UNSW CANBERRA

Asymetric Advantage in the Information Age:

An Australian Concept for Cyber-Enabled 'Special Information Warfare'

ACCS DISCUSSION PAPER NO. 5

Ben Johanson

December 2017

Asymetric Advantage in the Information Age:

An Australian Concept for Cyber-Enabled 'Special Information Warfare'

Ben Johanson

ACCS DISCUSSION PAPER NO. 5

DECEMBER 2017

Table of Contents

Introduction

The announcement of a new 'Information Warfare Division'[1] within the Australian Defence Force acknowledges the need for cyber-enabled warfare strategies to address the challenges of the information age. Implementing such force modernisation demonstrates a positive, albeit belated, approach to address the disruptive nature information technology is having on the character of modern warfare. This announcement presents an opportunity for Australia's Special Operations Command (SOCOMD) to maintain its position as the Government's military-strategic vanguard by developing a cyber-enabled 'Special Information Warfare' concept. This concept will call for bottom-up *action* that senior Government and Defence decision makers can support through policy and doctrinal *debate.*

The paper will be initiated by framing the future operating environment and hypothesising a technologically-enabled Special Operations Task Group deployed against a hybrid threat, demonstrating the utility in developing a unified strategy of 'Special Information Warfare'. Outlining Australia's current state of play will highlight the current gaps in policy and doctrine, demonstrating the need for a novel, asymmetric strategy. Analysis of Russia's New Generation Warfare, Chinese Distributed Warfare and Integrated Network Electronic Warfare, and the Islamic State's use of mass media will illuminate why Australia needs to adapt rapidly toward a strategy that can achieve 'information dominance' in future conflict. US cyber-enabled warfare strategies and doctrine provide an excellent point of reference to further support a unique Australian SOCOMD strategy. By benchmarking against Russia, China and the US, the political and military pressure for change can be realised, instigating *debate* and *action* aimed at implementing an innovative solution to maintain military relevance in the information age (Austin, 2016). Cyber-enabled 'Special Information Warfare' seeks to weaponise information, operationalise cyberspace effects and normalise an offensive adoption of Information Warfare within SOCOMD that spans the strategic to tactical level.

Characterising Future War & the Need for a Cyber-Enabled Asymmetric Approach

'The evolving character of conflict that we currently face is best characterized by convergence[2]. This includes the convergence of the physical and psychological, the kinetic and non-kinetic, and combatants and non-combatants.' (Hoffman, 2009, p. 34)

The character of war is developing toward an increasingly lethal battlefield fought amongst population centres in both a contested and congested environment (Pomerleau, 2017). The proliferation of connected devices is expected to reach fifty billion by 2020, highlighting cyberspace as a critical operational medium (Brown, 2017). An increased level of parity is emerging where military-technological advantage previously enjoyed by Western forces may

[1] The ABC's Ashlynne McGhee released an exclusive highlighting 'a major transformation' within the Australian Military with the announcement of a new Information Warfare unit to be established within the ADF (McGhee, 2017).

[2] 'Convergence' relating to cyberspace is further explained in the US Army TRADOC Cyber Army 2050 Report 2016: 'The consequent attribute of the cyber future will be convergence… between land and cyberspace operations. … between all the legacy domains, as cyberspace constitutes the connective ether that readily transfers effects from one domain to another … between time and space as enhanced information and communication technologies decrease the time and expand the reach of cyber actions … between electromagnetic (EMS) and cyberspace action … between defensive and offensive cyberspace operations to ensure one function informs the other … between information management (IM) and knowledge management (KM) as large data is leveraged to achieve advantage … between Army operational and institutional activities, creating an unprecedented level of interaction where operations impact institutional activities and vice-versa.' (US Army TRADOC, 2016, pp. 45-46).

not be so decisive in future conflict (McGrath, 2016, p. 17). Russia, China, and the Islamic State have identified the importance of 'information' for strategic success and continue to pursue strategies to effect success in cyberspace, a realisation that has yet to reach full maturity within the Australian context. Future conflict will consist of contested norms and persistent disorder, permeating through physical and virtual realms, necessitating an approach which combines the full suite of cyberspace capabilities with traditional physical military actions (US Army TRADOC, 2016, p. 4). These elements are explored in the following vignette.

Set no more than ten years into the future, a Special Operations Task Group (SOTG) has been deployed at short notice against a hybrid threat consisting of military-strategic conventional forces and a surrogate proxy. The operating environment is dense and distinguishing threat actors amongst the civilian population is near impossible. This is a multi-vector, multi-front and multi-theatre battlespace where effects are generated in milliseconds across the physical, informational and human domain (Austin, Shaping the Cyber Arms Race of the Future, 2016). The Commander is determined to provide niche Special Operations (SO) effects, as requested by Government, which encompass *indirect*[3] and *direct*[4] effects. Special Forces (SF) teams project into the operating environment, employing cyber-enabled strategies in an environment where military communications have been denied (Duggan, 2016, p. 2). Cyber-enabled SF relay voice and data in real-time across mobile, ad-hoc, and wireless mesh networks that have been encrypted (Duggan, 2016, p. 2). The multi-protocol mesh networks enable communications with a surrogate partner force, and will be solar powered enabling the facilitation of lethal effects through joint enablers (Duggan, 2016, p. 2). Manoeuvring through hyper-connected dense urban populations, the SF teams employ rolling cyber-enabled 'Movement to Contact' tactics, like rolling penetration tests to probe local networks, and exploitation of 'Internet of Things' devices (Duggan, 2016, p. 2). Another technically savvy SF team infiltrates an enemy's rear administrative area, utilising close-access waveforms, delivering a payload to spread malware throughout the adversary's air defence systems. Disruption of the enemy's cognitive capacity occurs in real-time as a neighbouring SF team initiates a critical influence campaign, utilising strategic reach-back capabilities to deliver cyberspace effects aimed at degenerating trust in the adversaries C2 and logistics nodes through cyberspace. Combat advisors working with cyber-enabled partner forces utilise cyberspace tools to generate disproportionate 'human domain' effects, influencing a large proxy force and shaping support amongst the civilian populace. Meanwhile, specialists within the Operations Centre are monitoring opportunities to deliver effects in, through and external to cyberspace to disable the adversary's ability to provide effective command and control. The combination of effects required a unified strategy that adopted an 'information dominance' approach, this strategy was 'Special Information Warfare'.

[3] The indirect approach is defined as Special Warfare in the US context, referring to the 'execution of activities 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 a permissive, uncertain, or hostile environment'. Proxy Guerrilla Warfare, Special Support Operations (Train/Advise/Assist and Advance Force Operations including Information Operations), and Support Operations constitute the *indirect* approach in the Australian context (Davies, A Versatile Force: The Future of Australia's SO Capability, 2014, pp. 10-11).

[4] The direct approach is defined as Surgical Strike in the US context, referring to the 'execution of activities in a precise manner that employ special operations in hostile, denied or politically sensitive environments to seize, destroy, capture, exploit, recover or damage designated targets, or influence adversaries or threats'. Special Reconnaissance, Precision Strike/Direct Action and Special Recovery Operations constitute *direct* actions in the Australian context (Davies, A Versatile Force: The Future of Australia's SO Capability, 2014, pp. 9-10).

Defining the Problem – Australia's 'State of Play' in the Information Age

Australia's establishment of an 'Information Warfare Division' within the Australia Defence Force (ADF) demonstrates serious consideration of cyber-enabled warfare, and acknowledgement of the challenges imposed by the information age as it relates to modern warfare. The announcement indicates a workforce that will grow from 100 to 900 personnel, presenting an opportunity to spark *action* and *debate* about force design, structure, training and doctrine (McGhee, 2017). This is a chance for the ADF to define its strategic identity regarding cyber-enabled warfare strategy, one that can incorporate the full spectrum of information-centric capabilities across all warfighting domains. The gaps in the latest Defence White Paper's strategic direction regarding cyber-enabled capabilities, dated Information Operations and Network-Centric Warfare doctrine, assessed task-saturation for the Australian Signals Directorate (ASD) in meeting Australia's cyberspace capability needs and recent announcements from Senior Leaders within the ADF all merge to suggest the need for a bottom-up plan of *action* for an asymmetric strategy to fight future, information-centric conflict where strategic risk is at its greatest. By unpacking the current state of play in the Australian context, it will highlight how pursuing a Special Operations concept can contribute to the ADF's effort to maintain relevance in the information age.

The Australian Prime Minister's announcement that an offensive cyber capability exists within the Australian Signals Directorate indicates a growing capability to produce effects in and through cyberspace (Nevill, 2016). Liam Nevill argues that this announcement also imbues a responsibility for Defence to formulate its thinking on how such a capability will be used, and how it can be employed in support of military operations (Nevill, 2016). This carries a degree of risk whereby the whole-of-government responsibilities entrusted in ASD may lead to task-saturation, and an inability to effectively employ cyberspace effects in support of full-spectrum military operations during future conflict. Ormrod and Turnbull's Military Cyber Maturity Model (2015) highlights a capability progression and field of employment model for ASD into the future, indicating the potential for task-saturation in support of future military operations.

The announcement of an 'Information Warfare Division' lead by Major General Marcus Thompson could not have come at a more critical time in the ADF's force modernisation, and will warrant innovate solutions in adopting asymmetric advantage with a relatively modest Defence Force (McGhee, 2017). Since 2003, Australia's military capability development has been geared toward the concept of Network Centric Warfare (NCW) (Davies & Davis, 2016, p. 3). This approach is likely to be surpassed as Australian senior leadership seeks to align modern strategy against the newly-defined US Multi-Domain Battle concept. Senior military figures within the ADF have commented on the challenges posed by the information age and the need to include cyber-enabled effects, yet have been unable to clearly define a unified strategy. Brigadier David Wainwright, Director General Land Warfare, during a panel discussion at the Williams Foundation seminar on integrated force design, commented that 'future land forces will face unprecedented levels of complexity in cluttered, congested, hyper-connected and lethal future operating environments… where the additional layers of informational and human complexity further complicate traditional geo-physical challenges' (Laird, 2017). A slide from the presentation captures the key challenges presented to the land force, which provides a foundation for discussion on the need for a novel Australia's Special Operations concept.

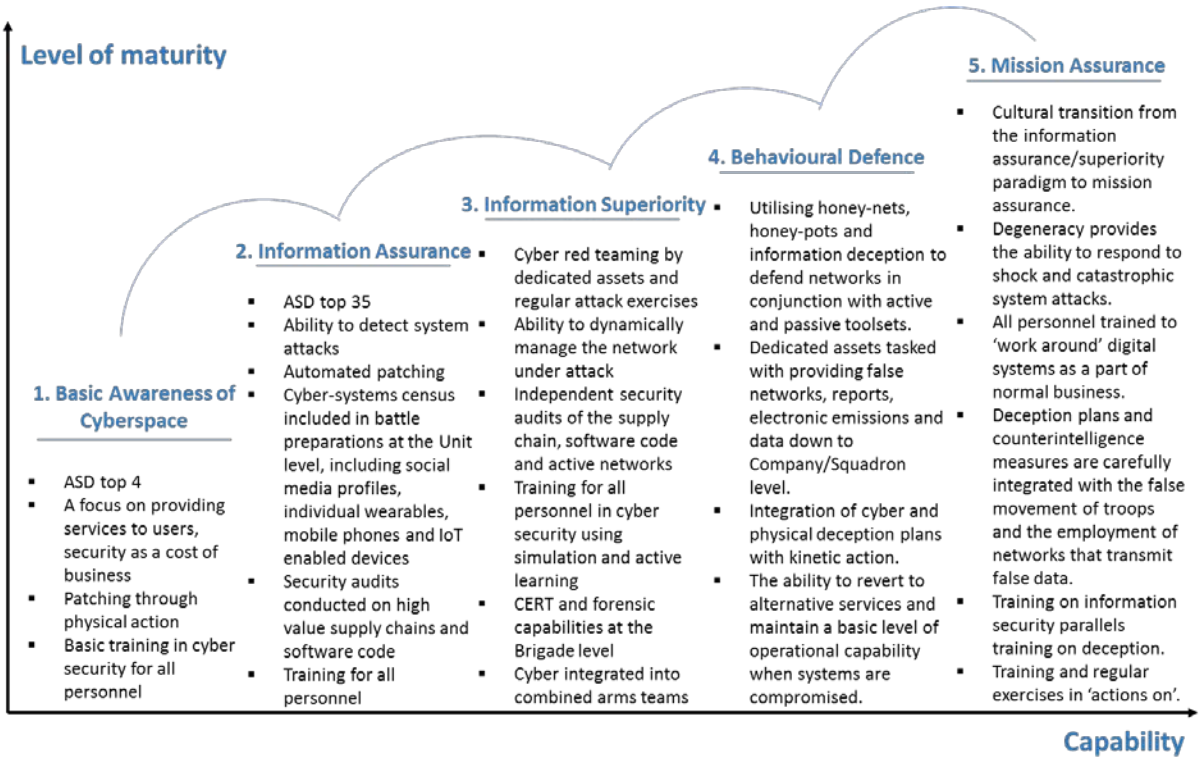

Figure 1. ASD Military Cyber Maturity Model (Ormrod & Turnbull, 2015)

Figure 2. Brigadier Wainright's presentation at the Williams Foundation seminar 2017 (Laird, 2017)

'Information Activities' is the traditional Australian doctrinal approach to operations in the Information Environment[5], documented in ADDP 3-13, 2013. It does not include cyberspace effects in great detail, as should be expected given the highly compartmented and relatively under-developed cyberspace capabilities within the ADF, particularly in comparison

[5] US Army Publication FM 3-12 defines the Information Environment as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information which is drawn from the US Joint publication, JP 3-13.

to the US, Russia and China. This doctrine presents an opportunity for concept development given the recent announcement for organisational change within the ADF toward a cyber-enabled warfare capability. It also serves as a reminder that Australia currently sits well below the base-line in comparison to the expanse of open-source US doctrine and strategy documents, highlighting the need for more open engagement and discussion to harness lessons learned by our principal partners.

Australia's reaction to the challenges imposed by technological proliferation in the information age can be summarised as slow at best. A number of challenges face the ADF as it attempts to identify a pathway to success for a new 'Information Warfare' workforce. It has become apparent through open debate by ADF's Senior Leadership that cyber-enabled, information-centric strategies that achieve supremacy across the physical, informational and human dimensions will be critical to future military advantage. As the Australian Army's Commander Forces Command, Major General Gus Gilmore, at an address to the Institute, commented:

"Cyber opportunities and risks must be an ongoing discussion. We have only scraped the surface of what this disruptive technology offers to us, and what combat vulnerabilities it exposes. The value and availability of information is changing, and through the modernisation process we must ensure that we are structured to maximise the benefits and mitigate the risks of the cyber and digital revolution." (Gilmore, 2016, p. 12).

Additionally, the Chief of Army, Lieutenant General Angus Campbell's stated in his address to the Lowy Institute that:

"the Australian Army is aware of the need for a change in approach. The Defence White Paper sets us a challenge well beyond the continental force of today. Some things we can see now. The linear progression of typical military practice is an uncertain path; our security interests in the 21st Century Indo-Pacific will require 'multiple domain' thought and action. We also know that we cannot rely on technology alone. Technology works best when enabling or partnering human endeavour." (Campbell, Address to the Lowy Institute, 2016).

Statements from ADF's Senior leaders highlight an appetite for ground-up action within Defence, invoking greater debate around a strategy capable of spear-heading a complimentary asymmetric approach in support of the newly established 'Information Warfare Division'. Such a strategy is suggested for the Australian Special Operations community, which can serve as a test bed for a concept of 'Special Information Warfare', where the importance and centrality of the Information Environment in executing technologically-enabled *direct* and *indirect* Special Operations in support of a Joint Force Commander can be realised. Such a concept acknowledges that future warfare will remain a human endeavour, and as such requires an approach where cyber-enabled effects in the Information Environment are nested with operations in the human dimension. As Australia is in its preliminary phase of capability development, a number of lessons can be gleaned by understanding adversary and potential adversary capabilities being employed and developed by Russia, China and the Islamic State.

The Rise of the Hybrid Threat and Information-Centric Challenges

Russian and Chinese military doctrine continues to evolve with a clear appreciation of 'information dominance' as key for modern military success. Russian synchronised political, diplomatic, military kinetic, cyberspace, Special Operations, surrogates, and mass information operations characterise a contemporary hybrid threat worth studying, and presents an indication of how Australia may have to fight in future conflict (USASOC, 2017, p. 2). The Ukraine conflict demonstrates a contemporary example where Russia employed an asymmetric strategy

that successfully synergised cyberspace effects with traditional physical actions (Nordmoe, 2015, p. 69). A battle in cyberspace raged on, with secure communications being hacked, telecommunication lines severed, Distributed Denial of Service (DDoS) attacks targeting government websites, offensive cyberspace effects penetrating financial and military institutions contributing to large-scale civil unrest (Nordmoe, 2015, p. 70). The strategy of New Generation Warfare, or 'hybrid warfare' as it is defined by the West, was adapted by General Valery Gerasimov, the Russian Chief of General Staff, which employs 'indirect action, informational campaign, private military organisations, Special Operations Forces, and internal protest, backed by the sophisticated conventional and nuclear military capabilities' (Adamsky, 2015, pp. 22-23). This strategy combines a 1980's reconnaissance-strike approach aimed at disrupting C4ISR systems with non-kinetic EW[6] and *maskirovka* doctrine which focusses on denial, deception, disinformation, propaganda, camouflage, and concealment (Adamsky, 2015, pp. 27-28). Figure 3 represents the synergy between technological and psychological effects which underpins the New Generation Warfare approach.

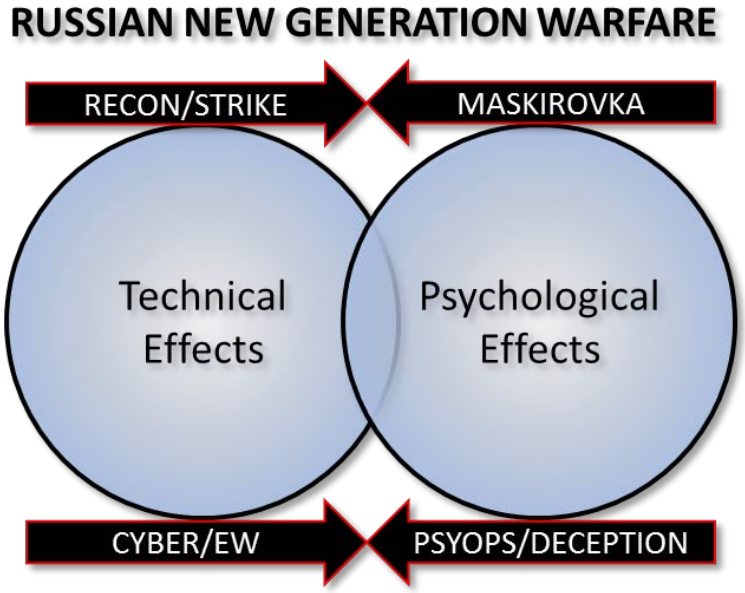

Figure 3. Russian 'New Generation Warfare' Strategy

Advancements in Chinese 'distributed warfare' acknowledge the benefit of cyber-enabled strategies at lower level formations, widely dispersed to achieve strategic effects in distant theatres (Austin, Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security, 2016, p. p7). This strategy should resonate with any modern military, whereby the application of cyberspace effects in support of disaggregated land forces, aimed at achieving superiority in the Information Environment, give cause for new thinking. China has also nested cyberspace and electromagnetic spectrum capabilities at the strategic level, under the concept of Integrated Network Electronic Warfare (INEW) aimed at disrupting an adversary's ability to process and use information (Lasiello, 2015, p. 25). Whilst the Chinese PLA have moved slowly to adapt to the opportunities presented during the information age, they have studied the US war machine and are developing inter-service capabilities that encompass advanced command and control systems and technologically advanced C4ISTAR capabilities, able to 'fight and win localised wars under informatised conditions' (Austin, AUSTRALIA REARMED! Future Needs for Cyber-Enabled Warfare, 2016, p. 10). The Chinese approach to cyberspace operations, and information warfare more broadly, is likely to

[6] EW – Electronic Warfare

reach maturity within the next ten years. Whilst this may seem like a distant future, it presents a case-study of high importance for any middle power where flashpoint conflict involving cyberspace, human and physical domain battle may eventuate at short notice.

State-based capability development is also coupled with the Islamic State's employment of cyberspace, particularly social media platforms, to spread violent extremist propaganda. The ability to shape and influence a global audience, mobilise willing Islamic fundamentalists across international borders, facilitate lethal aid and exercise command and control by issuing orders through cyberspace presents an international problem that spans the political, strategic, operational and tactical levels of conflict. A key lesson is the use of mass media and social media platforms to influence a global audience toward a common cause, demonstrating a superiority in the 'contest of wills'. Prime Minister Malcolm Turnbull commented in an address in Washington DC, that the Coalition was losing the battle of the narrative in cyberspace (Turnbull, 2016). This statement alone indicates the need for novel, asymmetric strategies that employ cyberspace capabilities nested with standing military options to shape and influence through cyberspace against potential State and Non-State adversaries.

The future operating environment will include a hybrid threat landscape where the physical and virtual environments will converge. Russia, China and the Islamic State offer timely lessons that Australia can learn from in the development of organic information-centric strategies. The lessons combine to form a foundation of understanding, which are further reinforced by acknowledging the pace-setting contribution of the United States.

A Comprehensive Approach – The US and Multi Domain Battle, Cyberspace Superiority and Special Operations

'Throughout the history of warfare, militaries have sought advantage through actions intended to affect the perception and behaviour of adversaries. Information is such a powerful tool, it is recognized as an element of U.S. national power – and as such, the Department must be prepared to synchronize information programs, plans, messages, and products as part of a whole of government effort.'

Former US Secretary of Defence, Ash Carter (US DoD, 2016)

A combination of open source US Strategic direction and doctrine provide a sound foundation that supports the development of an Australian concept of 'Special Information Warfare'. The US have realised that technological parity in the information age is increasing, leading to the introduction of the Third Offset Strategy. Multi Domain Battle has emerged in response to the Third Offset Strategy, addressing a cross-domain, holistic approach to fight and win future conflict against a peer adversary. US Special Operations Command's (USSOCOMD) involvement includes an increase in Special Warfare, operating in the Grey Zone left of spectrum and short of war. The Conventional and Special Operations strategies are both underpinned with an increased integration of cyberspace effect operations.

The Multi-Domain Battle concept defines an approach for combat operations targeted against a peer adversary in the 2025-2040 timeframe (US Army TRADOC, 2016, p. 1). The Multi Domain Battle (MDB) Concept acknowledges the overlapping and interconnected nature of the Land, Sea, Air and Space domains with the Human and Cyber domains. This operational approach acknowledges the centrality and importance of achieving 'information dominance' both in and through cyberspace. The characterisation of a future involving contested norms and persistent disorder places significant emphasis on cyberspace, the Information Environment more broadly, and the cognitive components of warfare (US Army TRADOC, 2016, p. 4).

In understanding the MDB concept, future strategic direction can be understood as it applies to the ADF. Lieutenant General Angus Campbell, Australian Chief of Army, recently addressed the Lowy Institute, presenting a clear indication that future Australian joint operations in the littoral would resemble the characteristics of US MDB:

"Innovation in today's non-geographically bound domains – air, space and cyber – is driving connectivity and complexity across the Indo-Pacific region. It's bringing the region closer and more tightly networked. And I think it means the idea of 'an army for a multiple-domain strategy' rather than only for a 'maritime strategy' might be a more useful holistic concept… We need to generate, coordinate and anticipate multiple cross-domain actions and reactions…Perhaps future conflict in the Indo-Pacific will require greater thought about the development and use of indirect approaches. our security interests in the 21st Century Indo-Pacific will require 'multiple domain' thought and action. We also know that we cannot rely on technology alone. Technology works best when enabling or partnering human endeavour." (Campbell, 2016).

The last two decades have instigated transformation within the US Army in its application of Information Operations doctrine, simply because the nature of information and its availability has evolved so rapidly (US Army, 2016, p. vi). The US Department of Defense (DoD) defines Information Operations as the 'integrated employment, during military operations, of Information-Related Capabilities (IRCs)[7] in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own' (US Army, 2016, p. 1). Highlighting cyberspace operations as a sub-component within Information Operations further exemplifies the importance of an over-arching 'Information Warfare' concept that unifies the effects generated in and through cyberspace.

A newly released publication is the US Army's FM 3-12 Cyberspace and Electronic Warfare Operations 2017. It states that the US Army conducts cyberspace and EW operations in the Information Environment, which includes the Physical, Informational and Cognitive Dimensions[8]. FM 3-12 highlights the relationship cyberspace has with the Information Environment by describing the cyberspace layers, which includes the Physical Network Layer, Logical Network Layer and Cyber-Persona Layer[9]. This relationship proves important when understanding the connection between cyberspace and the human domain, and between physical and virtual effects which continue to converge. The figure below highlights the level of connectedness a soldier has on today's modern battlefield through the cyber-persona layer,

[7] An IRC is a tool, technique or activity employed within the Information Environment that can be used to create operational effects and conditions. Other IRCs include Military Deception, Military Information Support Operations (MISO), Leadership Engagement, Civil Affairs, Combat Camera, Operations Security (OPSEC), Public Affairs, Cyberspace Electromagnetic Activities, Electronic Warfare, Cyberspace Operations, Space Operations and Special Technical Operations (US Army, 2016, pp. 2-3).

[8] To further describe the three dimensions that make up the Information Environment, the Physical Dimension includes the tangible network elements, communications networks, information systems and network infrastructures. The Informational Dimension consists of information itself, which acts as the link between the physical and cognitive dimensions. The Cognitive Dimension consists of the minds of those who transmit, receive, and respond to or act on information (US Army, 2017, pp. 12-13).

[9] To further describe the layers of cyberspace, the Physical Network Layer includes the geographic component within the physical dimension, it includes the hardware, system software, and infrastructure that supports the network and the physical connectors. The Logical Network Layer consists of the components that represent the requisite data moving through the network. The Cyber-Persona Layer is the digital representation of the individual or identity in cyberspace, which are the people using the network. (US Army, 2017, pp. 13-14).

which in turn provides an opportunity to provide effects in and through cyberspace in support of a higher 'information dominance' strategy.

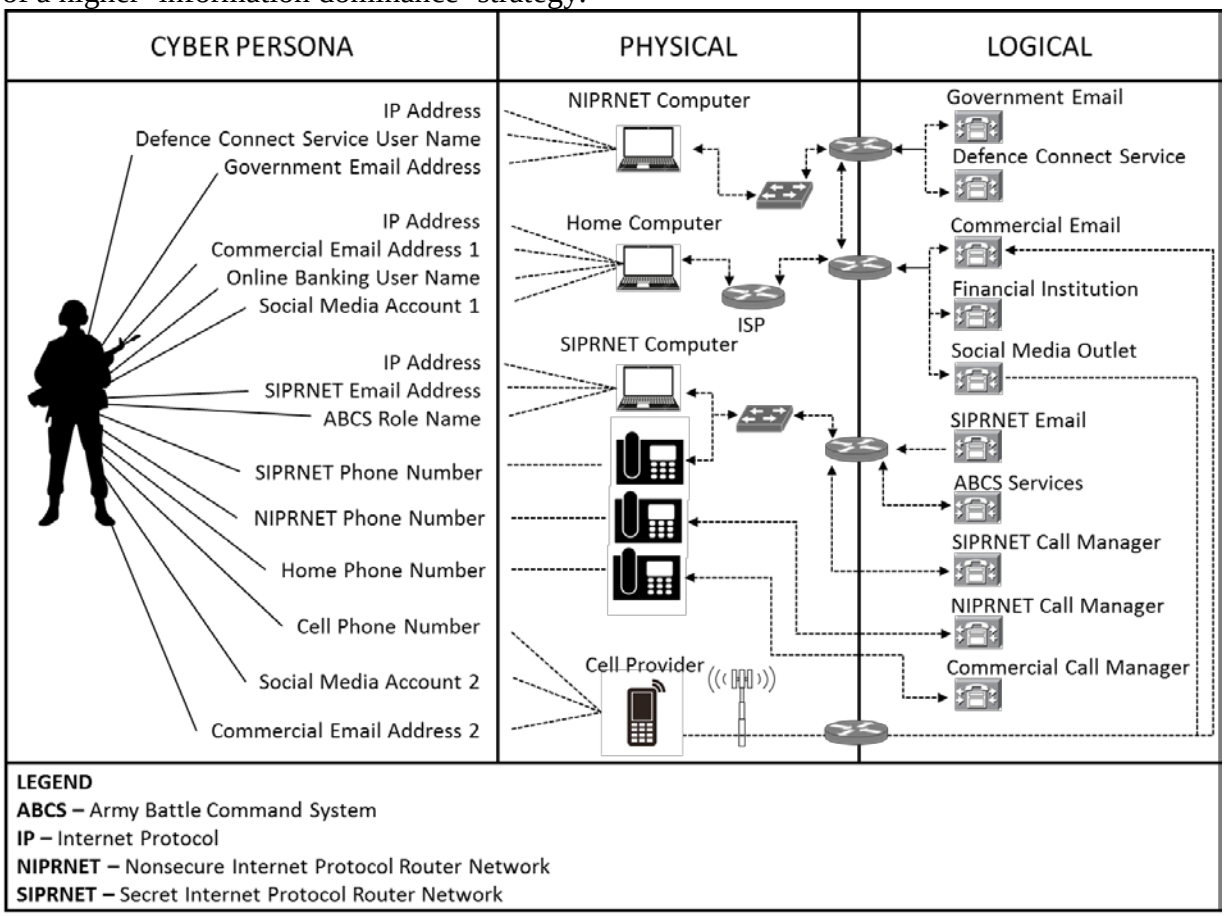

Figure 4. Layers of Cyberspace in the US context (US Army, 2017, pp. 13-14).

The US DoD Strategic Cyberspace Operations Guide 2016 stresses how complimentary cyberspace operations enhance physical domain effects as well as supporting other IRCs (US DoD, 2016, p. 17). This publication highlights the relationship of Cyberspace Operations when supporting Information Operations, which focuses on the denial or manipulation of enemy and potential adversary decision making (US DoD, 2016, p. 24). Further detail highlights effects which may include targeting an information medium (such as a wireless access point in the physical domain), the message itself, or a cyber-persona (an online identity co-ordinating C2 decision making and the dissemination of propaganda) (US DoD, 2016, p. 24).

Another powerful capability is the strategic reach-back support offered by organisations such as United Sates Cyber Command (USCYBERCOM) and its sister organisation, the National Security Agency (NSA), which can be compared to the Australian Signals Directorate. The recent release of USCYBERCOM's 'Beyond the Build' envisions a Joint Force of 2020 where Cyberspace Operations are fully integrated, and are a natural precursor for any future land, maritime, air and space-based operations (US CYBERCOM, 2015). US Army Cyber Command's (ARCYBER) LandCyber White Paper 2018-2030 presents a foundational argument where innovative integration of land and cyberspace operations at all levels of conflict is a necessity for future success in war. The convergence of land and cyberspace operations continues to inform a model applicable in the Australian context, where a complex operating environment requires increased interdependence, disaggregation and an ability to operate over strategic distance in disrupted and denied environments (US ARCYBER, 2013, p. v).

The establishment of US ARCYBER in 2010 has provided a significant amount of time to develop Cyberspace Operations in support of Joint Land forces. Australia can benefit from a slow start, and the application of lessons learned can be applied modestly in support of a holistic strategy with 'information dominance' at its core. US Cyberspace Operations highlight effects in, through and external to cyberspace that can be synchronised to achieve desired operational objectives against an adversary's decision-making process. These actions 'in' cyberspace can be used to disrupt an adversary's information, information systems or networks (US DoD, 2016, p. 15). Operations 'through' cyberspace can include standard joint functions to maintain operational functionality such as command and control, intelligence, fires, manoeuvre and sustainment functions (US DoD, 2016, p. 15). Figure 6 illustrates how effects can be generated in, through and external to cyberspace.

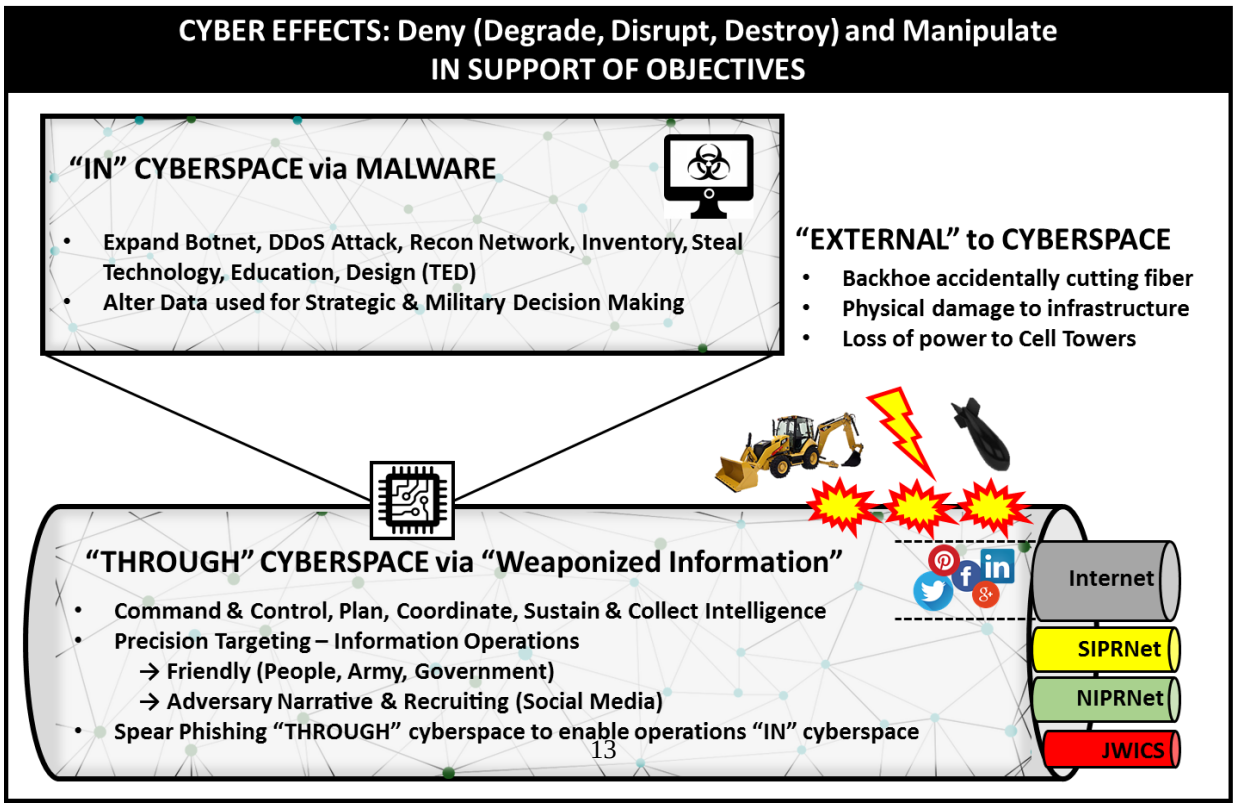

Figure 5. Example of Cyber Effects in the US context (US DoD, 2016, p. 15)

The deeper dimension of US cyberwarfare that extends beyond 'information operations' or 'cyber effect operations' can be seen in the expansive amount of information-centric doctrine, publications and public debate which places a premium on prompt 'information dominance' (Austin, Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security, 2016, p. 8). Cyberspace operations continue to serve as a subordinate component to a broader Information Warfare strategy, yet are fundamental when considering a unique 'Special Information Warfare' concept. A truly powerful combination is Cyberspace Operations, as part of a broader Information Warfare strategy, mixed with the potent *direct* and *indirect* capabilities of Special Operations Forces.

A history of cyberspace effects in support of US Special Operations can be traced back to 2007, where a Computer Network Operations Squadron was raised to support special operators during the Iraq War (Pomerleau, Cyber Operations Come out of the Shadows, 2016). United States Army Special Operations Command (USASOC) Army Special Operations Forces (ARSOF) 2022 White Paper provides a key point of reference to support the development of a 'Special Information Warfare' concept that suites the modest size of

Australia's Army, and especially Australia's Special Operations (SO) community. USASOC's delineation between Special Warfare[10] and Surgical Strike[11] presents an opportunity to develop a synchronised 'Special Information Warfare' concept that bridges the gap between the two mission sets. The figure below provides an insight into USASOC's two forms of special operations, and their mutually supporting relationship.

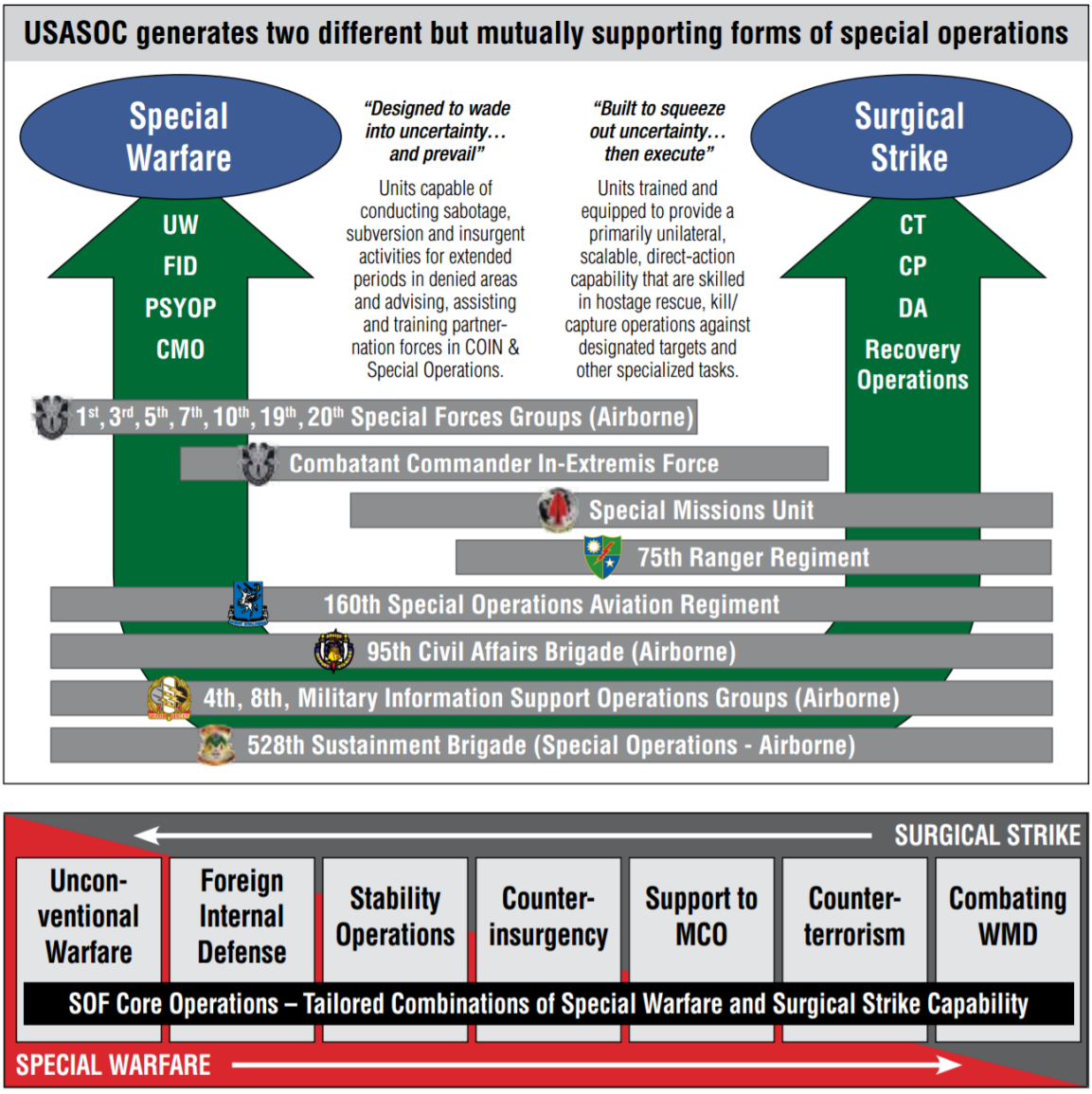

Figure 6. USASOC mission sets

ARSOF 2022 stresses the importance of identifying innovative ways to execute Find, Fix, Finish, Exploit, Analyse and Disseminate (F3EAD) targeting operations[12] as part of its

[10] Special Warfare is designed to work through and with an indigenous partner force or surrogate, with soldiers being training in combat-advisory skills, military deception, sabotage, foreign languages, relationship-building skilsl, cultural understanding, adaptive decision making and cognitive problem solving. This may include Foreign Internal Defence (working with a Host-Nation's security forces) or Unconventional Warfare/Proxy Guerrilla Warfare (working with surrogate, proxy forces). (USASOC, 2016, pp. 10-11)

[11] Surgical Strike represents mainly a unilateral, direct-action capability aimed at kill/capture, hostage rescue against specialised and designated targets (USASOC, 2016, p. 16)

[12] The F3EAD targeting cycle was first developed by General Stanley McCrystal during the Iraq War in 2004. It sought to synergise kinetic kill/capture operations with intelligence and exploitation functions to target Insurgent

Surgical Strike capability, as well as building and fostering relationships in the human domain as part of its Special Warfare capability. ARSOF 2022 highlights how both concepts require a mastery of the Cyber Domain for future success, where Army special operators will be trained in cyber operations, and have an ability to utilise cyberspace to enable operations (USASOC, 2016, p. 26). ARSOF 2022 covers potential solutions which include the formalisation of cyberspace synchronisation, manning, training and capability development across USASOC. Lastly, not only are offensive and defensive cyberspace capabilities included, but the increasing emergence of smart phones, mobile devices and social media and the capability it provides to influence campaigns (USASOC, 2016, pp. 26-27).

Given Australia's comparatively small Special Operations community, a concept of 'Special Information Warfare' that can blend cyberspace operations with human domain operations is worth investigating. This would enable Australian SOCOMD to spear-head an 'information-centric' warfighting strategy that takes advantage of the lessons learned from the US example, the opportunities presented by the information age, and better alignment to the trends of future warfare.

'Special Information Warfare' – A Cyber-Enabled Special Operations Strategy for the Australian Defence Force

'Machines don't fight wars. Terrain doesn't fight wars. Humans fight wars. You must get into the mind of humans. That's where the battles are won.'

Colonel John Boyd (Osinga, 2007, p. 44)

The Australian Government depends on the its Special Operations community to provide Special Operations effects through *direct* and *indirect* means in politically and strategically sensitive operating environments (Langford, 2014, p. 15). An example of the *direct* approach includes the Direct Action missions conducted by Australia's Special Operations Task Group to target insurgent leaders in Afghanistan (Davies, A Versatile Force: The Future of Australia's SO Capability, 2014, p. 9). The *indirect* approach includes Australia's strong history training indigenous partner forces, most recently demonstrated in a Special Operations Task Group's 'advise and assist' mission to support the Iraqi Counter Terrorism Service during the battle to retake Mosul from Islamic State militants (Greene, 2016). Australia's Special Operations community provides an important military option for Government, which includes options that cannot be undertaken by conventional forces, such as inserting at strategic distance behind enemy lines or in a theatre where there are no lines at all (Davies, A Versatile Force: The Future of Australia's SO Capability, 2014, p. 8).

Traditional Special Operations (SO) mission sets will not be exempt from the evolving nature of modern warfare caused by the information age. Contemporary applications of the *direct* and *indirect* approach require adoption of 'best practice' methods aimed at maintaining a capability edge over adversaries who are actively seeking to modernise using emerging disruptive technologies (Langford, 2014, p. 15). The announcement of an Australian 'Information Warfare Division' presents an opportunity to instigate *debate* amongst policy-makers and Senior Defence leadership as well as *action* through bottom-up development of capability that acknowledges the centrality of 'information dominance'. The concept of cyber-enabled 'Special Information Warfare' is a potential solution. Colonel Boyd's quote is a timely reminder that the human factor will continue to underpin actions in, through or external to cyberspace and should be considered when addressing a holistic strategy geared toward

networks (McChrystal, 2014, p. 152). It has since been adopted as the targeting model of choice within the Special Operations community.

'information dominance'. War will continue to be fought for the people and amongst the people in a contest of wills.

The vision for 'Special Information Warfare' is to develop technologically-enabled, human terrain oriented SOF tethered to strategic enablers that are capable of projecting power and influence in, through or external to cyberspace to target the cognitive decision making of an enemy, potential adversary, or designated stakeholder. Figure 8 highlights a conceptual vision, effects, and desired end-state.

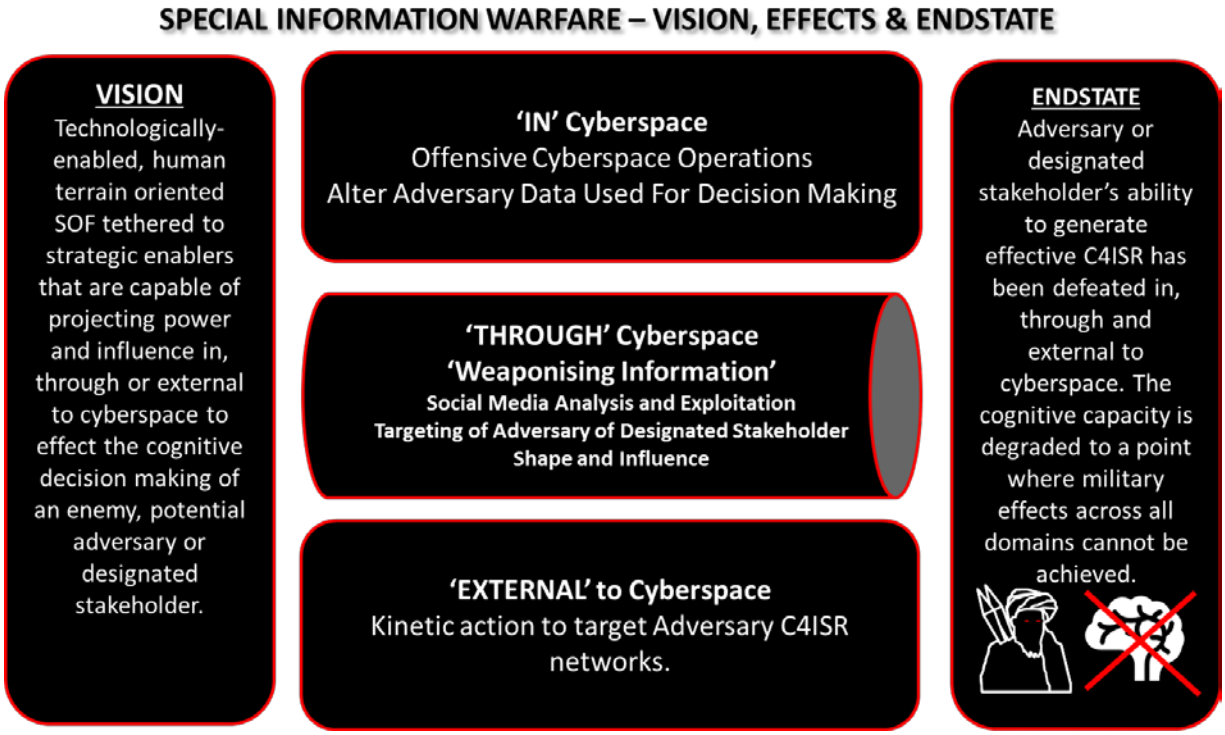

Figure 7. Special Information Warfare Vision, Effects and Endstate.

At a fundamental level, the concept of 'Special Information Warfare' can be defined as a blend between Special Warfare and Surgical Strike, harnessing the capabilities of cyberspace operations with traditional notions of information operations, with a unique relationship to the human domain. The term is chosen specifically to break the model of traditional 'information activities or operations', and reinforce the necessity to evolve a cyber-enabled Special Operations concept as an offensive form of warfare that accentuates the importance of 'information dominance'. Australian SOF represent a suitable force element for such a capability that employs small-scale, disaggregated forces over strategic distance empowered with cyber-enabled tools in contested and congested operating environments.

The USASOC ARSOF 2022 Mission Sets diagram provides a foundation to nest the 'Special Information Warfare' concept as a third Special Operations mission set. The adapted diagram below aims to spark further *debate* on how policy-makers and senior leadership can harness an asymmetric strategy that compliments current Australian Special Operations mission sets.

For any new capability to succeed, it needs two things. The first is a name, and the second is a home. This could take the form of a 'Special Information Warfare Branch' which could reside within the newly established 'Information Warfare Division' to support Raise, Train, Sustain and Capability Development functions. Brigadier Jason Blain, Director General Force Options and Plans Force Design Division, recently presented the various Capability Programs within Defence at the Williams Foundation seminar on integrated force design. This presentation highlights six capability streams across the core warfighting functions, presenting

an opportunity to nest 'Special Information Warfare' under the ISREW, Space and Cyber capability stream within Joint Integration. The responsibility would reside within VCDF Group and seek to provide the link between the 'Warfighting Innovation' and 'Asymmetric Response' capability programs (Blaine, 2017, p. 9). This suggestion is coupled with an acknowledgement that the concept of 'Special Information Warfare' would require further ground-up *action* within SOCOMD's tactical units.

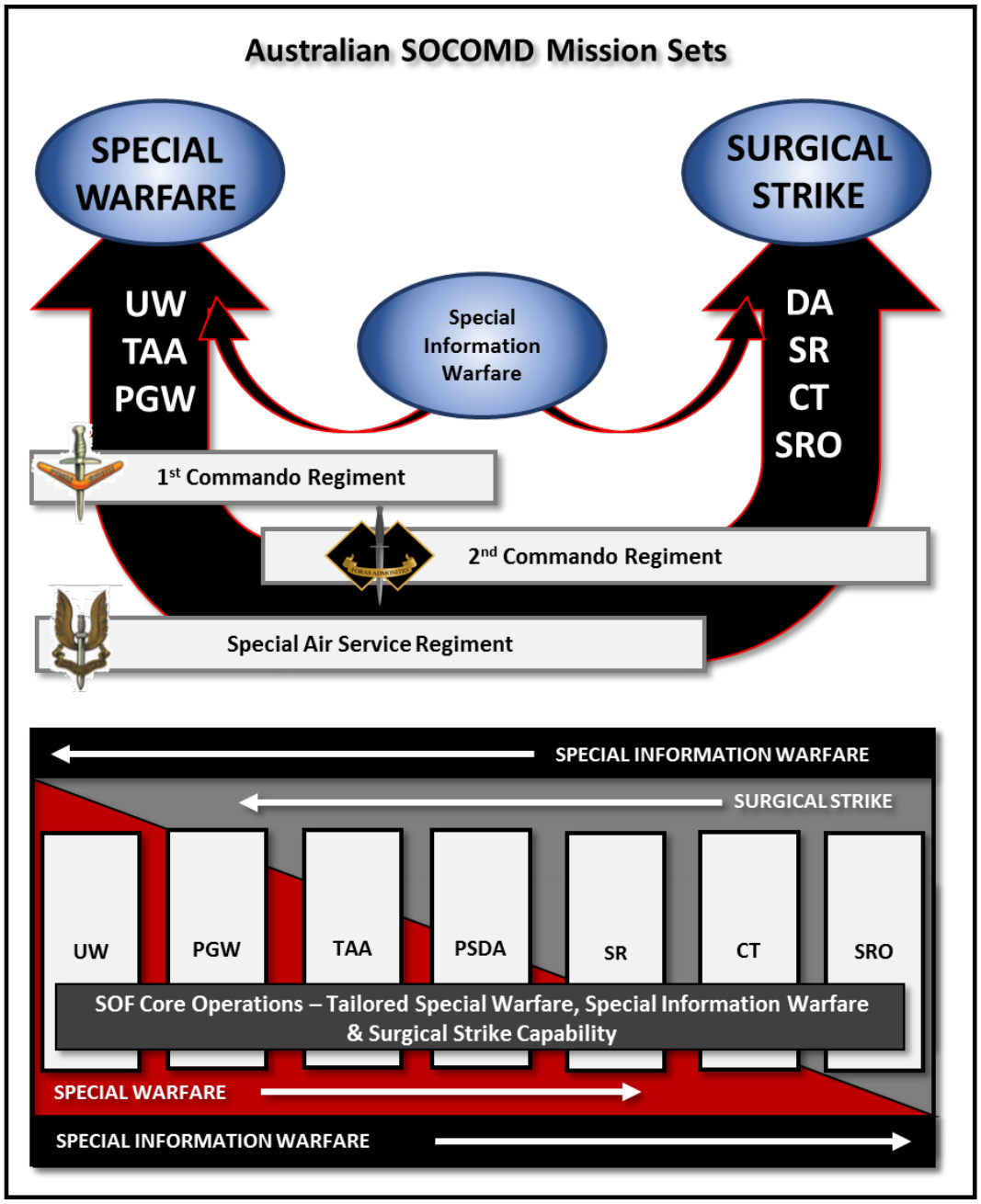

Figure 8. Adapted USASOC Mission Sets to Demonstrate a Concept for Australian Special Operations.[13]

[13] UW – Unconventional Warfare, PGW – Proxy Guerilla Warfare, TAA – Train, Advise, Assist, PSDA – Precision Strike/ Direct Action, SR – Strategic Reconnaissance, CT – Counter-Terrorism, SRO – Special Recovery Operations. This has been adapted from the traditional mission sets of Special Reconnaissance, Special Recovery Operations, Precision Strike/Direct Action, Special Support Operations and Support Operations.

To provide further detail to spark debate and inform action, the 'Special Information Warfare' force design would include a tailored and tethered work force, where operational effects are provided from the strategic to tactical level. The broader cyberspace workforce debate is a largely unanswered question, and the suggested 'Special Information Warfare' force design is aimed to complement broader workforce modernisation within the ADF. Figure 11 provides a prospective force design model as to what could constitute a 'Special Information Warfare' capability.

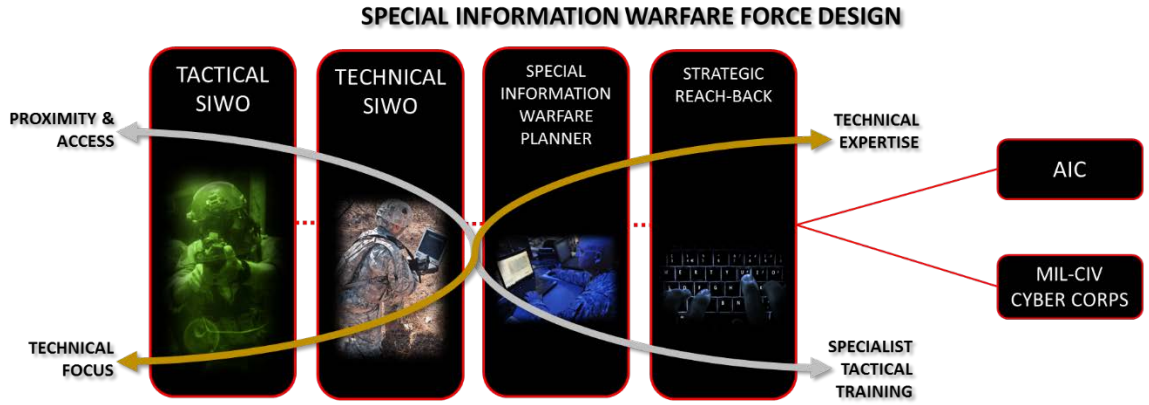

Figure 9. Special Information Warfare Force Design

The Special Information Warfare Force Design includes the development of a Tactical Special Information Warfare Operator (SIWO). The Tactical SIWO is a Special Forces soldier who has received cyberspace awareness training, influence, and information operations training, and is able to effectively utilise cyberspace tools to influence in, through and external to cyberspace. The cyberspace awareness training would focus on the physical layer of cyberspace, facilitating a tethered approach where proximity and access to prospective targets in denied areas can be effected through co-ordinated reach-back. Additional training in the cyber-persona layer to shape and influence partner forces, surrogates and the populace would also occur.

The Technical SIWO is a Signals Corps soldier, who has received advanced technical training in the application of offensive cyberspace tools to provide support at the tactical level. The relationship between the Tactical SIWO and Technical SIWO is complimentary as the Special Forces soldier would bridge the human domain whilst the Signals Operator would specialise in technical skills.

The SIWO planner is an officer and Senior Non-Commissioned Officer (SNCOs) position consisting of Intelligence, Signals or Arms Corps members. The SIWO planners will have received an Information Operations and Cyberspace Operations centric curriculum coupled with influence and critical thinking training. The SIWO planner position is nested at the tactical, operational and strategic operations centres where detailed planning occurs, and would require a headquarters staff designation.

The strategic reach-back includes a formalised relationship with the ASD and the broader Australian Intelligence Community. Additionally, the raising of a Military-Civilian Cyber Corps is included, which is suggested for broader discussion as an enabler to support the full suite of military cyberspace operations. The unique nature of this strategy is the generation of Special Operations effects (both direct and indirect) in, through and external to cyberspace under a unified theory aimed at achieving 'information dominance'.

An Operational Design focussed on SO effects utilising the *indirect* approach has been recommended to further instigate *debate* which focuses on influencing an adversary, population and partner or surrogate force aimed at achieving Cyber-Enabled Relative Superiority[14]. SOF are well suited to wage influence campaigns given their niche cultural skills and access to surrogate or partner 'special' forces during a conflict (Langford, 2014, p. 28). Enablement with cyber tools to maximise influence through social media will only enable greater influence and access. Figure 12 provides a point of reference for the concept of 'Special Information Warfare' utilising the *indirect* approach during Phase Zero operations.

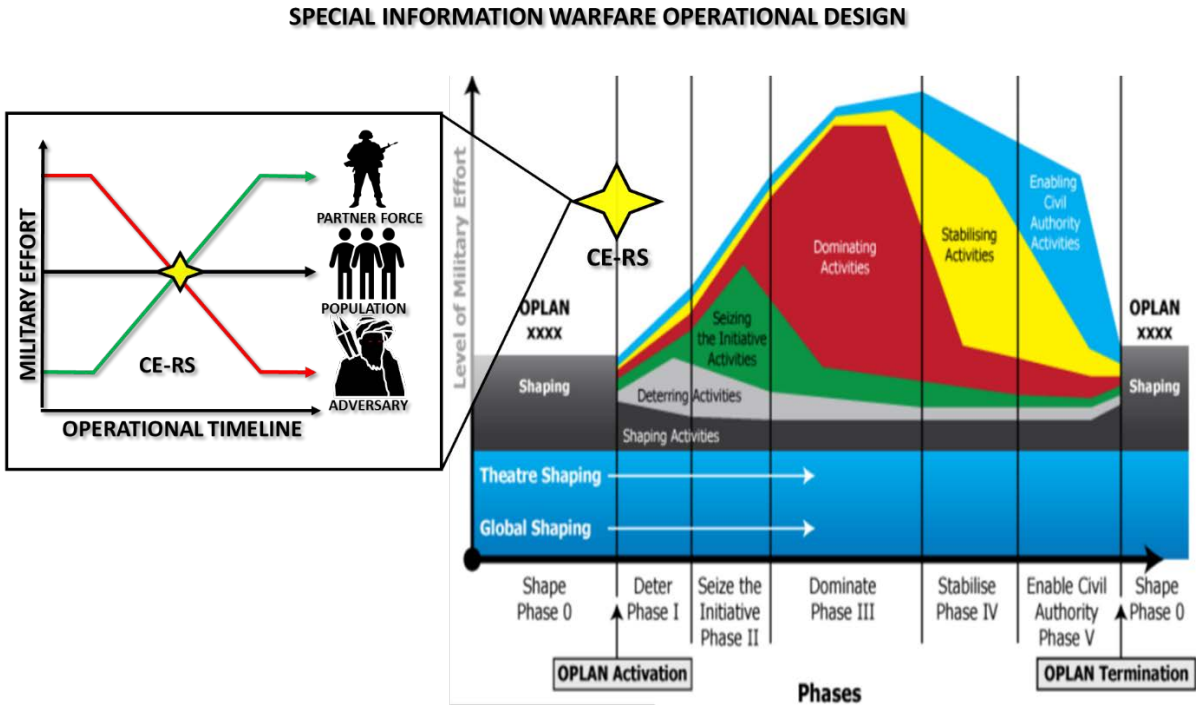

Figure 10. Special Information Warfare – Achieving Cyber-Enabled Relative Superiority

As the adversary is weakened, and the partner force demonstrates increasing capability, the point of Cyber-Enabled Relative Superiority is achieved and a transition occurs to focus military effort on rebuilding the confidence and capability of the indigenous partner force, maintaining positive support from the population and degrading the remaining adversarial threat.

While future cyberwarfare and the contest for 'information dominance' may require more keyboard warriors, small-scale SOF operating at strategic distance in congested and contested environments will be necessary for future success. Enabling such forces with an ability to operate with a technological advantage in, through and external to cyberspace, as well as the ability to interface with strategic cyberwarfare capabilities will provide battlespace situational understanding and effects that cannot be achieved by any other force.

[14] Will McRaven originally defined 'Relative Superiority' as a condition that exists when an attacking force gains a decisive advantage over an enemy (McRaven, 1996, p. 4). Cyber-Enabled Relative Superiority is defined as the moment in a campaign where effects in, through and external to cyberspace have successfully degraded the physical and cognitive decision-making of an adversary, reinforced support from the civilian population and enhanced the legitimacy and relationship with the partner force. The original phases of conflict graphic has been adapted from ADDP 3-13.

Conclusion

The creation of an 'Information Warfare Division' within the ADF highlights an evolving understanding of the importance for cyber-enabled warfare strategies. Whilst Australia has much ground to cover in comparison to pace-setter countries like the US, Russia and China, it demonstrates much needed progression. Australia's modest Defence Force warrants niche, novel, and asymmetric solutions to meet the demands of the information age, and calls for modernisation within its ranks. This concept of cyber-enabled 'Special Information Warfare' seeks to spark *action* and *debate* amongst policy makers and senior Defence leadership, presenting a technologically and socially aware Special Operations option to address future conflict where strategic risk is at its peak. A congested, contested future operating environment riddled with persistent disorder, hyper-connected population centres and hybrid adversary threats who have adopted information-centric strategies necessitates a commensurate asymmetric approach. Through *indirect* and *direct* Special Operations enabled with technological means at strategic distance, tethered to strategic joint enablers and capabilities, Australian SOCOMD can contribute to Australia's Information Warfare capability, maintaining relevance in an era where technological parity continues to rise.

References

Adamsky, D. (2015, Nov). *Cross-Domain Coercion: The Current Russian Art and Strategy*. Instit Francais des Relations Internationales. Retrieved Apr 27, 2017, from http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

ADF. (2013). *ADDP 3-13 Information Activities 2013*. Retrieved Jun 3, 2017, from http://www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf

Atkin, T. (2016). *House of Armed Services Committee*. Retrieved Jun 8, 2017, from http://docs.house.gov/meetings/AS/AS00/20160622/105099/HHRG-114-AS00-Wstate-AtkinT-20160622.pdf

Austin, G. (2016, Jan). *AUSTRALIA REARMED! Future Needs for Cyber-Enabled Warfare*.

Austin, G. (2016, Feb). *Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security.* Retrieved Jun 12, 2017, from https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/DISCUSSION%20PAPER%20Middle%20Powers%20REARMED%2027%20Jan%202016.pdf

Austin, G. (2016). *Shaping the Cyber Arms Race of the Future.* Retrieved Jun 10, 2017, from https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/Shaping%20Cyber%20Arms%20Race%20of%20the%20Future.pdf

Austin, G. (2017, May 18). *Australia's Military to Develop Cyber-Enabled Warfare Doctrine.* Retrieved Jun 20, 2017, from http://thediplomat.com/2017/05/australias-military-to-develop-cyber-enabled-warfare-doctrine/

Blaine, J. (2017). *Achieving an Integrated Force by Design.* Retrieved Jun 12, 2017, from https://www.slideshare.net/robbinlaird/brig-jason-blaine-force-design-department-of-defence-australia

Brown, R. (2017, Mar 20). *The Indo-Asia Pacific and the Multi-Domain Battle Concept.* Retrieved Jun 09, 2017, from https://www.army.mil/article/184551/the_indo_asia_pacific_and_the_multi_domain_battle_concept

Brown, R. (2017). *The Indo-Asia Pacific and the Multi-Domain Battle Concept.* Retrieved Jun 13, 2017, from https://www.army.mil/article/184551/the_indo_asia_pacific_and_the_multi_domain_battle_concept

Campbell, A. (2016). *Address to the Lowy Institute.* Retrieved Jun 13, 2017, from https://www.army.gov.au/sites/g/files/net1846/f/speeches/20161004_ca_address_lowy_institute_4_oct_16_edited_1500_4_oct.pdf

Davies, A. (2014). *A Versatile Force: The Future of Australia's SO Capability.* Retrieved Jun 16, 2017, from https://www.aspi.org.au/publications/a-versatile-force-the-future-of-australias-special-operations-capability/Special_operations_capability.pdf

Davies, A., & Davis, M. (2016). *ADF Capability Snapshot 2016.* Retrieved Jun 6, 2017, from https://www.aspi.org.au/publications/adf-capability-snapshot-2016-c4isrwinning-in-the-networked-battlespace/SI107_ADF_capability_snapshot_2016_C4ISR.pdf

Duggan, P. (2015). *Strategic Development of Special Warfare in Cyberspace*. Joint Force Quarterly, 49.

Duggan, P. (2016). *To Operationalise Cyber, Humanize the Design.* Retrieved Jun 9, 2017, from http://smallwarsjournal.com/jrnl/art/to-operationalize-cyber-humanize-the-design

Gilmore, G. (2016). *Raising and Training the Australian Army.* Retrieved Jun 02, 2017, from http://www.rusinsw.org.au/Papers/20160628.pdf

Greene, A. (2016, Oct 19). *Islamic State: Australia's Special Forces to assist Iraq Military in Battle for Mosul.* Retrieved Jun 11, 2017, from http://www.abc.net.au/news/2016-10-17/australian-special-forces-to-assist-military-operation-to-retak/7939556

Hoffman, F. (2009). *Hybrid Warfare and Challenges.* Retrieved Jun 17, 2017, from http://smallwarsjournal.com/documents/jfqhoffman.pdf

Laird, R. (2017). *Designing the Integrated Force.* Retrieved Jun 16, 2017, from http://www.sldinfo.com/designing-the-integrated-force-the-australian-defense-force-repositions-for-the-next-phase-of-21st-century-force-structure-development/

Langford, I. (2014). *Australian Special Operations: Principles and Considerations.* Retrieved Jun 02, 2017, from https://www.army.gov.au/sites/g/files/net1846/f/australianspecialoperations_b5_web.pdf

Lasiello, E. (2015). *Are Cyber Weapons Effective Military Tools.* Retrieved Jun 9, 2017, from http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/2_Iasiello.pdf

Leon, A. (2015). Impacts of Malicious Cyber Activities. Retrieved Jun 2, 2017, from https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/39429/LEON-THESIS-2015.pdf?sequence=1&isAllowed=y

McChrystal, S. (2014). *My Share of the Task: A Memoir*. Penguin Group

McGhee, A. (2017). *Cyber Warfare Unit Set to be Launched by Australian Defence Forces.* Retrieved Jul 1, 2017, from http://www.abc.net.au/news/2017-06-30/cyber-warfare-unit-to-be-launched-by-australian-defence-forces/8665230

McGrath, J. (2016). *21st Century Information Warfare and the Third Offset Strategy.* Retrieved Jun 12, 2017, from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-82/jfq-82_16-23_McGrath.pdf
McRaven, W. (1996). *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice.* (P. Press, Ed.)
Nevill, L. (2016). *Thinking Deeper About Australia's Offensive Cyber Capability*. Retrieved Jun 14, 2017, from https://www.aspistrategist.org.au/thinking-deeper-about-australias-offensive-cyber-capability/
Nordmoe, M. (2015). *The Ghost in the Machine: Defining SOF in Cyberspace.* Retrieved Jun 10, 2017, from https://www.academia.edu/12465632/The_Ghost_in_the_Machine_Defining_Special_Operations_Forces_in_Cyberspacehttps://outlook.office.com/owa/?realm=unsw.onmicrosoft.com
Ormrod, D., & Turnbull, B. (2015). *Toward a Military Cyber Maturity Model.* Retrieved Jun 10, 2017, from https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/Military%20Cyber%20Maturity%20Model%20v1.pdf
Osinga, F. (2007, Jan 24). *Science, Strategy and War: The Strategic Theory of John Boyd.* (Routledge, Ed.)
Pomerleau, M. (2016). *Cyber Operations Come out of the Shadows.* Retrieved Jun 18, 2017, from https://defensesystems.com/articles/2016/05/05/us-cyber-war-isis.aspx
Pomerleau, M. (2017, Apr 7). *The Relationship Between Third Offset Strategy and Multi-Domain Battle.* Retrieved Jun 10, 2017, from http://www.c4isrnet.com/articles/the-relationship-between-third-offset-strategy-and-multi-domain-battle
Selhorst, A. (2016, Apr 22). *Russia's Perception Warfare.* Retrieved Apr 23, 2017, from http://www.militairespectator.nl/thema/strategie-operaties/artikel/russias-perception-warfare
Turnbull, M. (2016, Jan 18). *Australia and the United States: New Responsibilities for an Enduring Partnership*. Retrieved Jun 18, 2017, from https://www.pm.gov.au/media/2016-01-18/australia-and-united-states-new-responsibilities-enduring-partnership
US ARCYBER. (2013). *The US Army Landcyber White Paper 2018-2030*. Retrieved Jun 4, 2017, from http://dtic.mil/dtic/tr/fulltext/u2/a592724.pdf
US Army. (2016). *FM 3-13 Information Operations*. Retrieved Jun 14, 2017, from http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf
US Army. (2017). *FM 3-12 Cyberspace and Electromagnetic Activities.* Retrieved Jun 18, 2017, from https://fas.org/irp/doddir/army/fm3-12.pdf
US Army TRADOC. (2016, Sep 14). *The 2050 Cyber Army.* Retrieved Jun 18, 2017, from https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwiitOqQpqHUAhXHjZQKHWUXAzYQFgguMAI&url=https%3A%2F%2Fcommunity.apan.org%2Fcfs-file%2F__key%2Ftelligent-evolution-components-attachments%2F01-9016-00-00-00-13-82-05
US Army TRADOC. (2017). *Multi-Domain Battle White Paper.* Retrieved Jun 06, 2017, from http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_WhitePaper.pdf
US CYBERCOM. (2015). *Beyond the Build, Delivering Outcomes Through Cyberspace*. Retrieved May 30, 2017, from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf
US DoD. (2016). *Strategic Cyberspace Operations Guide.* Retrieved Jun 01, 2017, from https://publicintelligence.net/usarmy-strategic-cyber-ops/
US DoD. (2016, Jun). *Strategy for Operations in the Information Environment.* Retrieved Jun 2, 2017, from https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf
USASOC. (2016). *ARSOF 2022.* Retrieved Jun 19, 2017, from http://www.soc.mil/Assorted%20Pages/ARSOF2022_vFINAL.pdf
USASOC. (2017). *USASOC White Paper.* Retrieved Jun 16, 2017, from http://www.soc.mil/USASOCTalks/Expandingmaneuver21Century.html