile capability and the Chinese are supposedly testing an electromagnetic railgun. Collectively, this proliferation of technology enhances the concept of “conventional deterrence.”³¹

Accelerated Warfare

Australia will face a decreasing technological advantage because of major power technological investment, the increasing economic weight of middle-powers in its region, and the continuing proliferation of advanced systems to non-state actors. This shift will limit Australia’s military options given the overarching political need to limit casualties.

Narrative groups like al-Qaeda, who attach themselves to large-scale military deployments that serve to support popular discontent, recruitment, and radicalization, make the conventional employment of land forces more problematic in this environment.³² Such deployments provide a plethora of targets to would-be insurgents. A balance-point is apparent as small-scale forces lack sufficient combat power for unilateral execution of their mission. Beyond this point, however, adverse propaganda effects yield diminishing returns.

A number of information-age methods might, however, exploit this operating environment and serve to harness the accelerating rate of change in warfare and characterize the nature of proxy warfare. These methods operate within the context of nuclear and conventional deterrence that constrains unilateral conventional escalation. These methods might be termed weapons of mass mobilization, instruction, subversion, and surveillance.

4. Weapons of Mass Mobilization

The development of modern communications systems is said to be ‘both index and agent of change in a total social system.’ Exposure to more attractive modes of life and the consequent intensification of value expectations is facilitated by system-wide communication networks. Perceptions of regime responses to discontent, and to disorder, are acquired through communication media. Communication among discontented

31. “Groupings of long-range air-, sea-, and land-based cruise missile carriers have been created on each strategic axis, capable of providing deterrence in strategically important regions... In the future, an increase in the capabilities of precision means of destruction, including hypersonic, will make it possible to shift the principal portion of strategic deterrence tasks from the nuclear to the nonnuclear forces.” Valery Gerasimov, “Russian General Staff Chief Valery Gerasimov’s 2018 Presentation to the General Staff Academy: Thoughts on Future Military Conflict—March 2018,” translated by Dr. Harold Orenstein, Military Review Online Exclusive, Army University Press, accessed 15 January 2019, <https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/2019/Gerasimov-2019.pdf>, 5-7.

32. “Whatever purpose they serve, large deployments of American conventional forces, as we have seen, allow al-Qaeda and its sympathizers to confuse the issue by calling for classic jihad to defend Muslim lands.” Michael W. S. Ryan, *Decoding Al-Qaeda’s Strategy: The Deep Battle Against America* (New York: Columbia University Press, 2013), 266.

but dispersed individuals may substitute for physical proximity in the development of organizations committed to violence.³³

Communication mediums have always influenced the conduct of social mobilization, potentially even toward violence and revolution. Written in 1970, the opening quote for this section highlights the influence of television—that it delivers current events and opinion to global audiences within a day of the event. It is no coincidence that this media revolution influenced the mobilization of public opinion in Vietnam, or the mobilization of foreign fighters to *jihad* in Afghanistan. Social media platforms have now accelerated the speed with which global audiences are connected to events—both real and fabricated. This has prompted a revolution in information-age recruiting and radicalization.

Traditional modes of irregular mobilization. Foreign fighters are nothing new; the printing press enabled the million-man armies of the industrial age and the mobilization of a globalized diaspora in conflicts such as the Spanish Civil War. Such fighters, mobilized by a sense of relative deprivation, that their kin (ethnic, nationalist, religious, ideological, communal, or fraternal) is suffering a relative deprivation that is being discriminately applied across a population.³⁴ This deprivation might be existential, economic or religious indeed—or only perceived to be—but this feeling of deprivation motivates men to arms. The communicative aspect to irregular mobilization is thus evident in the application of the speed, frequency, and density of the information flow that communicates how discriminatory practices apply to a certain group. It is this dynamic which enabled the guerrilla mobilization in the context of the French Revolution and Napoleonic Wars and continues to do so today.

This deprivation might be existential, economic or religious indeed—or only perceived to be—but this feeling of deprivation motivates men to arms.

What is new? In what Audrey Kurth Cronin termed the electronic *Levée en Masse*, global target audiences can recruit individuals to a cause—potentially connected only virtually.³⁵ Social media forums accelerate, simplify, and expand the concept of globalized recruiting and radicalization, which expands the traditional model of mobilization beyond what has generally been limited to within a nation-state. Indeed, this expansion is heightened by change in the Third World recently “opened” by mobile phone towers, and “jumping” stages of technological progress.

33. Ted Robert Gurr, *Why Men Rebel* (New Jersey: Princeton University Press, 1970), 223. Gurr further highlights this point by quoting George Rudé, *The Crowd in History: A Study of Popular Disturbances in France and England, 1730-1848* (New York: Wiley, 1964). Rudé had identified that “From the place of initial outbreak during the French Grain Riots of 1775 and the Luddite machine-breaking riots in 1811-12, the riots spread to surrounding areas no more quickly than a man could travel on foot or horseback.”

34. Gurr, *Why Men Rebel*.

35. Audrey Kurth Cronin, “Cyber-Mobilisation: The New *Levée en Masse*,” *Parameters* (Summer 2006), 78. The French term *levée* has two meanings in this context, both “levy” and “uprising,” each of which is important for understanding the nature of the *levée en masse* and its relationship to the dramatic changes that occurred in warfare at the time. This terminology of “uprising” should not be lost upon us noting the use of social media in the Arab Spring and the Colour Revolutions.

Why is this dangerous? The speed of information transmission risks near instantaneous mobilization of people suffering actual or perceived relative deprivation. Mass mobilization further erodes our Westphalian norms and empowers non-state actors in what Andrew Krepinevich has termed the “democratization of destruction.”³⁶ The now typical model of Western employment of overwhelming firepower is thus revealed in its counter-productive effects. Seemingly, indiscriminate employment of firepower, manifest in civilian casualty incidents, may serve to worsen this sense of relative deprivation to a global audience and thereby promote further radicalization.

A contemporary example of this method in practice. The war against Islamic State of Iraq and Syria (ISIS) demonstrated the use of weapons of mass mobilization. It is well known that ISIS globally recruited foreign fighters. This conflict also demonstrated the mobilization of foreign fighters to fight with the Kurds and virtual militia in the form of the hacktivist group, Anonymous.



Soldiers assigned to the Field Artillery Squadron, 3rd Cavalry Regiment, fire their M777 howitzer on Firebase Saham, Iraq, on 3 December 2018. The 3rd Cavalry Regiment is deployed in support of Operation Inherent Resolve, working by, with and through the Iraqi security forces and coalition partners to defeat the Islamic State of Iraq and Syria in designated areas of Iraq and Syria. PHOTO BY U.S. ARMY CAPT. JASON WELCH

The war against ISIS also demonstrates the seemingly wanton employment of firepower with little consideration of consequence. To achieve the military defeat of ISIS, Operation Inherent Resolve utilized 98,532 weapons in Syria and Iraq over a three-year timeframe.³⁷ This total, whilst pursuing a force estimated to be 30,000 strong, devastated Iraq’s Sunni and Turkmen populations—an approximately 1.9 million of whom remain displaced 2 years later. The short-term focus on the military defeat of ISIS belies the reality that such populations are vulnerable to recruitment to violent extremism as they seek to rebuild their lives in a war-scarred environment, likely to continue to lack housing, schooling, adequate health care, and employment

opportunities. The relative deprivation that motivates individuals to violence will be highly apparent given a seemingly Western and Shia-dominated, Iraqi government disinterest.

5. Weapons of Mass Instruction

Militaries have a cultural strength in their systems of force generation, coordinated by a backbone of doctrinal concepts. These very systems enable mass instruction in times of war, allowing significant

36. Andrew Krepinevich, “Get Ready for the Democratization of Destruction: The Way the World’s Militaries Wage War is Going to Change—Drastically,” *Foreign Policy Special Report* (15 August 2011), <https://foreignpolicy.com/2011/08/15/get-ready-for-the-democratization-of-destruction>.

37. United States Air Force Central Command, Combined Air Operations Centre, Airpower Summary (31 August 2017), <https://www.afcent.af.mil/Portals/82/Documents/Airpower%20summary/Airpower%20Summary%20-%20August%202017.pdf?ver=2017-09-07-104037-223>.

expansion under times of national mobilization. This concept was apparent in the Indochina wars, as the then nascent U.S. Special Forces (SF) dispatched small training teams to train, live, and conduct missions with irregular forces. This cadre model of instruction was a feature of the Cold War, with numerous examples evident in both ideological camps. The asymmetric effect of this model of instruction is perhaps most evident in the ultimately successful unconventional warfare campaign against the Soviet Union in Afghanistan, enabled by provision of personalized instruction from a small number of trainers to the mujahideen.

Traditional modes of military training and education. Napoleon's operational art, nationalism, and the influence of the Industrial Revolution unshackled the size of armies, which enabled the mass printing of training materials. Such methods had been institutionalized by World War I and mobilized millions of men to serve in theaters globally. By the end of the 20th century, instructional doctrine, field manuals, and operational analysis reports were extensive, and just starting to make their way onto the internet.

What is new? The democratization of information made possible by the internet (and the Internet of Things) has made it possible for individuals to be trained for military activity by virtual means. An individual can download the Anarchist's Cookbook, FM3-05.130 Unconventional Warfare, and the operating manual for a target power generation turbine. Thus, without contact with any military an individual might be capable of independently demolishing a target—previously considered a highly-specialized military task.

This democratization of information challenges the ability to control teachers and learners. The proliferation of military expertise undermines Westphalian norms of a state's monopoly of violence, when combined with the proliferation of man-portable lethality, such as anti-tank missile systems, surface-to-air missile systems, sniper rifles, and explosively-formed projectiles.

Why is this dangerous? A diffusion of lethality through man-portable weapon systems, combined with an inability to control military training and education, challenges traditional geographic state loyalties. The potential for leaderless resistance is thus evident. Theoretically, at least, given a sufficiently large impetus to mobilize a population, large-scale guerrilla warfare might be mobilized against Western interests, shielded by the urban environment in which they live—a hyper-inflated Grozny scenario.

Contemporary example of this in practice. Inspire and Dabiq magazines, promulgated online, are means that non-state actors are already using to empower individuals with education, fielding advice, and coordination of individual violent acts to generate global effects. Exerting a slightly greater level of control, the Lashkar-e-Taiba-coordinated attacks in Mumbai in 2008, demonstrate the improvement in tactical ability that can be generated with an online coordinator, leveraging news media to improve the situational awareness of the tactical team on the ground. States are likewise embracing the potential of virtual instruction. The U.S. development and fielding of virtual advise-

and-assist kits to Iraqi partners is an example in practice.³⁸ This employment paradigm holds the potential to link highly effective national military capabilities with the tactical elements of foreign nations, without incurring the political risk of boots on the ground.

6. Weapons of Mass Subversion

Using propaganda and disinformation is not new. What is new is the ease, global reach, speed of propagation of ideas, efficiency and low cost of such efforts, coupled with our political sensitivity to national and global opinion.³⁹

The manner in which information operations are planned, executed, and evaluated are being accelerated by the proliferation of connectivity, both in terms of speed and scale. The need to inform global audiences about Australian actions, and illuminate the fiction surrounding adversary counternarratives, is thus of increasing importance in the battle of narratives.

Within the constrained environment of an urbanizing littoral, the opportunities for exerting influence upon a population are significant, ranging from person-to-person contact, news/media, and virtual channels. It is this proliferation of channels, content, and cycles that indicates the potential for mass subversion of populations.⁴⁰

Traditional modes of military information operations. The era of print media carried an ability to influence populations through exclusivity of message, when combined with repressive measures. The Bolsheviks understood this well and it became a characteristic of Communist insurgencies. Exclusivity of message could be attained through population control—where disinformation cannot be filtered from truth.

The Viet Cong doctrine of *binh van* exhibits the concept of subversion in practice. “Through agitation, persuasion, coercion, and threats, Viet Cong operatives targeted key officials, both military and civilian, to weaken the government’s ability to rule as well as to swell the ranks of the insurgency.”⁴¹ The Viet Minh method was thus highly personalized in contrast to American counterefforts that were highly impersonal, such as letter drops or radio broadcasts. At a strategic level, the Vietnamese efforts at subversion were ably abetted by the advent of television as a medium for influencing American public opinion, in a way that ultimately subverted the national war effort. The Vietnamese were also assisted by America’s counterproductive actions.

38. Christopher Thielenhaus, Pat Traeger, and Eric Roles, “Reaching Forward in the War Against the Islamic State,” *PRISM*, Volume 6, no. 3, (2016), <http://cco.ndu.edu/PRISM-6-3/Article/1020215/reaching-forward-in-the-war-against-the-islamic-state/>.

39. U.K. Ministry of Defence, *Joint Concept Note 2/18 Information Advantage* (September 2018), 4.

40. Subversion is defined as being “designed to undermine the military, economic, psychological, or political strength or morale of a governing authority.” Paul J. Tompkins, U.S. Army Special Operations Command, ed. Robert Leonhard, *Undergrounds in Insurgent, Revolutionary, and Resistance Warfare* (Fort Bragg, North Carolina: U.S. Army Special Operations Command, 25 January 2013).

41. Tompkins, U.S. Army Special Operations Command, *Undergrounds in Insurgent*, 38.

What is new? The Russian “Firehose of Falsehood” is an evolution of the Communist notion of population control and exclusivity of message.⁴² Exclusivity in today’s information age is seemingly impossible—even with tight national internet controls. The flipped approach is one of flooding the media with grades of mistruths, from subtle to blatant, such that discrimination of verifiable, accurate reporting becomes difficult, nigh impossible. This approach has demonstrated to global audiences the fragility of democratic systems seeking to defend their constitutional norms, leveraging instantaneous globalized information networks.⁴³ The responsiveness of social media platforms challenges our ability to verify information, but this veracity is also seemingly less important.

Today, thanks to smartphones, the Internet and social media, our perception of the world is being manipulated at an extraordinary pace and on a previously unimaginable scale ... Experts are out, opinion is in; it matters not how verifiable the assertion, it only matters that it attracts attention.⁴⁴

The democratization of information through social media plays to individual heuristics. Although the information is not coming from recognized authoritative sources, we often trust it implicitly given the often personalized tone of such communication.

“Fake news” introduces a new situation and undermines the ability for governments to react quickly, due to confirmation taking time. Indeed, “fake news” can undermine the government itself—as the 2016 U.S. elections exhibit.⁴⁵

Why is this dangerous? “Salami slicing” tactics secure strategic gains through minor fait accompli. Each gain is seemingly short of justifying a military response. Obscured by subversive tactics, mistrust of information enables the attainment of such fait accompli. A competitor must both disprove the information surrounding the action, and then generate a sufficiently compelling counternarrative to warrant escalation. Often, this asymmetry in favor of the aggressor is too great to overcome.

Such a threat is particularly prescient to an Australian Defence Force (ADF) with minimal workforce trained to develop, defend, and nuance a battle of the narratives that is moving at the speed of Twitter.⁴⁶ Paraphrasing Margaret Thatcher, the international news media serves as the

42. Christopher Paul and Miriam Matthews, *The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, California: RAND Corporation, 2016), <https://www.rand.org/pubs/perspectives/PE198.html>.

43. “Russia’s interest in and application of active measures does not seem to have abated, and has perhaps even intensified via social media and proliferating fake news outlets in the last several years.” Dr. Frank G. Hoffman, “Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges,” *PRISM*, Vol 7, no. 4, (2018).

44. U.K. Ministry of Defence, *Joint Concept Note 2/18 Information Advantage* (September 2018), 1.

45. Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, ICA 2017-01D, 6 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

46. Audrey Kurth Cronin again offers useful advice in this area. “In its naïve enthusiasm for the information age, the West has lost control of the narrative ... In the long run, the ‘swarming’ that really counts is the wide-scale mobilisation of the global public.” Audrey Kurth Cronin, “Cyber-Mobilisation: The New *Levée en Masse*,” *Parameters* (Summer 2006): 86-87.

oxygen of instability, sustaining the fire of discontent that radicalizes the next generation of adversaries.

Contemporary example of this in practice. Relative deprivation might be felt globally due to an action locally, because of a perceptive adversary manipulating the information space. The Siege of

The sensitivity of some audiences to certain information holds the potential for honest mistakes to have dire consequences, just as much as it holds the potential for deliberate manipulation.

Mecca, which 20 November 1979, is a good example. On 21 November, a radio report broadcast in Islamabad suggested U.S. involvement in Mecca enraged the local population and led to the overrun of the American embassy. The sensitivity of some audiences to certain information holds the potential for honest mistakes to have dire consequences, just as much as it holds the potential for deliberate manipulation. Western military planners cannot predict the global consequences of

subversive messages when they resonate with a disaffected population (who may not even be the target audience for said subversion).

7. Weapons of Mass Surveillance

The presence of camera-enabled smartphones means any action—from an air strike to a simple equipment move—not only can, but almost certainly will, be filmed and posted online in near real time, probably with its exact GPS coordinates.⁴⁷

The globalized availability of information now extends the concept of *every soldier is a sensor* to *every smartphone-enabled citizen is a sensor, an analyst, and a gauge of effectiveness in information operations*. Indeed, this already is a reality, presenting a significant threat when an adversary has a mature reconnaissance-strike complex. The opening quote for this section highlights this reality in an analysis of the lessons of the air wars in Libya, Syria, and Yemen.

Traditional surveillance operations. Traditional conduct of ISR tasks involve tasking of an asset to report against specific information requirements. In Gulf War I in 1991, the challenge of warfare was thus one of assigning ISR assets against targets, “fixing” the target, then assigning a “shooter” to prosecute. This system thus enabled prosecution of the air war that significantly attrited the Iraqi Army.

What is new? The networking of billions of devices in real-time with developments in artificial intelligence holds the potential for “Big Data” to facilitate surveillance, analytics, and information/psychological operations assessments on an unprecedented scale. Tasking of a collection asset in this environment is seemingly antiquated—the information has been collected perhaps multiple times over. With such a level of networked surveillance, discriminate targeting is enabled through an

47. Ben Nimmo, “Lessons from the Air Campaigns over Libya, Syria and Yemen,” *Parameters*, Vol. 46, no. 1, (Spring 2016): 90.

inability to remain below the detection threshold. Over time, it may be difficult to remain below the discrimination threshold.

In Libya in 2011, citizen journalism via platforms such as Twitter, Google Maps, and Facebook evolved to become a disaggregate ISR network and nonviolent protest movement.⁴⁸ A global cyber militia provided analytic efforts to this network. NATO leveraged this environment to support targeting efforts. Indeed, anecdotal evidence suggests that this environment provided better and faster information than traditional military intelligence channels.⁴⁹

Why is this dangerous? The coupling of miniaturizing surveillance devices with networked connectivity challenges the military's ability to remain below the detection threshold. Indeed, there is clear potential for the deployment of such a surveillance model into contested environment. The penetration of companies such as Huawei into foreign markets might be reinterpreted as a measure to set conditions for future operations.

This capacity for open-source surveillance in the urbanized littoral conversely holds the potential to accelerate the concept of a reconnaissance-strike complex, if able to be effectively harnessed by Western forces. For the Australian Army, the asymmetric effect of creating a proxy surveillance network through open source collection means within a targeted location is a significant concept—particularly if it is a cluttered urban area with marginal airborne ISR performance. This is due to the Australian Army being reliant upon asymmetric concepts to offset its limited resources.

Contemporary example of this in practice. The Chinese Communist Party has adopted such surveillance systems to an unprecedented level.⁵⁰ The deliberate establishment of surveillance networks in the cities of Xinjiang province to monitor the Uyghur population appears to have been effective in supporting the suppression of the Uyghur separatist/Salafi terrorist organizations.⁵¹

8. Implications for the Coalition Operations

Globalization with its attendant liberalization of markets and currencies, integration of transportation, infrastructure, information and economies is knitting together a new network of corporate and individual interests that have a stake in proxy conflict outcomes.⁵²

48. John Scott-Railton, *Revolutionary Risks: Cyber Technology and Threats in the 2011 Libya Revolution* (Rhode Island: U.S. Naval War College, CIWAG Case Studies, 2013), 79.

49. Scott-Railton, *Revolutionary Risks*, 79.

50. Anna Mitchell and Larry Diamond, "China's Surveillance State Should Scare Everyone," *The Atlantic*, 2 February 2018, <https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203>.

51. This terminology notes that for the Chinese Communist Party (CCP), separatism, terrorism and religious fundamentalism are the "Three Evils" and thus are seemingly viewed synonymously. The paucity of information regarding events in Xinjiang province both challenge the ability to quantify the effectiveness of CCP suppression and serve as an illustration of the autocratic counter to information age methods discussed herein.

52. Rondeaux and Sterman, *Brief: Twenty-First Century Proxy Warfare*.

Generic Implications. In the context of an urbanizing global population deterred from undertaking conventional warfighting, these four information age adaptations present both significant threats and opportunities for the Army, and military forces in general. It is a mistake to think the challenge is merely military. The sheer scale of industrial espionage via cyber channels, and criminal activity leveraging some or all of the four methods described above, highlight the integrated nature of the strategic concepts that need to be devised.

In the military domain, information age unconventional warfare may become the only kinetic option against an adversary with mature A2/AD capabilities—that is, an adversary who at present affects “conventional deterrence” through a robust air defense, surveillance, and anti-ship network. The A2/AD challenge in the physical domain suggests value inherent in alternate pathways within the multidomain battle environment such as informational, cyber, or proxy force. To provide military options for government, land forces will need to look beyond the “forces assigned”—those that we control—to “forces available”—those we can influence.

Threat forces are already adapting to this environment. Abu Mus’ab al-Suri’s call for the adoption of a “leaderless resistance” strategy was proposed in 1991, refined by 2004, and has since been adopted by ISIS to coordinate attacks against Western nations.⁵³

Although the means are new, the theory for the employment of proxy forces is not. The use of proxies carries significant hidden risk through the management of patron-client relationships. Walter Ladwig demonstrates this area as complex and of significant importance in eventual strategic performance.⁵⁴

A refined approach to proxy engagement requires a nuanced strategic framework, which at present, is absent.⁵⁵ This mode of warfighting is not simply Western exploitation—indigenous resistance groups should be expected to seek Western interest, resources, and possibly intervention to further their cause. Such groups may indeed exploit a lack of Western focus by providing local intelligence, social media reporting, or fake news that manipulates Western political opinion toward imprudent action.

53. Michael W. S. Ryan, *Decoding Al-Qaeda’s Strategy: The Deep Battle Against America* (New York: Columbia University Press, 2013), 237. Ryan quotes al-Suri: “In consideration of the expanse of the ummah and the vast arenas in which the targets and interests of the invading enemy are to be found ... our path [forward] will be based on guiding the Muslim, who desires to participate and [be part of] the resistance, to operate where he resides or where he is able to [act] naturally and go about his public life normally while practicing jihad and resistance secretly by himself or with a small cell of trusted people, who form a secret, independent [unit] for jihad and resistance, as well as individual jihad.”

54. Walter C. Ladwig III, *The Forgotten Front: Patron-Client Relationships in Counterinsurgency* (Cambridge: Cambridge University Press, 2017). Furthermore, “this alleged panacea for the state’s problem of shaping post-modern conflicts is not without negative consequences. Most of these are related to the principal-agent problem within the surrogate relationship, namely the loss of patron control amid a constant surrogate quest for more autonomy.” Andreas Krieg and Jean-Marc Rickli, “Surrogate Warfare: The Art of War in the 21st Century?” *Defence Studies*, Vol. 18, no. 2 (2018): 127.

55. At present, the Oxford Research Group is conducting research into remote warfare, <https://www.oxfordresearchgroup.org.uk/Pages/Category/remote-warfare>, and New America have initiated research into Proxy Warfare, <https://www.newamerica.org/international-security/future-proxy-warfare/>.

Implications for Australia

There is an active threat to Australian interests.⁵⁶ Recognition of the threat posed by cyber actions in particular but information warfare in general, has resulted in significant funding allocation, estimated as 0.18 percent of Australia's gross domestic product over 10 years.⁵⁷ Despite this investment, Australia currently lacks a holistic strategic doctrine for proxy warfare.

The ADF should seek to offer niche contributions to coalition operations, that serve to develop the asymmetric concepts described herein. Asymmetry is an enduring requirement for the ADF to pursue as it will rarely enjoy an overwhelming manpower advantage over a near-peer adversary. Such contributions would serve as an alternate model to the current "little America" model of like capabilities within a small force element.⁵⁸

The ADF should consider a greater willingness to assume a coalition-lead in areas with strategic importance to Australian interests (i.e. South-West Pacific), hence offsetting where Australia's limitations constrain broader military contributions. Such commitment provides the long-term focus upon the human terrain that proxy actions require.

The ADF requires a better ability to understand human terrain when seeking influence effects. To do so, the ADF may need to professionalize in the provision of certain information age effects. Australia's current lack of a U.S. SF-equivalent oriented toward special warfare and psychological operations expertise are exemplar deficiencies.⁵⁹

In an Australian context of relatively low-threat yet, high securitization, the ADF might need to consider how it plans military options in light of the advice from Andreas Krieg and Jean-Marc Rickli:

The more abstract the nature of securitization, e.g. the definition of threats and risks, the more difficult it becomes for the community to accept the human costs borne by the soldier as the trinitarian agent. The surrogate therefore provides the sovereign with a means to externalize these human and material costs to a substitute security provider.⁶⁰

56. "Recent reports that China is operating deep inside Australia to destabilize the Australian government and turn it toward Chinese aims suggest that Beijing's doctrine is more than merely academic." Dr. Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM*, Vol. 7, no. 4, (2018).

57. Edward Morgan and Marcus Thompson, *Information Warfare: An Emergent Australian Defence Force Capability*, Discussion Paper 3, (Center for Strategic and International Studies, October 2018), 3.

58. Colonel John Angevine, *Dangerous Luxuries: How the Quest for High-End Capabilities Leaves the ADF Vulnerable to Mission Failure and More Dependent on the United States* (Sydney, Australia: Lowy Institute, 2011), https://archive.loyyinstitute.org/sites/default/files/pubfiles/Angevine%2C_Dangerous_luxuries_web_1.pdf.

59. In the Australian Army psychological operations is a component of Intelligence Corps, rather than a specialized streaming.

60. Krieg and Rickli, "Surrogate Warfare," 125.

Implications for the United States

For the foreseeable future, Western nations will continue to look to the United States as the lead nation for military interventions. As the lead nation, the United States will continue—perhaps unfairly—to be expected to orchestrate Western strategy. Where a strategy employs a proxy nation, the United States will need to improve its ability to influence its client to address the often-legitimate grievances that continue to fuel contemporary conflict. Western nations must improve this facet of their strategic approach to employing proxies. As Daniel Byman notes:

U.S. allies that are fighting al-Qaeda-linked insurgencies often have four categories of structural problems that explain some of their distinct interests and lead to particular challenges against insurgents: illegitimate (and often repressive) regimes; civil-military tension manifested by fears of a coup; economic backwardness; and discriminatory societies.⁶¹

Western nations ignoring Byman’s observation risk “forever wars” as legitimate grievances will remain unaddressed.

The United States must recognize the economic factors influencing the decisions of their partners. The ability for junior partners to keep pace with the 3rd Offset strategy (in order to maintain interoperability) may be challenged by their domestic economic constraints. This reality risks the ability to conduct seamless coalition operations. Indeed, dangerous luxuries are an enticing trap for junior coalition partners that undermine their ability to operate independently in their region. Thus, U.S. technological modernization is also perversely creating the very dependency upon U.S.-led military interventions that Washington seeks to avoid. A Lowy Institute study by Angevine into such dangerous luxuries notes:

Australia’s current defence strategy does not correspond with the realities of Australia’s security situation. The plan for the modernisation of the Australian Defence Force (ADF) is focused on expensive maritime and air capabilities for conflict the ADF couldn’t fight alone. Consequently, the ADF is exposed with an atrophying ground force and expeditionary capability for the low-level regional operations in which it will be the most likely to engage.⁶²

Partners are not the only ones who are financially constrained, and thus struggle to emulate American approaches. Jahara Matissek criticizes the result as ‘*Fabergé Egg* armies’ that are unsustainably expensive and inherently fragile, as the Iraqi Army of 2014 attests.⁶³

61. Daniel L. Byman, “Friends Like These: Counterinsurgency and the War on Terrorism,” *International Security*, Vol. 31, no. 2, (Fall 2006): 81.

62. Colonel Angevine, *Dangerous Luxuries*.

63. “Following 9/11, American security aid focused on making weak countries develop stronger security forces. Unfortunately, this created *Fabergé egg* militaries: expensive and easily broken by insurgents.” Jahara Matissek, “The Crisis of American Military Assistance: Strategic Dithering and *Fabergé Egg* Armies,” *Defense and Security Analysis*, Vol. 34, no. 3, (2018): 267.

Proxy warfare is a little studied field, most of which is English language- and Western-biased.⁶⁴ Understanding the doctrinal approaches of Western coalition partners and red-team thinking may improve the employment of proxies and the resultant theory of victory.

Overall, a more nuanced approach to strategy may be required of American-led military planning, that leverages coalition and virtual partners for the benefits that they afford, rather than seeking to employ such forces in a similar manner.

9. Conclusion

The power in leveraging information age concepts was apparent in the Kremlin's ability to win the Crimea⁶⁵ and Beijing's ability to seize the South China Sea.⁶⁶ It has been seen in the Libyan opposition following the Arab Spring, who "used social media and the Internet ... to contribute too many aspects of the fight."⁶⁷

The conduct of proxy warfare that leverages like-minded partners, will increasingly become the norm within this multipolar, constrained, security environment.⁶⁸ T.E. Lawrence said that the printing press is the greatest weapon in the armory of the modern commander. Taking this industrial age paradigm into the information age, may see a savvy officer with a Twitter handle, backed by big data analytics trawling open-source media, as the most important member of a battalion staff.

The utility of employing proxies to achieve strategic ends has increased with the arrival of the information age. This paper illuminates why proxy options appeal to government. The opportunities inherent in information age access, reach, and penetration to proxy forces overcome certain deterrence effects and thus appeal to political leadership. For the Australian Army and its partners, understanding information age proxy warfare will be a security imperative.

64. Rondeaux and Sterman, *Brief: Twenty-First Century Proxy Warfare*.

65. United States Army Special Operations Command, "*Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine, 2013-2014*" (Fort Bragg, North Carolina: United States Army Special Operations Command, June 2015), http://www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf, accessed 9 December 2017.

66. Brahma Chellaney, "Who Lost the South China Sea?," *The Strategist*, ASPI (15 June 2018), <https://www.aspistrategist.org.au/who-lost-the-south-china-sea/>.

67. John Scott-Railton, *Revolutionary Risks: Cyber Technology and Threats in the 2011 Libya Revolution* (U.S. Naval War College: CIWAG Case Studies, 2013), 112.

68. "The organization of violence has departed from the employment of the state's soldier as the primary bearer of the burden of warfare to a mode of war where technological and human surrogates enable the state to manage the risks of post-modern conflict remotely," Krieg and Rickli, "Surrogate Warfare," 113.



JOINT SPECIAL OPERATIONS UNIVERSITY
DEPARTMENT OF STRATEGIC STUDIES
7701 TAMPA POINT BLVD.
MACDILL AFB, FL 33621

