Australian Army
Research Centre

Special Information Warfare:

Evolving Australian and Allied Special Operations Forces to Fight and Win in the Chaos

Benjamin Johanson

Australian Army Occasional Paper No. 9

Australian Army
Research Centre

Special Information Warfare:

Evolving Australian and Allied Special Operations Forces to Fight and Win in the Chaos

Australian Army Occasional Paper No. 9

Serving our Nation

The views expressed in this publication are those of the author(s) and do not necessarily reflect the official policy or position of the Australian Army, the Department of Defence or the Australian Government.

ISSN (Online) 2653-0406
ISSN (Print) 2653-0414

All enquiries regarding this publication should be forwarded to the Director of the Australian Army Research Centre.

To learn about the work of the Australian Army Research Centre visit researchcentre.army.gov.au.

Contents

Foreword

The contemporary conflict environment is complex, cluttered and highly connected. In an urbanised, heavily populated, informationally dense environment, regular armed forces (including the ADF) now face an enormously varied and lethal range of both state and non-state threats. As Benny Johanson notes in this paper, the explosion of electronic connectivity since the turn of the century and the resulting rise in lethality and precision available to irregular warfare actors, along with the acceleration of great-power competition, have transformed the operating environment for Special Operations Forces (SOF). It is in the information domain, broadly understood—from narrative competition, through cognitive shaping of adversaries, to coercive statecraft that blends multiple elements of national power and, ultimately, kinetic disruption of cyber and information systems—that this transformation has been most rapid and intense.

This transformed operating environment, sometimes characterised as one of ‘grey zone’ conflict, hybrid warfare or liminal manoeuvre, has profound implications for every operator, not just for SOF. But the special operations space was one of the earliest to be affected by this transformation—in the emergence of Russia’s ‘little green men’ in Crimea, information-enabled special warfare in Iraq and Syria, and the rise of cyber-kinetic operations in great-power competition. As in previous eras, features that first appear in the special operations space soon proliferate, requiring adaptive responses from the whole force. Thus, this paper offers lessons for all operators, not just SOF. It suggests that, far from being a stand-alone form of conflict (or a bloodless replacement for lethal kinetic warfare), information represents an adjunct manoeuvre space that must be understood, exploited and dominated alongside traditional domains such as land, air, sea, the electromagnetic spectrum and, increasingly, the space-warfare domain.

Today, Australian planners face a much more threatening yet, somehow, far less concrete environment than at any time since the 1930s. As Johanson notes, the intangibility of information warfare—its ambiguity and cognitive slipperiness—makes grey-zone operations simultaneously more important and harder to grasp. This paper offers important insights for anyone seeking to get a grip of what has happened, what it means, and how we might adapt to it, now and into the future.

David Kilcullen

August 2021

Abstract

The proliferation of information technologies, the rapid pace of military modernisation and the return to great power competition are challenging traditional notions of national security as they apply to Australia and its coalition partners. The impact of information as it relates to modern warfighting is unhinging the asymmetries traditionally afforded to Australian and allied special operations forces (SOF) calling for new ideas, concepts and capabilities. To effectively respond to this evolving information-centric environment, a new way of warfighting is needed. Lessons from the US's 'Multi-Domain Operations' and Russia's 'New Generation Warfare' indicate that this new way of warfare requires an evolution in Australian special operations information warfighting capabilities. It is these capabilities that will position the Australian military to operate effectively in the grey zone between competition and conflict—a zone characterised by chaos: volatile, uncertain and ambiguous. This paper proposes special information warfare as a new capability for SOF to fight and win in the chaos.

Introduction

In a time of unprecedented global uncertainty, Australian SOF and its coalition SOF partners face rising challenges to protect national security interests and assure combat asymmetry on the future battlefield. This is due largely to the exponential expansion of the information environment (IE) which has become increasingly ubiquitous and is having more influence on the outcome of military operations across the spectrum of conflict than ever before.[1] The increasing role of information in modern warfighting is driving the need to change, whether it is recognised and acted upon immediately, or realised and reacted to once decisive contact with an adversary has willingly or unwillingly occurred.

While awareness of the challenges inherent in the contemporary IE remains nascent among some analysts, the implications of information warfare (IW) for national security have been known for over 20 years. They were clearly outlined back in 1997 by the US Naval War College when it identified that IW poses a new threat to a national security posture reliant on ‘secured lines of communication, friendly borders, unmatched human and material resources, unlimited mobilisation capability, and nuclear hegemony’.[2] More than two decades later, the threat posed by IW to national security has only intensified. SOF have long been charged to uphold the safety and security of Australian and coalition partner nations against foreign influence, interference and violence.

Although the challenge to be addressed is clear, the question remains: how do SOF evolve to meet the increasing challenges posed by an information-dominant environment to assure a credible national security posture against pacing global threats? The Chief of Army[3] has released several guiding documents to meet the growing demands of modern warfare and to appropriately drive change, modernisation and innovation within Army in order to support Australia's national security posture. A key contribution to Defence strategy and a consideration for Australia's allies is a fighting force that is both 'ready now' and 'future ready'. This position recognises the need for Army to maintain high levels of operational readiness while also focusing on force structuring, innovating and modernising for future conflict environments. The impetus is the rapid rate of regional military modernisation, the return to great power competition and the relevance of emerging technology—such as robotics and autonomous systems, artificial intelligence, quantum computing and big data—that has changed the nature of warfare. An additional multiplier is the increased pace with which new conflict environments are emerging due to the fast pace of innovation in emerging technologies. These factors constantly shift not only what 'future ready' might look like but also how asymmetry can be achieved to be 'ready now'.

As recognised as early as the 1990s (and arguably much earlier), IW has demonstrated the potential both to disrupt critical information infrastructure through cyber attacks and to facilitate broad-scale social unrest through social media and misinformation. The often intangible nature of IW and the accelerated pace of technological development pose serious issues for Australian and coalition partner SOF in their pursuit of asymmetric advantage against regional and global threats.

The Australian Army and Australian Defence Force (ADF) plan and contribute to operations across a spectrum of cooperation, competition and conflict. But there is a tendency for planning to be stove-piped, neglecting the overlapping zone between competition and conflict. This is a volatile, uncertain and ambiguous zone, which can be characterised as the chaos of conflict. Chaos, is one of the key changes in the character of war. It is directly linked to the rise of the information age, where cyberspace has weaponised the use of information, making it more insidious, undetectable and untraceable. This change is further characterised by the proliferation of information technology, advances in artificial intelligence (AI) and robotics and autonomous systems (RAS), and the increased number of attack surfaces available to operations conducted in, through and external to cyberspace. Australian and coalition partner SOF provide governments with the ability to respond to wicked problems on behalf of the nation in situations or crises without precedent. It is within the chaos of battle where SOF, more than any other Army or defence capability, have significant utility for government and military decision-makers.

While volatility was already a characteristic of the information age security environment, the COVID-19 pandemic has brought into sharp relief the need for nations to pre-emptively adapt. The pandemic has highlighted significant gaps in Australia's national security infrastructure and posture, with a lack of sovereign manufacturing capability, vulnerable international supply chains, and work-from-home information and communication infrastructure susceptible to cyber attack. The challenge posed by COVID-19 has affected the entire national security apparatus, not just SOF. But the national response to COVID-19 has fast-tracked the development of new concepts of national security based on cyber security alongside compatible emerging technologies such as AI, and these developments engage SOF interests more than most. It is incumbent upon SOF, as a contributor to the Defence enterprise, to create more agile approaches to innovation in order to gain and maintain IW asymmetry in the chaos.[4]

This paper takes a uniquely Australian perspective, recommending special information warfare (SIW) as a new contribution to Defence strategy. As the shift to great power competition continues, SIW presents as an opportunity to complement current Army, Defence, joint and whole-of-government information warfighting development initiatives in an effort to keep pace with emerging technologies, pacing global state-based threats and allied modernisation initiatives. It proposes what 'future ready' could look like for SOF armed with a cyber-enabled SIW capability. It also provides timely information-centric considerations for partners as focus shifts more heavily to great power competition in a time of heightened global instability and uncertainty.

The proposed 'future ready' cyber-enabled SOF emerges from an examination of trends in the employment of cyber and IW capabilities by US SOF under its multi-domain operations (MDO) national security and force posture, alongside Russia's new generation warfare (NGW) concept. It draws on experiential learning gained since the 2017 publication of the author's original underpinning work *Asymmetric Advantage in the Information Age: An Australian Concept for Cyber-Enabled 'Special Information Warfare'*.[5] That foundational paper proposed an approach of top-down *direction and resourcing* and bottom-up *action and innovation* to realise a SIW capability. This paper acknowledges several contemporary changes and challenges that have occurred since 2017 to both build and reinforce aspects of the original concept. It argues that land combat, cyberspace operations and information operations should not be conceived as independent stovepipes, and that the convergence of physical and non-physical domains amongst people will be the norm on the future battlefield.

This paper first examines Australia’s current state of play in light of the strategic direction provided by the Chief of Army, the operating environment, the convergence of technology and the need to think about ‘information’ differently. It then draws on insights from the US pursuit of the MDO operating concept from both a conventional and a SOF perspective to highlight the lessons that support the argument for an SIW capability. This is followed by an examination of Russia’s NGW theory and practice, providing a warning about warfare to come and the need for change to respond to emerging threats posed by such developments. Lastly, this paper draws together the key lessons from the US and Russian examples, underpinned by the strategic direction from the Chief of Army, to make the case for an SIW capability within Australian Special Operations Command. Its message is aimed at key political and military decision-makers that form part of the solution in modernising SOF. If nothing else, it serves as a warning that a lack of action in building an SIW capability heightens national security risks and could lead to *strategic miscalculation, operational paralysis* and *tactical irrelevance* on tomorrow’s battlefield.

Part 1: Future Ready': The Australian Army and Accelerated Warfare

The Chief of Army's Call to Be 'Future Ready' in an Uncertain Future

The Chief of Army has given marching orders to address the problem of being 'future ready'. In his 2020 Command Statement, Lieutenant General Rick Burr explains that 'being future ready is a way of challenging the status quo; constantly evolving and transforming how we think, equip, train, educate, organise and prepare for cooperation, competition and conflict'.[6] A series of nested strategic documents including *Army's Contribution to Defence Strategy, Aide for Army's Teams, Good Soldiering and Accelerated Warfare* underpin the Chief of Army's 'Army in Motion' narrative, acknowledging the need for change to meet the demands of the future. These demands include the rapid expansion of information technology, advances in RAS and AI and the pursuit by Australia's potential adversaries of technological advantage in those areas.

The Chief of Army's Command Statement captures the trends that demand attention regarding future force design, modernisation priorities and the future order of battle. This includes strategic competition where both state and non-state entities will exercise liminal[7] actions to operate below the threshold of conflict to achieve political and strategic goals, aiming to undermine traditional warfighting strengths of western militaries. Increased interconnectivity, globalisation and technology convergence have enhanced the speed at which decisions and action will take place in future conflict in both the physical and digital realms, and at strategic through to tactical levels. Traditional conceptual confinement of decisions and actions to a geographical battlefield are breaking down as contests occur across domains and geographic areas where strategic, operational and tactical effects can be delivered at much greater range and with much less attribution.

The combination of low-cost RAS and the increased employment of weaponised information technologies across all domains—at all ranges—not only highlights the borderless nature of contemporary warfare but also stresses the increasing convergence of physical, virtual and cognitive factors. Coupled with this convergence is the increased physicality[8] of the IE, where even though effects will be delivered in, through and external to cyberspace, they will ultimately require physical components, whether the human operator, the keyboard or computer, the data centre, the military long-range strike weaponry or space-based assets—all of which remain targetable in the physical domain and increase the lethality of the operating environment. The borderless nature of contemporary warfare will mean that the traditional 'area of operations' will not be the only place where attacks will occur.

In addition to the above, advances in AI will increase the speed of intelligence, surveillance, reconnaissance and targeting acquisition capabilities. This rate of change will challenge cognitive capabilities at all levels—from the strategic to the tactical—and also highlight the ethical choices around delegating decision-making to autonomous systems. In summary, the character of warfare has changed. This has been characterised by the Chief of Army as 'accelerated warfare' where 'geopolitics, technology and demographics are driving changes in the character of warfare at a rate faster than many of Army's processes, concepts, capabilities and structures were designed for'.[9] The changing character of war necessitates a review of Australia's national security posture using a whole-of-government approach alongside a review of Army's force structure and capabilities to support a new posture.

In the context of SOF potentially achieving greatest effect in the chaos, Australian and coalition partner SOF, in contributing to a new national security posture, must respond to these trends and remain ready to be tasked to operate during ambiguous levels of contest along the spectrum of conflict, either independently or forward of the joint force. To achieve the traditional special operations tenets of speed, surprise and stealth in an expeditionary environment—to provide *access, persistence* and *lethality* in support of the joint force—a step-change in capability is required. What is suggested is the introduction, experimentation and realisation of SIW as a contribution to Defence strategy and national security. The foundations for this enhanced SIW capability are outlined below.

The Capability Gap—an Absence of Cyber-Enabled Warfighting Capability at the Tactical Level

> *When our Commanders think of kinetic and non-kinetic effects as one and the same, we will be on our way to winning.*
>
> *Major General Marcus Thompson (Ret.)*[10]

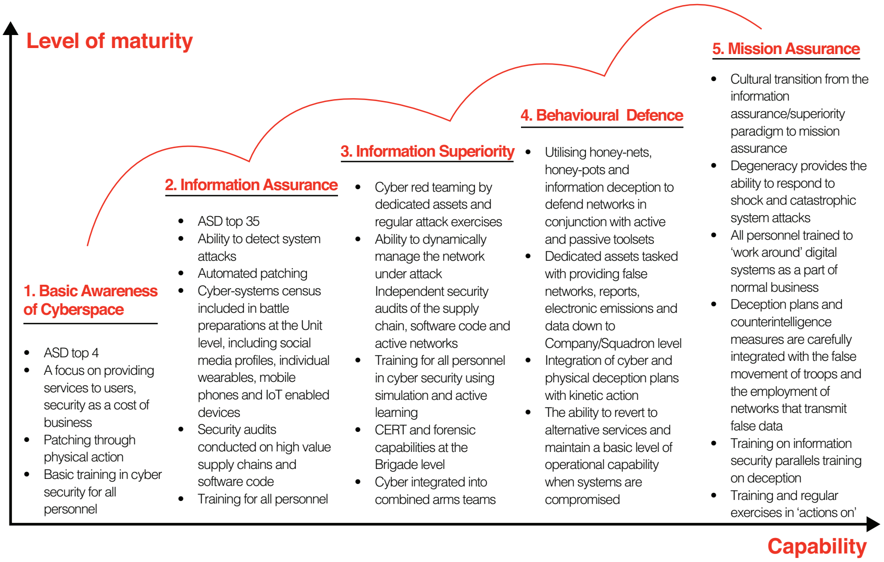
In June 2017, the Australian Government announced the establishment of an Information Warfare Division within the ADF. At the same time, the author's original concept paper for SIW was produced to spark top-down debate and bottom up action for a unique cyber-enabled SIW capability to deliver asymmetric advantage in the information age.[11] Since then, there has been relatively glacial movement in the implementation of information warfighting capabilities in Army, highlighting the need to move much faster to assure asymmetric advantage against pacing threats to national security in the immediate region.

Major General Marcus Thompson (Ret.), the architect of the Information Warfare Division, stated that 'whilst much needed progress has occurred, more needs to be done'. SIW represents a direct contribution to Major General Thompson's mission to ensure 'the ADF has the right people, skills, equipment and resources to combat the growing threat of IW to Australia's warfighting capability and Australia's national interests'.[12] In an address to the Australian Academy of Technology and Engineering in March 2019, Major General Thompson stated:

> *Information war bodes a new era of state-on-state conflict. It isn't just the 'same old thing' as wars we have already seen. It is real, present, different, dynamic and evolving…the information environment today is so pervasive that anything short of a full assessment of its reality could jeopardise Australia's ability to respond militarily in ways we are used to. The world has shifted. I believe we have to fundamentally shift with it.'*[13]

Currently, Australia's information warfighting capability primarily resides at the strategic level, functionally dislocated and disconnected from the tactical military action arms that will be required to operate in the chaos between competition and conflict. Capabilities resident within the Australian Signals Directorate (ASD) that would otherwise be supporting military operations in the lead-up to any conflict would likely be surging resources to counter liminal activities below the threshold of conflict on ASD's networks. This would limit their capacity to support tactical and operational demands. Figure 1 shows the span of responsibility of ASD and underscores its strategic orientation.

Figure 1: Cyber-maturity model[14]



1. Basic Awareness of Cyberspace

- ASD top 4
- A focus on providing services to users, security as a cost of business
- Patching through physical action
- Basic training in cyber security for all personnel

2. Information Assurance

- ASD top 35
- Ability to detect system attacks
- Automated patching
- Cyber-systems census included in battle preparations at the Unit level, including social media profiles, individual wearables, mobile phones and IoT enabled devices
- Security audits conducted on high value supply chains and software code
- Training for all personnel

3. Information Superiority

- Cyber red teaming by dedicated assets and regular attack exercises
- Ability to dynamically manage the network under attack Independent security audits of the supply chain, software code and active networks
- Training for all personnel in cyber security using simulation and active learning
- CERT and forensic capabilities at the Brigade level
- Cyber integrated into combined arms teams

4. Behavioural Defence

- Utilising honey-nets, honey-pots and information deception to defend networks in conjunction with active and passive toolsets
- Dedicated assets tasked with providing false networks, reports, electronic emissions and data down to Company/Squadron level
- Integration of cyber and physical deception plans with kinetic action
- The ability to revert to alternative services and maintain a basic level of operational capability when systems are compromised

5. Mission Assurance

- Cultural transition from the information assurance/superiority paradigm to mission assurance
- Degeneracy provides the ability to respond to shock and catastrophic system attacks
- All personnel trained to 'work around' digital systems as a part of normal business
- Deception plans and counterintelligence measures are carefully integrated with the false movement of troops and the employment of networks that transmit false data
- Training on information security parallels training on deception
- Training and regular exercises in 'actions on'

Figure 1 highlights that, depending on the level of maturity of ASD's cyber capability, it will be unable to support military operations on multiple fronts in a time of increased chaos and conflict.

The Need to Think Differently about Information

> *Given the increasing centrality of data and information to modern life and warfighting, the side that can accurately gather information, understand it correctly, and act on it more quickly—while resisting adversary attempts to exploit, disrupt, or deny this ability—will likely have a decisive advantage.*[15]

As already noted, the changing character of warfare is defined by the convergence of physical, virtual and cognitive realms as a result of the information age. This convergence disrupts our traditional understanding of geographically bounded tactical, operational and strategic actions and warrants a rethink of both national security posture and force structure and capabilities. For example, a tactical action conducted in (or through) cyberspace may achieve strategic effects or be conducted deep in contested territory without attribution. This necessitates a heightened acceptance of the fundamental centrality of the IE in war and how the intent around disruptive, defensive or offensive operations feeds into a national security posture that both protects and projects national power. Traditionally, western military planners who hear 'information' associate it with information operations as a narrow subset of information-related capabilities.[16] This fails to appreciate that the permeation of information has caused a convergence of physical and psychological aspects in contemporary warfare. It also fails to acknowledge that substantial physical effects can now be generated through the technical application of information.

While the character of warfare has changed as a result of the information age, the nature of war as a contest of wills has not. This contest exists in the minds of political and military decision-makers, adversaries and the population. Warfare is, and will ultimately remain, a human endeavour. But the fundamental centrality of information as it relates to our decision-making processes and perceptions is yet to be fully realised in western militaries. It is important therefore to understand what the information environment is, and why western militaries need to increasingly think about it as central to the character of war, including its impact on how wars will be fought.

The US Joint Operating Concept for Operating in the Information Environment 2018 defines the information environment as follows:

> *The IE is comprised of and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. The IE also includes technical systems and their use of data. The IE directly affects and transcends all OE.*[17]

This is the contemporary western description that most accurately captures the converging psychological and physical aspects, as well as the technical systems as they relate to physical and digital capabilities. It further supports the argument that the changed character of warfare necessitates adoption of information at the crux of military planning and operational art.

An important change since 2017 worth acknowledging is the announcement in 2018 by General Joseph Dunford approving information as the seventh joint warfighting function. This is the first modification to the joint warfighting functions in over 20 years.[18] The addition was intended to complement the desired end state of the 2016 Department of Defense Strategy for Operations in the Information Environment:

> *Through operations, actions and activities in the IE, DOD has the ability to affect the decision-making and behaviour of adversaries and designated others to gain advantage across the range of military operations.*[19]

The follow-on effects of the addition were modifications to US Doctrine JP 3-13 Information Operations and the generation of the Joint Concept for Operating in the Information Environment to acknowledge and institutionalise information as a joint warfighting function.[20] Both changes recognise the need to deepen the relationship between physical and informational power, and that:

> *To achieve success in the future security environment, the Joint Force must shift how it thinks about information from an afterthought and the sole purview of information professionals to a foundational consideration for all military activities.*[21]

US Doctrine JP 3-0 Joint Operations, which was updated in October 2018, accurately captures the increasing importance of information as it relates to the contemporary operating environment:

> *To operate effectively requires understanding the interrelationship of the informational, physical, and human aspects that are shared by the OE and the information environment. Informational aspects reflect the way individuals, information systems, and groups communicate and exchange information. Physical aspects are the material characteristics of the environment that create constraints on and freedoms for*

> *the people and information systems that operate in it. Finally, human aspects frame why relevant actors perceive a situation in a particular way. Understanding the interplay between the informational, physical, and human aspects provides a unified view of the OE.*[22]

There are a number of reasons that necessitate a greater acknowledgement of information's centrality to all warfighting functions. The traditional reliance on information operations as a subset of joint planning as a staff function in western application of military power will not provide the necessary combat advantage in an era of accelerated warfare. A battlefield that, as a result of information technology, now spans the perceived safety of sovereign bases and infrastructure—across strategic distances to adversarial held territories—necessitates a greater understanding of information across all warfighting functions. As noted in the US 2018 National Cyber Strategy, information (as it relates to warfare) is also an integral and fundamental component of 'financial, social, government, and political life'.[23] This definition firmly establishes information as a substantial and ongoing threat to national and global security. Cyber attacks by Russia, China, Iran and North Korea in recent years have targeted perceived vulnerabilities in private and public cyber infrastructure and commercial activities, costing trillions of dollars. These attacks have also 'exploit[ed] cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners' and challenged the US values of 'belief in the power of individual liberty, free expression, free markets, and privacy'.[24] The challenge to national security posed by IW is reflected in the US MDO concept described below.

Technology Convergence—Increased Physicality of the Information Environment

Technology has also converged as a result of the IE. A hyperconnected operating environment spanning all domains, all the way from sovereign to adversary held territory, continues to be disrupted by emergent technologies in the fields of RAS, AI and big data. The proliferation of RAS and unmanned aerial systems, plus internet protocol connected warfighting capabilities, have merged the physical and non-physical environments. The IE permeates all physical domains, and effects generated in—and through—the IE will have significant and continuing effects in the physical world. This situation will require SOF to generate the ability to effectively *function* against command, control, communication, computers, intelligence, surveillance, reconnaissance, electronic warfare (C4ISREW) disruption and degradation in order to achieve set mission profiles.

The pursuit of human-machine teaming (HUMT) at lower tactical echelons within the US, Russia and most contemporary militaries provides an example of the convergence of the physical and virtual realms. Advances in AI[25] military application, coupled with HUMT capabilities, highlight the increasing number of connected physical and virtual entities influencing the speed at which data sharing and decision-making will occur on the modern battlefield. This technology convergence links to the overwhelming centrality of information and its impact on contemporary warfighting, as all connected devices will require assured data, electromagnetic links and electrical power to function effectively.

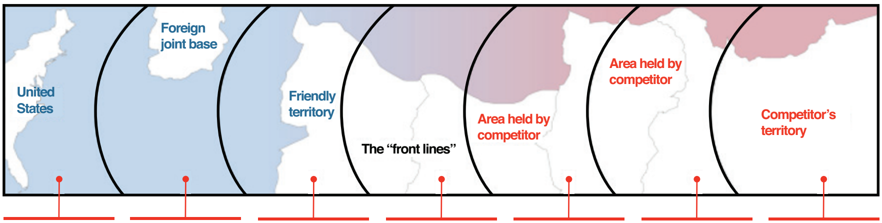
Part 2: US Multi-Domain Operations and the Future of US Special Operations Forces

Overview of Multi-Domain Operations

Another change since the inception of the SIW concept and the establishment of the ADF Information Warfare Division in 2017 is the refinement of the original MDO concept by the US Army into the operating concept The U.S. Army in Multi-Domain Operations 2028. This refinement aims to more accurately capture the holistic nature of operating across domains and to drive tangible change down to the tactical level. It acknowledges the inherently joint nature of modern warfare and provides much more detail on how to apply MDO as a 'basis for functional concept development, further experimentation and force development'.[26]

As the Australian Army is challenged to 'constantly evolve and transform how we think, equip, train, educate, organise and prepare for cooperation, competition and conflict',[27] so too is the US Army. To achieve this the US Army is adapting doctrine, organisation and training to develop a fighting force capable of engaging in great-power competition with Russia and China through multi-domain operations by 2028.[28] This is in recognition of the 'strategic atrophy'[29] sustained after more than two decades of counterinsurgency operations, and a threat-based requirement to return to great-power competition. Figure 2 illuminates the expanded battlefield in the context of MDO.

Figure 2: US Army's expanded battlefield in multi-domain operations



Strategic Support Area
Extends from a theater of operations to the United States, or another combatant commander's area of responsibility, and includes the air and seaports supporting the flow of forces into the theater. Most friendly space and cyber capabilities are controlled from here. Assumed to be under surveillance at all times and targeted by long-range cyber and strike capabilities.

Operations Support Area
Friendly-held area where many key Joint Force command and control, sustainment, and air-or-sea-based strike capabilities are located. This area normally encompasses many entire nations; assumed to be targeted by enemy reconnaissance, information warfare, and long-range strike capabilities.

Tactical Support Area
Area held by friendly forces that directly enables military operations by providing sustainment, artillery, and command and control. Friendly units must be able to endure enemy information warfare, unconventional warfare, and artillery, and defeat infiltrating enemy ground forces.

Close Area
Friendly and enemy formations are imminent physical contact. A commander's ability to take advantage of multi-domain effects from formations away from the battle is limited due to the immediacy of combat.

Deep Maneuver Area
Highly contested area held by a competitor where friendly ground forces can operate, but commanders must make a concerted effort to do so. Ground operations require significant support from air, cyber, and space domains. Generally, the objectives of an offensive military campaign lie within this area.

Operational Deep Fires Area
Territory held by a competitor that is potentially targetable by friendly artillery, air strikes, space and cyber capabilities. Operations here may seek to disrupt the enemy's operational reserves or prevent long-range cannon, rocket, or missile fires. Only friendly special operations ground forces operate here.

Strategic Deep Fires Area
A competitor's home base, generally unreachable by friendly ground forces due to geography or policy (e.g., on the other side of an international border). Potentially targetable by space and cyber capabilities.

Figure 2 reinforces the borderless nature of the operating environment and the growing need to have capable forces able to operate effectively in all areas, in both the physical and virtual realms.

Operational Focus of MDO

From an operational standpoint, the US MDO operating concept aims to solve the military problem of 'how does the Army enable the joint force to compete with China and Russia below armed conflict, penetrate and dis-integrate anti-access and area denial systems and ultimately defeat them in armed conflict and consolidate gains, and return to competition?'.[30] The US Army has broken this military problem down to address five problems posed by great-power competitors in competition and conflict:

> *#1 How does the Joint Force compete to enable the defeat of an adversary's operations to destabilize the region, deter the escalation of violence, and, should violence escalate, enable a rapid transition to armed conflict?*
>
> *#2 How does the Joint Force penetrate enemy anti-access and area denial systems throughout the depth of the Support Areas to enable strategic and operational maneuver?*

> *#3 How does the Joint Force dis-integrate enemy anti-access and area denial systems in the Deep Areas to enable operational and tactical maneuver?*
>
> *#4 How does the Joint Force exploit the resulting freedom of maneuver to achieve operational and strategic objectives through the defeat of the enemy in the Close and Deep Maneuver Areas?*
>
> *#5 How does the Joint Force re-compete to consolidate gains and produce sustainable outcomes, set conditions for long-term deterrence, and adapt to the new security environment?*[31]

Figure 3 provides a graphic depiction of how these problems superimpose on the MDO framework. Of note, it highlights the narrow, yet very important, gap between competition and conflict. This area of chaos is where forward operating forces, primarily SOF, will experience deep targeting of C4ISREW networks, disrupted communications, denied navigation and timing, unconventional warfare and IW disrupting the ability to function and target adversarial decision-making systems in support of larger follow-on forces. In this zone, the ability of SOF to accurately inform decision-makers to avoid confrontation with a level of assurance in a timely manner will also be challenged.

Figure 3: **Five problems superimposed on the MDO framework**[32]

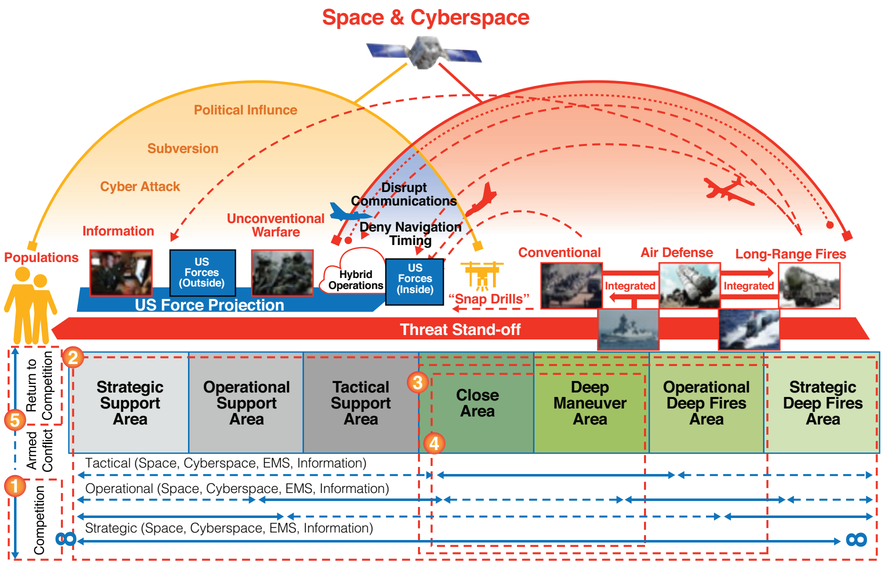
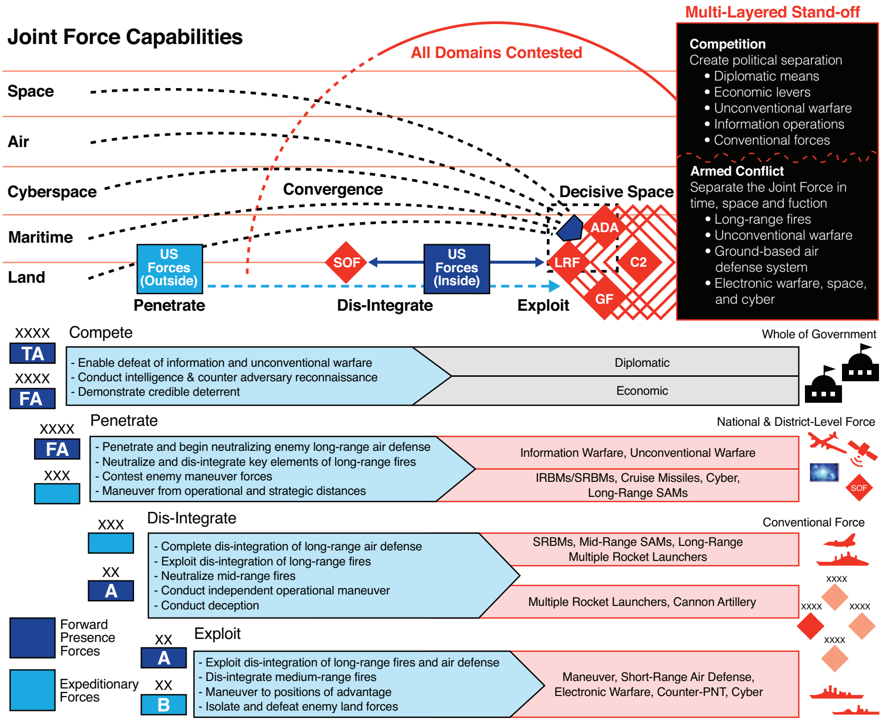


Figure 3 overlays the problems identified onto the MDO framework, illuminating the borderless nature of MDO and the gap between competition and conflict. Although far smaller in size and capability, the Australian Army will also be forced to address the same problem in support of a joint force facing an adversary with peer or superior capabilities. This further exemplifies the requirement to adopt the lessons offered from MDO and apply them to the unique model of SIW (addressed later in the paper) in order to function, while providing *access, penetrating adversary decision-making systems* and providing *lethality* across the spectrum of conflict.

There are significant operational applications within the MDO 2028 operating concept which could be applied to smaller western militaries such as Australia's. However, one of the more applicable upgrades in the 2018 MDO operating concept—one that is central to supporting the need for an SIW capability—is the redefined consideration of 'convergence',[33] which aims to create cross-domain synergy and layering of options across domains to improve friendly freedom of action and impose complexity on an adversary.[34] Figure 4 provides a graphic depiction of MDO solutions, highlighting the ambiguity between competition and conflict, which is not addressed in detail.

Figure 4: MDO solutions for convergence into decisive spaces[35]


Joint Force Capabilities
Multi-Layered Stand-off
All Domains Contested
Space
Air
Cyberspace
Maritime
Land
Convergence
Decisive Space
US Forces (Outside)
SOF
US Forces (Inside)
LRF
ADA
C2
GF
Penetrate
Dis-Integrate
Exploit
Competition
Create political separation
• Diplomatic means
• Economic levers
• Unconventional warfare
• Information operations
• Conventional forces
Armed Conflict
Separate the Joint Force in time, space and fuction
• Long-range fires
• Unconventional warfare
• Ground-based air defense system
• Electronic warfare, space, and cyber
XXXX TA
XXXX FA
Compete
Whole of Government
- Enable defeat of information and unconventional warfare
- Conduct intelligence & counter adversary reconnaissance
- Demonstrate credible deterrent
Diplomatic
Economic
XXXX FA
XXX
Penetrate
National & District-Level Force
- Penetrate and begin neutralizing enemy long-range air defense
- Neutralize and dis-integrate key elements of long-range fires
- Contest enemy maneuver forces
- Maneuver from operational and strategic distances
Information Warfare, Unconventional Warfare
IRBMs/SRBMs, Cruise Missiles, Cyber, Long-Range SAMs
SOF
XXX
XX A
Dis-Integrate
Conventional Force
- Complete dis-integration of long-range air defense
- Exploit dis-integration of long-range fires
- Neutralize mid-range fires
- Conduct independent operational maneuver
- Conduct deception
SRBMs, Mid-Range SAMs, Long-Range Multiple Rocket Launchers
Multiple Rocket Launchers, Cannon Artillery
XXXX
XXXX
XXXX
XXXX
Forward Presence Forces
Expeditionary Forces
XX A
XX B
Exploit
- Exploit dis-integration of long-range fires and air defense
- Dis-integrate medium-range fires
- Maneuver to positions of advantage
- Isolate and defeat enemy land forces
Maneuver, Short-Range Air Defense, Electronic Warfare, Counter-PNT, Cyber

This application of cross-domain capability is underpinned by 'stimulate-see-strike' or 'see-strike' combinations to 'disrupt, degrade, destroy or disintegrate enemy systems or create windows of superiority to enable friendly exploitation of the initiative'.[36] This is an important consideration as it provides a foundational aiming mark for the development of scaled 'convergence' capabilities needed by middle powers to achieve the same 'stimulate-see-strike' or 'see-strike' combinations to target enemy systems or create windows of opportunity. This resonates with contemporary employment of SOF in the understanding of relative superiority[37] and the 'find, fix, finish, exploit, analyse, disseminate' (F3EAD)[38] targeting model, and can be adapted to demonstrate cyber-enabled targeting and strike capabilities as part of an SIW operating concept.

Organisational, Training and Workforce Considerations to Realise MDO by 2028

In 2017, the US Army was only just beginning to figure out what was required to execute the MDO operating concept. Since then, the US Army has focused heavily on four areas: doctrine review, organisation and workforce changes, training model review, and modernisation. The US Army is currently reviewing and updating its doctrine to include aspects of MDO, with a significant focus on cyberspace and the electromagnetic spectrum.[39]

To achieve the organisational demands of the MDO operating concept, the US Army is moving at an accelerated pace and accepting increased levels of risk. This pursuit involves the recent creation and design of a number of new cyberspace and electronic warfare (EW) units to realise the MDO concept. This includes the 915th Cyber Warfare Support Battalion, and new EW companies and platoons.[40] The 915th Cyber Warfare Support Battalion will look to provide offensive cyberspace operations across corps, division and brigade combat teams.[41] Electronic warfare capabilities will be fielded to plan and conduct EW operations at corps level and below.[42] Additionally, a recently activated intelligence, cyber, electronic warfare and space (ICEWS) unit will provide planning and direct operations across multiple domains and in any area of the battlefield.[43] The US Army is seeking to field two ICEWS units by the end of 2020 as part of a larger multi-domain task force.[44] Lastly, the US Army is conducting a significant restructure to create cyberspace and electromagnetic activities planning teams in the headquarters of over 125 Army formations ranging from Special Forces units to theater-level Army headquarters.[45]

The collective training focus at the US Army's combat training centres has shifted from a focus on counterinsurgency operations to operations against great-power competitors. Commander US Army Forces Command guidance for 2019 focused heavily on training for MDO, with direction to design 'warfighter exercises that focus on units conducting operations in contested EW, cyber and space environments'.[46] The US Army is also addressing its workforce training model for cyberspace and EW personnel to include a review of the US Army Cyberspace Operations Training Strategy to account for new doctrine, equipment, and tasks to be performed by newly raised units.[47] The US Army is pursuing a cyber training solution called the Persistent Cyber Training Environment to allow for experimentation, unit certification, and assessment and development of the cyber mission force in a virtual environment.[48] One observation is the substantial focus on training, certification and execution in a virtual environment. Consideration of more disaggregated multi-domain capabilities within an Australian Army context should take into account the centrality of the IE as it permeates into physical domains.

The US Army as an Innovation Leader

To achieve the modernisation requirements necessary to achieve the MDO operating concept, the US Army established Army Futures Command in July 2018 at Austin, Texas. Army Futures Command has been described as 'the vehicle that the Army will use to break free of its Industrial Age business model to move at the speed of the Information Age'.[49] Army Futures Command provides an interesting point of reflection for the Australian Army—that doctrine, organisational change and training models need an equally agile, innovative modernisation function to keep pace with the increasing rate of technological change in the information age. The US Army identified six capability areas critical to operationalising MDO, built a four-star headquarters and six cross-functional teams, and is now focusing on a 'need for speed', accepting risk in innovation and experimentation and addressing its innovation culture. The US Army has focused its modernisation on long-range precision fires, next-generation combat vehicles, future vertical lift, Army network, air and missile defence, and soldier lethality—all of which ultimately have an interrelated relationship with information technology. This is an important consideration when thinking deeply about future cross-domain capabilities that will be needed to *function* with information assurance. It highlights the requirement to invest heavily in information warfighting capabilities that span the tactical to strategic levels, from the individual operator through to strategic long-range precision strike capabilities. The establishment of a four-star command—to match the operational, organisational and training changes to meet the MDO operating concept end state—highlights the importance of matching the modernisation effort with operational concept realisation.

Challenges with Accelerated Execution and Innovation

A number of challenges the US Army is facing regarding the accelerated growth of specialist capabilities in ICEWS were raised in a 2019 report by the US Government Accountability Office.[50] The findings offer a valuable insight about the difficulty in effectively raising and equipping cyberspace and EW capabilities to realise the MDO concept.

The accelerated rate of restructuring and change within the US Army brings with it a number of difficulties, challenges and increased acceptance of risk. For example, the US Army activated its first ICEWS unit in 2018 as a pilot with only 32 per cent of its personnel, and not necessarily with people holding the right skills.[51] Additionally, as of March 2019 the 915th Cyber Warfare Support Battalion was operating with only 20 per cent of its dedicated staff.[52] The US Government Accountability Office report also indicates a lack of risk assessment in activating the ICEWS capability, and that its implications in the provision of capability in support of the multi-domain task force may not be fully understood.

The ICEWS capability rollout provides three critical lessons for the Australian Army, specific to the raising of an SIW capability. The first stems from the report calling for increased risk assessment prior to activation. While this is a valid consideration in the context of the US Army, the current Australian Chief of Army's mantra of 'think big, start small, and move fast' challenges commanders to intelligently accept increased risk in the pursuit of being 'future ready'. Through experimentation and intelligent failure, commanders can build small, technologically enabled units of action that can provide the asymmetric combat advantage necessary to fight and win in the chaos. This indicates acceptance of organisational, technological and human factors risk which should be accepted through specific experimentation and innovation activities within Army. This lesson acknowledges a fundamental *need* for accelerated execution in an era of 'accelerated warfare'.

The second lesson that can be gleaned from the US example is that getting the right personnel into specialist cyberspace and EW roles will be equally challenging, even considering the substantially reduced scale of any future workforce. This is due to the high demand for skilled personnel across the whole-of-government enterprise, which requires a large portion of skills transfer to support other activities across the Defence and government enterprise.

As a contemporary contribution to special operations theory, SIW looks to address these lessons and capability demand signals. It also serves as an opportunity to further identify the requirements to scale a tactically oriented, strategically enabled, technically proficient cyber-enabled information warfighting capability. Components of this have been understood by US Army SOF (ARSOF), which has sought to identify the future value proposition of SOF in relation to great-power competition.

The Future of US Special Operations Forces in Great Power Competition

> *The 2018 National Defense Strategy was clear in its call to shake off strategic atrophy—to maintain competitive advantage against our Nation's adversaries we must evolve … The ARSOF Strategy charts our course to drive evolutionary changes in how man, train and equip our formations in the Information Age.*[53]

As the US Army and US Department of Defense transition to great power competition, the US SOF enterprise has also begun to question its value proposition as it transitions to be able to contribute in peer-on-peer or state-based conflict against capable adversaries.

In 2012, then US SOCOM Commander Admiral William McRaven provided a description of US SOF applying direct and indirect approaches.[54]
In addressing what has changed for SOF since 2012, the evolved character of warfare indicates that the application of direct and indirect approaches is absolutely immersed in activities and actions involving the IE. Whether it is activities conducted in (or through) cyberspace or conducted utilising the electromagnetic spectrum, or physical activities disrupting adversaries' information technology critical infrastructure, SOF direct and indirect approaches are evolving to accept the impact the information age has had on the character of warfare.

In a March 2019 recommendation to US Congress, a call was made for the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict to review United States Special Operations Command (USSOCOM) for the 'purposes of ensuring that the institutional and operational capabilities of special operations forces are appropriate to counter anticipated future threats across the spectrum of conflict'.[55] The transition to great-power competition indicates the requirement to balance SOF capabilities to be able to address the chaos between competition and conflict.

In the original 2017 SIW concept paper, the ARSOF 2022 paper, published in 2014, was reviewed, including the core competencies of 'Special Warfare'[56] and 'Surgical Strike'.[57] The updated doctrine reaffirms the core competencies as outlined in ARSOF 2022. It also reinforces the impact of the IE, highlighting the continued absence of a core competency that specifically leverages (or counters) adversaries' IW capabilities as they relate to SOF operations. A point worth stressing is that traditional information operations remain deeply nested as one of 13 special operations activities.[58] The isolated or stove piped nature of information operations capabilities, without a unified operating concept addressing the centrality of information as it relates to SOF operations, is destined to limit the effectiveness of SOF in future competition, chaos and conflict.

In the lead-up to conflict, US Army SOF tasks include:

> *… operate in denied areas to leverage indigenous populations and other human networks, open denied areas,thwart anti-access efforts, facilitate and execute deep operations for joint task force component commanders, provide sensors, combat information, and intelligence from beyond the fire support coordination line and conduct combat identification to inform engagement decisions.*[59]

This list is drawn directly from US Army Defence Publication (ADP) 3-05. Given the changed character of war, the ability to achieve such tasks will require an ability to *function*. This in turn implies assured communications and dominance over the electromagnetic spectrum to achieve sufficient force projection and application.

The ARSOF Strategy document of 2019 acknowledges that there is a tangible shift in SOF operations moving away from inhabiting secure forward operating bases, to 'surviving and thriving in large-scale combat operations'.[60] This sees ARSOF aim to 'provide the nation with disciplined and premier problem solvers who are the Army's force of choice in completion and set conditions to win in war'.[61] A key lesson that can be drawn from the ARSOF Strategy document is an acknowledgement of global hyper-connectivity and an expanded competition space as it relates to the operating environment. This approach is consistent with the rapid diffusion of technological change that will 'favor those with the agility and creativity to quickly exploit emerging capabilities and *weaponize information'*.[62] It also recognises the expanded competition space, giving weight to an understanding that chaos exists between competition and conflict where 'rapid technological change will expand the competition space across the physical, virtual and cognitive aspects of the environment'.[63] Importantly, this document acknowledges ARSOF's contribution to MDO both in competition below armed conflict and in large-scale combat operations.

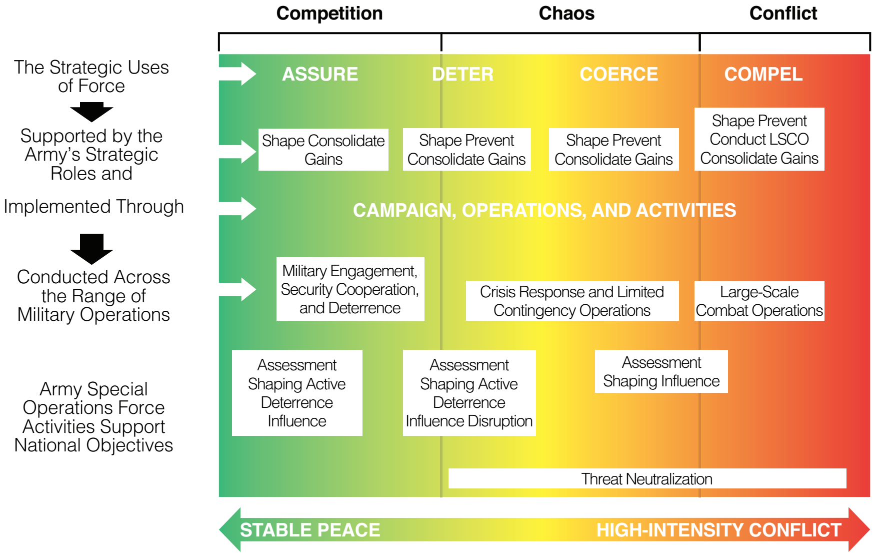
The July 2019 release of the updated *ADP 3-05 Army Special Operations* also provides insight into how US ARSOF is looking to address a return to great-power competition. The doctrine provides an overview of how 'Army meets the Joint Force Commander's needs to achieve unified action by appropriately integrating Army conventional and special operations forces'.[64] US Army Special Operations Command (USASOC) and its subordinate units provide a useful case study, as they look to:

> *… support objectives that focus on deterring, preventing, or resolving joint transregional, all-domain, and multifunctional threats and conflict, as well as supporting Army operations over a multi-domain extended battlefield.*[65]

One of the key challenges that makes an appearance in this doctrine is the 'effects created by the speed, propagation, and reach of information'.[66] Combined with the directed operational imperatives of 'understand the operational environment … anticipate psychological effects and the impact of information … provide sufficient intelligence'[67] and the challenge presented by the IE, USASOC has recognised an important factor—the centrality of information as it relates to the success of future SOF operations. To be *discreet, precise and scalable*, US ARSOF needs to be able to *function* during the stages of conflict in order to ensure a high level of confidence in the information utilised to achieve the operational imperatives listed above.

In further understanding ARSOF's focus as outlined in the ARSOF Strategy, the stated challenges stress the advantages that an SIW capability would offer to fill the void between surgical strike and special warfare. Additionally, such capability would complement conventional MDO, aiming to achieve convergence over multiple domains and across multiple battlefield areas. Figure 5 highlights that the use of force, roles, range of operations and objectives for US ARSOF still amounts to a relatively reactive posture in the chaos between competition and conflict. The figure has been adapted to stress the gap between competition and conflict.

Figure 5: Employment of SOF activities at stages of conflict[68]


Competition
Chaos
Conflict
The Strategic Uses of Force
ASSURE
DETER
COERCE
COMPEL
Supported by the Army's Strategic Roles and
Shape Consolidate Gains
Shape Prevent Consolidate Gains
Shape Prevent Consolidate Gains
Shape Prevent Conduct LSCO Consolidate Gains
Implemented Through
CAMPAIGN, OPERATIONS, AND ACTIVITIES
Conducted Across the Range of Military Operations
Military Engagement, Security Cooperation, and Deterrence
Crisis Response and Limited Contingency Operations
Large-Scale Combat Operations
Army Special Operations Force Activities Support National Objectives
Assessment Shaping Active Deterrence Influence
Assessment Shaping Active Deterrence Influence Disruption
Assessment Shaping Influence
Threat Neutralization
STABLE PEACE
HIGH-INTENSITY CONFLICT

Legend LSCO: large-scale combat operations

While ADP 3-05 acknowledges the centrality of information as it relates to SOF missions, it still falls short of acknowledging the requirement for a full-spectrum, multi-domain SIW capability able to effectively operate in chaos.

Lessons from US MDO and US SOF Modernisation

US and coalition SOF have been executing high-end, intelligence-driven targeting operations against terrorist threats for decades. This has resulted in the capabilities needed for great power competition becoming atrophied. The requirement to counter extremist threats is unlikely to subside. However, risk needs to be taken to ensure SOF are poised appropriately to meet the demands of the future operating environment against adversaries employing potent hybrid tactics. While the above review captures the changes US ARSOF is looking to make in strategy and doctrine to acknowledge the importance of the information age, there are four key considerations that should drive future SOF modernisation.

Firstly, the collection and use of intelligence has been—and will continue to be—fundamental to future SOF operations across the spectrum of conflict, especially in the chaos between competition and conflict. The traditional F3EAD model will be challenged against peer-adversaries. Reliance on human intelligence (HUMINT) and signals intelligence (SIGINT) to inform decision-making in times of uncertainty and volatility will increase and ultimately require a layered collection capability ranging from forces forward deployed in denied or contested areas through to strategic collection agencies to provide accurate and reliable intelligence. This will require closer relationships with partner and proxy forces, with intelligence collection organisations providing HUMINT, SIGINT and open-source intelligence (OSINT) capabilities at the edge.[69] The proliferation of information technology and the convergence of physical, virtual and cognitive realms will challenge the F3EAD cycle's ability to *function* as adversaries aim to disrupt, dissuade, misinform and deny access to information to inform intelligence requirements.

Secondly, people are the cornerstone for any future SOF operating concept. The SOF truth that 'people are more important than hardware' remains enduring. While the operating environment is increasingly becoming hyper-connected in both physical and digital realms, the requirement for complex problem-solvers, networkers and innovators who can operate under high stress, and in denied environments will remain. As Lieutenant General (Ret.) Tovo, previous US Army Special Operations Forces commander, stated:

> *We are selecting and assessing individuals based on a series of character traits that all add up to what we believe is the right kind of person to do this work … It's always being refined,*

> *especially as we now try to apply big data and machine learning to finding people. What is it in someone's background that allows them to succeed?*
>
> *In the end, we're looking for people who are empathetic, adaptive problem-solvers, who don't freak out in the complexity of chaotic situations … One of my predecessors used to say, "Our job is to wade into chaos and manage it." Our missions are often undefined—go in and figure it out, you tell us what the mission is. Write your own problem statement.*[70]

How and who to appropriately select, train and equip for the future threat requires consideration to ensure the right people are being recruited to meet the needs of any evolving SOF enterprise.

Thirdly, cyber-enabled warfighting capabilities need to be considered equally important as the traditional SOF warfighting capabilities. Selecting, training, equipping and operationalising cyber-enabled forces able to operate across the spectrum of conflict, especially in the chaos, in symbiosis with traditional physical capabilities, is fundamental to SOF survival in future conflict. This acknowledges not only the centrality of information in future warfare but also the convergence of physical, virtual and cognitive realms.

Lastly, there is a growing demand to institutionalise innovation and experimentation at lower tactical echelons, seeking to employ blended cyber-kinetic effects. Similarly to the MDO operating concept, the ARSOF Strategy can only be realised by resourcing the right people with the right ideas in the right places. The US Army has built a four-star command to address this need. USSOCOM has invested heavily in the SOFWERX model to harness industry, academia and the scientific community to move fast in solving innovative SOF solutions.

The Australian Army and its SOF equally need to invest, take intelligent risk, and 'think big, start small and move fast', which requires a modernisation guidance similar to that of MDO and the ARSOF Strategy. It also requires relative and commensurate dedicated innovation and experimentation capabilities at the edge, and an acceptance that accelerated change comes with its complexities and risks. The need to accept increased complexity and risk in execution is reinforced by understanding Russia's approach, which continues to threaten western power and influence in the wake of the global COVID-19 pandemic.

Part 3: Russia's New Generation Warfare in Theory and Practice and a Warning of Warfare to Come

Defining New Generation Warfare (Voini Novogo Pokoleniia)

> *Over the last several years, Russian experts have been energetically conceptualising the changing character of war. This activity, aimed at analysing the emerging military regime and at distilling relevant military innovation, has been an old Soviet-Russian military tradition.*[71]

As the US and its coalition partners have been heavily engaged in counter-terrorism operations over the last two decades, Russia has been actively seeking out how to undermine western power and influence. This has manifested in NGW, often referred to as hybrid warfare, and has been observed in operations in Ukraine and Syria. The Russian example offers a warning of warfare to come, demonstrating how the character of warfare has changed. Russia has acknowledged the centrality of information and harnessed the convergence of physical and virtual capabilities from the tactical through to the strategic level, with the employment of Spetsnaz SOF supported by strategic cyber-enabled information warfighting capabilities. Their example, while offering a warning, stresses the requirement to have a foundational cyber-enabled information warfighting capability that can operate across the spectrum of conflict if asymmetric success and information dominance is to be attained in future competition, chaos and conflict.

Russian NGW theorises victory by minimising kinetic fighting, defeating an adversary through non-military forms of influence, and maximising cross-domain coercion (Adamsky, 2015, p.22).[72] Russian modus operandi has often been misrepresented as 'hybrid warfare' by western analysts. The term 'hybrid warfare' originally appeared in western sources in the mid to late 2000s with little reference to the Russian way of warfare, focusing more on Israeli and western warfighting against non-state entities in the Middle East.[73] This is an important distinction as the US transitions to MDO and cross-domain manoeuvre. A true understanding of NGW provides insight into how Russia aims to reduce western political and military power and influence by adopting capabilities brought about by the emergence of the information age and the proliferation of information technology.

Numerous titles have arisen to codify Russia's contemporary approach to warfare; they include 'hybrid warfare', 'not so new warfare', 'non-linear warfare' and 'New Generation Warfare'. The Russian-preferred term New Generation Warfare best captures Russia's acknowledgement of the growing trend in how wars are fought, and how the character of war has changed, and is not necessarily a newly devised strategy.[74] NGW has also been referred to as the 'Gerasimov Doctrine', which was originally coined by Dr Mark Galeotti, a modern Russia scholar, in 2014 after translating an article by General Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, on 'the value of science in foresight' published in the Military-Industrial Kurier in 2013.[75] The term 'Gerasimov Doctrine' has since been retracted by Galeotti,[76] who stated that it was not a 'blueprint' or actual Russian doctrine and was 'more a description of how the Russian General Staff interprets contemporary *Western* methods of warfare'.[77]

While it is not a blueprint or doctrine, Gerasimov's description and ideas in the 2013 article outlined key features of future warfare which underpin the NGW operating concept and have since been seen in action during Russia's annexation of parts of Ukraine. NGW includes a focus on undeclared actions, the consistent use of kinetic and non-kinetic tools in close coordination, blurred military and civilian domains, and battles that take place in the information space as well as physical arenas.[78] It draws a parallel with the US understanding of convergence between physical, virtual and cognitive realms and applies this specifically to the ability to exert power and influence.

NGW is the amalgamation of hard and soft power across numerous domains, through the application of coordinated military, diplomatic and economic tools, representing an approach targeted at national and global security vulnerabilities across the spectrum of conflict.[79] The ratio of non-military or non-kinetic effects to military or traditional kinetic effects is underpinned by a four to one ratio.[80] Initial targeting of the population, economic destabilisation, suppression of civil resistance and disruption to critical military and state infrastructure, underpinned by selective application of intelligence capabilities, SOF, conventional capabilities, mercenaries and proxies, constitute the characteristics of NGW.[81] This operational preparation of the environment, utilising cyber-enabled tools with forward-deployed SOF (as seen in Ukraine) offers a warning of adversarial action where the gap between competition and conflict can vary and chaos can span geographic boundaries below the threshold of declared war. Effectively operating in such a contested space presents a dilemma for SOF in their efforts to provide strategic utility for the joint force.

The proliferation of information technology, especially in the early stages of NGW, has provided greater penetration of asymmetric actions against critical elements and systems of an adversary.[82] This is magnified by the increasingly connectedness of battlefields, opening the attack surface aimed at targeting state, political, diplomatic, social, technical, sociotechnical, energetic, financial, cyber, socio-cyber and information systems.[83]

NGW across the Stages of Conflict

In understanding the requirement for an SIW capability to gain and attain asymmetric advantage across the spectrum of conflict, it is worth highlighting how the information age has changed the character of warfare as it applies to NGW. Russia's approach seeks to wage a type of warfare that combines political, economic, social and kinetic in a style that 'recognises no boundaries between civilian and combatant, covert and overt, war and peace'.[84] This is a direct targeting of national and global security postures where multiple components may be challenged simultaneously, requiring agile and innovative responses—particularly in the chaos between competition and conflict where intent and attribution may not be easily identifiable.

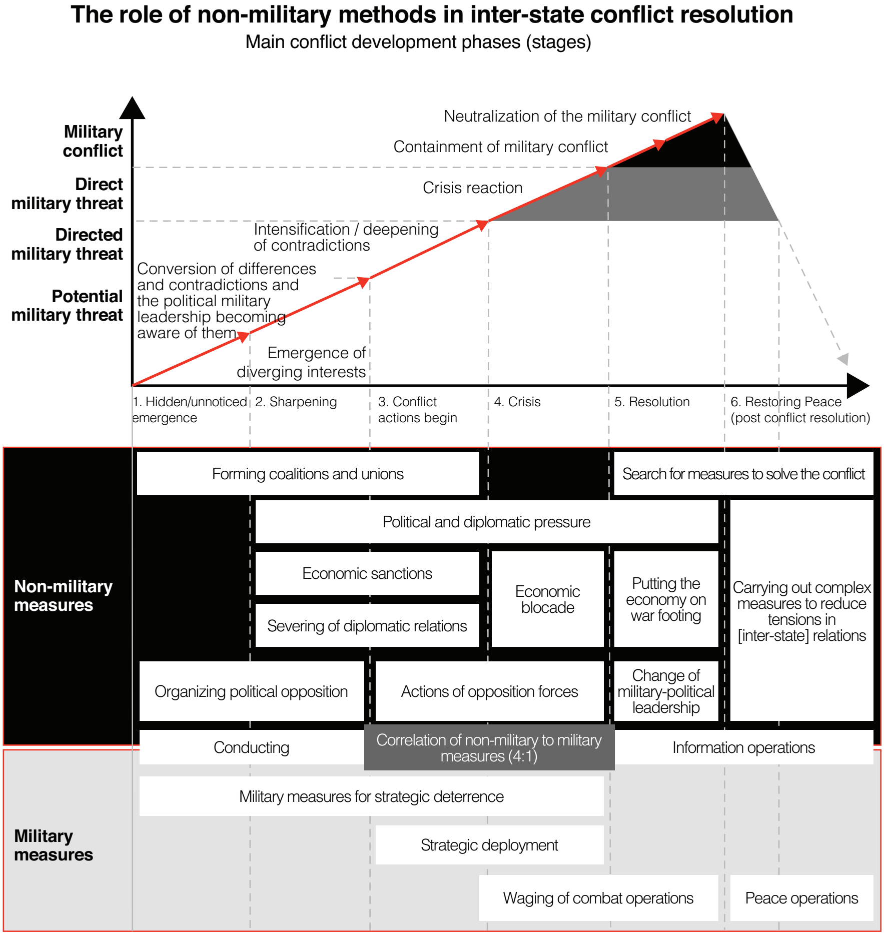
The following actions would otherwise be represented as phases; however, in the NGW context they are expected to overlap, representing the complexity and uncertainty in the gap between competition and conflict:

> *One, peacetime groups of forces start military action (without war declaration or preparatory deployment). Two, highly manoeuvrable stand-off combat actions conducted by combined arms forces. Three, degradation of adversary's military-economic potential by destruction of military and state critical infrastructure. Four, large employment of Precision Guided Munitions, Special Operations, Unmanned weapon systems, weapons based on new physical principles, and involvement by armed civilians or proxies in combat activities. Five, simultaneous [physical and virtual] strike on enemy forces and other targets in entire territorial depth. Six, simultaneous military action in all physical and informational spaces. Seven, employment of asymmetric and indirect methods. Eight, managing troops and means in a unified informational sphere.*[85]

If only half of the above activities were happening in concert, traditional warfighting approaches (whether SOF or conventional) would find it extremely challenging to operate with a definitive level of freedom of manoeuvre. While the list above offers a theoretical example, lessons from Ukraine offer a cautionary example of adversary capabilities expected to be deployed on the modern battlefield that are unconstrained by geographic boundaries and that merge the physical, virtual and cognitive realms. Decision paralysis, inability to gather accurate intelligence, difficulty in strategic force deployment, and uncertainty in navigating complex human and informational terrain will all be omnipresent. The US MDO operating concept and ARSOF Strategy acknowledge this threat, forcing others to consider following suit.

The translated chart below (Figure 6) from Gerasimov's 2013 article 'The Value of Science in Foresight' highlights the stages of NGW and the role of non-military methods in inter-state conflict resolution.[86] It indicates that competition would be in effect during phases 1 and 2, and that transition to conflict occurs in phases 3 through 6. The chaos is expected to be most volatile and uncertain in phases 2 and 3. A key observation is the execution of military and non-military IW across all stages, necessitating the need for counter-capabilities to be able to function in the execution of military action across the spectrum.

Figure 6: Translated Gerasimov chart on the role of non-military methods in interstate conflict resolution[87]



The role of non-military methods in inter-state conflict resolution
Main conflict development phases (stages)
Military conflict
Direct military threat
Directed military threat
Potential military threat
Neutralization of the military conflict
Containment of military conflict
Crisis reaction
Intensification / deepening of contradictions
Conversion of differences and contradictions and the political military leadership becoming aware of them
Emergence of diverging interests
1. Hidden/unnoticed emergence
2. Sharpening
3. Conflict actions begin
4. Crisis
5. Resolution
6. Restoring Peace (post conflict resolution)
Non-military measures
Forming coalitions and unions
Search for measures to solve the conflict
Political and diplomatic pressure
Economic sanctions
Severing of diplomatic relations
Economic blocade
Putting the economy on war footing
Carrying out complex measures to reduce tensions in [inter-state] relations
Organizing political opposition
Actions of opposition forces
Change of military-political leadership
Conducting
Correlation of non-military to military measures (4:1)
Information operations
Military measures
Military measures for strategic deterrence
Strategic deployment
Waging of combat operations
Peace operations

In comparison to western approaches, one key distinction for NGW is that ‘the struggle within “information space” is more or less constant and unending. It knows no boundaries, physical or temporal’.[88] This is where Russia sees offensive cyberspace operations playing a supporting, albeit significant, role in enabling the state to achieve information dominance throughout the stages of conflict.[89] As Gerasimov stresses, information warfare (informatsionnaya voyna) is conducted continuously prior to a conflict, long before physical military confrontation occurs.[90] The strategic employment of continuous information warfare effects, not independent cyberspace operations or information operations, coupled with covert special activities and the use of proxies, represents a highly potent approach that will be difficult to counter. NGW also acknowledges that IW coupled with SOF and proxy activities can be expected well before the threshold for conflict is reached.

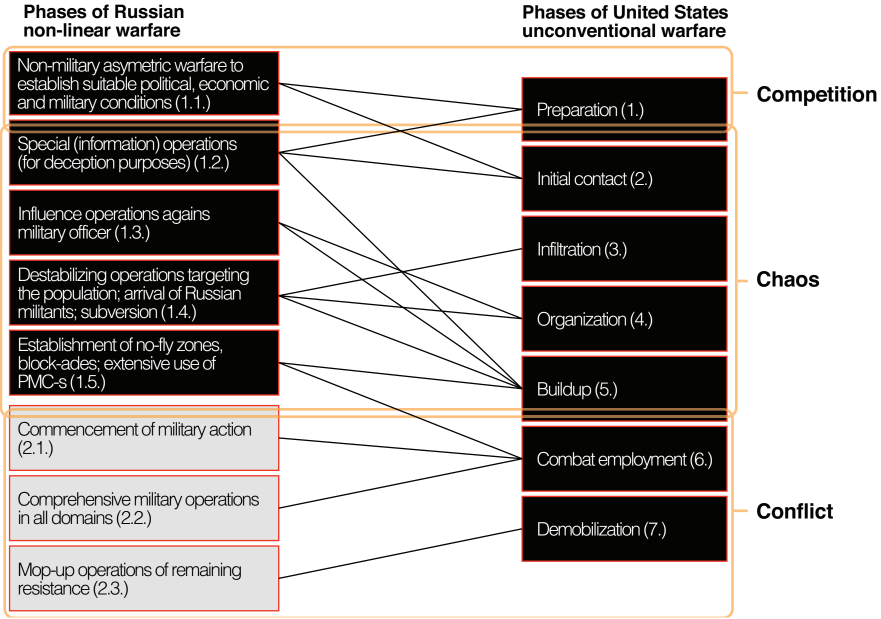
NGW and the Chaos between Competition and Conflict

> *The greatest victory is that which requires no battle.*
>
> *Sun Tzu*

Russian NGW has acknowledged the gap between competition and conflict, characterising it as ‘controlled chaos’ designed ultimately to feed instability, weaken a society’s social fabric and undermine decision-making ability.[91] This controlled chaos can be used to adjust the intensity of both kinetic and non-kinetic operations, favouring exploitation of covert, SOF-enabled conscious employment of blended kinetic and non-kinetic effects to maximise effects short of war.[92]

Figure 7 has been adapted from NATO’s comparison of the phases of Russian NGW and US unconventional warfare, to further understand NGW’s focus on the employment of blended non-kinetic and kinetic effects below the threshold of conflict, traditional US unconventional warfare phases, and the gap between competition and conflict.

Figure 7: Comparing the phases of conflict between Russian NGW and US unconventional warfare[93]


Phases of Russian non-linear warfare
Phases of United States unconventional warfare
Non-military asymetric warfare to establish suitable political, economic and military conditions (1.1.)
Special (information) operations (for deception purposes) (1.2.)
Influence operations agains military officer (1.3.)
Destabilizing operations targeting the population; arrival of Russian militants; subversion (1.4.)
Establishment of no-fly zones, block-ades; extensive use of PMC-s (1.5.)
Commencement of military action (2.1.)
Comprehensive military operations in all domains (2.2.)
Mop-up operations of remaining resistance (2.3.)
Preparation (1.)
Initial contact (2.)
Infiltration (3.)
Organization (4.)
Buildup (5.)
Combat employment (6.)
Demobilization (7.)
Competition
Chaos
Conflict

This seam between competition and conflict has been dubbed the 'grey zone' between peace and war and can be defined as:

> *… an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events.*[94]

The grey zone—the chaos—between competition and conflict, is characterised by liminal actions below the threshold of warfare, where traditional notions of conventional and special operations combat power are challenged substantially as a direct result of how the information age has changed the character of war. The ability to operate in chaos, at the seam of competition and conflict, enables political and military objectives to be achieved 'without fighting and even without conflict'.[95]

NGW and Ukraine: Cyber-Enabled Russian SOF and a Warning of Warfare to Come

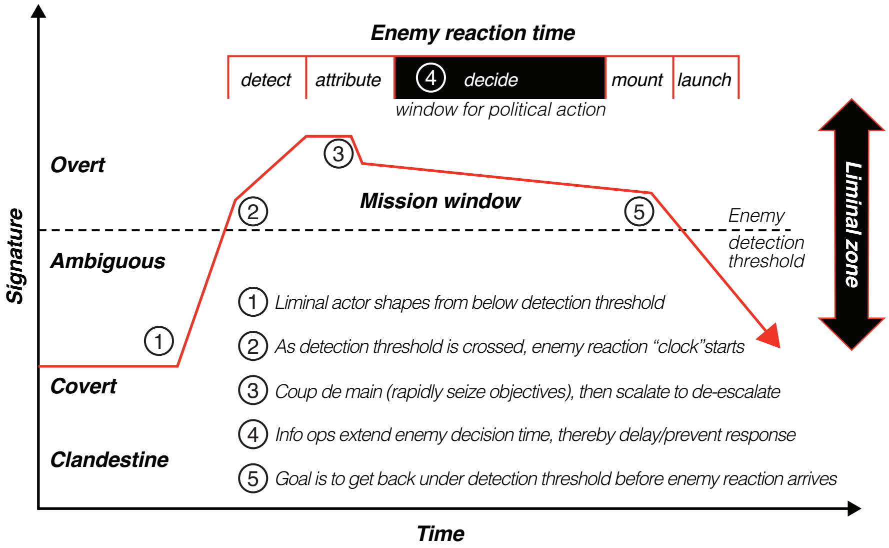
> *The very 'rules of war' have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness … All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces.*
>
> *Gerasimov, 2013*[96]

In late February 2014, unmarked, well-armed gunmen, suspected to be Russian SOF, seized Sevastopol and Simferopol international airports, marking the beginning of a well-planned Russian military operation to seize the Crimea.[97] Concurrently, armed soldiers tampered with fibre-optic cables, targeting the facilities of Ukrainian telecom firm Ukrtelecom, which stated afterwards that 'it had lost the technical capacity to provide connection between the peninsula and the rest of Ukraine'.[98] Combined offensive cyberspace operations targeted Ukrainian government websites and parliamentarians' cellular devices, disabling any effective Ukrainian response.[99] Strategic influence activities targeting NATO and western political and military decision-makers negated any tangible response. Four key characteristics underpin Russia's use of NGW in Ukraine: liminal actions, use of SOF, dominating the IE, and strategic influence. Together they illuminate the convergence of the physical, virtual and cognitive realms and serve as a useful warning of warfare to come.

Liminality[100]

The employment of NGW as observed in Ukraine further exemplifies Gerasimov's recent rebranding of a 'strategy of limited actions' for the advancement of national interest beyond Russian borders.[101] This commentary builds on the ability to operate in the chaos between competition and conflict, utilising the operational experience gained in Ukraine through to operating in an expeditionary capacity in Syria.[102] This strategy of limited actions using clandestine SOF-enabled non-kinetic and kinetic actions below the threshold for conflict is a style of operation difficult to counter. Dr Kilcullen's characterisation of 'liminal warfare' in relation to the evolution of unconventional warfare draws parallels to the chaos where there is increased ambiguity between overt and clandestine or covert activity.[103] One of the key considerations regarding a strategy of limited actions[104] is the temporal dimension, where 'liminal actors and their sponsors do not need permanent deniability, just temporary ambiguity'.[105] Figure 8 highlights Kilcullen's 'Sequence of a Liminal Warfare Operation' whereby counter-liminal strategies require an ability to rapidly detect and attribute activities to inform swift, trusted and reliable decisions to limit the success of overt action during the mission window.

Figure 8: Sequence of a liminal warfare operation[106]


Enemy reaction time
detect
attribute
4 decide
mount
launch
window for political action
Overt
Mission window
3
2
5
Enemy detection threshold
Liminal zone
Signature
Ambiguous
1
Covert
Clandestine
1 Liminal actor shapes from below detection threshold
2 As detection threshold is crossed, enemy reaction "clock"starts
3 Coup de main (rapidly seize objectives), then scalate to de-escalate
4 Info ops extend enemy decision time, thereby delay/prevent response
5 Goal is to get back under detection threshold before enemy reaction arrives
Time

The temporal nature is important to note, as this approach seeks to transition from stealth in phases 1 and 2 to speed during phase 3, as the clock is ticking and adversarial response, in whatever form, is inevitable.[107] The characteristics of liminal warfare include proximity with stealth in the preliminary phases (which include shaping operations to sew ambiguity through obfuscating, confusing or manipulating perceptions to create temporary doubt or confusion) before transitioning to speed, surprise and violence of action to secure objectives, before reducing activity and minimising signature. Countering such a strategy requires a commensurate capability.[108] Liminal actions will occur in the gap between competition and conflict where securing time for prevention, action or reaction will require non-traditional, unconventional operating concepts to fight and win in the chaos.

This style of warfare needs to be considered in the future force design and employment of western special operations and conventional forces. Its liminality points to the requirement for SOF in the modern age to be capable, enabled and focused on fighting and winning in chaos, the space between competition and conflict.

Strategic Influence

Long before Russian SOF crossed the Ukrainian border in March 2014, a strategic IW campaign was underway to discredit Ukrainian government authorities, armed forces and authorities, and encourage separatist activities.[109] Strategically planned offensive cyberspace operations, coupled with coordinated SOF activities, led to the annexation of Crimea and military conflict in Ukraine. The inability of Ukraine to respond to such an effective IW campaign preceding physical troop movement highlights its inability to apply countermeasures to NGW in application.

The IW campaign prior to—and throughout—the 2014 military occupation in parts of eastern Ukraine aimed to avoid a global response or interference from NATO or the US and overt military action by the Ukrainian military in a meaningful manner.[110] It was based on three pillars: offensive cyberspace operations; influence operations; and strategic communications spanning political, strategic, operational and tactical effects.

Evidence of Russian involvement in the barrage of cyber attacks in the lead-up to February 2014 is not definitive, but there are strong indications that the Kremlin directed the attacks against key Ukrainian targets.[111] Russia appears to have successfully employed an effective IW campaign employing activities both in and through cyberspace[112] in a coordinated way prior to military operations to create uncertainty and confusion in what can be identified as the chaos.[113] Russia maintained an ongoing IW capability as part of its NGW campaign. The concentration of coordinated IW activities highlights the challenge of being able to effectively operate with the proliferation of information delivery systems in the information age. Figure 9 provides a non-exhaustive list of some of the concepts and examples of Russian IW as it relates to the application of NGW.

Figure 9: Russian IW concepts relating to NGW[114]

Concept	Definition	Example	Domestic/Foreign/ Hybrid Use
Active measures	Using false or intentionally misinterpreted information to undermine the opponent's legitimacy or military power; using various forms of political repression to silence critics.	Forging letters about the implications of Sweden's future membership in NATO.	Hybrid
Deception (*maskirovka*)	A complex set of actions meant to deceive the enemy and hide true intentions through surprise, camouflage, deception maneuvers, concealment, use of decoys and dummies, or disinformation.	The appearance of "little green men" in Ukraine despite Russian denials of military involvement in the country.	Foreign
Reflexive control	"Conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action"	Disseminating information about alleged fascists in Ukraine and would-be benefits for citizens of eastern Ukraine if it became part of Russia.	Hybrid
Propaganda (black, gray, and white)	The use of information in a selective (white), partly true (gray), or outright wrong (black) manner that aims to convince the recipient to take or fail to take certain actions.	Information strategy employed by state-sponsored Russian media at home and abroad when reporting on Russian international engagements.	Hybrid
Censorship	Limiting freedom of expression under certain conditions, enforced either actively (e.g., through physical interruptions to digital connectivity) or through indirect influence (e.g., leading to self-censorship)	Active Russian control of domestic media and the Internet and preventing opposition figures from developing a large following.	Domestic
Intimidation	Influencing individual choices by implicitly threatening retaliation for undesirable choices or using nonlethal force, sham court trials, and other tool to indicate which behaviors are to odd: with the interests of the intimidator.	Intrusions into the apartments of foreign journalists based in Moscow.	Domestic

Figure 9 illuminates Russia's holistic employment of IW across the physical, virtual and cognitive realms. Two factors are reinforced by the practice of Russian SOF in executing *maskirovka*[115] at the tactical level—through to strategic propaganda and censorship —using state-sponsored media domestically and abroad. The first is that state and non-state adversaries seeking to undermine US and coalition military combat power now have a useful case study to learn from in adopting NGW characteristics for asymmetric advantage. The second is the reinforcement of a warning to western military forces that an effective counter-NGW strategy is required to maintain relevance across the spectrum of conflict. This danger is further intensified by Russia's pursuit of prototyping new military capabilities to expand NGW effectiveness with advanced technologies in Syria. Russian forces are actively experimenting with RAS, EW, remote sensors and precision-guided munitions to build NGW capability.

Russian Innovation and Experimentation in Syria

Russia's expeditionary intervention into Syria enabled effective tactical-level innovation and experimentation. Two key technology areas that illuminate the increasingly merged physical and virtual realms are the experimentation with RAS and the employment of EW capabilities.

General Gerasimov stressed the need to adopt RAS and intensify AI research in the 'value of science in foresight' report he presented at the Academy of Military Sciences in 2013.[116] Russian forces in Syria have been able to take that comment and put it into action. For example, Russia has been experimenting with the Rosoboroneksport's 10 tonne Uran-9 armed unmanned ground vehicle.[117] Additionally, Russia's finessing of its recon-strike complex under NGW includes increased employment of unmanned aerial vehicles (UAVs) ranging from the Forpost system, offering up to 18 hours of persistent intelligence, surveillance and reconnaissance (ISR) to the large-scale use of the Orlan-10 system.[118] An important consideration, given Russia's focus on IW, is how RAS will further converge the physical and digital realms as well as the increased number of physical agents congesting the future battlefield.

Secondly, Russia has invested heavily in its use of EW capabilities in Syria. One example of this is the use of EW capabilities to attack position, navigational and timing data to spoof legitimate global navigation satellite systems (GNSS).[119] As the majority of western military C4ISREW capabilities rely heavily on GNSS, this presents a substantial threat to future freedom of manoeuvre. Figure 10 highlights several systems that have been reported or are assessed to be operating in Syria, two of which were reported to have been used to conduct counter-UAV targeting.[120]

Figure 10: Russian EW systems assessed to be in Syria[121]

Electronic Warfare System	Reported Capabilities	Spotted in Syria
Krasukha-4	Conflicting reports on capabilities, believed to be a multifunctional jammer capable of jamming radars on aircraft and LEO reconnaissance satellites.	c. October 2015 and June 2017 at Khmeimim Airbase.
R-330Zh 'Zhitel'	"SATCOM/GPS/GSM jamming station (detection, direction-finding, analysis and suppression of UHF radio signals). Part of R-330M1P Diabazol automated jamming system."	c. December 2016 possibly spotted at Aleppo Airport.
Samarkand	Allegedly capable of GPS jamming and spoofing in addition to interference with C41SR systems. Possibly a stationary system.	No confirmed signtings.
Shipovnik-Aero	UAV control signal jamming, GNSS jamming, possibly GNSS spoofing.	No confirmed signtings.

Figure 10 offers an insight into capabilities that US and coalition forces are not used to fighting against. The ability to use EW to target GNSS data, ultimately degrading C4ISR command nodes and UAV platforms, will also require counter-strategies to defeat across the spectrum of conflict.

Just as the US and Australia, like the majority of western military forces, are seeking technological advantage, so are countries like Russia who have a higher tolerance for risk and fewer constraints on the exploration of novel capabilities. While the Uran-9 is being experimented with a 30 mm cannon in a combat setting, the Australian Army has only recently succeeded in demonstrating a tele-operated M113 Armoured Personnel Carrier and continues to face significant challenges in overcoming policy constraints in the employment of trusted lethal autonomous weapons. While this is an instrumental milestone in the Australian Army's RAS progression, keeping up with leading-edge lethal capabilities will require additional risk acceptance if true asymmetric capability is to be attained.

Key Risks

There are three key risks that can be observed from the US and Russian examples. The first is strategic miscalculation, the second is operational paralysis and the third is tactical irrelevance.

The lessons from Russia's actions in Ukraine highlight an ability to operate effectively in the chaos between competition and conflict. The speed at which that gap can shift to conflict requires an ability to operate against liminal actions—cyber-enabled SOF working with proxy forces supported by strategic information warfighting capabilities targeting political and military cognitive decision-making and will to act, as well as critical infrastructure anywhere from the close fight back to sovereign territory. A failure to have forces that can accurately distinguish and recognise differences across the spectrum of conflict, specifically in the chaos short of conflict, could result in *strategic miscalculation*.

The convergence of the physical, virtual and cognitive realms—and the impact information technology has had on the character of war—significantly challenge current SOF operating models. The ability to target adversaries or stakeholders now includes an increased incentive to both understand the IE and be able to move and act quickly enough, with enough assurance that the actions taken are correct. Working with proxy forces now includes a significant focus on increasingly available open-source intelligence data, as well as the ability to weaponise information to wage influence in both the virtual and physical domains. Adversarial pursuit of the advantages offered by the convergence of physical, virtual and cognitive realms, as seen in practice by Russia, could lead to *operational paralysis* for future SOF looking to provide options and effects to government using traditional SOF mission profiles.

Lastly, failing to acknowledge the centrality of information as it relates to the future operating environment—by having capable information warfighting capabilities at a much higher ratio with an ability to generate such capability down to the tactical level in support of forward-deployed SOF—could lead to *tactical irrelevance* in the event of a contemporary conflict. This would occur if the application of more traditional physical warfighting functions is deemed redundant due to adversarial cyber-kinetic targeting, dominance of the IE and influence over key stakeholders in the battle space.

Part 4: Making the Case for a Cyber-Enabled Special Information Warfare Capability

Challenging the Status Quo

> *Advantage lies with the side who can excel in cooperation, who can best prepare the environment in competition and who can adapt the fastest in conditions of volatility, uncertainty, complexity and ambiguity.*
>
> *Lieutenant General Rick Burr*[122]

The original vision for SIW in June 2017 was to develop technologically enabled, human terrain oriented SOF—tethered to strategic enablers that were capable of projecting influence in, through or external to cyberspace—in order to target the cognitive decision-making of an adversary or designated stakeholder.[123] However, experiential learning and lessons gleaned from developments in US MDO, Russian NGW in theory and practice, large-scale partnered combat operations against technically savvy ISIS forces in Iraq, and developments within the ADF indicate that the original vision did not meet the Chief of Army's intent to 'think big, start small and move fast'. It did not adequately answer how cyber-enabled SOF would fight and win in the chaos of great-power competition.

The 2017 SIW vision has evolved as a direct contribution to contemporary special operations theory. Notwithstanding the continued requirement for Australia's SOF to conduct national domestic and offshore hostage recovery options, the future value proposition for SOF comprises a task-organised, interagency SIW Task Force that addresses the requirement to fight and win in the chaos between competition and conflict.

The fundamental core of targeting acknowledges both the centrality and physicality of the IE, comprising physical, virtual and cognitive aspects that can be targeted across domains to achieve political and military objectives. Just as adversaries will seek to employ effects across domains, in physical and virtual spaces, at strategic support bases and in the close fight, so will future SOF in support of the joint force. SIW aims to complement the capabilities of current and emerging strategic defence and intelligence services—as well as ADF information and joint force warfighting capabilities—by focusing on the highly volatile and uncertain component of the spectrum of conflict: the chaos.

Australia has a modest army. To say it will have a decisive role in the preliminary stages of great power conflict would be difficult at best. However, the transition to great-power competition requires that SOF adopt the necessary posture to provide bespoke effects to government and provide support to the joint force in the chaos preceding conflict. One way to do this is to stand up a new SOF operational capability—an SIW Task Force. The idea for an SIW Task Force is supported by a review of the SOF truths.

The SOF Truths as Principles for SIW Forces

The US SOF truths—that people are more important than hardware, quality is better than quantity, SOF cannot be mass-produced, competent SOF cannot be created after emergencies occur, and most special operations require non-SOF assistance—have been principles of SOF since as far back as 1987 and provide a guiding light for the growth of a new SIW capability.[124]

Although the character of war has changed, the SOF truths have not, and they still provide a timeless guide to recruit, train, equip and operationalise SIW specialists. These specialists will include tactical force elements armed with technical capabilities, and technical force elements armed with tactical capabilities, strategically tethered to strategic capabilities capable of operating across domains at the tactical, operational and strategic levels. Their capabilities will require an increased focus on cyberspace, EW, intelligence, RAS and AI-enabled warfighting to constitute an SIW Task Force. The original SOF truths apply even more in the information age, and lay a foundational framework for the recruiting, training, equipping and operationalising of an SIW Task Force to meet the demands of the future operating environment in the information age.

Warfare is, and will continue to be, ultimately a human endeavour, executed against people and in amongst the population. SOF are selected for their ability to think, learn, reason and rapidly adapt to chaotic and unprecedented combat conditions.[125] The change to the strategic operating environment and the character of warfare necessitates forces that can apply non-conventional solutions to complex and demanding strategic, operational and tactical problems. In understanding the human dimension, building an SIW Task Force that houses an increasing number of technical specialists will require people who can demonstrate operational agility, discovery learning, adaptive thinking and innovative leadership as well as technical proficiency to achieve operational effectiveness. Talent acquisition and management for specialist technical personnel is as important as selecting the traditional tactical SOF operators. The mindset of equipping the man over manning the equipment is paramount in building an information warfighting capability.[126] As people are more important than hardware in the traditional sense, people are also more important than technology as it relates to SIW.[127]

The second SOF truth of ‘quality over quantity’ has only increased in importance given the impact of the information age on the character of war. Small-scale, highly trained and specialised SOF have long been the tool of choice for government in chaotic, complex and strategically sensitive operational theatres. The increasingly porous operating environment extending beyond geographic boundaries, where activities can be executed with tactical, operational and strategic impact, exemplifies the importance of commensurate technical specialists able to navigate the strategic sensitivities of operations conducted in, through and external to cyberspace. The requirement to generate scalable, tactical, proximal cyberspace and electromagnetic effects, as well as talented technical specialists operating in support of deployed SOF as part of an SIW Task Force, necessitates the identification of and investment in talented personnel.

The third SOF truth, that SOF cannot be mass-produced, is equally important to the raising and training of an SIW Task Force. Traditional SOF recruitment, selection, initial training and specialist training takes years of investment. Diverse tradecraft options are available to SOF operators as they progress through various roles as part of a specialised organisation.[128] The pursuit of excellence is an ongoing mandate for SOF operators, where maintaining technological advantage necessitates a dedicated, prolonged commitment to education and training that cannot be mass-produced. This is even more paramount for technical specialists who remain in high demand from conventional formations, as well as from competitive private sector stakeholders. The exponential and rapid rate of information technology change increases the difficulty of building mission-ready tactical and technical specialists able to effectively employ both proximal and remote cyber-enabled toolkits to support an SIW Task Force. While a challenge, it is achievable given the right talent, resources and time, but surging such a capability effectively to meet additional mission requirements will be unachievable. The SIW workforce will not be able to be mass-produced in a time of chaos.

The specific requirement to grow an SIW Task Force supports the ADF's capacity to effectively contribute to the joint force against peer or superior adversaries in the gap between competition and conflict—the chaos. Competent SIW forces cannot be created after an emergency occurs. The proliferation of information technology and the need to visualise and achieve effects in, through and external to cyberspace and the electromagnetic spectrum—at tactical, operational and strategic levels—will only increase the requirement for capable forces able to rapidly navigate the chaos in between competition and conflict. The mission profiles expected of an SIW capability will not be generated overnight and will need significant focus in training and relative peacetime to ensure asymmetric advantage can be attained at a time of crisis.

The last SOF truth—which was later adopted by Admiral Eric Olson, former commander of USSOCOM—is arguably the most important. It is that 'most special operations require non-SOF support'. Admiral Olson included this truth—which was originally penned but left off the list in 1987—to acknowledge the contribution of key enablers to the mission success of special operations.[129] There are two key factors here. Firstly, the growth of an SIW capability will require increased workforce contribution from the conventional force across the Signals, Intelligence and Artillery Corps, among others; the joint force; and other government agencies (OGAs). Such a capability will also require its leading innovators and experimenters to interface with leading industry, academia and science and technology partners similarly to the US Army Futures Command, US SOFWERX and Australian SOCOMD's Innovation and Experimentation Group (IXG).

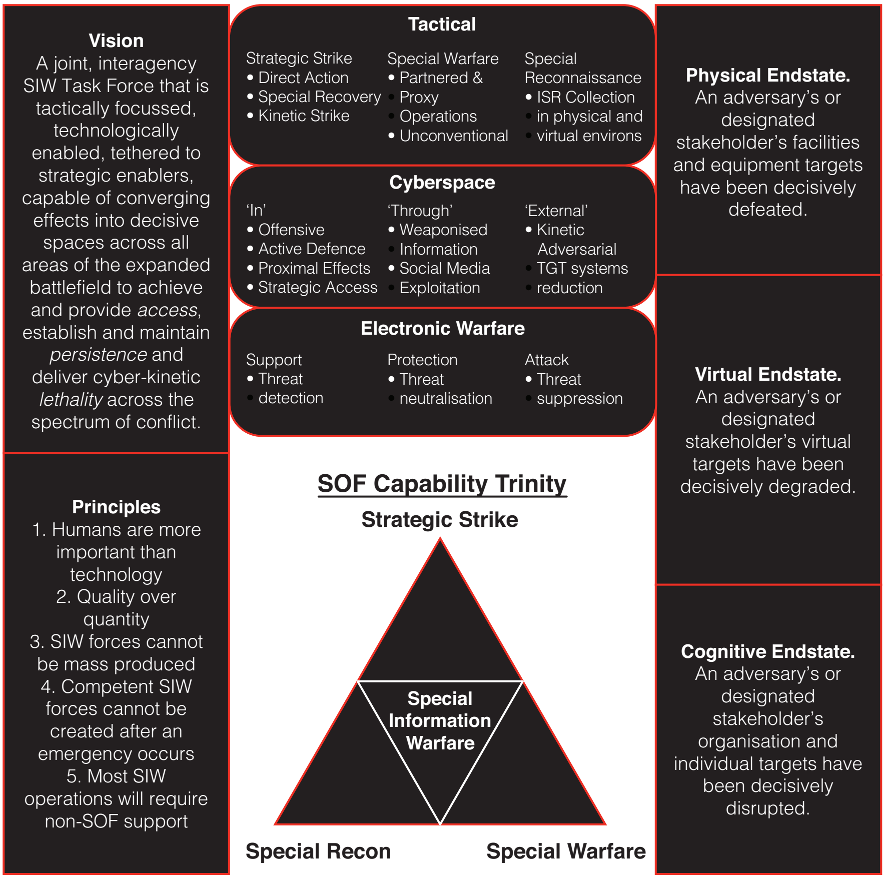
The creation of a revolutionary joint, interagency, tactically tailored yet strategically nested SIW capability will need to draw resources where resources are already scarce. This points to the Chief of Army's acceptance of additional risk in being 'ready now' to be 'future ready'. The other factor is the increasingly important requirement to build and maintain habitual physical and virtual relationships with current and emerging conventional information warfighting capabilities, as well as strategic agencies operating in both the human and information domains.

The SOF truths provide a foundational set of principles that apply to the creation and generation of an SIW capability. Tactical and technical SOF operators will ultimately require a variation of specialist skills which will require a strong vision with room for growth, change and innovation to realise such a unique capability.

Envisioning an SIW Capability

In acknowledging the lessons available from the US and Russian contexts, as well as recent operational lessons learned advising and assisting the Iraqi Counter Terrorism Service in Iraq, the original SIW concept has evolved to further recognise the centrality of information and the convergence of the physical, virtual and cognitive domains. It has also increased in scope to recognise the value proposition of an SIW capability to operate in the chaos between competition and conflict to support national security objectives and support the joint force. Figure 11 represents the vision and principles; the tactical, cyberspace and EW effects; the SOF capability trinity; and the physical and virtual desired end state for an SIW Task Force.

Figure 11: SIW vision, principles, effects, capability trinity and end-state matrix[130]



Vision
A joint, interagency SIW Task Force that is tactically focussed, technologically enabled, tethered to strategic enablers, capable of converging effects into decisive spaces across all areas of the expanded battlefield to achieve and provide *access*, establish and maintain *persistence* and deliver cyber-kinetic *lethality* across the spectrum of conflict.

Principles
1. Humans are more important than technology
2. Quality over quantity
3. SIW forces cannot be mass produced
4. Competent SIW forces cannot be created after an emergency occurs
5. Most SIW operations will require non-SOF support

Tactical

Strategic Strike
- Direct Action
- Special Recovery
- Kinetic Strike

Special Warfare
- Partnered & Proxy Operations
- Unconventional

Special Reconnaissance
- ISR Collection
- in physical and virtual environs

Cyberspace

'In'
- Offensive
- Active Defence
- Proximal Effects
- Strategic Access

'Through'
- Weaponised Information
- Social Media Exploitation

'External'
- Kinetic Adversarial TGT systems reduction

Electronic Warfare

Support
- Threat detection

Protection
- Threat neutralisation

Attack
- Threat suppression

SOF Capability Trinity

Physical Endstate. An adversary's or designated stakeholder's facilities and equipment targets have been decisively defeated.

Virtual Endstate. An adversary's or designated stakeholder's virtual targets have been decisively degraded.

Cognitive Endstate. An adversary's or designated stakeholder's organisation and individual targets have been decisively disrupted.

Figure 11 provides an overarching representation of SIW as a core capability. It has a symbiotic relationship to the pre-existing SOF capabilities as a direct result of the requirement to heighten the importance of information. Realising the vision and principles to guide the delivery of blended cyber-kinetic effects as a core SOF capability that acknowledges the centrality of information to achieve the desired physical, virtual and cognitive target system end states across the spectrum of conflict is the kind of revolutionary change needed for Australian SOF to remain relevant in future conflict.

Figure 12 presents the value proposition of an SIW Task Force consisting of a tactical applications element (TAE), a research and experimentation detachment (RED) and a joint targeting element (JTE) in the chaos between competition and conflict.

Figure 12: The SIW chaos value proposition diagram

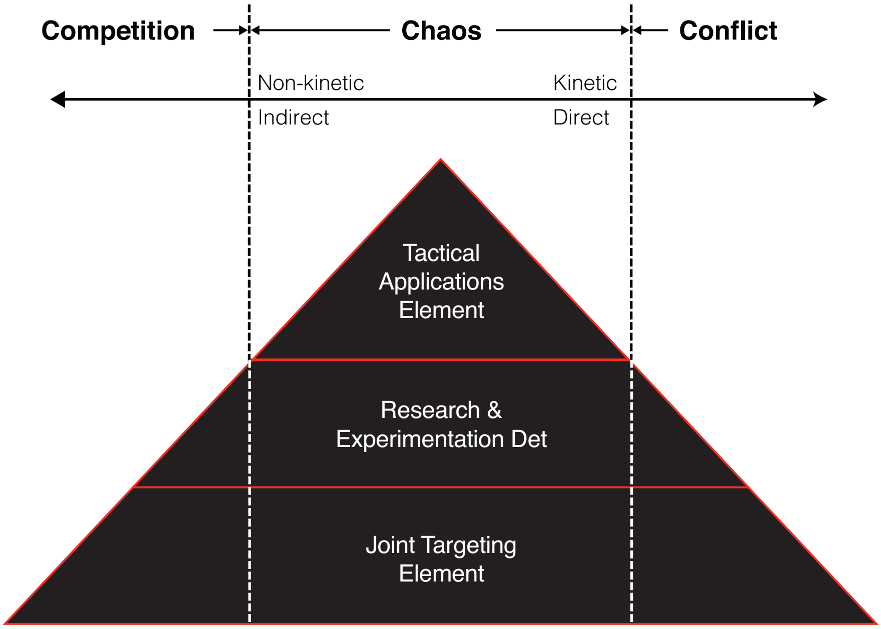


Figure 12 provides a model of an SIW Task Force that is capable of employing non-kinetic and kinetic planning and targeting, bespoke threat-centric experimentation and threat-benchmarking, and tactical non-kinetic SOF across the spectrum of conflict. The apex of the chaos value proposition diagram can rapidly shift left or right along the spectrum in support of national security objectives and in response to threat aggression. The diagram provides a simple means of understanding the increased ratio of non-kinetic to kinetic capability, which will be further explored in thinking more deeply about how to organise for SIW.

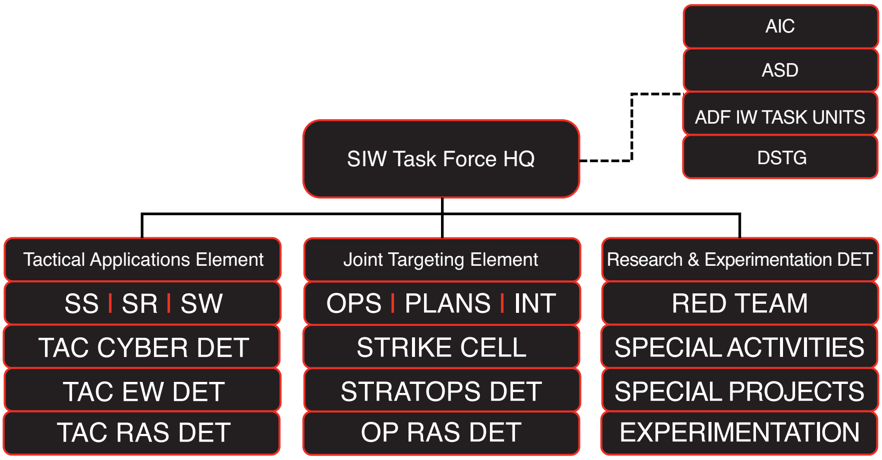
How to Think about SIW—the Future Unit of Action

The Chief of Army's direction to 'think big, start small and move fast' can best be captured through a discovery learning[131] approach. Thinking big is the revolutionary opportunity of realising a tactically oriented, strategically nested future warfighting capability able to fight and win in the chaos against peer and superior threats. Starting small is the argument to build a 'future unit of action' based on the skills, tools and capabilities required. It is suggested that this 'future unit of action' is an SIW Task Force that, as part of its research and experimentation detachment (Figure 12 and 13) is able to apply innovative start-up methodologies to scale after successful top-down direction and bottom-up action and experimentation are achieved. Moving fast necessitates an acceptance of risk similar to that of the US MDO ICEWS capability. It will not be perfect, and discovery learning and the acceptance of intelligent failure and risk in becoming 'ready now' in order to be 'future ready' will support its successful growth. It is recommended that a dedicated, habitual working group be stood up to identify the fundamental inputs to capability requirements to realise an SIW Task Force. If the determination is four years to reach initial operational capability, then make it two.[132] Adversarial capability development and the rate of technological change highlight the need to move faster.

Organising for SIW

It is argued that the task organisation of SOF requires adaptation to match how the character of war has changed and the importance of information as it relates to future SOF operations. For future success it also requires the habitual exercising of an SIW task force that can effectively function across domains and the spectrum of conflict with cyber-enabled strike, reconnaissance and special warfare capabilities. The original SIW concept of 2017 was too narrow in its approach to organising for such a capability. It did not take into account the need to scale the non-kinetic to kinetic ratio, as well as the fifth SOF truth: to include non-SOF assistance. Figure 13 presents a conceptual SIW Task Force model to trigger greater discussion on what would be required to realise such a capability.

Figure 13: **SIW Task Force organisation model**



The force design of the SIW Task Force deliberately aims to devolve key enabling capabilities to the tactical level with a mechanism for operational and strategic reach-back to organic Task Force sub-elements, as well as external organisations able to provide increasingly technical effects. It is based on a tailorable deployment model based on the scale of conflict, strategic circumstance and operational necessity for forward-deployed forces. The tailorable model provides flexibility in being able to operate across the different areas of the battle space, where tactical through to strategic effects can be generated to support national security objectives or support the joint force. The tactical applications element (TAE) combines SOF strike, reconnaissance and special warfare operators with tactical cyber, EW and RAS force elements able to generate potent lethal and non-lethal effects, supported by an enterprise-style joint targeting element (JTE). The JTE includes an edge strike cell capability able to deliver non-lethal and lethal effects in support of the TAE or strategic targets. The strategic operations detachment (STRATOPS) is an OGA detachment able to nest effectively with the broader strategic enabling agencies. The operational RAS detachment is able to utilise persistent ISR in support of the TAE and JTE strike cell. The inclusion of a dedicated innovation capability within the Task Force provides a threat-focused red-teaming, experimentation and rapid prototyping capability with specialist knowledge in advanced threat tactics, techniques and procedures and disruptive technologies. The concentration of blended technical and tactical operators, specialists and planning staff at such a disaggregated level deliberately seeks to address how the character of war has changed and the threat to asymmetric advantage in a high-end, complex and chaotic conflict.

Training for SIW

The convergence of the physical, virtual and cognitive realms indicates a requirement to review traditional training and education models. The blending of the synthetic environment with actions in the physical environment demands training facilities and environments where cyber-kinetic training serials can be executed. The increasing connectedness of the future operating environment indicates a need to create sandboxed virtual spaces that overlap with the physical environments in which traditional SOF training profiles take place. To realise an SIW capability, mission profiles will need to include the application and execution of tactical through to strategic cyberspace operations, EW activities and specific intelligence capabilities to ensure standard operating procedures (SOPs) and tactics, techniques and procedures are operationalised—and synchronised—for when they are needed most.

Equipping SIW through Institutionalised Innovation

Among the changes that have taken place since publication of my first SIW concept in 2017 is the announcement of Project Greyfin: the provision of $500 million of a $3 billion investment in Australia's SOF over the next 20 years.[133] In 2019, Prime Minister Scott Morrison stated:

> *… the first stage of funding enables our Special Forces to engage with intelligence, science and technology, and innovation organisations to ensure future threats and opportunities are assessed, to make sure we are delivering them the capability they need in the future.*[134]

Michael Shoebridge's comments reinforce this need:

> *Special forces have often been the innovation leaders for the broader Australian Army. Now they need to be pathfinders for Australia's national security community in another way—establishing how procurement principles and practice can change to shift the risk approach from one concentrated on reducing project risks to one that's more focused on limiting capability risks by embracing more rapid technological change.*[135]

Equipping an SIW Task Force will require an ability to deliver capability that keeps pace with technology. It ties to the SOF truth that people are more important than hardware and the need to equip based on force design for future threat. What is needed is a 'system of systems' approach spanning tactical and technical trades operating at tactical, operational and strategic levels in a converged physical, virtual and cognitive space. Challenging traditional procurement methods based on individual items, to solve singular capability-centric problems, will need to be addressed if unique asymmetric capability is to be delivered.

Project Greyfin presents an opportunity for the Australian Army to deliver unique capability, beyond iterative improvement. Through initiatives such as the IXG[136] it is positioned to embrace rapid technological change, acknowledge the centrality of information as it relates to special operations and meet the demand signal to 'do more' as expressed by Major General Thompson and Lieutenant General Burr. In a time of relative peace, realising an SIW capability would not only positively contribute to the broader programs of work underway within the Information Warfare Division (IWD), ASD and Army[137] more broadly but also be achievable if the right champions were to carry the concept through to realisation and the commensurate resources were apportioned to take a revolutionary approach.

Conclusion

Increasing global instability and uncertainty, the proliferation of information technologies and adversarial pursuit of advanced capability challenge the current value proposition of Australian and coalition partner SOF. The Chief of Army's challenge to accept risk in being 'ready now' to be 'future ready' necessitates novel and unprecedented approaches to meet the pacing threat in support of the national interest.

Combined with the US shift to great power competition, Russia's pursuit of information-centric warfighting capabilities under NGW, Iran's and North Korea's pursuit of advanced military capabilities, and China's persistent and increasing influence in the region, the dilemma for future combat asymmetry in an era of 'accelerated warfare' is driving the need for change. The US has made a concerted effort to improve the understanding of information as it relates to character of war and how it has changed as a result of information technology. The success of Russia's utilisation of information-centric capabilities reinforces the imperative to acknowledge and embrace IW as integral to modern warfighting and national security apparatus. China's increasing influence and reliance on soft power also necessitates a method of countering influence and information dominance in the region. In a time of increasingly blurred geographical boundaries across the spectrum of conflict, SIW serves as a means to contribute to national security in the chaos between competition and conflict.

Australian and coalition partner SOF face a dilemma of relevance in future conflict. The borderless nature of future conflict necessitates an operating concept capable of functioning across geographic boundaries—and in multiple domains—in support of the national interest. Not only is a broader acknowledgement of IW required, but also an acknowledgment that there is a gap between competition and conflict—the chaos—where SOF will be most expected to operate. This will require a suite of highly cyber-enabled units of action—SOF that are capable of carrying out SIW across the spectrum of conflict to support broader defence and national security objectives.

The original SIW concept presented in 2017 has been overhauled against the backdrop of increasing global uncertainty in the wake of the COVID-19 global pandemic, lessons and observations offered by the US MDO operating concept, and Russia's NGW in theory and practice as seen in Ukraine and Syria. Failure to evolve at a pace commensurate with emerging information technologies, rising great power competition and increasing global uncertainty threatens the national interest, both for Australia and for its allies. This failure to evolve will ultimately increase the risk of *strategic miscalculation, operational paralysis* and *tactical irrelevance* against a capable adversary—a risk that can be avoided by evolving SOF to include an SIW capability to fight and win in the chaos.

Endnotes

[1] RAND, 2018, *Lessons from Others for Future U.S. Army Operations in and through the Information Environment* (RAND Corporation), p. iii. Retrieved 18 December 2020 from https://www.rand.org/pubs/research_reports/RR1925z2.html

[2] A. DeVries, 1997, *Information Warfare and Its Impact on National Security* (U) (US Naval War College), p. ii. Retrieved 18 June 2020 from https://www.hsdl.org/?viewanddid=459698

[3] All references to the Chief of Army in this paper are in reference to the Australian Chief of Army.

[4] The Australian Army has responded with the launch of the Information Warfare Transformation Team initiative, which aims to ‘integrate experts from across different fields including psychological operations, civil-military operations and public affairs’ (Australian Army, 2019, *Army in Motion: Aide for Army’s Teams*. Retrieved 15 February 2020 from https://www.army.gov.au/sites/default/files/publications/aideforarmysteams-print.pdf). The Australian Defence Joint Capabilities Group’s Information Warfare Division, established in 2017, is ‘developing the information warfare capabilities for the ADF to employ in all its activities, such as protecting its networks and missions systems, conducting exercises and training events, supporting the community and the region in disaster relief, stability and security operations through to full conflict and war’. (Australian Government, 2017, *Information Warfare Division*, Joint Capabilities Group. Retrieved 14 February 2020 from https://www.defence.gov.au/jcg/iwd.asp). The Information Warfare Division includes the Joint Cyber Unit, which is being developed to deliver defensive and offensive military cyberspace effects in support of ADF operations and is ‘still in an embryonic state’ (Australian Government, 2018, *ADF iWar Capability Development*, Department of Defence. Retrieved 21 March 2020 from https://www.defence.gov.au/annualreports/17-18/Features/iWar.asp). Major General Marcus Thompson, Head of Information Warfare Division, acknowledges ‘the nation has only just started to think through the information warfare challenge’ (M. Thompson, 2019, *Information Warfare—What’s Next* (Transcript), Joint Capabilities Group., p. 7. Retrieved 21 February 2020 from https://www.defence.gov.au/JCG/docs/HIW_Speech_ATSE_UQ_BNE_21Mar19.pdf), necessitating attention across Defence, including SOF.

[5] B. Johanson, 2018, *“Asymmetric Advantage in the Information Age: An Australian Concept for Cyber-Enabled ‘Special Information Warfare”*, Australian Army Journal XIV(2): 79–107. Retrieved 23 November 2020 from https

[6] Australian Army, 2020, *Army in Motion: Command Statement by Lieutenant General Rick Burr, AO, DSC, MVO*, p. 2. Retrieved 18 February 2020 from https://www.army.gov.au/sites/default/files/2020-05/CommandStatement.pdf

[7] Dr David Kilcullen's 'The Evolution of Unconventional Warfare' provides a detailed description of liminal warfare which recognises 'the need to move beyond a simple overt/clandestine dichotomy, recognising that the zone of ambiguity between overt and clandestine activity is a manoeuvre space in its own right, where resistance actors (and their sponsors) can operate in the gap between detection, attribution and response' (D. Kilcullen, 2019, 'The Evolution of Unconventional Warfare', Scandinavian Journal of Military Studies 2(1): 61–71, p. 68. Retrieved 4 March 2020 from https://sjms.nu/articles/10.31374/sjms.35/). Kilcullen also addresses 'liminal warfare' and 'liminal manoeuvre' as it applies to Russia's modus operandi in his recently released *The Dragons and the Snakes: How the Rest Learned to Fight the Rest* (D. Kilcullen, 2020, Oxford University Press, New York, pp. 115–166).

[8] The US Army Research Lab further expands on the increased physicality with the Internet of Battle Things, which includes larger amounts of sensors, actuators and devices (computers, vehicles, robots, wearables), infrastructure (networks), analytics (on-node, in-network and centralised) on the battlefield (A. Kott, A. Swami, B. West, 2016, *The Internet of Battle Things*). Retrieved 29 January 2020 from https://www.researchgate.net/publication/311215660_The_Internet_of_Battle_Things

[9] Australian Army, 2019, *Army in Motion: Army's Contribution to Defence Strategy*, p. 7. Retrieved 18 February 2020 from https://www.army.gov.au/sites/default/files/publications/armyscontributiontodefencestrategy-print.pdf

[10] Major General Thompson (Ret.) was the Commander of the Information Warfare Division. Quotation from a personal conversation.

[11] Johanson, 2017.

[12] Australian Government, 2017.

[13] Thompson, 2019, pp. 4–8.

[14] D. Ormrod and B. Turnbull, 2015, *Toward a Military Cyber Maturity Model*, p. 1. Retrieved 29 January 2020 from https://www.unsw.adfa.edu.au/australian-centre-for-cybersecurity/sites/accs/files/uploads/Military%20Cyber%20Maturity%20Model%20v1.pdf

[15] C. Dougherty, 2019, *Why America Needs a New Way of War* (Center for a New American Security, Washington D.C.), p. 19. Retrieved 18 January 2020 from https://s3.amazonaws.com/files.cnas.org/CNAS+Report+-+ANAWOW+-+FINAL.pdf

[16] S. Thomson and C. Paul, 2018, 'Paradigm Change: Operational Art and the Information Joint Function', *Joint Force Quarterly 89*, p. 11. Retrieved 22 November 2019 from https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-89/jfq-89_8-14_Thomson-Paul.pdf?ver=2018-04-11-125441-307

[17] US Department of Defense (DOD), 2018, *Joint Concept for Operating in the Information Environment*, p. 42. Retrieved 8 December 2019 from https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830

[18] Thomson and Paul, 2018, p. 8.

[19] Ibid.

[20] Ibid.

[21] US DOD, 2018, *Joint Concept for Operating in the Information Environment*, p. viii.

[22] US DOD, 2018, *Joint Operations Joint Publication 3-0*, pp. IV–2. Retrieved 22 November 2019 from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910

[23] US Government, 2018, *National Cyber Strategy of the United States of America*, p. 1. Retrieved 25 June 2019 from https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[24] Ibid.

[25] AI in this context can be distinguished into three tiers: narrow AI, where machine intelligence equals or exceeds human intelligence for specific tasks; general AI, where machine intelligence meets the full range of human performance across any task; and artificial superintelligence, where machine intelligence exceeds human intelligence across any task (Hague Centrefor Strategic Studies, 2017, *AI and the Future of Defense*, p. 30). Retrieved 21 March 2020 from https://mk0hcssnlsb22xc4fhr7.kinstacdn.com/wp-content/uploads/2017/05/Artificial-Intelligence-and-the-Future-of-Defense.pdf

[26] US Army TRADOC, 2018, *The US Army in Multi-Domain Operations 2028*, p. 5. Retrieved 22 November 2019 from https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

[27] Australian Army, 2020, *Army in Motion: Command Statement*, p. 2.

[28] US Government, 2019, *Future Warfare: Army is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organisations*, p. 2. Retrieved 8 December 2019 from https://www.gao.gov/assets/710/700940.pdf

[29] In an unclassified summary of the 2018 National Defense Strategy, the US DOD concluded that after a 'decade of counterinsurgency operations in Iraq and Afghanistan, its competitive military advantage in contested security environments is eroding' (US DOD, 2018, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, p. 1).

[30] US Army TRADOC, 2018, p. 15.

[31] Ibid., p. 16.

[32] Ibid.

[33] Convergence is defined in the MDO 2028 operating concept as 'the rapid and continuous integration of capabilities in all domains, the EMS, and the information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative. The Joint Force currently converges capabilities through episodic synchronization of domain-federated solutions. Future operations against a near-peer threat, however, will require the Joint Force to conduct continuous and rapid integration of multidomain capabilities to gain cross-domain overmatch at decisive spaces. Decisive spaces are locations in time and space (physical, virtual, and cognitive) where the full optimization of the employment of cross-domain capabilities generates a marked advantage over an enemy and greatly influences the outcome of an operation. Convergence complicates the enemy's attempts to conceal and defend its center of gravity by providing the Joint Force with multiple options for attacking the enemy's vulnerabilities at decisive spaces. Multi-domain formations, at echelon, utilize convergence during competition and conflict to apply capabilities against vulnerabilities in an adversary's or enemy's systems' (*US Army TRADOC*, 2018, p. 20).

[34] Ibid., p. 20.

[35] Ibid., p. 26.

[36] Ibid., p. 20)

[37] Will McRaven originally defined 'Relative Superiority' as a condition that exists when an attacking force gains a decisive advantage over an enemy in the execution of direct action missions (W. McRaven, 1996, *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice* (Presidio Press), p. 4).

38 General Stanley McChrystal, commander of TF 714 during Operation Enduring Freedom in 2003, created the F3EAD targeting model to 'prevail over a complex enemy that made effective use of information-age technologies' in reference to Al-Qaeda in Iraq'. It demonstrated organisational learning and innovation to adapt traditional counter-terrorism operations to firstly acknowledge the importance of information to successful targeting operations, secondly the adversaries' use of information technologies, and lastly the tempo required to stay ahead of an asymmetric threat actor (R. Shultz, 2016, *Military Innovation in War: It Takes a Learning Organisation—A Case Study of Task Force 714 in Iraq* (Joint Special Operations University Press), p. 3. Retrieved 21 March 2020 from https://www.sofx.com/wp-content/uploads/2016/07/JSOU16-6_Shultz_TF714_final1.pdf).

39 US Government, 2019, p. 10.

40 Ibid., p. 15.

41 Ibid.

42 Ibid.

43 Ibid., pp. 15–16.

44 Ibid., p. 16.

45 Ibid.

46 Ibid., p. 13.

47 Ibid.

48 Ibid., p. 14.

49 S. Roper and J. Grassetti, 2018, *Seizing the High Ground—United States Army Futures Command* (Institute of Land Warfare), p. 1. Retrieved 20 February 2020 from https://www.ausa.org/sites/default/files/publications/SL-18-4-Seizing-the-High-Ground-United-States-Army-Futures-Command.pdf

50 US Government, 2019.

51 Ibid., p. 17.

52 Ibid.

53 US Army, 2019, *Army Special Operations Forces Strategy*, p. 1. Retrieved 8 December 2019 from https://www.soc.mil/AssortedPages/ARSOF_Strategy.pdf

54 'The direct approach is characterized by technologically enabled small-unit precision lethality, focused intelligence, and interagency cooperation integrated on a digitally networked battlefield … The direct approach alone is not the solution to the challenges our nation faces today, as it ultimately only buys time and space for the indirect approach and broader governmental elements to take effect. Less well-known but decisive in importance, the indirect approach is the complementary element that can counter the systemic components of the threat. The indirect approach includes empowering host nation forces, providing appropriate assistance to humanitarian agencies, and engaging key populations. These long-term efforts increase partner capabilities to generate sufficient security and rule of law, address local needs, and advance ideas that discredit and defeat the appeal of violent extremism … One way [special operations forces achieves] this goal through the indirect approach is through forward and persistent engagement of key countries. Small in scale by design, this engagement directly supports the country teams' and [geographic combatant commands'] theatre plans to counter threats to stability.' (L. Robinson, 2013, *The Future of U.S. Special Operations Forces* (Council on Foreign Relations), pp. 10–11. Retrieved 22 November 2019 from https://www.cfr.org/report/future-us-special-operations-forces

55 D. Feickert, 2019, *US Special Operations Forces (SOF): Background and Issues for Congress* (Congressional Research Service), p. 10. Retrieved 18 December 2019 from https://fas.org/sgp/crs/natsec/RS21048.pdf. This review (which, at the time of writing, had a 270-day deadline which coincided with the release of this paper) highlighted the timeliness of SOF modernisation to face future threats.

56 'Special warfare is the execution of capabilities that involve a combination of lethal and nonlethal actions taken by a specially trained and educated force that has a deep understanding of cultures and foreign language, proficiency in small-unit tactics, and the ability to build and fight alongside indigenous combat formations in permissive, uncertain, or hostile environments' (US Army, 2019, *ADP 3-05 Army Special Operations*, pp. 1–3. Retrieved 10 December 2019 from https://fas.org/irp/doddir/army/adp3_05.pdf).

57 'Surgical strike is the execution of capabilities in a precise manner that employ special operations forces in hostile, denied, or politically sensitive environments to seize, destroy, capture, exploit, recover or damage designated targets, or influence threats' (Ibid.).

58 Ibid., pp. 1–7.

59 Ibid.

60 US Army, 2019, *Army Special Operations Forces Strategy*, p. 2.

61 Ibid.

62 Ibid.

63 Ibid.

64 US Army, 2019, *ADP 3-05*, p. iv.

65 US Army, 2019, *Army Special Operations Forces Strategy*, p. ix.

66 Ibid., p. x.

67 Ibid., p. x.

68 US Army, 2019, ADP 3-05, p. 82.

69 While SOF could rely on emerging ADF IW capabilities to support peacetime operations, the gap between competition and conflict is expected to see significant task saturation and degradation of strategic networks for sovereign IW capabilities in support of the joint force and national security requirements. The chaos between competition and conflict will see all ADF and other government agency (OGA) information warfighting capabilities 'in contact' with an adversary, which necessitates SOF to hold an organic capability that can ensure independent mission success while complementing the IW capabilities of the ADF and OGAs.

70 J. Taft, J. Mariani and L. Gormisky, 2019, *Special Operations Forces and Great Power Competition: Talent, Technology, and Organizational Change in the New Threat Environment* (Deloitte). Retrieved 18 December 2019 from https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-special-operations-forces-great-power-competition.html

71 D. Adamsky, 2015, *Cross-Domain Coercion: The Current Art and Strategy* (Institut Français des Relations Internationales), p. 22. Retrieved 12 February 2020 from https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

72 Ibid., p. 21.

73 Ibid., pp. 21–22.

74 M. Kofman and M. Rojansky (2015), *A Closer Look at Russia's 'Hybrid War'*. Kennan Cable No. 7, p. 2. Retrieved 25 November 2019 from https://www.wilsoncenter.org/sites/default/files/media/documents/publication/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

75 Kilcullen, 2020, p. 161.

76 Galeotti further explains there is no single Russian 'doctrine', which makes its campaign approach increasingly dangerous as there is no 'single organising principle'. He further explains that Gerasimov was talking about subversion to prepare the battlefield before intervention as seen in the Ukraine (M. Galeotti, 'I'm Sorry for Creating the "Gerasimov Doctrine"', *Foreign Policy*, 5 March 2018. Retrieved 22 March 2020 from https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/). Gerasimov, in reference to western more than Russian methods of warfare, whether subconsciously or not was revealing that Russia had shifted toward 'wartime coevolution in response to the moves of an identified enemy' (Kilcullen, 2020, p. 163).

77 Kilcullen, 2020, p. 161.

78 F. Hansen, 2017, *Russian Hybrid Warfare: A Study of Disinformation* (Danish Institute for International Studies), p. 4. Retrieved 24 November 2019 from https://pure.diis.dk/ws/files/950041/DIIS_RP_2017_6_web.pdf

79 Adamsky, 2015, p. 23.

80 Ibid.

81 Y. Danyk, T. Maliarchuk and C. Briggs, 2017, *Hybrid War: High-tech, Information and Cyber Conflicts* (Partnership for Peace Consortium of Defense Academies and Security Studies), p. 6. Retrieved 24 November 2019 from https://www.jstor.org/stable/pdf/26326478.pdf?refreqid=excelsior%3Ac4a84091224a2c0d9859f9e4e3937660

82 Ibid., p. 7.

83 Ibid., p. 9.

84 M. Galeotti, '(Mis)Understanding Russia's Two 'Hybrid Wars', *Eurozine*, 29 November 2018. Retrieved 21 March 2020 from https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/

85 Adamsky, 2015, pp. 23–24.

86 B. Sohl, 2017, 'Influence Campaigns and the Future of International Competition: The Intersection of Increased Democratization and a Revolution in Information Technologies', *RealClear Defense*. Retrieved 21 March 2020, from https://www.realcleardefense.com/articles/2017/09/12/influence_campaigns_and_international_competition_112280.html

87 Ibid.

88 M. Connell and S. Vogler, 2016, *Russia's Approach to Cyber Warfare* (CNA Analysis and Solutions), p. 5. Retrieved 18 February 2020 from https://www.realcleardefense.com/articles/2017/05/09/russias_approach_to_cyber_warfare_111338.html

89 Ibid., p. 5.

90 U. Franke, 2015, *War by Non-military Means: Understanding Russian Information Warfare*, p. 41. Retrieved 24 November 2019 from http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf

91 Hansen, 2017, p. 10.

92 Ibid.

93 Adapted by the author from V. Sazonov, 2016, *Russian Information Campaign Against the Ukrainian State and Defence Forces* (NATO Strategic Communications Centre of Excellence), p. 59. Retrieved 28 November 2019 from https://www.stratcomcoe.org/russian-information-campaign-against-ukrainian-state-and-defence-forces

94 L. Morris, M. Mazarr, J. Hornung, S. Pezard, A. Binnendijk and M. Kepe, 2019, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold for Major War* (RAND Corporation), p. 8. Retrieved 29 January 2020 from https://www.rand.org/pubs/research_reports/RR2942.html

95 Hansen, 2017, p. 11.

96 V. Gerasimov, 'The Value of Science in Prediction', *Military-Industrial Kurier*, 27 February 2013. Retrieved 18 February 2020 from https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf

97 B. Perry, 'Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations', *Small Wars Journal*, 14 August 2015. Retrieved 8 December 2019 from https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera

98 T. Maurer, 2015, *Cyber Proxies and the Crisis in Ukraine* (NATO CCD COE Publications, Tallinn), pp. 79–80. Retrieved 24 November 2019 from https://ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf

99 Ibid.

100 'Liminal' is drawn from the Latin word for 'threshold' (Kilcullen, 2019, p. 68).

101 D. Johnson, 2019. *Review of Speech by General Gerasimov at the Russian Academy of Military Science* (North Atlantic Treaty Organisation Defense College, Russian Study Series 4/19). Retrieved 21 February 2020 from http://www.ndc.nato.int/research/research.php?icode=585#

102 Ibid.

103 Kilcullen, 2019, p. 68.

104 Dr Kilcullen describes this contemporary phenomenon of 'liminal warfare' as an evolution of Russian practice that emphasises the 'liminal, or threshold-manipulation' aspect which has been present in Russian thinking since Soviet times (Kilcullen, 2020, p. 150). Kilcullen further describes Russia's approach as 'liminal manoeuvre', where Russia 'ride[s] the edge, operating right on the detection threshold—taking sufficiently few and ambiguous actions to achieve core political objectives, but not enough to trigger a military reaction' (Kilcullen, 2020, p. 150). 'Liminal warfare' and 'liminal manoeuvre' further stress the gap between competition and conflict, where the chaos represents an operating space where counter-liminal strategies are needed.

105 Kilcullen, 2020, pp. 157–158.

106 Ibid., p. 158. Kilcullen's chart has similarities with General William McRaven's theory of special operations, coined 'relative superiority', which is a 'condition that exists when an attacking force, generally smaller, gains a decisive advantage over a larger or well defended enemy' (W. McRaven, 1993, *Thesis: The Theory of Special Operations* (Naval Postgraduate School), p. 2. Retrieved 21 March 2020 from https://apps.dtic.mil/dtic/tr/fulltext/u2/a269484.pdf). The original concept paper by the author proposes the concept of 'cyber-enabled relative superiority' that emphasises the importance of shaping operations to gain advantage prior to, as Kilcullen characterises them, phase 3 activities (Johanson, 2017, p. 18).

107 Kilcullen, 2020, p. 159.

108 Ibid., pp. 159–160.

109 Danyk, Maliarchuk and Briggs, 2017, p. 10.

110 A. Atay, 2016, *Strategic Utility of the Russian Spetsnaz* (Naval Postgraduate School, Monterey, California), p. 57. Retrieved 19 January 2020 from https://calhoun.nps.edu/bitstream/handle/10945/51562/16Dec_Atay_Abdullah.pdf?sequence=1andisAllowed=y

111 Connell and Vogler, 2016, p. 14.

112 'In' cyberspace refers to the use of disinformation and psychological manipulation utilising cyberspace as the means. 'Through' cyberspace refers to the delivery of offensive cyberspace effects against critical information technology infrastructure.

113 Connell and Vogler, 2016, p. 14.

114 RAND, 2018, p. 161.

115 Maskirovka, which translates to ‘disguise’, differs from the traditional understanding of military deception (MILDEC). It aims to create uncertainty, ambiguity and doubt to influence the outcome and achieve operational goals (J. Vowell, 2016, *Maskirovka: From Russia with Deception*). Retrieved 12 February 2019 from https://www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html. Russia treats *maskirovka* as an activity conducted on a daily basis and on all levels, whereas MILDEC in a US/western context is applied to single operations or campaigns (R. Heickero, 2010, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Swedish Defence Research Agency), pp. 25–25. Retrieved 22 March 2020, from http://www.highseclabs.com/data/foir2970.pdf).

116 A. Zakvasin, 2018, ‘“The Contours of the War of the Future”: How the Russian Army Is Preparing for New Generation Conflicts’, *RT*, 27 March 2018. Retrieved 12 February 2019 from https://russian.rt.com/russia/article/496787-gerasimov-voina-novoe-pokolenie

117 A. Savitsky, 2018, ‘Uran-9: the Russian Army Leads the World in Ground-Combat Robots’, *Strategic Culture Foundation*, 2 June 2018. Retrieved 3 March 2020 from https://www.strategic-culture.org/news/2018/06/02/uran-9-russian-army-leads-world-in-ground-combat-robots/

118 V. Karnozov, 2019, ‘Russia Advances UAV Forces, Sheds Light on Syrian Experiences’, *AINonline*, 6 October 2019. Retrieved 12 February 2020 from https://www.ainonline.com/aviation-news/defense/2019-10-06/russia-advances-uav-forces-sheds-light-syrian-experiences

119 C4ADS, 2019, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria*, p. 3. Retrieved 23 February 2020 from https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf

120 Ibid., p. 48.

121 Ibid.

122 Australian Army, 2019, *Army in Motion: Accelerated Warfare Statement by Lieutenant General Rick Burr, AO, DSC, MVO*, p. 2.

123 Johanson, 2017, p. 17.

124 S. Fogarty and J. Nasi, 2016, *Special Operations Forces Truths—Cyber Truths* (Army Cyber Institute), p. 19. Retrieved 4 March 2020 from https://www.jstor.org/stable/pdf/26267355.pdf?refreqid=excelsior%3A0ae1e5da17f21132e17ff75f96dc4757

125 Ibid., p. 22.

126 Ibid.

127 Ibid. The proliferation of RAS and AI capabilities, as well as the pursuit of HUMT operating concepts, further underpins a requirement to recruit, select train and retain the right people. There is a serious risk of cognitive overload for military decision-makers in times of high stress and demand as a result of information technology proliferation, indicating a need to have forces able to counter interference or AI-enabled HUMT capabilities.

128 Fogarty and Nasi, 2016, p. 23.

129 H. Yarger, 2013, *21st Century SOF: Toward an American Theory of Special Operations* (Joint Special Operations University), p. 36. Retrieved 2 February 2020 from https://www.socom.mil/JSOU/JSOUPublications/13-1_21st%20Century%20SOF_Yarger.pdf

130 This has been adapted from the original SIW concept's vision, effects and end-state graphic (Johanson, 2017, p. 3). The target types that constitute the end-state conditions are drawn from the Canadian Joint Targeting Centre of Excellence's Joint Targeting Staff Handbook. The facility target type is a geographically located, defined physical structure that contributes to a target system's capability. The equipment target type is a device that provides a function to the target system's capability. The virtual target type is an entity in cyberspace or in the electromagnetic spectrum that provides a function that contributes to the target system's capability. The organisation target type is a group or unit that provides the function that contributes to a target system's capability. The individual(s) target type is a person or people who contribute to a target system's capability (Joint Targeting Centre of Excellence, 2019, *Joint Targeting Staff Handbook 2019* (Canadian Armed Forces Paperback, UNCLASSIFIED), p. 20).

131 Discovery learning is a method that can be traced back to the late 1950s. It focuses on promoting a way of active learning that is process-oriented, self-directed, self-seeking, self-finding and self-investigating (A. Kistian et al., 2017, 'The Effect of Discovery Learning Method on the Math of the V SDN 18 Students of Banda Aceh, Indonesia', *British Journal of Education* 5(11): 1–11, p. 1. Retrieved 29 January 2019 from http://www.eajournals.org/wp-content/uploads/The-Effect-of-Discovery-Learning-Method-on-the-Math-Learning-of-the-V-Sdn-18-Students-of-Banda-Aceh-Indonesia.pdf). Brigadier Ian Langford, Director General Future Land Warfare Branch, is an advocate of the discovery learning model within the Australian Army and has started several initiatives to develop this within Army.

132 Fundamental inputs to capability (FICs) are the capability inputs within Defence: personnel, organisation, collective training, major systems, supplies, facilities, support, and command and management (Australian Government, 2006, *Defence Capability Development Manual* (Defence Publishing Service), pp. 4–5. Retrieved 22 March 2020 from https://www.defence.gov.au/publications/dcdm.pdf). When developing Defence capability all individual FICs must be examined to determine what changes need to be made to realise a collective capability. IOC, as outlined in the Australian Defence Capability Development Manual, is the 'date when the first elements of capability would be ready for operational use' (Australian Government, 2006, p. 18). It represents a capability state on the pathway to Final Operational Capability (FOC), which is the point at which the 'final subset of a capability system that can be operationally employed is realised' (Australian Government, 2006, p. 90).

133 S. Morrison, 2019, 'Backing Our Special Forces with Cutting Edge Equipment', Media Release, 12 August 2019. Retrieved 24 February 2020 from https://www.pm.gov.au/media/backing-our-special-forces-cutting-edge-equipment

134 Morrison, 2019.

135 M. Shoebridge, 2019, 'Special Forces' Approach to Technological Change a Model for Others', *The Strategist* (Australian Strategic Policy Institute), 13 August 2019. Retrieved 4 December 2019 from https://www.aspistrategist.org.au/special-forces-approach-to-technological-change-a-model-for-others/

136 IXG is a Chief of Army initiative within SOCOMD. It is a unit-level initiative generated in response to the delivery of Project Greyfin to address capability gaps and advance the adoption of emerging technology, organisational processes and human performance factors (Australian Army, 2019, *Army in Motion: Aide for Army's Teams*. Retrieved 15 February 2020 from https://www.army.gov.au/sites/default/files/publications/aideforarmysteams-print.pdf).

137 Another Chief of Army initiative is the formation of the Information Warfare Transformation Team to integrate experts from across different fields including psychological operations, civil-military operations and public affairs to build understanding and concepts for the future-ready Army.

researchcentre.army.gov.au