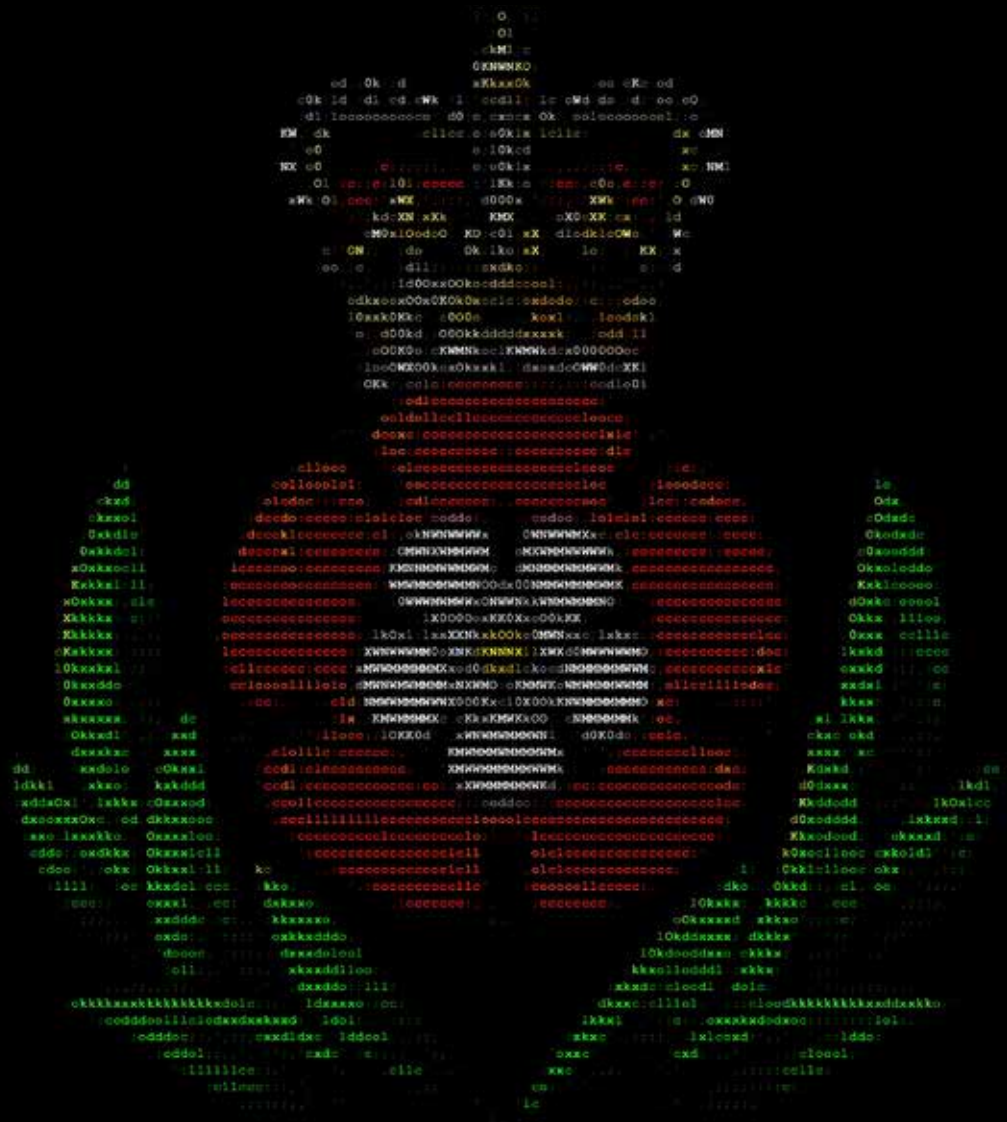
The Australian
Intelligence Corps

Forewarned, Forearmed

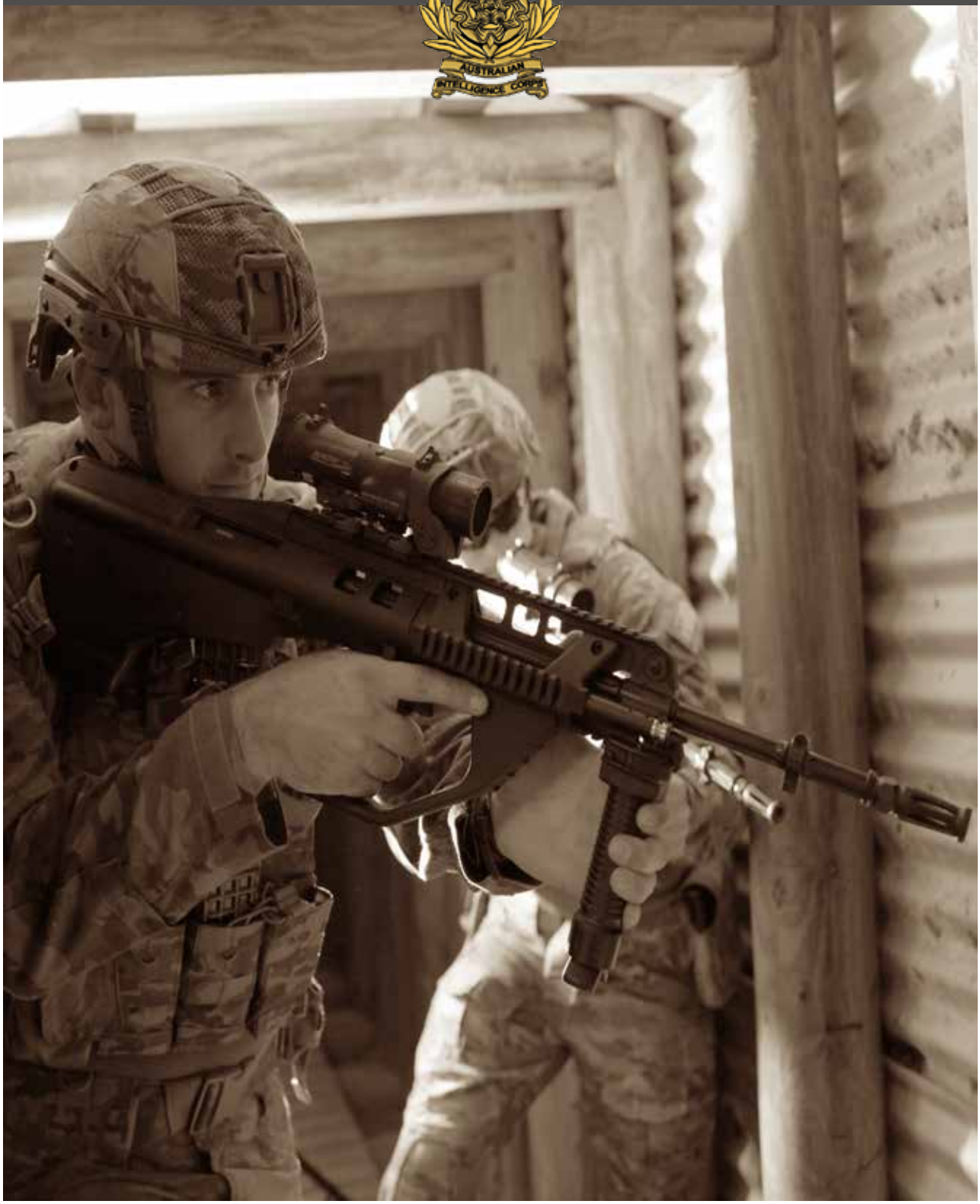


THE BRIDGES REVIEW

The Journal of the Australian Intelligence Corps

2017 Edition

THE BRIDGES REVIEW



CONTENTS

HEAD OF CORPS
BRIG S.J. Beaumont, AM
Ph: (02) 6265 4847
email: stephen.beaumont@defence.gov.au

EDITOR
MAJ Corinne Jones
Ph: (07) 5618 7003
email: corinne.jones@defence.gov.au

GRAPHIC DESIGN
Mario Cicivelli
Ph: (03) 9256 4080
email: mario.cicivelli@defence.gov.au

PRINTED
Defence Publishing Service
Ph: (03) 9256 4593
email: simon.glies@defence.gov.au

The Australian Intelligence Corps *The Bridges Review* Journal is produced in the interest of promoting AUSTINT Corps history, heritage and espirit de corps.

WRITERS GUIDE: Manuscripts should avoid formal Defence Service Writing conventions and write in active voice, avoiding acronyms and jargon. The length may vary, but manuscripts should generally not exceed 3500 words. For reasons of space, it may be necessary to reduce the length of some contributions. Care will be taken to avoid overly editing submissions. Articles selected for publication are accepted as original or previously unpublished (unless otherwise specified). The Editor of the Bridges Review reserves the right to edit all articles to conform to good writing techniques. Authors are encouraged to submit artwork, photos or cartoons to accompany their article. High resolution (300DPI) digital images should be emailed to the Editorial Team, or sent via mail on CD.

The Bridges Review is an UNCLASSIFIED publication. Some articles may require clearance prior to publication and authors are requested to obtain clearance, prior to submitting articles.

Front Cover: PTE Daniel Fahey, 7 SIG REGT. Winner of Art Cover Competition 2017

FOREWORD:

HEAD OF CORPS, AUSTRALIAN INTELLIGENCE CORPS

Brigadier Stephen Beaumont AM

Dear Colleagues,

It is with good deal of pride that I write this foreward to the 2017 Edition of The Bridges Review. Reviewing the articles in this edition reminds me of the broad scope of activity our Corps is involved in, and of the quality of individuals that make up the Corps. There are some terrific items presented here and they are all the more impressive given the tempo of the Corps and that the contributors have found the time to think, and then put pen to paper. To all contributors 'thank you' for your commitment! I am very grateful. Before I make some remarks about the articles in the Review let me first offer a perspective as Head of Corps.

Since the last Bridges Review was published in late 2015, the Corps has been in the spotlight in a way unmatched in recent history. *Plan Athena*, the Chief of Army's Plan to remediate hollowness within the ECN003 trade, has been with us since mid-2016 and it has shaped much of what we do with regard to soldier development, recruitment, training and retention. It has been a significant success with the Corps reducing the gap in the CPL and SGT ranks and building a strong cohort of PTE and LCPL that will fill out our ranks in future years. There is still much work to be done with regards to retention, soldier development and, encouraging those who have recently transitioned to return to the ranks, but we are on the right path. Our collective challenge is to maintain the momentum - to develop our most junior soldiers, to provide them the skills, mentoring and leadership they need so they can perform at their best. Developing our junior soldiers remains one my highest priorities.

In addition to Plan Athena, during the second half of 2016 we had the review of the Corps conducted by MAJGEN (retd) Steve Day. *The Day Review* shone on a penetrating light on the Corps – its structure, capability suite, and personnel. I say penetrating as the Review was presented to CASAC in late 2016 with almost all 26 recommendations accepted by Chief of Army and other CASAC members. Two key outcomes of the Review were the decisions to re-distribute AUSTINT personnel into Aviation and Armoured Cavalry Regiments – units that had been without an AUSTINT cell in recent years – and to conduct a review of the culture within AUSTINT.

The purpose behind the *re-distribution of AUSTINT positions* was to provide an intelligence staff to Army's key land ISR units, and to help build an intelligence culture within those units. While these positions will be harvested from Bde HQ and HQ 1 Div, this is a short term measure until new growth returns these positions back to the formation HQs. I think this has been a sound move though we all need to acknowledge that from Jan 2018 we will have small teams spread more broadly across Forces Command. I ask the leaders of the Corps, particularly those in Bde and Div HQ, to work hard to ensure these small teams are successful. This will require engagement with the supported unit, and at times, hands-on assistance to the intelligence staff in these units.

Another key Day Review artefact was CASAC's agreement that the Head of Corps conduct, with the support of the team from Rapid Context, a review of the culture of AUSTINT. I will not comment on the findings of the *Culture Review* – that is for later – but I would like to make some brief remarks about culture. I am a believer in the oft used quote, 'culture eats strategy for breakfast'. This statement simply makes the point that to any organisation, its culture is more important than its strategy. Get the culture right and an organisation is well set to develop and execute it strategies. But if an organisation gets its culture wrong, or neglects its culture, then the most perfect strategies and plans will not save it. Be clear that MAJGEN Day recommended a culture review not because he thought our culture was unsound or unhealthy, but he saw an opportunity for the Head of Corps, with the support of a contractor, and with the backing of CASAC, to improve the culture that exists in the Corps. No organisation's culture is perfect. The minute you think it is, that organisation is in trouble. I see the Review as a golden opportunity to tune our culture, to shine a light on those elements of our culture that need remediation, and to reinforce those things that work well for us. Our culture is sound, but it is not perfect – some of the articles in the Bridges Review point to this – and so I look forward to working with you to address the recommendations of the Culture Review once it is complete.

To close, let me offer some remarks on the articles in this edition of the Bridges Review.

The first thing to point out is that the contributions here reflect the views of the authors, not the Corps as a whole, and not Army. Our journal is designed to stimulate thought and discussion, and positive change where necessary. For this reason journal articles will sometimes be challenging and provocative. We have a few such articles in this edition. I welcome these. We should be a Corps of thinkers. As a Corps that prides itself on ability to analyse and dissect a problem, we need to be open minded to ideas and theories, and be able analyse the strength of the arguments and deductions.

The two most provocative articles suggest the Corps has either 'lost its way' or is 'sick'. The first makes this claim arguing the Corps has lost its emphasis on combat intelligence , while the second argues leadership within the Corps is not what it should be. I encourage everyone to read these articles as they present two separate challenging, and concerning perspectives. Read the articles and talk about them. You may find your discussion will dovetail neatly with some of the discussions we will have across the Corps as we roll-out the recommendations from the Culture Review later this year.

I would also highlight the excellent article on the challenge of leading and retaining our youngest members of the Corps, those that belong to that demographic collectively known as the millennials. We have a large cohort of exceptionally talented millennials in the Corps, many of whom will be the future leaders of the Corps. It can be argued whether millennials require a specific leadership approach, but what I am certain of is that this group, and all members of the Corps, expect good leadership. At the article points out, 'individuals don't quit their jobs, they quit their bosses'.

I commend this year's journal to you. I thank the contributors who have found the time to offer their view with the intent of improving the Corps. That you have done this speaks volumes for your commitment. I also thank the editorial staff who have spent long hours working with contributors to get articles in the right shape for publication.

Sincerely,
Brigadier Stephen Beaumont AM
Head of Corps

FOREWORD:

REGIMENTAL SERGEANT MAJOR OF THE CORPS

Warrant Officer Class 1 Tom McCrone

It is my absolute honour to have been asked to provide comment for the Bridges Review 2017. I remain proud to be associated with you all, and am aware that many of you have been tested in your skills and leadership through your ongoing support to training, exercises and operations. I have thoroughly enjoyed my time as Corps RSM. I have had many opportunities to speak to, and receive feedback on, a number of issues from officers and, more importantly, the soldiers of the Corps. Issues highlighted have ranged from remuneration, training, unit establishments, to *Esprit de Corps* - much like the articles contained within the current issue of the Bridges Review. The Head of Corps Cell views all of these matters with great importance, and they have been raised at higher levels.

Publications like the Bridges Review provide a forum for the expressions of ideas that may benefit the professional knowledge of all, but more importantly the articles stimulate discussion and debate, as some of the articles have identified a problem or issue that the author believes needs to be rectified. The way we deliver intelligence will constantly change, but the underlying principles will remain, and these articles could be considered the first step in the process of driving change and will enable us as a Corps to adapt and enable us to be forward leaning into the future.

Since the last Bridges Review was published, the Corps has undergone many changes in particular to its manning at all ranks and in all units. We are only now starting to see the effect of the Corps Review in 2015, with numbers increasing at the junior levels; however we still have a way to go to remediate the hollowness within the Corps. With the influx of soldiers through the ab-inito recruiting scheme direct into the Corps, the success of this strategy rests on the training and mentoring provided to the soldiers in the workplace, by their supervisors at all levels.

Everyone in the Corps in a command and leadership position - from JNCO to officer - is vital because of the structure of the various units and the direct influence you will have on your subordinates through your actions. I urge all leaders to always remember where you came from, and make every effort to ensure that previous areas of frustration for you are not again inflicted on your subordinates. I do not say this lightly, our soldiers are our greatest asset and we need to retain them past their four years. The best way to do this is through inspirational leadership. We cannot compete with money outside, so all leaders at all levels in the Corps need to create an environment that has people work for us because they love what we do. You will need to show that resilience, courage, sense of duty and commitment are not just some throw away words given in briefs and put on posters around the barracks. Above all,

you will need to have confidence in your soldiers and they have confidence in you. The profession of soldiering requires each and every one of us to excel at what we do, and to ensure we are contributing to the best of our abilities at all levels. Remember, our soldiers are our greatest assets, and also the future of our Corps.

The strength of our Corps remains the professionalism and dedication of our people; this is demonstrated by the breadth of articles from all ranks contained within the Bridges Review. Even though some may be controversial, it will generate debate. In closing, I would like to say it has been a privilege to serve as Corps RSM, and as I come to the end of my tenure and hand over responsibility, I take this opportunity to thank all and your families for the service provided to the Corps.

FOREWORD:
DEPUTY HEAD OF CORPS

Lieutenant Colonel Chris Alder

It is my honour to contribute opening remarks for the Bridges Review. I would like to start by acknowledging the efforts of MAJ Corinne Jones and MAJ Karen Hunter in supporting the compilation of this year's journal. Both continue to serve the Corps exceptionally well in direct support of Head of Corps cell activities, and are to be commended for their tireless service.

In my dual role as Deputy Head of Corps AUSTINT and Commanding Officer of the Defence Force School of Intelligence (DFSI), I am privileged to observe quality training being delivered to AUSTINT Corps members on a daily basis. AUSTINT staff at the school are passionate about their work, and committed to nurturing members to achieve academic excellence. AUSTINT learners at DFSI continue to impress me; our courses are being undertaken by highly capable individuals, who are motivated and responsive to the instruction they are receiving. We are very fortunate being part of a tri-service school, constantly learning from the excellent training being delivered by our Navy and Air Force counterparts.

However I have always had the view the training being delivered by DFSI - as impressive as it is - is a small part of an AUSTINT Corps member's professional development. This is important when one considers the competency based training system at the school. This model reduces content down to a short focal length, and excludes from the field of vision, elements that are irrelevant to designated learning outcomes. This is a deliberate approach, borne out of a necessity to graduate members in a prescribed timeframe, 'on time and on standard' to employment specifications contained in the AUSTINT Corps Employment Manual. However it is an approach that constrains learning, and will always be deficient in generating individuals with the necessary understanding of war and warfare required to defeat complex enemies. To bridge this gap, we need AUSTINT Corps members who are committed to reading broadly and thinking critically, and engaged in discussion about the best ways the Corps can support the warfighter.

Given our inquisitive nature, all AUSTINT Corps members should have a penchant for seeking out professional development resources. However, building time for personal reflection can often be challenging in high tempo work environments, where 'busy-ness' is often a mainstay. While I appreciate the very real constraints imposed by our high work rate, it is prudent for all AUSTINT leaders to consider how they are encouraging professional development in the workplace. Simple acts such as drawing attention to reading resources, and sharing insights into professional development experiences, can go a long way to establishing an active learning culture that encourages members to maximise self development opportunities.

While we should all be committed to a lifelong process of professional development, the way in which AUSTINT Corps members are encouraged to undertake professional development should not

be prescriptive. Each individual will have a different learning style and process of acquiring relevant information. My own approach has been to consider current operational vignettes, and overlay this against historical case studies to ensure issues are considered in appropriate width, depth and context. Regardless of approach, I would offer that a focus on professional development that ensures the past is appropriately considered, while also looking to how we can support decision making in complex and ambiguous situations, is the best preparation we can undertake to steel ourselves for the rigors and ugliness of war.

This year's Bridges Review, as with preceding publications, provides an important forum for professional discourse by AUSTINT Corps members and friends of the Corps who are focused on advancing the intelligence function. It is a sign of a Corps with a healthy approach to professional development; a Corps which gives due attention to the past, but which is also prepared to think broadly and challenge the status quo. I commend this journal to you and thank all those who have taken the time to contribute to it.

INTELLIGENCE AT THE OPERATIONAL LEVEL OF WAR

Major Paul Baker

> *Nowhere do we find an unambiguous definition of operational level intelligence, encompassing its unique perspective, specific purpose, and particular focus. The astute reader of current doctrine may be able to organize a joint intelligence center and describe its tasks in general terms, but he has only the fuzziest of notions of where and how to focus the organization's efforts. At best he will have divined that operational level intelligence is a sort of hybrid of strategic and tactical intelligence — Strategic in scope but tactical in detail, bounded in some way by a geographic theatre.*[1]

Major Linden's observations from her US Army Staff College monograph are as prescient today as they were in 1990. They continue to apply to the ADF, whose doctrine and training fails to prepare intelligence analysts for their role at the operational level of war. I recently enjoyed a month with the ADF's Deployable Joint Forces Headquarters (DJFHQ) on Exercise Talisman Sabre; a divisional headquarters commanding several coalition brigades, fleets and air components, each directing sometimes-joint, sometimes-independent operations towards a common strategic goal. Throughout the exercise, I asked staff officers about our proximity to the operational level, and the associated intelligence requirements. As good scholars of Clausewitz, Australian military planners recognised the tactical level as 'the use of armed forces in the engagement' and the strategic, 'the use of

engagements for the object of the war'.[2] However, the same planners were comfortable describing the operational level in terms of sizes of activities, headquarters, areas of operations and 'jointness'. Made worse, when describing intelligence activities conducted at such a level, they relied on tautologies based on '*intelligence support to* …' the same activities, headquarters and areas that define the operational level itself. This paper will posit that the ADF's mediocre understanding of the operational level prevents its intelligence analysts from looking beyond tactical battles. Initially, it will argue that despite common reference to an operational level, the concept remains unclear to contemporary planners, particularly given the dynamic character of contemporary warfare. It will suggest that there is incomprehension of an operational level of intelligence, with doctrine and academia struggling to define it, or discern unique analysis required to support it. Finally, it will submit that such

[1] Linda L Linden, *Operational Level Intelligence: An Alternate Approach* (Fort Leavenworth, 1990), 17.
[2] Carl Von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (New York: Oxford University Press, 2007), 74.

incomprehension prevents the Australian intelligence community from formally preparing analysts for analysis at the operational level.

Despite the operational level of war emerging in western military scholarship in the 1980s, the concept remains easy to misunderstand. The level emerged to reflect the evolution of military art as a result of mobilisation of mass armies, mechanisation of manoeuvre, extended fronts, complimentary maritime and air capabilities and information technologies bourgeoning throughout the twentieth century. No longer did a single general command his army in battle to achieve national strategy, but multiple generals commanded multiple armies across multiple theatres.[3] The level is defined neatly in *LWD 1 The Fundamentals of Land Power* as 'planning and conducting campaigns incorporating joint forces … to achieve one or more strategic objectives.' [4] The joint *ADDP 3.0 Campaigns and Operations* provides further clarity stating that 'in the Australian context the operational level commander is the Chief of Joint Operations (CJOPS)'; [5] implying that lower level commands are absolved from operational level planning. Brian Tyler's detailed 2014 exploration of operational intelligence suggests characteristics that distinguish the operational level.

1. It is removed from the political agency that resides at the level of strategy.
2. It is distinct from the actual employment of forces, which occurs at the tactical level.
3. It extends spatially beyond the tactical engagement but is less than global, often stopping before the international boundaries that demark the strategic.
4. It is sandwiched between the immediate and the enduring. [6]

While perhaps valid through the aging lens of world wars, Tyler's characteristics are aspirational in the context of the contemporary operating environment.

There are valid arguments that the contemporary operating environment weakens the concept of an operational level of war. Strategic policy advisers are deployed to tactical units, the employment of force—particularly non-kinetic—can be coordinated from afar, and Westphalian sovereignty poses less constraint to both adversary groups and coalition effects. Some scholars argue that modern information technologies bridge the strategic-tactical divide altogether; wherein tactical actions can have strategic consequences and strategic decision-makers can influence tactical actions on a daily basis. The same technologies mean 'a central strategic headquarters [can] employ multidimensional tactical means that can compress close, deep and rear battles into one continuous and simultaneous strike.' [7] A second criticism blames the operational level (which was conceptualised for the command of 'large wars') for recent western failures in 'small wars', involving asymmetry and non-state actors. Such criticisms suggest that maintaining the modern dislocation of strategy and tactics is counterproductive; leading to strategic ideas that make incoherent tactical actions and tactics that are disadvantageous to strategy. [8] While independently valid, such arguments are mutually defeating. A 'continuous and simultaneous strike' coordinated at the strategic level, may be appealing, but risks being incoherent with other tactical actions. Thus, such arguments are flawed by the operational level's intrinsic nature. Regardless of location and level of command, there must be a commander synchronising dislocated tactical actions across a theatre to achieve a declared strategic objective.

[3] Tom McDermott, "DEF Australia Letters from HAMEL Part 3: The Operational Level of War. What Is It Good For?," Grounded Curiosity, 2016, http://groundedcuriosity.com/def-australia-letters-from-hamel-part-3-the-operational-level-of-war-what-is-it-good-for/; Michael Evans, "The Closing of the Australian Military Mind: The

[4] Australian Army, "Land Warfare Doctrine 1 The Fundamentals of Land Power" (Canberra: Commonwealth of Australia, 2014), 19.

[5] Department of Defence, "Australian Defence Doctrine Publication 3.0. Campaigns and Operations" (Canberra: Commonwealth of Australia, 2012), 1–7.

[6] Tyler, "Intelligence and Design. Thinking about Opertional Art," 13.

[7] Evans, "The Closing of the Australian Military Mind: The ADF and Operational Art," 109–10.

[8] McDermott, "DEF Australia Letters from HAMEL Part 3: The Operational Level of War. What Is It Good For?"; Evans, "The Closing of the Australian Military Mind: The ADF and Operational Art," 109.

Debate also exists as to whether there is a unique Australian operational level of war. Michael Evans writes that Australia's primary role as junior alliance partner for most of the twentieth century precluded an Australian understanding of the operational level. He writes that until the International Force East Timor (INTERFET) in 1999, Australia had had only two operational commanders. The first being General Sir Thomas Blamey's role as Commander-in-Chief of Australian Military Force and his direction of operational-level campaigns in New Guinea in 1943-44. The second was Air Vice Marshall Frederick Scherger, as Air Officer Commanding Malaya in 1953-1955.[9] Evans deduces that the Australian way of war has led to significant tactical experience yet 'a tradition of inexperience at the operational level'.[10] He concludes that the ADF must develop an operational art that embraces Australia's place as a global junior partner and an independent regional actor or coalition leader.[11] Therefore given the nature of the numerous successes Australia has enjoyed as a coalition leader for regional stability and humanitarian assistance missions, if Australia has a unique operational level, it should be considered joint, coalition, interagency, regional and low intensity.[12]

If the operational level remains poorly understood, intelligence analysis at that level remains incomprehensible. Australian and US doctrine define operational intelligence in tautologies. Our joint *ADFP 2.0.1 Intelligence Procedures*, suggests 'operational intelligence is that required by operational level commanders for planning and conducting campaigns and operations within theatres'.[13] Tyler writes that prior to the First World War, there were only two levels of intelligence and that 'operational intelligence was tactical reconnaissance writ large'. Still most scholars consider intelligence at only the tactical and strategic level;[14] John Keegan's seminal 2003 work divides intelligence into either tactical or strategic, only hinting at something in between.[15] Unfortunately, despite his best efforts, Tyler's exploration led to another lacklustre definition of operational intelligence: '… state activity to understand foreign entities and potential battlespaces for the purpose of planning and conducting campaigns and major operations'.[16] Given doctrine and academia's inability to coherently define operational intelligence, it is no surprise that Australian analysts cannot recognise it, let alone discern its associated tasks.

In attempting to delineate between intelligence responsibilities, *Intelligence Procedures* starts with clarity, presenting strategic responsibilities of the Defence Intelligence Organisation (DIO) including strategic warning, order-of-battle production and Defence economic intelligence analysis.[17] There is also clarity when it presents responsibilities of a tactical Joint Task Force (JTF) J2.[18] However confusion emerges at the operational level, wherein J2, Headquarter Joint Operations Command (HQJOC) is made responsible for intelligence tasks that look surprisingly like tactical tasks or have merely had the word '*operational*' added.[19] It must be acknowledged that *Intelligence Procedures* also suggests J2 HQJOC is responsible for intelligence force-generation governance such as 'designing and developing intelligence architecture'.[20] Also, ADF publications agree that it is at the operational

[9] Evans, "The Closing of the Australian Military Mind: The ADF and Operational Art," 112–13.

[10] Evans, "The Closing of the Australian Military Mind: The ADF and Operational Art," 106.

[11] Evans, "The Closing of the Australian Military Mind: The ADF and Operational Art," 106 and 123.

[12] Australian Army, "Land Warfare Doctrine 1 The Fundamentals of Land Power"; Department of Defence, "Land Warfare Doctrine 2-0. Intelligence" (Canberra: Commonwealth of Australia, 2014); Evans, "The Closing of the Australian Military Mind: The ADF and Operational Art."Tyler, "Intelligence and Design. Thinking about Opertional Art," 13.

[13] Department of Defence, "Australian Defence Force Publication 2.0.1. Intelligence Procedures" (Canberra: Commonwealth of Australia, 2015), p1-3; The same flaw plagues coalition doctrine, see Tyler, "Intelligence and Design. Thinking about Opertional Art," 14.

[14] Tyler, "Intelligence and Design. Thinking about Opertional Art," 15.

[15] John Keegan, Intelligence In War: Knowledge of the Enemy from Napoleon to Al-Qaeda (New York: Alfred A. Knopf, 2003), 18.

[16] Tyler, "Intelligence and Design. Thinking about Opertional Art," 15.

[17] Department of Defence, "Australian Defence Force Publication 2.0.1. Intelligence Procedures," p3-5.

[18] Department of Defence, "Australian Defence Force Publication 2.0.1. Intelligence Procedures," p3-2.

[19] Department of Defence, "Australian Defence Force Publication 2.0.1. Intelligence Procedures," p3-4.

[20] Department of Defence, "Australian Defence Force Publication 2.0.1. Intelligence Procedures," p3-4.

level in which intelligence estimates and support plans are produced, and that in general, significant more detail of analysis can be expected.[21] However, *analysis* tasks otherwise reflect the same operational intelligence tautology; that operational level intelligence is the same as tactical intelligence but … in support of operations.

Intelligence Procedures is also responsible for detailing how intelligence should support the Joint Military Appreciation Process (JMAP). This support, encapsulated in the Joint Intelligence Preparation of the Operating Environment (JIPOE), is described in 20 pages, none of which discern how the support differs at different levels of war.[22] The obvious counterargument is that tactical intelligence support to planning is detailed in LWP-INT 2-1-8 '*Intelligence Preparation of the Battlespace*' (IPB). However, the latter is Army doctrine for which there is no equivalent publication guiding Navy or Air Force analysis, and it too avoids discerning between analysis at the difference levels. The enthusiastic analyst must turn to US Army doctrine to find a whole chapter describing how the IPB differs at the three levels of war.[23] Such a common flaw across ADF doctrine defines operational intelligence by what it supports, rather than discerning the intrinsic nature of such support. It fails to harness the complexity of synthesising and sequencing remote operations and battlespace conditions that Australian operations planning doctrine so richly describes.

The most valuable doctrine for operational level planners, the joint *ADDP 3.0 Campaigns and Operations*, misses an opportunity to discern operational intelligence. It suggests the need to analyse the adversary centre of gravity (COG) and 'broad patterns of adversary activity and trends'.[24]

Most planners recognise that our concept of COG derives from Clausewitz's concept of schwerpunkt; 'the hub of all power and movement, on which everything depends... the point against which all our energies should be directed.'[25] Some will also recognise our approach to planning as Schwerpunktbildung, building an operational plan that synchronises all efforts against the COG. However, few will be familiar with the concept of a commander's *fingerspitzengefühl*; literally a general's *fingertip feeling* of the situation throughout the theatre. A developed *fingerspitzengefühl* is what gives an operational level commander a sense of what is possible throughout the theatre, rather than what is planned. The *fingerspitzengefühl* is hard to develop, and a result of years of professional military education, experience and a well directed intelligence apparatus. *Fingerspitzengefühl* is what generals like Erwin Rommel and James Mattis were famous for having throughout their respective careers,[26] but some argue Admiral Yamamoto lacked in the South West Pacific Campaign in 1943.[27] In the Australian context, *Fingerspitzengefühl* is what British General Richards observed General Peter Cosgrove demonstrate as Commander INTERFET in 1999:

> I must have been developing a much better grasp of the link between the tactical and the strategic. It is what a German General would call *fingerspitzengefuhl* … As Clausewitz's aphorism suggests, war is an extension of politics by other means; you win by deploying a multiplicity of weapons systems, only one of which is military. My time in East Timor under Cosgrove, not least observing the ease with which he switched from the tactical to the operational to the strategic, and communicated so well at all three levels, was to serve me well…[28]

[21] Department of Defence, "Australian Defence Force Publication 2.0.1. Intelligence Procedures," p4-5; Department of Defence, "Australian Defence Doctrine Publication 3.0. Campaigns and Operations," 3–9.

[22] Department of Defence, "Australian Defence Force Publication 2.0.1. Intelligence Procedures," Chapter 5.

[23] Department of Defence, "Australian Defence Force Publication 5.0.1. Joint Military Appreciation Process" (Canberra: Commonwealth of Australia, 2015); Department of Defence, "Australian Defence Force Publication 2.0.1. Intelligence Procedures"; Headquarters Department of the Army, *Field Manual 34-130 Intelligence Preparation of the Operating Environment* (Washington D.C., 1994).

[24] Department of Defence, "Australian Defence Doctrine Publication 3.0. Campaigns and Operations," p3-9.

[25] Von Clausewitz, On War, 242.

[26] Terry Brighton, *Master of Battle, Monty, Patton and Rommel at War* (UK: Penguin, 2009), 64; Dick Camp, *Operation Phantom Fury: The Assault and Capture of Fallujah* (Minneapolis: Zenith Press, 2009), 34.Camp, *Operation Phantom Fury: The Assault and Capture of Fallujah*, 34.

[27] H.P. Willmott, "Isoroku Yamamoto: Alibi of a Navy," in *The Great Admirals: Command at Sea, 1587-1945*, ed. Jack Sweetman (Annapolis: Naval Institute Press, 1997), 454.

[28] David Richards, *Taking Command* (London: Headline Publishing Group, 2014), p102-103.

While important for operational planning, understanding the scope of the commander's *fingerspitzengefühl* is critical for operational intelligence analysis. Therefore, it is not in discussion of intelligence, but in operational art that the astute reader can detect and construct a definition of operational intelligence.

It is at the operational level in which intelligence staff must take a systems approach, and question an adversary's ability to synchronise distributed operations,[29] to exploit 'spatial and temporal depth', and 'mould an array of diverse tactical actions into a coherent ensemble of military force' congruent with strategy.[30] It is the level at which the staff must query the adversary's ability to sequence and resource multiple lines of effort, assessing which 'FE may need to pause, defend, resupply, or reconstitute, while other FE continue'.[31] It is therefore the level where the staff must deduce the adversary's operational reach, 'the distance and duration across which a unit can successfully employ military capabilities.'[32] It is the level in which the staff must start to assess the character of warfare in which various stakeholders will engage, not just the courses of action that each stakeholder group will adopt.[33] It is also the level in which the staff must recognise the importance of time, and predict 'how the problem might evolve during the campaign'.[34] Most important of all, it is the level in which the intelligence staff must assess the characteristics that define the confluence of multiple diverse tactical stakeholder actions across time and domains that define the theatre. Thus Linden was correct in 1990, suggesting 'the essence of operational level intelligence is the assessment of enemy operational level linkages, not the linkage itself of our own tactical and strategic intelligence.'[35]

Unfortunately, the poor understanding of operational level intelligence may have limited the training of

Air Commodore Frederick R.W. Scherger and Major General E.J. Milford, General Officer Commanding of the 7th Division, 1945.

Australia's intelligence enterprise. If weaknesses in the ADF's understanding of operational art, as Evans suggests, have been 'camouflaged' by tactical success in Iraq and Afghanistan,[36] so too has our failure to develop operational intelligence. Almost every contemporary analyst has deployed to Iraq, Afghanistan or East Timor on more than one occasion.[37] Those in the Army have invariably supported a task group based on a traditional battalion headquarters, augmented with specialist joint and coalition intelligence collection platforms. Those in the Navy have usually provided intelligence to a single ship tactical operation. Similarly, those in the Air Force have usually deployed in support of a single tactical capability (e.g. air mobility). Only a lucky few have worked in an Australian formation or JTF headquarters, and luckier still are the few to have been embedded in operational and strategic coalition headquarters or intelligence fusion centres. Thus, the sheer majority of intelligence lessons that are brought home and invested in ADF training, are trapped by our successes at the tactical level of war. Throughout their subsequent careers these

[29] Tyler, "Intelligence and Design. Thinking about Opertional Art," 93.

[30] Evans, "The Closing of the Australian Military Mind: The ADF and Operational Art," 108–9.

[31] Australian Army, "Land Warfare Doctrine 1 The Fundamentals of Land Power," 20. Department of Defence, "Australian Defence Doctrine Publication 3.0. Campaigns and Operations," p2-13.

[32] Department of Defence, "Australian Defence Doctrine Publication 3.0. Campaigns and Operations," p5-18.

[33] Department of Defence, "Australian Defence Doctrine Publication 3.0. Campaigns and Operations," p2-2.

[34] Department of Defence, "Australian Defence Doctrine Publication 3.0. Campaigns and Operations," p4-4.

[35] Linden, *Operational Level Intelligence: An Alternate Approach*, 33.

[36] Evans, "The Closing of the Australian Military Mind: The ADF and Operational Art," 106.

[37] On average, the 20 officers and other ranks manning the Land Intelligence Wing at the Defence Force School of Intelligence have spent over two years on active deployment.

successful tactical analysts graduate to operational employment at HQJOC or DJFHQ, not as a result of formal training, but by merely the passage of time and the posting cycle.

The contemporary ADF planning staffs have a wonderful pedigree built on tactical successes over the last 100 years of operational service. So too do the contemporary instructors of military intelligence apply the lessons learnt from effective intelligence at the tactical level. Yet it remains important that we don't naively consider operational intelligence a hybrid of strategic and tactical intelligence, '*strategic in scope but tactical in detail*', and expect deployed operational intelligence staffs to answer the information requirements of strategic intelligence, but with the manning, training and systems of a tactical unit. The same intelligence staffs must strive to understand their *Campaigns and Operations* vocabulary—and for that matter their Clausewitz—as well as their operational planning colleagues. Not only to ensure congruence between the analysis of the operating environment and the operational plan, but also to deduce those characteristics defining the confluence of multiple domains and diverse stakeholder actions across time and space; thus amplifying the *fingerspitzengefühl* of the operational commander.

BIBLIOGRAPHY

Australian Army. "Land Warfare Doctrine 1 The Fundamentals of Land Power." Canberra: Commonwealth of Australia, 2014.

Brighton, Terry. *Master of Battle, Monty, Patton and Rommel at War*. UK: Penguin, 2009.

Camp, Dick. Operation Phantom Fury: The Assault and Capture of Fallujah. Minneapolis: Zenith Press, 2009.

Department of Defence. "Australian Defence Doctrine Publication 3.0. Campaigns and Operations." Canberra: Commonwealth of Australia, 2012.

———. "Australian Defence Force Publication 2.0.1. Intelligence Procedures." Canberra: Commonwealth of Australia, 2015.

———. "Australian Defence Force Publication 5.0.1. Joint Military Appreciation Process." Canberra: Commonwealth of Australia, 2015.

———. "Land Warfare Doctrine 2-0. Intelligence." Canberra: Commonwealth of Australia, 2014.

Evans, Michael. "The Closing of the Australian Military Mind: The ADF and Operational Art." Security Challenges 4, no. 2 (2008): 105–31.

Headquarters Department of the Army. *Field Manual 34-130 Intelligence Preparation of the Operating Environment*. Washington D.C., 1994.

Keegan, John. *Intelligence In War: Knowledge of the Enemy from Napoleon to Al-Qaeda*. New York: Alfred A. Knopf, 2003.

Linden, Linda L. *Operational Level Intelligence: An Alternate Approach*. Fort Leavenworth, 1990.

McDermott, Tom. "DEF Australia Letters from HAMEL Part 3: The Operational Level of War. What Is It Good For?" *Grounded Curiosity*, 2016. http://groundedcuriosity.com/def-australia-letters-from-hamel-part-3-the-operational-level-of-war-what-is-it-good-for/.

Richards, David. *Taking Command*. London: Headline Publishing Group, 2014.

Tyler, Brian. "Intelligence and Design. Thinking about Opertional Art." Air University Press, 2014.

Von Clausewitz, Carl. *On War*. Edited by Michael Howard and Peter Paret. New York: Oxford University Press, 2007.

Willmott, H.P. "Isoroku Yamamoto: Alibi of a Navy." In *The Great Admirals: Command at Sea, 1587-1945*, edited by Jack Sweetman, 442–57. Annapolis: Naval Institute Press, 1997.

A CORPS AT THE CROSSROADS: THOUGHTS FROM A BRIGADE S2

Major Mark Gilchrist

Most members of AUSTINT will be able to recite (at least in part) the infantryman's creed,[1] yet I would wager that very few, if any, could agree on a similar all-encompassing description of our role. And herein lies a critical problem for the Corps – our sense of identity is shaped by competing views of what it is that we do, based largely on the disparate and often competing activities that our small corps undertakes.[2] While we have achieved very good results in non-core roles[3] there comes a time when Army must question whether these activities detract from the Corps' ability to deliver its critical function? This is linked to the need for Army to provide clear and unambiguous direction on what is actually required from its limited AUSTINT workforce.

In my view, the role of intelligence must be based around enabling commanders and staff to achieve decision advantage through a detailed understanding of, and recommendations about the adversary and operational environment. By implication, our core function is therefore the delivery of predictive and pre-emptive assessments through the medium of combat intelligence and mastery of the IPB process. Our current foundation doctrine, *LWD 2-0: Intelligence*, seems to reinforce this, as it is almost exclusively focused on the intelligence staff function and its role in enabling commanders' decision-making.

[1] The role of Royal Australian Infantry Corps (RAInf) is to seek out and close with the enemy, to kill or capture him, to seize and hold ground and to repel attack, by day or night, regardless of season, weather or terrain.

[2] AUSTINT is expected to deliver multiple Joint enabling capabilities, but in the absence of clear direction that indicates their relative priority against the core function of providing intelligence staff support.

[3] Taken here to mean Human Source Operations, Psychological Operations and Full Spectrum Exploitation.

My experience tells me that this is also what most of Army expects from us – particularly inside the Combat Brigade where the majority of Army lives, learns and grows. Alas, this is also the area where we appear to be weakest. A fact exacerbated by a lack of clear direction about the relative priority of combat intelligence proficiency. This weakness in combat intelligence, and an associated lack of tactical acumen,[4] undermines our collective credibility as we are often not expert in the skill sets commanders expect from us. This is reinforced by failing to consistently invest and develop the Corps' best and brightest where they will have the most to do with the most of Army – inside the Combat Brigade. This ensures that the perception of what AUSTINT does by many arms corps officers (who become Army's future commanders) is shaped by the absence of a suitably trained and resourced combat intelligence asset.

The Australian Army is a tactically focused Army – this focus on actions at formation and below is both its strength and its weakness. However, understanding this fact must shape the way that each corps contributes to the delivery of Australian Land Power.[5] While 'tactical Army' [6] receives great benefit from our representation in the strategic agencies and at HQJOC, conversely it suffers from the lack of tactical experience and expertise resident within AUSTINT that results from this external representation. Indeed, the biggest criticism often labelled at AUSTINT by commanders and staff is our lack of tactical acumen. This is perhaps not unfair when we acknowledge that more than 50% of the Corps is not employed in tactical organisations conducting combat intelligence. The situation is compounded by the fact that there is no further training dedicated to understanding tactics post-IET/ROBC, and officers have not been pushed to

[4] Taken here to mean the ability to intuitively understand tactical problems involving both state and non-state threat actors, and apply synchronised and orchestrated military effects to make the most of fleeting battlespace opportunities in order to disrupt or dislocate an adversary plan.

[5] As articulated in *LWD-1: The Fundamentals of Land Power*, Chapter 2.

[6] Taken here to mean Forces Command, but particularly the Combat Brigades that constitute the fighting force.

attend COAC to gain a similar tactics education to their arms corps peers.[7] If we are a tactical army, and combat intelligence is, at least in theory, our raison d'être (and what commanders judge us by – not our specialist capabilities) then a collective lack of tactical acumen would appear to be a critical failing. In my estimation, it is this issue which is most significant in the way that AUSTINT is perceived by our manoeuvre brethren.

Most of Army grows up in the Combat Brigades, but more importantly they are where the majority of Army's senior decision-makers had, and continue to have, their formative experience. Therefore, the comparative absence of green lanyards within the Combat Brigade, and the lack of emphasis placed on combat intelligence competence, ensures that AUSTINT can be perceived by those we are meant to support as surplus to requirements. While a lack of central direction for the intelligence capability has contributed to this situation,[8] our Corps must also take responsibility for not seeking to clearly codify and articulate a unifying core role. This has led to an emerging crisis of relevance that many within AUSTINT are unaware of, precisely because they have not served at the formation level or below.

An intelligence professional that hones their skills at the tactical level will more than likely achieve effective results at the operational and strategic levels. Unfortunately, the reverse path tends to be less successful due to the lack of emphasis placed on consolidating critical intelligence processes and procedures. This is reinforced by the predisposition towards broad, rather than focused analysis. The 'fuzziness' usually associated with strategic assessment is impractical at the tactical level. Here, the intelligence requirement is for specific detail to support planning. This in turn, is heavily reliant on tactical acumen. As such, an intelligence professional's intuitive understanding of tactics and how the adversary might seek to employ them is

fundamental to the force's ability to execute more effective operations to close with and destroy the adversary. The development of this tactical acumen forms the basis of the military training and education of our warfighting brethren. For intelligence personnel, however, it is an afterthought at best and a gaping hole in our training at worst. This is exacerbated by the allocation of the intelligence asset, as well as changes to our training and doctrine which have further reduced an already tenuous organisational understanding of how to analyse and apply tactics.

The combat intelligence asset

The *Day Review* made it clear that there needed to be more intelligence touch points across Army – implying inside Forces Command – to enable a better culture of intelligence across the force.[9] This is laudable and very timely based on the issues I have touched on above. Currently only 26% of AUSTINT Captains, 10.5% of AUSTINT Majors and only 25% of AUSTINT soldiers[10] (PTE – WO1) are employed in Land force tactical intelligence billets.[11] This includes only 83 AUSTINT personnel, across all ranks, inside the three Combat Brigades and the Aviation Brigade. By comparison, intelligence specialisations[12] make up approximately 27% of postings for soldiers, not

[7] While this is likely to change as a result of the Day Review, the retrospective up-skilling of current O3 and O4 will be a significant challenge.

[8] *A Review of Army's Intelligence Capability*, Major General Stephen Day, November 2016, p2.

[9] *Day Review*, p5.

[10] Figures provided by AUSTINT Career Advisors at DOCM-A and SCMA.

[11] Taken here to mean formation and battle group HQs both inside FORCOMD and SOCOMD, does not include DFSI.

[12] Taken here to mean Psychological Operations, Human Source Operations, Full Spectrum Expoitation, Signals Intelligence and Cyber (does not include the All Source Capability).

including the instructor liability or staff positions within the Intelligence Battalion. This figure rises to over 40% of the AUSTINT soldier asset when positions in HQJOC, DIO, training establishments and 1 Int Bn staff positions are included. While many of these positions conduct analysis, they cannot be considered as combat intelligence focused.

These figures suggest that the absence of clear Army direction on what was expected from AUSTINT has resulted in an imbalance between the combat intelligence capability and the growth of intelligence specialisations – an imbalance that is likely to increase based on the demand for cyber and signals intelligence support.[13] This is imbalance is problematic when one considers the exponential increase in data that requires analysis as a result of the proliferation of collection capabilities – particularly at the tactical level.[14] This relative under-investment now leaves AUSTINT in a precarious position, where our lack of presence has almost taught tactical Army how to survive without combat intelligence, thus feeding the perception issues that the *Day Review* identified.[15]

The immediate response to the *Day Review* recommendations by Forces Command has been to re-distribute an already fragile combat intelligence workforce (83 personnel) across more units. This dilutes the capacity of the Intelligence staff at both Battle Group and Formation level to process the volume of data they are already struggling to analyse. It also removes any redundancy and depth inside the intelligence function to cope with deployments, courses, welfare etc. Included in the redistribution is the loss of two intelligence Captains at the Brigade Headquarters. This will greatly reduce the enemy's vote in our planning process, thus increasing the chance of blue focused plans that fail to account for a thinking adversary. This action is far from the reinvestment of intelligence capability envisaged by the *Day Review*; instead it is a disingenuous weakening of the very thing that should have been reinforced.

To an extent, AUSTINT was able to mitigate the lack of intelligence staff at formation level and below during the peak operational period circa 2006-2012. During this time, most soldiers and officers deployed overseas and had the opportunity to interact with intelligence personnel in a relatively low-threat environment where a lack of tactical acumen could be concealed. However, after the operational peak circa 2012 we entered what is best termed the 'Hamel era', or a return to foundation war fighting, and a focus on tactical excellence against a peer adversary. While Army sought to reinvest in its tactical acumen and a focus on enabling the Combat Brigade as a unit of action, it did not authorise a commensurate investment in combat intelligence resources to support it. However, as a Corps we have also not done enough to become better at the tactical analysis Army has required from us. As a result, inside tactical Army, Intelligence has struggled to retain the equal footing with Operations that was gained through hard-won operational experience. While exercise design, the lack of all-corps individual and collective training regarding intelligence, and myriad other issues contributed to this situation, the absence of a suitable combat intelligence function cannot be understated. While fault does lie with a lack of centralised direction, AUSTINT cannot absolve itself of the lack of prioritisation of, and advocacy for, the combat intelligence capability.

The lack of investment within the Combat Brigades raises some disquieting questions about the future of

[13] 2016 *Defence White Paper*, Australian Government – Department of Defence, 2016, p86.
[14] *Day Review,* p7.
[15] *Day Review*, p4.

our Corps. Not least of which is how do we actually develop the necessary tactical acumen for our soldiers and officers? Furthermore, how can Army hope to grow a pool of future combat intelligence leaders and experts, when the numbers prove that our Corps does not serve in the environment that teaches these skills? Indeed, our trade model makes it increasingly likely that the majority of officers and soldiers in the Corps may never have the opportunity to serve in a combat intelligence role. How then can we grow the intelligence war fighting experts we need to outthink determined foes in an increasingly unstable world?

If we do not provide opportunity for combat intelligence training to be consolidated in the workplace after it is received (particularly noting the changes to training mentioned below) the ability to become expert in them over a career, and at different rank levels, is critically undermined. This ensures that collective mastery of combat intelligence is unlikely to be achieved – particularly when soldiers are posted between specialisations that largely ignore the foundations of combat intelligence. Furthermore, our soldier development plan under Plan Athena makes no specific mention of how to develop the tactical acumen of our people to make them more credible within the Land force. Instead, it is focused on how to give them a broadening of experience, which implies inter-agency and outside of tactical Army.[16] This emphasis further undermines the development of the skillset Army needs most, and extends the perception that our Corps focus is on intelligence outside of the tactical domain.

Shortening the AUSTINT IET course

The reduction in length of the IET course, combined with a downgrade to the security clearance required for training,[17] has further reduced our overall combat intelligence capability and shifted the individual training liability from the school to the workplace. While I understand the requirement to grow the Private asset quickly to expand our Corps, the impact this has had on the ability to deliver the intelligence effect is marked. If the training was temporarily shortened, using lower levels of classification to achieve an expedited filling of the Corps, this approach would make sense. However, a permanent de-skilling of the backbone of our capability seems a poor choice at time when the requirement for detailed intelligence is only growing. This is particularly so when ab-initios clearly demonstrated the ability to assimilate the full course before it was reduced.[18] Furthermore, the manual of army employment actually offered an opportunity to define what was needed from our Private soldiers in a way that enhanced our baseline capability. Instead the decision was made to reduce the capability of the soldiers we rely upon the most – the analysts.

As a tactical army, we must be credible at discussing and analysing tactics, and this lower level of training has left our Corps exposed. This further undermines existing perceptions of competency, relevance and utility - all of which feed a culture of 'ambivalence' towards intelligence as identified in the *Day Review*.[19] The training deficiency that now exists for our junior analysts is not the fault of these smart, keen and willing young Privates; however, they are the ones who feel the impact when thrown into the fray of a Combat Brigade. This reduction in training length has ensured that graduates, by their own admission, do not understand the role of IPB in enabling intelligence procedures.[20] Those posted to a Combat Brigade are quickly forced to learn and consolidate through immersion. Unfortunately, those who are not will likely be at a comparative disadvantage that will hamper their ability to provide combat intelligence throughout their careers.

We would not consider sending armoured vehicle crew to an ACR without the baseline skills to safely operate and fight their vehicle. Yet this is exactly

[16] *Plan Athena Soldier Development Plan*, AUSTINT Directive 01/17, Australian Intelligence Corps Head of Corps Cell, 23 Jun 17.

[17] This decision to train at the NV1 level is incongruous with the 08 Jun 17 amendment to the AUSTINT employment specifications that indicate that all Analyst Intelligence Operations require a PV clearance to be retained throughout their career..

[18] I base this both on my time running the IET course at DFSI in 2013 and on DFSI figures from 2015 that indicated a lower failure rate for ab-initios than lateral transfers.

[19] *Day Review*, p1.

[20] *See Bridges Review 2017* article 'Deficiencies in DFSI training when implemented in the Combat Brigade environment'.

what we have done to those relied upon to assist these same crew to find and defeat the adversary. Our Private soldiers are not simply map markers, nor data-loggers – they are the analysts upon which the entire intelligence enterprise is built. By failing to equip them with the skills necessary to conduct baseline tactical analysis we distort the delivery of the intelligence effect and diminish the potential of the highly intelligent soldiers we have recruited.

Had the IET course remained at its previous length AUSTINT could have developed a new JNCO/SNCO training continuum that built on the inherent strength of a credible skill set. This would have ensured that the focus could shift to developing the leadership and management of the intelligence asset, rather than catching up the skills no longer taught. This approach would have, and can still be, an important driver for achieving positive cultural change for AUSTINT.

The removal of Monitoring from IPMB

Monitoring the operational environment, understanding change, and predicting how it will affect tactical actions is a fundamental part of what AUSTINT should provide. Explicitly recognising this in our foundation process ensured that IPB became more than a PowerPoint brief and made understanding how it supports operations easier to understand. It made clear that IPB drives all intelligence operations and assessments through the continuous review and revision of battlespace understanding. While monitoring was only in doctrine for a few years, the reversion in nomenclature has been far more than simply cosmetic. It has re-shaped the way that IPB is (mis)understood - and in turn, is taught. This simple change has removed the clear understanding of how IPB supports the execution, not just the planning of operations. Indeed, *LWP-INT 2-1-8: Intelligence Preparation of the Battlespace* now fails to actually discuss how IPB is a cyclical process that uses collection to understand the battlespace in an iterative fashion – this is a major failing in our philosophical approach to supporting operations.

Step 4 – Determine Adversary Courses of Action – remains the most important part of the IPB because it synthesises all previous analysis to create the tools by which an intelligence staff can battle-track (SITEMP, event overlay, ISR plan etc). While monitoring was still explicit in the IPB it reinforced the requirement to use these tools in

the current intelligence area. This ensured a clear link between the predictions made by intelligence plans, to the conduct of collection operations, to the attendant intelligence reporting that enabled better understanding of the battlespace and shared situational awareness. Since the removal of the M from IPMB we have seen a corresponding drop in the battle-tracking ability of intelligence staffs as evidenced by CTC trends reports over the last four years.[21] Poor battle-tracking leads to missed opportunities, resulting in criticisms about a lack of actionable intelligence to drive operations. In short, this apparently small change has undermined the effectiveness of the process designed to mitigate our Corps' lack of intuitive tactical understanding.

Conclusion

As we stand at the crossroads, our Corps must acknowledge that the unhealthy ambivalence towards intelligence identified in the Day Review is partly of our own making. AUSTINT has simultaneously failed to invest in tactical Army, while also failing to push back on the expectation that such a small corps can credibly fill all of the specialisations foisted upon us. The net result is that we are increasingly failing to do our core job as well as expected – that being the ability to enable decision advantage for commanders and staff in an austere field environment against a challenging state-based adversary. Again, it comes back to what our core competency is: if it is combat intelligence, including mastery of the IPB (and the management of collection operations inherent in this), then we do not need to own the methods of collection that support the effect. Therefore, is it time to divest ourselves of those skills that detract from our ability to do a core job well? The success of all-corps HUMINT makes me think yes. Along with this I offer the following recommendations:

Recommendations

- An AUSTINT creed is developed that explicitly recognises combat intelligence as our core role. This should be agreed upon through the medium of the Corps conference and endorsed by Chief of Army through AUSTINT Head of Corps.
- Clear direction should be sought from AHQ on who the capability manager for Psychological Operations, Human Source Operations and Full Spectrum Exploitation is inside Army. Linked to this should be an all-corps coding for operators in each specialisation and appropriate resourcing applied based on the agreed priorities. As a result the AUSTINT asset should be proportionately drawn down and re-invested in combat intelligence positions inside of the Combat Brigades. This would see a return to CMC17 manning inside of formation headquarters and the creation of four person Intelligence bricks inside all direct command units (including CSSB, the Artillery Regiment and CER).
- The IET course returns to a 12-week program with a minimum NV2 C/D security clearance requirement. This should be supported by a review of all AUSINT career courses with a greater focus on management of the intelligence function rather than revision of baseline combat intelligence skills that have been allowed to atrophy.
- AUSTINT introduces a dedicated, Corps wide effort to improve the tactical acumen of its people. This should be supported by the introduction of a dedicated line of effort in the soldier development program; compulsory attendance for officers on COAC; and the creation of a self-paced (chain of command enabled) professional development program including readings and activities to assist in the development of tactical acumen at all ranks.
- Monitoring is reintroduced to the IPB and *LWP 2-1-8: Intelligence Preparation of the Battlespace* undergo a full review to ensure it demonstrates the cyclical nature of the process. This should be undertaken in concert with the review of *LWD 2-1: Intelligence Staff Duties* to ensure the clear link between IPB conduct by the S25 and IPB monitoring and action in S23.

[21] Available from *http://legacy/TeamWeb2010/ARMY/1div/1%20DIV%20DCU/CTC/HQCTC/SitePages/Trends%20Report.aspx*

- Options should be considered to incentivise combat intelligence postings at all ranks. This should be supported by Manager Intelligence Operations positions in Combat Brigades and SOCOMD being treated as equivalent to CSM positions.
- The AUSTINT trade model should be reviewed to provide clear pathways inside of the combat intelligence skillset that lead to senior combat intelligence leadership positions (both officer and soldier).
- Postings to SOCOMD for ab-initio soldiers should only occur after a period of consolidation inside a Combat Brigade. This is likely to entail shorter tenures inside the Combat Brigades and a flexibility in career management not currently exercised.
- A clear responsibility for Intelligence raise, train and sustain issues must be established inside Forces Command to assist Combat Brigade S2s to enhance the delivery of intelligence, surveillance and reconnaissance effects and enable all-corps training about the intelligence capability.

Ultimately, however, all these recommendations rest on Army's clear determination about what is expected from its limited intelligence work force and the successful implementation of the *Day Review* recommendations to assist in changing Army's culture of intelligence. Supporting this, however, is the requirement for AUSTINT to be constantly vigilant about how our own performance and culture can lead to a feeling of antipathy towards intelligence taking root.

FUSION INC: A CONTRACTED ALL SOURCE SOLUTION TO REDUCE UNCERTAINTY

Captain Nicolas Barber

Some components of military force, such as infantry and armour, fall uniquely in the realm of uniformed service. All source analysis is not one of those elements of fighting power.

This paper aims to stimulate discussion regarding the future of all source analysis within the Australian Intelligence Corps (AUSTINT). I will argue that the Australian Army should contract all source analysis in order to enhance decision support for tactical commanders and build efficiency in Army's intelligence architecture. Firstly, I will outline Army's increasing requirement for all source analysis. This capability need is derived from the pressure for greater certainty in military decision-making and increased collection within a world of mass data and information. Secondly, I will consider the structural and personnel shortfalls of Army's existing all source capability. Finally, to remedy this situation, I will recommend the augmentation of Army's intelligence capability with a contracted all source solution.

Army's demand for all source analysis

The utility of all source analysis is founded in the enduring uncertainty of war.[1] Uncertainty is a state of limited or imperfect information. *LWD 1 The*

Image courtesy of BAE Systems.

Fundamentals of Land Power accurately outlines that uncertainty can never be fully eliminated from war.[2] Yet, although war may never be mathematically certain, all aspects of warfare are not absolutely uncertain.[3] The degree of certainty in a given problem-set lies on a spectrum of probability. Arguably, one method of reducing uncertainty in war is through intelligence.[4]

By definition, intelligence is the directed acquisition and analysis of information regarding the environment and threat stakeholders.[5] Critically, great strategists have identified that intelligence is more than simply the collection of information, but instead

[1] Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret, Oxford University Press, Oxford, 2007, pp 88-89; Australian Army, *Land Warfare Doctrine 1 - The Fundamentals of Land Power*, 2014, p 14.

[2] Australian Army, *Land Warfare Doctrine 1 - The Fundamentals of Land Power*, 2014, p 14.

[3] Antoine-Henri Jomini, *The Art of War*, translated by G H Mendell and W P Craighill, J B Lipponcott & Co, Philadelphia, 1862, pp 274-276.

[4] Ismael Rodriguez, 'Uncertain about Uncertainty: Improving the Understanding of Uncertainty in MI doctrine', *Military Intelligence*, Apr-Jun 2011, pp 40-44; Sun Tzu, *The Art of War*, translated by John Minford, Penguin Books, Melbourne, 2009, pp 1-4; Antoine-Henri Jomini, *The Art of War*, translated by G H Mendell and W P Craighill, J B Lipponcott & Co, Philadelphia, 1862, pp 274-276.

[5] Australian Army, *Land Warfare Doctrine 2-0 - Intelligence*, 28 Oct 2014.

involves an evaluation of available information from all sources.[6] This process can be defined as all source analysis.[7] Indeed, collection of information without analysis contributes to the 'fog of war' and only promotes uncertainty.[8]

The growing demand for all source analysis within the Australian Army is underpinned by three key trends. Firstly, Army's commanders are under increasing pressure to reduce risk in war in order to protect Australian soldiers on operations as well as decrease collateral damage to non-combatants.[9] To make better decisions, commanders are turning to their intelligence staff to provide answers to the unknown, particularly following exposure to some excellent examples of tactical intelligence fusion on operations in Central Asia and the Middle East in recent years.[10]

Secondly, recent operations have highlighted the need for Army intelligence to be active in peacetime, building situational awareness of possible land operating environments to avoid 'cold-starts' when conflict erupts.[11] Intelligence will not adequately reduce uncertainty if collection and analysis only commences when soldiers embark for foreign soil. Consequently, Army Headquarters has espoused an 'always on' mentality and an enterprise approach to intelligence to provide timely and accurate support to Army's decision makers.[12]

Finally, sustained operations since 1999 have brought a wide range of new sensors into the ADF that are all collecting data on the threat and the environment.[13] Combined with exponential advances in technology and a more interconnected information environment, senior AUSTINT officials recently proclaimed, 'the Australian Army is now capable of gathering more information, faster, than at any other time in its history.'[14] Yet, as was discussed above, enhanced collection without a commensurate increase in analytical capability arguably contributes to the 'fog of war'. With these trends in mind, Army has recently embarked on a journey to answer the demand for all source analysis.

Challenges to AUSTINT all source analysis

Although 'all source' is a principle of all intelligence,[15] not all intelligence cells can conduct all source analysis. The ability to truly analyse information from all sources and provide fused intelligence requires access to time and resources that is often beyond the scope of overworked unit and formation combat intelligence cells. Consequently, Army assembled analysts into standing dedicated All Source Cells within the 3rd Company (3 Coy), 1st Intelligence

---

[6] For example, Jomini espoused that 'by multiplying the means of obtaining information; for, no matter how imperfect or contradictory they may be, the truth may often be sifted from them'. See Antoine-Henri Jomini, *The Art of War*, translated by G H Mendell and W P Craighill, J B Lipponcott & Co, Philadelphia, 1862, p 274. By contrast, Clausewitz was sceptical of intelligence, contending that 'most intelligence is false, and the effect of fear is to multiply lies and inaccuracies.' See Cf Carl von Clausewitz, On War, edited and translated by Michael Howard and Peter Paret, Oxford University Press, Oxford, 2007, p 64.

[7] Bowman Miller, 'Improving All-Source Intelligence Analysis: Elevate Knowledge in the Equation', *International Journal of Intelligence and CounterIntelligence*, Vol 21, 2008, pp 337-354.

[8] Scott Gills et al., 'Improvements and Challenges for Army's ISR Enterprise', *On Ops*, University of New South Wales Press, Sydney, 2016, p 124; Nicholas Barber, 'A Warning from the Crimea: hybrid warfare and the challenge for the ADF', *Australian Defence Force Journal*, Iss 198, Nov-Dec 2015, pp 11-22.

[9] David Barno and Nora Bensahel, 'Six Ways to Fix Army's Culture', *War on the Rocks*, 06 Sep 2016; Arthur Rizer, 'Lawyering Wars: Failing Leadership, Risk Aversion, and Lawyer Creep – Should we expect more lone survivors?, *Indiana Law Journal*, Vol 90, Iss 3, Summer 2015, pp 935-974; James Brown, 'Fifty Shades of Grey: Officer Culture in the Australian Army', *Australian Army Journal*, Vol 10, Iss 3, 2013, pp 244-254.

[10] Scott Gills et al., 'Improvements and Challenges for Army's ISR Enterprise', *On Ops*, University of New South Wales Press, Sydney, 2016, p 128.

[11] Nicholas Barber, 'Harnessing Army's intelligence capacity for contingency', *Land Power Forum*, 01 Oct 2015

[12] Scott Gills et al., 'Improvements and Challenges for Army's ISR Enterprise', *On Ops*, University of New South Wales Press, Sydney, 2016, p 130.

[13] Mark Mandeles, *The Future of War: Organisations as Weapons*, Potomac Books, Washington DC, 2005, p 122; Isaac Porche III et al, *Data flood: helping the Navy address the rising tide of sensor information*; National Defense Research Institute, Santa Monica, 2014.

[14] Scott Gills et al., 'Improvements and Challenges for Army's ISR Enterprise', *On Ops*, University of New South Wales Press, Sydney, 2016, p 126.

[15] Australian *Army, Land Warfare Doctrine 2-0 - Intelligence*, 28 Oct 2014.

Battalion, postured to reinforce other analytical teams and provide greater certainty to commanders.[16]

Yet, 3 Coy is not rightly situated within Army's intelligence architecture to reduce uncertainty where it is most pervasive. Although the requirement to minimise risk is most apparent to commanders in theatres of war or preparing for contingency operations, Army's all source analysis capability is held under Forces Command, an organisation that is charged with the mission to 'raise, train and sustain' the Army.

It is acknowledged that Army's all source support to Forces Command has benefits. Most importantly, it allows intelligence analysts to train with Army's unit and formation commanders, and develop relationships and processes to enhance decision-support on future deployments.[17] But this outcome does not meet Army's immediate need for all source analysis to reduce uncertainty as outlined in the previous section.

However, the solution is not to simply transfer 3 Coy to an operational command. Combat units and formations in Forces Command are the foundation of Army's warfighting capability and routine interaction provides the basis for instituting a culture of intelligence-led operations across Army.[18] Even if 3 Coy was assigned to an operational command, continuity of analysis would remain disrupted by other Army personnel considerations, including individual and collective readiness, exercises, deployments, career courses and posting cycles. A lack of continuity makes an 'always on' mentality difficult to achieve.[19]

It is also unfeasible to simply dedicate additional AUSTINT personnel to all source analysis in support of training as well as reducing uncertainty for operations and contingency planning. Even despite an increase in AUSTINT recruiting to rectify 'hollowness',[20] AUSTINT numbers remain inadequate for Army's needs. Armour and aviation units are without organic intelligence staff, and the prevalence of dedicated Combat Team S2s is diminishing.[21] Retention of qualified and experienced staff within AUSTINT is also proving challenging. In short, AUSTINT has no extra capacity within its ranks to dedicate more people to all source analysis.

The result is that 3 Coy is torn between national intelligence efforts in support of operations on one hand and training within Forces Command on the other. Interestingly, despite force generating dedicated All Source Cells, Army has not deployed a formed All Source Cell from 3 Coy; instead, preferring to design bespoke intelligence cells for each new operating environment. Force assignment across chains of command remains difficult and constant changes of intelligence focus prevent all source analysts from deeply understanding the complexity of a problem set. Ultimately, neither operations nor training probably receive the support 3 Coy is capable of providing, and the pressures to reduce uncertainty within Army remain.

In re-examining methods of answering Army's demand for all source analysis, there is an opportunity for AUSTINT to consider augmenting uniformed personnel with a contracted all source solution.

---

[16] According to Australian Army, *Land Warfare Doctrine 2-0 - Intelligence*, 2014: The All Source Cell is designed to focus collection and production in support of decision makers, and the size and scope of the All Source Cell is determined by the task. Details regarding 3 Company can be found at Australian Army, *Australian Army – Aide Memoire*, Apr 2014, pp 11-12; Ned Robinson, 'Intelligent Preparation', *Australian Army Newspaper*, 09 Apr 2015, p 11; Royal Australian Survey Corps Association, Bulletin, Christmas Ed, No 61, Dec 2015, p 5.

[17] Other identifiable reasons include valuable opportunities to improve skills and processes amongst all source analysts, and the ability of all source analytical teams to provide decision support to a wide array of Forces Command customers who may not have dedicated intelligence staff.

[18] Brad Wellsandt, 'The State of the Intelligence Warfighting Function in the US Army Brigade Combat Team', *The Tactical Leader*, (Website) available at: https://www.thetacticalleader.com/blog/the-state-of-the-intelligence-warfighting-function-in-the-us-army-bct, 06 Jun 2017, Adam Sparkes, 'The Ready Acorn', *The Bridges Review*, 2015, pp 78-81.

[19] Scott Gills et al., 'Improvements and Challenges for Army's ISR Enterprise', On Ops, University of New South Wales Press, Sydney, 2016, p 130.

[20] Arran Hassell, 'Our Corps', *The Bridges Review*, 2015, pp 46-48.

[21] Russell Gadenne, 'Optimising Intelligence Support to Combat Commanders', *The Bridges Review*, 2013, p 68; some discussion of Combat Team S2 positions can be found in James Morrison, 'Fixing the AUSTINT Training Continuum', *The Bridges Review*, 2015, pp 39-40.

Contracting an all source solution

A contracted all source solution would suit Army's requirement to reduce uncertainty.[22] In this context, I consider a contracted solution more than simply individual civilians employed within a military intelligence cell. Rather, I define a contracted solution as contractor all source teams/agencies within a competitive free market seeking to answer specific intelligence requirements determined by Army leadership and managed by J2 Headquarters 1st Division.[23] A contracted solution would most likely be employed in reachback,[24] allowing AUSTINT to prioritise uniformed personnel to combat units and formations for support to training and deployments.[25] Such a construct will offer Army some unique benefits.

Firstly and most importantly, a contracted all source solution forces intelligence to be command-driven.[26] By doctrine, commanders use Priority Intelligence Requirements (PIR) to direct the intelligence effort.[27] Although PIRs focus intelligence assets, the relative worth of PIRs for command decision-making is often unknown. Commanders are more likely to consider the significance of PIRs if they can purchase intelligence support on contractual terms because the financial commitment forces one to quantify the value of reduced uncertainty. Contracting compels a commander to question: firstly, 'What do I need to know?' and secondly, 'How important is answering this requirement?'

Secondly, a contracted intelligence solution promotes greater flexibility in answering intelligence requirements.[28] *LWD 2-0 Intelligence* outlines that an All Source Cell should be determined by the size and scope of the task,[29] but 3 Coy is not task organised. Instead, 3 Coy is a set of analytical capability bricks whose personnel, resources and information flow are defined by Army's cultural and technical constraints and restrictions.[30] A contracted solution removes the requirement for standing All Source Cells from Army and instead allows a senior intelligence officer, such as J2 Headquarters 1st Division, to design and manage the contract based on analytical output.[31] The 'how' of intelligence production, including structure, number of analysts and training/resources, becomes a risk for the market, not Army.

Thirdly, a contracted intelligence solution provides Army with greater intelligence continuity. Without the requirement to attend exercises, courses or postings, a contractor can develop a greater depth of understanding on a topic or theme and finally allow Army to achieve a persistent stare to intelligence areas of interest. Stability for contractors and their families is arguably superior, particularly if employed in a desirable reachback intelligence construct.

Finally, a contracted intelligence solution can produce more accurate intelligence outcomes for Army commanders. In a competitive free market, commanders have the option to choose intelligence support from competing companies – whose cost

---

[22] Harry Dies, 'Guide to the proper use of civilian intelligence contractors in the War on Terrorism', *Military Intelligence Professional Bulletin*, Vol 33, Iss 3, Jul-Sep 2007; Glenn Voelz, 'Commercial Augmentation for Intelligence Operations', *Defense Acquisition Review Journal*, 2015, pp 418-433.

[23] Headquarters 1st Division prepares Army Force Elements to meet specific operational and contingency requirements as well as forms the ADF's Deployable Joint Force Headquarters. See Australian Army, *Aide-Memoire*, Apr 2014.

[24] Phillip Radzikowski, ''Reach-back' – A New Approach to Asymmetrical Warfare Intelligence', *Army*, Dec 2008, pp 24-26.

[25] Support to Battlegroup and Brigade intelligence cells has previously been argued as a priority for both exercises and deployments. See Russell Gadenne, 'Optimising Intelligence Support to Combat Commanders', *The Bridges Review*, 2013, pp 67-69.

[26] Mark Gilchrist, 'Why intelligence surveillance and reconnaissance fails', *Land Power Forum*, 08 Jul 2014

[27] Australian Army, *Land Warfare Doctrine 2-0 - Intelligence*, 28 Oct 2014, p 28.

[28] Morten Hansen, 'Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community', *Intelligence and National Security*, Vol 29, No 1, 2012, pp 76-77.

[29] Australian Army, *Land Warfare Doctrine 2-0 - Intelligence*, 28 Oct 2014, p 90.

[30] For example, Army's hierarchical organisational structure or specialisations/disciplines can prevent information from reaching the decision maker in a timely manner. See Scott Gills et al., 'Improvements and Challenges for Army's ISR Enterprise', *On Ops*, University of New South Wales Press, Sydney, 2016, p 129.

[31] See for example the benefits of unclassified commercial imagery discussed in David Cave, 'Intelligence for sale: Commercial Space Sensors and their use', *Land Power Forum*, 19 Apr 2015

and performance provide the basis for their ability to secure the contract. Driven by performance-based criteria, intelligence analysis is driven to efficiency. Moreover, the breadth of available intellectual talent is enhanced due to the absence of strict military entry and readiness requirements. Collectively, these conditions promote greater personnel diversity,[32] and increased scope for selective employment and management of gifted analysts to support Army's requirements.

Defending a contracted solution

Opponents to a contracted intelligence solution likely base their case on several features. Firstly, some suggest there are fundamental ethical, and possibly legal, questions regarding the employment of contractors in providing intelligence support to military operations.[33] While the legal challenges are beyond the scope of this paper, the ethical concerns are probably not insurmountable. Although not identical, there are certainly similar ethical considerations between purchasing intelligence and purchasing weapons from private companies if such actions can be considered for the public good.

Secondly, critics highlight the danger that contractors are self-interested;[34] arguing that contractors simply produce intelligence analysis that is favoured by the contracting officer. While contractors certainly have financial motivations, US studies suggest there is no evidential basis to suggest that contractors are any less devoted to national security than military members.[35] Regardless, even if it is conceded that contractors are self-interested, contracted intelligence is likely to be assessed on its accuracy in a results-based approach. Drawing on the concepts espoused by economist and philosopher Adam Smith, self-interest can ultimately benefit the public good in a competitive environment.[36]

Thirdly, opponents contend that contracted intelligence lacks the tactical grounding provided by uniformed personnel and is too difficult to quality control. However, this argument fails for several reasons. First, it does not recognise that many contracted intelligence analysts are likely to be former military members. Second, there is no quantitative basis to an assertion that non-military members cannot learn tactics. The Ab Initio program underlines the fact that effective military intelligence analysts can be generated without military experience.[37] But most importantly, the only measure of quality control in intelligence is the ability to reduce uncertainty. For contracted solutions, the market provides the best means for quality control – those that provide effective intelligence will survive, those that fail to meet decision-making requirements will not.

Finally, critics will argue that contracting will not be cost-effective. Further, they attest that a contract would not be flexible enough to respond to an evolving mission or problem set in a timely manner. The financial argument is superficially attractive – but fails to recognise that the ability to purchase expert knowledge and experience probably outweighs the re-focussing of multiple standard military analysts who take time to build subject matter knowledge on a given topic from a cost-benefit evaluation.[38] It is agreed that contracts will be inflexible and wasteful

[32] Department of Defence, *Defence Diversity and Inclusion Strategy 2012-2017*, Jun 2014.

[33] Glenn Voelz, 'Contractors and Intelligence: The Private Sector in the Intelligence Community', *International Journal of Intelligence and Counterintelligence*, Vol 22, Iss 4, 2009, pp 606-607; Siobhan Martin, 'Spying in a Transparent World: Ethics and Intelligence in the 21st Century', *Geneva Papers*, 19/16 Research Series, 2016.

[34] Tim Shorrock, *Spies for Hire*, Simon and Schuster, New York, 2008.

[35] Morten Hansen, 'Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community', *Intelligence and National Security*, Vol 29, No 1, 2012, pp 65-75.

[36] Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, Strahan and Cadell, London, 1776.

[37] The Ab Initio program is a direct entry AUSTINT recruiting scheme. See Jesse Pitstick, 'Direct Recruiting: Experience of an Ab Initio', *The Bridges Review*, 2013, p 36; Arran Hassell, 'Our Corps', *The Bridges Review*, 2015, pp 46-48.

[38] Morten Hansen, 'Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community', *Intelligence and National Security*, Vol 29, No 1, 2012, pp 75-76.

unless there is careful wording of the contract award and appropriate contract management.[39] Yet, this is not an argument against contracting; but rather, a timely reminder for those that draft the contract.

Conclusion

The Army is faced with a conundrum. On one hand, Army commanders are demanding greater certainty from intelligence to decrease risk in war. On the other hand, the battlespace remains complex and increasing levels of information requiring analysis are only further complicating efforts to reduce uncertainty. Army's response to this analytical need, largely centred on 3 Coy, is challenged by structural and personnel issues. A contracted solution presents some unique benefits. More flexibility, better intelligence outcomes and improved continuity are foreseeable results of this approach. War will still be dangerous, fraught with friction and subject to chance – but the collective effect of these attributes will aid in the reduction of uncertainty and support Army in achieving decisive results against its future adversaries.

[32] Glenn Voelz, 'Commercial Augmentation for Intelligence Operations', *Defense Acquisition Review Journal*, pp 418-433.

THE ELEPHANT IN THE ROOM: CRISIS OF SNCO LEADERSHIP IN AUSTINT

Warrant Officer 2 Nathan Herbert

The Australian Intelligence Corps (AUSTINT) is sick; and it has been for some time. It is kept alive by smart, dedicated, and driven soldiers and officers, who are determined to achieve the mission. Some in the Corps are blissfully unaware, but most know the dirty truth - the middle management leadership in the Corps is broken.

Leadership in any organisation is important, but particularly relevant when organisations are growing, or in a fragile state. With the introduction of the *Ab Initio* Scheme and Plan ATHENA, AUSTINT is vulnerable. The Corps is rapidly growing to remedy the challenges of 'hollowness', and young soldiers and officers are plentiful. To reach the objectives of Plan ATHENA, the Corps needs sound leadership to guide it through this period of change. We need quality, not quotas. The role of leading and mentoring junior soldiers is the responsibility of the Senior Non-Commissioned Officer (SNCO), and Warrant Officers Class 2 (WO2); unfortunately most AUSTINT SNCOs and WO2s are not ready to undertake this challenge. For reasons of brevity, I have coupled SGTS and WO2s as SNCOs. I apologise to any WO2s in advance if this offends. I must also state that this paper does not pertain to all SNCOs or WO2s. Some WO2s and SNCOs are fine examples of what leadership should be, but some are not.

This paper will discuss the elephant in the room – the widespread poor leadership of the SNCOs in AUSTINT. Some words I use are harsh, but this issue can only be understood and remedied through self-reflection. Firstly, I will define leadership within small teams. Secondly, I will outline the leadership shortfalls of AUSTINT SNCOs, including: one dimensional leadership, failing to inspire, and lack of experience. Finally, I will discuss the way forward, and look to some existing strategies that are already being implemented at the Defence Force School of Intelligence (DFSI) as a possible pathway.

Defining Leadership in AUSTINT

What is leadership, and what makes a good leader? At its simplest, Iszatt-White and Saunders wrote that, 'leadership is to have followers'. [i] However, such a definition is unworkable in a military context, where soldiers are legally obligated to follow. A more suitable model defines leadership through the attributes required to inspire followers to achieve the leader's intent. Carol Dalglish and Peter Millers discussed several traits of a good leader:

- Creating a vision, setting goals and providing direction
- Be a good communicator
- Aligning people [ii]
- Affirming, and reaffirming values
- Serving as a symbol
- Trust, and self-management [iii]
- Being an expert, or experience

[i] Iszatt-White, S. (2014). Leadership. New York: Oxford Press. P 19.

[ii] J.P. Kotter A force for change, New York: The Free Press, 1990

[iii] Dalglish, Miller. (2010). Leadership: understanding its global impact. Prahran:: Tilde University Press

These qualities are not revolutionary and are certainly applicable to leadership in AUSTINT. For example, when I was the CSM of 2 Coy 1 Int Bn in 2015, I conducted a leadership survey that canvassed over 50 soldiers, JNCOs and SNCOs within 1 Int Bn and 7 Bde. One of the questions asked respondents to circle words that best described leadership. Words like trust, mentorship, competence, and inspiration were at the fore. Consequently, the attributes expected of AUSTINT leaders are consistent with those identified in leadership theory. Unfortunately, many AUSTINT SNCOs and WO2s do not demonstrate these characteristics, and are instead troubled by several leadership shortcomings.

Our Shortfalls

One dimensional leadership

Sadly, some AUSTINT SNCOs have little to no experience in leading teams, and this influences their leadership style. Their lack of confidence leads to what I coin 'one dimensional leadership', where they apply a single leadership methodology across their team. They tend to favour arbitrary leadership tactics, such as autocratic [iv] or benevolent styles,[v] when they are not appropriate for the situation. This approach degrades the team dynamic, and undermines their credibility. During my time at 1 Int Bn, I witnessed newly promoted SGTs make leadership mistakes that infantry LCPLs would make. By then, I would argue, it is too late. Poor leadership has contributed to a selfish and individualistic mindset within our Corps, where soldiers regularly undercut and undermine each other. I found this quite confronting after 13 years in the infantry, where *esprit de corps* in the team, and the unit was paramount.

My experience in both infantry and intelligence has informed my opinion that it is best not to rely on just one form of power, or leadership style, because this makes your leadership ineffective in certain situations. Appreciation of the environment is especially relevant with the introduction of the *Ab Initio* Scheme and Plan ATHENA. Prior to these changes, the Corps could generally focus on supporting and delegating tasks to soldiers, due to their maturity. We could be more relaxed. Now, leadership in AUSTINT is more challenging because of a diversity of experience, background, age, gender and culture. A one dimensional leadership style is simply insufficient.

Inspiration

Carol Dalglish and Peter Millers, as well as the AUSTINT soldiers who completed the leadership survey, identified *inspiration* as a key attribute of good leadership. Most AUSTINT SNCOs are not inspirational, and I think it all starts with our health and fitness.

Although much intelligence work is conducted in an office environment, physical fitness cannot be neglected – in fact being 'physically tough' is one of Army's core behaviours, and part of our contract with Australia. Physical training (PT) is the first thing that we do in the morning, and our first chance as leaders to inspire our soldiers. Past and present Commanding Officers of the Defence Force School of Intelligence (DFSI) regularly participate and compete in physical activities, including cross country and military skills competitions. Their participation inspires their soldiers to also volunteer, because if the CO has time, we have time. This attribute is not limited to officers, or men. A female WO2 at DFSI was determined to be MEC J42 for a period of 12 months due to an injury. However, through grit and determination, she recovered, was upgraded to J2 and recently passed the PESA. Unfortunately, although her attributes are inspirational, they are not celebrated.

Sadly, most AUSTINT SNCOs passively partake in PT, and some are 'too busy' to join at all. It is not good enough to simply attend; SNCOs must demonstrate drive, compete with the soldiers, and lead. However, I believe that most SNCOs do not

[iv] Autocratic was described by Rensis Likert as a dictatorial approach from autocratic leaders. Delegation and involvement in decision making is minimal. People are motivated by punishment or fear of punishment. Team members do not feel free to discuss things about the job with their leader. Rensis Likert The human organisation, New York, 1967, p. 4

[v] Benevolent authorative; delegation and involvement is still minimal. But people are motivated by rewards. Demonstrates confidence and trust but as a master to servant. Team members not comfortable discussing things about the job with their leader. Rensis Likert The human organisation, New York, 1967, p. 4

strive during PT because they are overweight, and unhealthy. To me, and the majority of the soldiers, they have given up. As leaders, this promotes a bad image, and sets a poor example for those we are seeking to inspire.

The US military has identified similar issues, and sought to remedy this very cultural deficiency by having biannual height and weight tests. Tests need to be presented to promotion boards, and members who are deemed overweight, do not get promoted.

Experience

Experience underpins a SNCO's ability to lead. Yet, many AUSTINT SNCOs lack sufficient experience to be effective leaders, and this situation is only becoming more desperate with the emphasis on rapid promotion to fill Corps 'hollowness'. When soldiers become CPLs, they need the opportunity to lead. My observations from my time at 1 Int Bn were that Captains would dominate the management of intelligence teams, removing responsibility from CPLs and SGTs. CPLs were not given the chance to make mistakes, and develop their leadership style. A lack of leadership experience in the workplace was evident during the last Subject Four for SGT Course at DFSI, where 42% of the students were assessed as needing more time in rank, or even another posting cycle, before being considered suitable for promotion. [vi]

Good SNCOs also need a diversity of experience. Streamlining in specialist intelligence can foster and retain expertise in niche capabilities, such as psychological operations, human and signals intelligence. However, a diversity of experience is necessary to be able to provide expert guidance to commanders and soldiers. Spending the majority of your career in one capability should seriously challenge your suitability for leadership roles, such as CSM and RSM. I have often seen individuals found wanting when they were required to provide leadership or technical advice because of a lack of diverse experience.

Having a diverse experience of basic soldiering can also help with confidence and inspiration. SNCOs must be seen to be comfortable conducting foundation warfighting, which includes the ability to deploy to the field environment. This does not mean that they need to be as proficient as an infantry recon soldier. But AUSTINT SNCOs must be able to provide expert advice on basic soldier skills, including: how to best wear webbing and carry a pack, how to shoot, and how to put up a hootchie. With the introduction of the *Ab Initio* Scheme, our soldiers may not receive this advice from anyone else, and these skills are essential for credibility when deploying with combat units and formations.

Furthermore, AUSTINT needs to continue to diversify our demographics. Young female soldiers in our Corps have regularly lamented that they have no mentors to look up to. The Corps therefore loses really talented, vibrant and energetic female soldiers, who bring different skillsets and leadership styles to our capability. We, as a Corps, must continue to embrace the wave of diversity, and support our female soldiers.

The way forward

The burden for improving AUSTINT SNCO leadership rests both on the individual and the Corps.

Individuals must be self-aware of their leadership shortfalls. Adopting a one dimensional leadership approach, because of a lack of confidence or experience, only undermines your credibility. Particularly with the diversity in AUSTINT, I would recommend that SNCOs consider a situational leadership model. Paul Hersey, Ken Blanchard and Dewey Johnson defined situational leadership as, "leadership behaviour [that] could change not just for each situation, but for each subordinate ". [vii] They further argued that leaders should adapt their leadership style to different stages, which included the following. [viii]

[vi] POST ACTIVITY REPORT – SUPERVISOR INTELLIGENCE OPERATIONS SUBJECT 4 FOR SERGEANT AUSTINT OPS SESSION 0011 27 FEB – 07 APR 17

[vii] Paul Hersey, Kenneth H. Blanchard & Dewey E. Johnson Management of Organizational Behavior: Leading Human Resources, Pearson Education, 2008

[viii] Iszatt-White, S. (2014). Leadership. New York: Oxford Press.

- **Instructing**. When new to an organisation, an employee's level of commitment is unusually high, but their level of expertise is low. They need to be given clear directions and instructions.
- **Coaching**. As the employee's level of expertise rises, the initial euphoria of starting a new appointment evaporates. Employees can be asked questions, and they can look for the answers themselves.
- **Supporting**. After their level of expertise has risen further, there are two very different things that could happen to an employee's motivation. It could decrease because the job is boring, or the prevailing management style is too controlling; or it could increase, often because they have been given more independence. In either case, amongst other things, scholars recommend encouraging the employee to come up with their own ideas.
- **Delegating**. With good leadership and time, the employee is fully empowered in control of their work. The employee's level of motivation will generally be high, and they can be given their own projects and lead their own teams.

In AUSTINT, the ability to tailor one's leadership style does not mean favouring one soldier over another. It means that your approach to an ex-infantry male soldier may be completely different to the young female soldier who has entered AUSTINT through the *Ab Initio* Scheme. A situational leadership model is healthy, and will likely improve team outputs based on the requirements of individual team members, and the leadership context.

Individuals should also seize opportunities to inspire their soldiers. They should demonstrate drive in all activities within the Corps, and not fall into a habit of avoiding or passive attendance at PT. Some will argue that the emphasis on physical fitness is overstated. However, performance at PT is important, and reflects one's holistic approach to leadership. It provides a SNCO with the credibility to adopt a situational leadership style, and inspire their team to achieve an end state.

For the Corps, we cannot underestimate investment in SNCO leadership. We must build a culture of good leadership and teamwork, and this starts with training. Positively, DFSI is already seeking to improve the leadership training it provides to future AUSTINT SNCOs. The first week of the Subject Four for SGT course now entails an AUSTINT leadership week. During this week, we discuss Corps issues and strategies to improve or fix problems identified. We also consider leadership issues faced in small teams in high stress environments, and throughout the course, learners are now assessed as leaders, by their outputs, and control of their syndicate. More broadly, DFSI is seeking to promote a culture of teamwork amongst all learners. For example, the syndicates during courses are treated as teams during exercises. I emphasise to my teams that if one learner is deemed not yet ready or competent, all members of the team should feel as though they have let the team down. This is not unlike the training conducted at the School of Infantry, where the emphasis is on mateship and teamwork. Already, I see the familiar signs of teamwork and bonding, when the syndicates are observed huddled together, like I observed of sections and platoons in infantry. Over time, this will improve our soldiers understanding of team dynamics, and value of adopting a situational leadership model when they become our future leaders.

We are also promoting diversity in the corps by introducing female mentoring. During the last SGTs course, staff facilitated discussion on the aim of mentoring, the need for mentoring in a female context, and advice on perceived issues experienced by serving females, such as the detriment to career progression as a result of starting a family. The discussion forum has been well received by the female learners. [ix]

[ix] POST ACTIVITY REPORT – SUPERVISOR INTELLIGENCE OPERATIONS SUBJECT 4 FOR SERGEANT AUSTINT OPS SESSION 0011 27 FEB – 07 APR 17

But what is to be done with WO2s who have been in rank for an extended time? Some of these WO2s have provided exemplar service to the Corps, and have superior knowledge. However, they are tired, and some are financially conscripted, waiting out retirement. Policy makers should consider the following two options;

- Voluntary redundancy not dissimilar to that given to WO1s
- Opening postings to exploit their extensive experience and knowledge, with little scope for leading troops.

As an organisation, we must also provide our soldiers with the opportunity to gain leadership experience prior to receiving more responsibility. Officers must empower JNCO and SNCOs to develop by delegation and accountability, and career management should ensure that soldiers have had a diverse range of appointments prior to undertaking greater responsibility.

Finally, assessors need to honestly report on the suitability of their soldiers for leadership appointments. Assessors should look at outputs and results, not hours worked, as a measure of performance. Hard conversations must be had and may include phrases such as 'you are overweight', 'you do not inspire, mentor or motivate the soldiers', 'you are a grumpy, rank bully', and 'you need more experience in this area, and therefore need to diversify'. Only through accurate and honest reporting will AUSTINT promote the right people into positions of responsibility.

Conclusion

I make no apologies for the direct way I have portrayed my opinions and theories. We should not shy away from the elephant in the room - we need to address it. I think we are in a delicate place, and time is of the essence. We need to provide soldiers and NCOs with the opportunities to build experience in a wide range of skills. We need to celebrate those leaders who inspire soldiers and motivate teams. We need to expand our diversity to bring in different views, skillsets and leadership styles. And finally, we need to continue to foster a team culture, and rid ourselves of the toxicity that we have all witnessed. I believe we need to fix the shortfalls soon, before the next generation of SNCOs believe the current state of SNCO leadership is normal. I fear if we do nothing, we'll need another war, and ten years of deployments to realign.

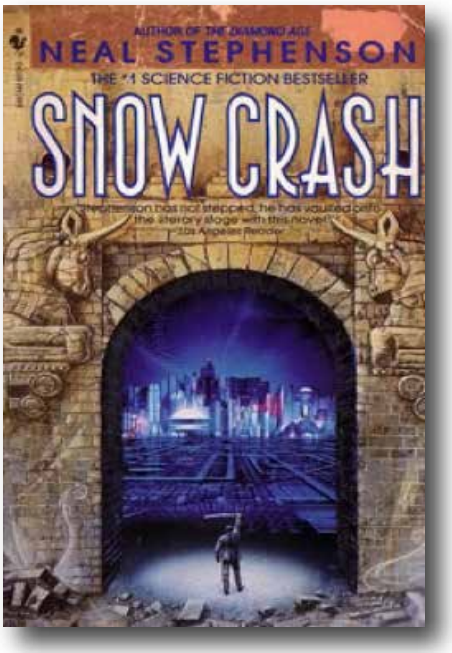
AN ANTIDOTE TO SYMMETRY: THE VALUE OF READING SCIENCE FICTION

Lieutenant Colonel Ping Han Chua

The 9/11 Commission famously concluded that the intelligence agencies had suffered a failure of imagination, in failing to accurately assess the threat Al Qaeda posed, and the means of attack. However, to devoted readers of Tom Clancy's Jack Ryan novel series, the concept of using airliners as high-payload, precision-guided munitions should not have been surprising (no further spoilers).

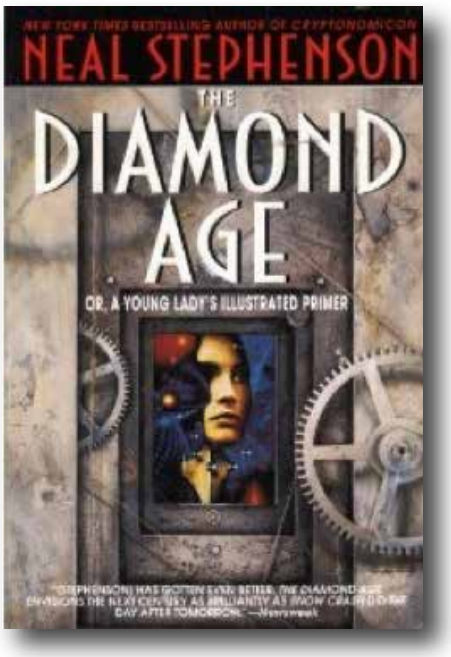
Indeed, if we are to treat warfare as a race towards asymmetry, how then do we resist the urge to conceive of our adversaries as like-minded, symmetric counterparts to our military? Fighting symmetric foes is ingrained into our training systems and indelibly etched into our mindsets - why else would we choose to simulate our operations against 'near-peer' enemies? As intelligence professionals, it should be our task to imagine ways in which new and emerging technologies could be employed by hostile actors, or how existing technology could be used in novel ways. For example, the US Marine Corps has gone so far as to publish a 'Science Fiction Futures' paper in collaboration with notable authors.

Reading good science fiction (including the sub-genre of 'technical fiction', pioneered by authors such as Tom Clancy) can thus be a good antidote to our tendency towards symmetry. This need not be exclusive to military science fiction, which can be too narrow, but the broader corpus of science fiction which imagines entire environments. For example, I generally enjoy reading dystopian fiction that is strongly grounded in the world we inhabit (sorry, no wizards and dragons here folks). A good author will take current trends and extrapolate them in ways that our institutionalised, military minds would struggle to grasp. Thus, when I read good quality science fiction I inhabit that created world in which I can project My list of favourite science fiction books should illustrate this:



Snow Crash

Neal Stephenson is revered in science fiction circles as one of the pioneers of the so-called 'cyberpunk' sub-genre. In his best-regarded book, Stephenson creates a hyper-globalist world in which free-market capitalism has overtaken the nation state - the affluent congregate in corporatised sovereign 'burbclaves' (suburban enclaves) guarded by private militaries. A virtual reality world consumes the lives of many (the 'Metaverse'), and a mysterious virus causes users to go brain-dead in real life. The plot then weaves in ancient Sumerian religious myths, the mafia underworld and dark, subversive humour. Snowcrash is a deeply funny introduction to a world replete with the disruptive technology of augmented and virtual reality, and non-state armed actors.

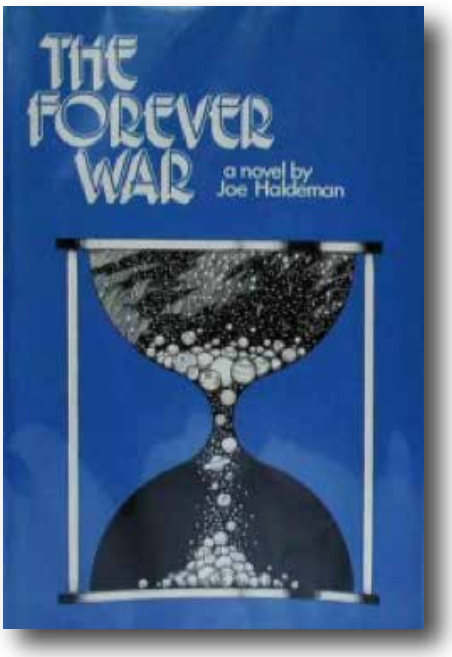


The Diamond Age

Following 'Snowcrash', Stephenson constructs another new world in which neo-Victorian values are blended with hyper-powerful companies that hold the monopoly on 'matter generators'. This is a world in which nanotechnology pervades everyday life, completely changing the concept of personal and public domain. Physical security, privacy, espionage are all upturned when nearly-undetectable substances can change physical states, store and transfer information, or be used as weapons. Nanotechnology has the potential to make humans take the next great leap, but none of us can predict its impacts, let alone its myriad military applications. Therefore, I found 'The Diamond Age's exploration of nanotechnology helps us envision this Brave New World.

The Wind-Up Girl

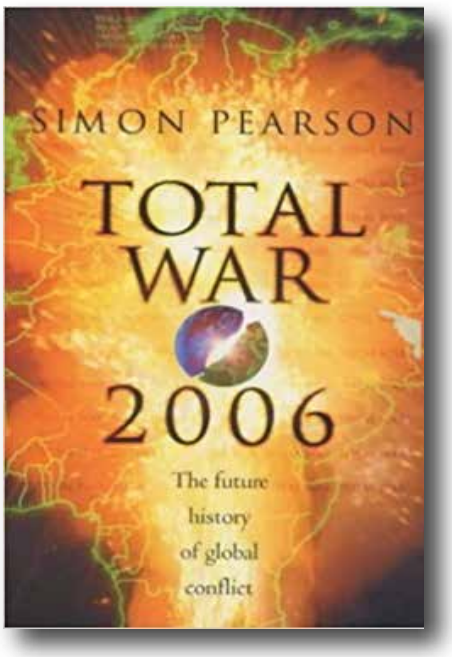
Closer to current-day events, the Wind-Up Girl is set in a world beset by climate change and near-exhausted fossil fuel supplies. The so-called 'Great Contraction' has led to less international travel, a smaller world population and a generally slower pace of life. The world has also been ravaged by natural and man-made pestilence that has depleted both the quantity and variety of food supplies. In a neo-Bangkok that is spared from high sea levels by massive levees, the Wind-Up Girl sees a covert corporate agent trying to discover the secret location of the Royal Thai seedbank. The plot is a chequerboard of inter-departmental rivalries, royal politics and industrial espionage. However, the book's backdrop of global warming and a contracted world is a sobering reminder of how present-day water and food scarcity will increasingly impact military operations.



The Forever War

This is the only 'must-read' on this list. I am still amazed at how Haldeman, a US veteran of the second Indochina War, combines physics, military tactics and heartfelt sentimentality in such efficient prose (the novel is barely 200 pages long). While the other books deal with disruptive technologies and asymmetric enemies, The Forever War also deals with the ultimate disruptive/asymmetric environment: space and relative time. Haldeman follows the combat career of William Mandela, a member of a new interstellar military cadre formed to fight a newly-encountered alien race. The book lays out in realistic detail how the recruits adapt to the hostile environment of space and new combat suits. Far more are killed from mishaps than enemy action, much like the costly lessons of early naval aviation.

However, it is faster-than-light travel that complicates interstellar warfare - because of time dilation, a military campaign that lasts a few months in relative time equates to decades and even centuries in 'real' Earth time. The humans may fight an enemy that they only encountered a few months ago, but in fact has had centuries to adapt – Army's learning loops would be literally thrown out! The most poignant moments in the book are the episodes of Mandela's social dislocation when he returns to an Earth that he does not recognise. It is these moments that you appreciate that this is a book written by a veteran, for other veterans.



Total War 2006

You may be still wondering at how the theoretical, high-minded concepts of science fiction could possibly relate to the intelligence profession. To bring us closer back to our time, I have drawn on lessons from two books: Tom Clancy's 'Red Storm Rising' and Simon Pearson's 'Total War 2006', to formulate enemy courses of actions during simulation and staff course exercises. In these books, the asymmetric tactics, used by an enemy with little regard for its own losses (the Soviet Union desperate for new energy sources, and a neo Islamic Caliphate respectively), devastate the vaunted technological superiority of western military forces. I adapted these ideas to formulate high-risk, high-payoff enemy courses of actions to destroy or disable the ADF's two LHDs and thus foil a simulated expeditionary force deployment.

As intelligence professionals, we must not only draw on current trends and contemporary information, but also our imagination and cunning when discerning threats to our nation. When placing ourselves in the shoes of our adversaries, we must combine elements of deception, a higher risk appetite, use of emerging technology and innovation to genuinely test our own military planning. In other words, it is simply not good enough to present a 'near-peer' adversary. Good sci/tech fiction can help expand our minds and break out of our institutional moulds. And one day, perhaps avoid a failure of imagination.

THE MILLENNIAL CHALLENGE: ISSUES FOR RETENTION AND CAPABILITY WITHIN THE AUSTRALIAN INTELLIGENCE CORPS

Private Christopher Cianter

Australian Intelligence Corps (AUSTINT) is currently suffering from an issue of hollowness.[1] This is in part the result of boredom, a poor Corps culture, career mismanagement and an inability to compete with government and civilian sectors.[2] The other component of this problem is that AUSTINT is largely failing to adapt to the challenge of millennial employees. This monograph will identify significant differences in employee generations and how these impact on leadership and managerial practices. Additionally, some critical factors will be examined which generate issues for employee motivation and workforce sustainability. The monograph will conclude with a number of recommendations on how AUSTINT can address some of these concerns, and thus ensure it retains a viable talent pool into the future.

The millennial employee challenge

Today's workforce landscape is shifting from the traditional careerist approach, to a more dynamic approach to careers.[3] This shift is the by-product of a number of identified differences between newer generation employees, and their older counterparts. One of the primary differences is the 'need' for millennial employees to have increased job mobility and flexibility.[4] This need is driven by early compromises in career paths, the lack of significant annual wage increases, unfulfilled desires for self-expression, economic concerns including increased debt, and the constant seeking of better

[1] Australian Army, *Plan Athena AUSTINT Corps other ranks hollowness remediation*: 2016-2019, CA Directive 18/16, Canberra: Army Headquarters, 2016.

[2] 2 Coy, 1 Int Bn, *Supplementary Intelligence Report 002/16 Transfer and Retention to AUSTINT*, Brisbane: 1st Intelligence Battalion, 11 May 2016.

[3] Pricewaterhouse Cooper, *Talent mobility 2020 and beyond – the future of mobility in a globally connected world*, New York: PwC, 2012. Accessed 02 Nov 2016, http://www.pwc.com/gx/en/managing-tomorrows-people/future-of-work/pdf/pwc-talent-mobility-2020.pdf

[4] Jeromy Lloyd, 'The Truth About Gen Y', *Marketing Magazine* 112, no. 19, (2007): 12-22.

opportunities often linked to learning, development and leadership.[5] These drivers mean millennial employees are transient in their employment nature. Millennial employees spend on average, just 4.2 years in any one job prior to moving on – a period only 2 months longer than the minimum period of ADF service.[6]

Short tenure periods generate significant issues for capability and retention, including high employee turnover,[7] equating to financial losses for the organisation. Recent workforce analysis indicates the separation rate for Army is approximately 12 percent.[8] AUSTINT alone has experienced approximately 106 discharges between 2012 and 2015. The cost to replace these personnel could be as high as $2 million. This money is better channelled into capability development as opposed to recruitment. Other equally damaging consequences of high employee turnover include: low workplace morale, downturn in productivity, increased training liabilities drawing on limited resources, lack of motivation, slow organisational advancement, and the loss of critical corporate knowledge which is not easily replaced.[9]

AUSTINT has largely failed to implement a comprehensive strategy addressing the factors underpinning employee dissatisfaction. Plan Athena advocates a series of remediation strategies; however such strategies are unlikely to rectify retention issues as it largely fails to address the complex and interconnected factors contributing to the current hollowness. Factors such as: boredom, lack of tangible capability, feelings of increasing irrelevance, lack of significant pay rises, lack of flexibility in the workplace, irregular feedback, mismanagement and a lack of learning and development at the junior ranks all combine to contribute to employee dissatisfaction. The crux of the issue is the inadequacy of AUSTINT to fundamentally rethink how it recruits and retains a millennial talent pool. Essentially, the millennial employee challenge becomes one of culture fit.[10]

AUSTINT projects an image of a rewarding career that is flexible, has genuine capability, provides training/learning opportunities that transition into civilian life, and an ability to generate tangible effect for the organisation, even at the lowest rank.[11] This image is not aligned to the reality of employment within AUSTINT. This is an important factor given employment specialists report workers are often compelled to leave when their actual duties and workload do not align to their expectations.[12] This is one of the primary reasons AUSTINT members commonly elect to serve out only their minimum obligation period prior to discharge. Millennial employees expect a challenging, meaningful and rewarding career. When this does not occur, the job market, employee education and Army-gained experiences facilitate a relatively easy transition.

Millennial employees place significant emphasis on personal learning and development.[13] A Deloitte employment study found 71 percent of those considering separation from their organisation were unhappy with the training they were receiving, and

---

[5] Chris Pash, 'Millennials are thinking about job changes so much, recruiters have coined a new name for them', *Business Insider Australia*, 23 Aug 2016. Accessed 02 Nov 2016 http://www.businessinsider.com.au/australian-millennials-are-so-busy-job-hopping-that-recruiters-call-them-continuous-candidates-2016-8

[6] Bureau of Labour Statistics , *Employee tenure summary in 2016*, Washington, DC: United States Department of Labour, 2016. Accessed 03 Nov 2016, https://www.bls.gov/news.release/pdf/tenure.pdf

[7] Jeffrey Peterson, *The Effect of Personnel Stability on Organizational Performance*, Santa Monica, CA: RAND Coporation, 2008. Accessed 03 Nov 2016.

[8] Australian Army, *Army's Workforce: current and future analysis*, Canberra: Department of Defence, May 2016.

[9] Kemal Surji, 'The Negative Effect and Consequences of Employee Turnover and Retention on the Organization and Its Staff'. *European Journal of Business and Management* 5, no.25, (2013): 53.

[10] Bob Moritz, 'Keeping Miellennials Engaged', *Harvard Business Review*, Nov 2014. Accessed 04 Nov 2016, https://hbr.org/2014/11/the-us-chairman-of-pwc-on-keeping-millennials-engaged

[11] Defence Force Recruiting, Analyst Intelligence Operations, Accessed 04 Nov 2016, http://www.defencejobs.gov.au/Army/jobs/AnalystIntelligenceOperations/

[12] Peter Berry Consultancy. 'What are the main drivers of employee turnover'. 2014. Accessed 04 Nov 2016, https://peterberry.com.au/what-are-the-main-drivers-of-employee-turnover/

[13] Timothy Reisenwitz & Rajesh Iyer. 'Differences in Generation X and Generation Y: Implications for the Organization and Marketers', *The Marketing Management Journal* 19, no. 2 (2009): 91-103.

how they were being professionally developed.[14] Lack of development by an organisation is further compounded by millennial employees having access to near boundless information. The internet provides a means of self-education and a readily available repository of solutions. This generates issues for successful engagement of millennial employees, who not only want to receive more training, be developed faster and receive regular coaching, but also want to work on new and challenging problems.[15] Millennial employees will actively seek out organisations that appreciate personal learning, provide development opportunities and embrace flexibility, adaptability and innovation.

Good leadership is critical to the retention of employees irrespective of generation.[16] The quality of the supervisor to subordinate relationship is a determining factor in employee tenure.[17] Important factors within this relationship is how much an employee's immediate supervisor shows interest, provides direction, empowers them to perform duties and provides frequent feedback. As such, AUSTINT retention issues may be indicative of a number of leadership shortcomings. Millennial employees do not respond well to top-down management, and instead prefer a more democratic and inclusive approach to leadership.[18] This hierarchal top-down approach is acutely felt in AUSTINT where there is a high ratio of Officers to Other Ranks. The result of such a top heavy organisation is overly competitive rank progression. For officers to succeed, careful and calculated career management is required. Such career management commonly comes at the cost of leadership styles more aligned to engagement of millennial employees.

Closely aligned to the aforementioned is the desire to receive feedback from leaders. The millennial employee is much more interested in feedback then older generations.[19] This is to be expected. Millennial employees have grown up in an era of near-instantaneous feedback, largely enabled by technology.[20] The expectation of consistent feedback has now transitioned into the workplace with some employees requesting weekly, if not daily feedback.[21] This feedback is not purely about praise, but also about improvement pathways, and gauging progress towards goals. Importantly, it is also about understanding how their efforts contribute to the overall success of the organisation.

Pathways to Millennial Engagement and Retention

The demographic challenge of millennial employees is not going away. The complex combination of new priorities, and changing employee environments, means new solutions are required. In order to meet this challenge, AUSTINT needs to implement deeper organisational changes through a number of pathways. These pathways include new management and leadership practises that are better aligned to the needs of millennial employees; development of capabilities that incentivise millennial retention; and better engagement policies that compel millennial employees to stay within the organisation. Included below are a number of recommendations based on a combination of AUSTINT feedback, and a 2016 Gallup employment survey on what millennial employees want from their employer.[22]

[14] Deloitte, 'The 2016 Deloitte millennial survey: winning over the next generation of leaders', 2016. Accessed 04 Nov 2016, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-millenial-survey-2016-exec-summary.pdf

[15] Jay Gilbert. 'The Millennials: A new generation of employees, a new set of engagement policies'. *Ivey Business Journal*, 75, no. 5 (2011). Accessed 04 Nov 16, http://iveybusinessjournal.com/publication/the-millennials-a-new-generation-of-employees-a-new-set-of-engagement-policies/

[16] Amy Rees Anderson, 'Good Leaders Are Invaluable To a Company. Bad Leaders Will Destroy It', *Forbes*, 14 Jan 2013. Accessed on 05 Nov 2016, http://www.forbes.com/sites/amyanderson/2013/01/14/good-leaders-are-invaluable-to-a-company-bad-leaders-will-destroy-it/#633c5dc125b6

[17] Donna Brown, 'Employee engagement – the crucial role of the supervisor', ISS White Paper, 2014. Accessed on 05 Nov 2016, http://www.au.issworld.com/-/media/issworld/au/Files/About%20ISS%20documents/Employee_Engagement%20White%20Paper%202014.pdf

[18] Lauren Brousell, 'How millennials challenge traditional leadership', *CIO Magazine*, 04 Aug 2015. Accessed on 06 Nov 16, http://www.cio.com/article/2956600/leadership-management/how-millennials-challenge-traditional-leadership.html

[19] Valerie Grubb, *Clash of the generations: managing the new workplace reality*, Hoboken: New Jersey: John Wiley & Sons, 2016, p. 47.

[20] Melissa Bailey, 'Instant Feedback is the Norm for Millennials', *Article Universum Global*, 08 Dec 2014. Accessed on 06 Nov 2016, http://universumglobal.com/articles/2014/12/instant-feedback-norm-millennials/

[21] Dora Wang, 'The best time to ask for employee feedback', *The Tinypulse Blog*, 04 May 2015. Accessed on 06 Nov 2016, https://www.tinypulse.com/blog/employee-engagement-survey-the-best-time-to-ask-for-feedback

[22] Gallup, *How Millennials Want to Work and Live: The six big changes leaders have to make*, Washington, DC: Gallup, 2016.

1. **Recognise and enable the personal and professional goals of millennial employees**. Acknowledge millennial employees are individuals with specific goals. Many of these goals are professional and focused on development and learning. Employees want their job to give them a chance to make a positive contribution. Placing millennial employees on special rotations or secondment assignments will contribute to a culture of development and learning. These secondments can include private enterprises, policing organisations and/or other government intelligence agencies. Noting a large percentile of millennial employees wants to stay within their current organisation - engaging them through such exchanges will actually degrade the risk of millennial employees transitioning to these organisations. [23] Additionally, millennial employees need to be challenged. Allow millennial employees to own problems, and come up with new innovative solutions. Millennial employees also have a strong desire to work overseas. As such international exchange programs open to Other Ranks would increase retention, and grow knowledge within the organisation. Such a program would align personal goals to organisational ones.

2. **Narrow the disparity between perception and reality**. It is important for employers to explain what they are offering, but also what is expected in return. What an employer promises must be what they deliver. Failure to do so will contribute to high rates of employee turnover, and associated costs to the enterprise. Clearer explanations of the roles and responsibilities of AUSTINT soldiers associated with various appointments, along with broadening the range of available postings to junior members, will improve recruitment by attracting candidates with a realistic expectation of employment. By reducing disparity through the initial recruitment process, retention will concurrently be improved.

3. **Practise mission command**. Millennial employees work well under incisive leadership, particularly when they have a sense of personal responsibility for achieving outcomes.[24] For this reason, millennial employees do not respond well to micromanagement, or being given the exact formula for how to achieve results. Instead, managers should set deadlines and standards, coaching them only when they fail to achieve declared targets. More importantly, managers should not dictate how to achieve the task, but instead seek to confirm, through feedback loops, the task has achieved the set standard. Once achieved, managers should provide immediate feedback focusing on the positives and a pathway to improvement. Notably, this style of feedback is taught on all-Corps promotion courses, however intermittently conducted in the work place.

4. **Encourage learning and development**. Millennial employees want to experience as much training as possible.[25] Presently AUSTINT is more focused on developing officers and SNCO's. By focusing exclusively on these ranks, AUSTINT risks losing future talent by failing to engage millennial employees during the critical initial period of service. AUSTINT should consider allocating special projects to talented millennials which fall outside their normal duties; provide opportunities to engage in training that results in real world qualifications; and encourage cross-skilling in intelligence collection mediums and skills. Importantly, AUSTINT needs to encourage millennial employees to connect, collaborate and build networks. Whilst there is a risk members subject to the abovementioned will leave prior to fulfilling long and productive careers, there is a strong correlation between training and the retention of employees.[26]

---

[23] *Ibid*.

[24] Stephen Bungay, *The Art of Action: How Leaders Close the Gaps Between Plans, Actions and Results*, Boston, MA: Nicholas Brealey Publishing 2010, p. 76.

[25] Margery Weinstein, How Much Training do Employees want?, *Training Magazine*, 23 Oct 2016. Accessed 06 Nov 16, https://trainingmag.com/how-much-training-do-employees-want

[26] Business Review Australia, Employees want more training and skill development, *Business Review Australia* 06 May 2014. Accessed on 06 Nov 16, http://www.businessreviewaustralia.com/leadership/96/Employees-Want-More-Training-Skill-Development

5. **Educate leaders to be more attuned to millennial employees**. Presently, Army leadership is not necessarily conducive with millennial employees. As the saying goes, *'employees do not quit their job; they quit their bosses'.* The style of leadership that worked on previous generations has far less impact on millennial employees. As such, leaders and managers need to be taught how to recognise generational differences and adapt appropriately. They should not attempt to change their workforce, but instead be taught better leadership and management strategies. Leaders that engage millennial employees will be participative, team focused, human-orientated and charismatic.[27] Leaders who fail to engage millennial employees will be hierarchical and autonomous.[28] Most importantly, current leaders wanting to lead their millennial workforce will create more leaders, by helping their millennial employees learn to sustain success and to perform at a high level consistently.[29]

6. **Generate capabilities**. Generate capabilities that are professionally rewarding and challenging. Such capabilities should be uniquely held by AUSTINT, and have operational validity. By enhancing capability development, AUSTINT provides additional learning and development opportunities which encourage retention. Advanced analytics and enhanced collection capabilities serve as an example.[30] Upon completion of courses, particularly advanced courses, AUSINT should request a return so as to retain and distribute the capabilities across the workforce. For example an Advanced Source Operator's Course could incur a return of service obligation (ROSO) of 12-24 months

7. **Recognise they will leave**. Millennials are motivated and driven to succeed, just as much, if not more so than older generations. This is a powerful attribute to be harnessed. However, AUSTINT needs to recognise millennial employees are likely to dedicate five years to the organisation before moving on. This timeframe will be lessened where the organisation restrains employee drive or motivation. The corps should seek to harness it whilst they can. Moreover, in the event AUSTINT wants to retain such soldiers in the long term, it would be beneficial to streamline the process for transitioning in and out of Defence. This would allow members to take a sabbatical from Defence, but also a quick and easy conduit back into the organisation should they choose. Doing so would mean members can come and go at ease, often returning into the organisation with different approaches and best practises acquired from external and corporate enterprises.

Conclusion

The millennial generation is the largest in history, armed with the most impactful technology created to date. This combination has resulted in a tectonic plate movement regarding the employment landscape. Evidently, to deal with the changing landscape and the millennial challenge in particular, organisations will need to change. Defence is not immune from this need, albeit it has considerably more factors to consider. However, failure to do make significant changes will mean the challenge of the transient employee will only intensify in the near future. By implementing a number of recommendations, and seeking to address retention more holistically, AUSTINT will be better positioned to recruit, retain and harness viable talent.

PTE Christopher Ciantar is currently employed as an intelligence analyst and holds two Masters degrees from Macquarie University.

[27] Jennifer Deal, Sarah Stawiski, William Gentry and Kristin Cullen, *What Makes a Leader Effective? U.S. Boomers, Xers, and Millennials Weigh In*, Centre for creative leadership, 2014. Accessed on 06 Nov 16, http://www.ccl.org/wp-content/uploads/2015/04/WhatMakesLeaderEffectiveUS.pdf

[28] *Ibid*.

[29] Justice Calo Reign, 'Leadership for the millennial generation', *Conscious*, Issue 1, Winter, (2015). Accessed on 06 Nov 16, http://www.conscioucompanymagazine.com/blogs/press/16408221-leadership-for-the-millennial-generation

[30] Robert Caruso, Here's How the US can Build Intelligence Capability, *Business Insider Australia*, 09 Sep 2014. Accessed 06 Nov 16, http://www.businessinsider.com.au/the-us-needs-better-humint-to-beat-isis-2014-9

THE IMPORTANCE OF NON-FINANCIAL REMUNERATION FOR AUSTINT SOLDIERS

Corporal Dave Hemer

While financial benefits are a key factor in maintaining employment and remediating the hollowness within AUSTINT Corps, non-financial benefits can amplify a soldier's satisfaction with their role and their motivation to remain in the Corps. Consequently, soldiers will consider their work environment, autonomy, training opportunities, career development, work/life balance, flexible working arrangements and other non-financial issues against their financial income when evaluating whether to remain within the Corps or to seek external employment opportunities. Even the best paid soldiers will reconsider their employment if they are dissatisfied with these aspects of their role. While remuneration is a fundamental concern for many AUSTINT soldiers, by integrating robust non-financial incentives, the Corps will continue to attract, motivate and most importantly, retain more personnel.

Solely employing financial benefits as the principle performance motivator can encourage soldiers to prioritise the particular aspect of their job which will earn them an immediate reward rather than pursuing long-term career development and job satisfaction. Further, supplementary financial incentives often

encourage compliance with norms to receive rewards rather than incite creativity and innovation. Emphasising non-financial benefits creates an enhanced work environment wherein employees are physiologically and emotionally satisfied, they are motivated to participate and are encouraged to think outside the box, all of which combine to generate better outcomes for soldiers and the Corps.

Soldiers within the Corps require a degree of independence and trust. Clear direction on what is required and the time frame in which it is to be achieved is still needed; however, they desire autonomy to execute the task on their own or within their team. When they are continually checked on, questioned and micromanaged they do not feel valued or trusted, resulting in discontentment and reduced job satisfaction. Enriching work experiences by satisfying the intrinsic motivator of autonomy can result in increased enthusiasm and enhanced outputs from the Corps' soldiers.

Motivated soldiers do not like stagnant situations; they prefer to remain engaged and feel as if their forward momentum is contributing – they want to achieve. These soldiers want additional responsibilities, different training opportunities and new challenges on a daily basis and as they progress through the ranks. Soldiers who perceive their work is not contributing towards an articulated goal or has no impact or value will likely feel under-employed and eventually disgruntled, turning their frustrations towards the Corps and may pursue fulfilling external opportunities. Ensuring work remains stimulating, of real-time value and provides opportunities for varied training and continual progression will result in not only more knowledgeable and skilled soldiers, but also more satisfied ones.

While soldiers join or transfer to AUSTINT Corps for myriad reasons, an underpinning motivator is the pursuit of a challenging work environment. Such an environment must be monitored – continual operational deployments or demanding exercises can take their toll, leading to burnout and/or over-stressed individuals. Our Corps contains smart people, not inexhaustible super humans. Non-financial benefits, such as proper implementation of work/life balance, contribute greatly to moderating the additional stressors and challenges imposed upon our soldiers within a challenging work environment and become significant factors to their continued employment. By understanding their soldiers, along with soldiers' individual motivators, units will be better equipped to assist soldiers, enhance job satisfaction and retain the corporate knowledge and experiences of Corps' members.

As soldiers develop, their families often grow with them. While the demands of a challenging work environment often includes after-hours or weekend work along with absences in the field, the demands of family life increase commensurately; so begins the tenuous balancing act confronting soldiers of reconciling absences from their families against workplace expectations and their innate motivations to achieve. It is easy for soldiers to feel trapped – while still satisfied with their job, they are unable to meet the current demands of their families. Flexible work hours and co-located postings become more significant motivators than increased financial incentives. While flexible work arrangements exist in policy, the implementation of such procedures is varied. Offering soldiers the option to vary their work hours – whether starting or finishing earlier or later – can make a huge difference in their lives and in their level of job satisfaction.

As AUSTINT soldiers await alignment between their current financial remuneration and those in similar roles in other services or civilian agencies, the importance of incorporating adaptable and robust non-financial benefits increases. In the absence of comparative fiscal rewards and well-developed, widely applied non-financial benefits, commanders have leveraged soldiers' altruism as a means of motivation. This, however, is unsustainable and leaves soldiers feeling exploited and replaceable, ultimately contributing to the hollowness observed within the Corps in recent years. Soldiers need to feel valued; whilst suitable financial rewards are imperative, a pecuniary incentive alone will not satisfy the motivators of AUSTINT soldiers – it must be complemented by practical non-financial benefits to create a holistic reward system. Consequently, creating and applying adaptable non-financial benefits will improve employment satisfaction within the Corps as much as, if not more than, improved financial incentives.

THE ROLE FOR AUSTINT IN A WHOLE-OF-GOVERNMENT COUNTER-TERRORISM CAMPAIGN

Major Michael Mann

The threat posed by Islamic extremism to Australia, and Australian interests, will be one of our greatest national security challenges for the foreseeable future. International and regional instability continues to provide ungoverned space for transnational terrorist groups to consolidate and project force into the Western world. The potential return of a wave of Australian and regional *jihadis* from the ailing Islamic State – radicalised, networked and with recent operational experience – combined with an increasing home-grown threat will serve to stretch Australia's national security community.[i]

The Australian whole-of-government response to the domestic and regional terror threat is primarily a law-enforcement activity, though this does not mean the ADF has no role to play. AUSTINT in particular has a range of knowledge and skills that can make a meaningful contribution to the whole-of-government counter-terrorism (CT) effort. While these skills have traditionally been drawn from SOCOMD, there is a range of formations and establishments that can contribute. This article will focus on the capabilities that can be applied prior to a major terrorism incident [ii], as part of the first phase of a whole-of-government CT campaign.[iii] Critically, it should be noted that these capabilities can be applied both offshore, and domestically.

The opportunity

So how can the ADF contribute to a law-enforcement problem? In simple terms, the ADF is designed to raise capabilities, plan, and lead complex multi-agency operations. Defence's strength in these areas was made evident by the success of the Joint Inter-Agency Task Force running Operation SOVEREIGN BORDERS, an activity which remains the benchmark for whole-of-government cooperation on a national security issue.[iv] In the CT domain, the federal Government has recognised that there are shortfalls in whole-of-government capability and coordination, as demonstrated by the decision to

[i] PBS ASIO 2017/18 – Section 1.1 Strategic Direction Statement, p.171. https://www.ag.gov.au/Publications/Budgets/Budget2017-18/Documents/PBS-ASIO-2017-18.pdf

[ii] Equivalent to the Prepare and Prevent stages of the NCTP.

[iii] Note: Should an ADF call-out occur in response to a domestic terrorism event, there are a number of tactical intelligence functions we would expect to support the ADF response, similar to any other operation. These activities can be considered business-as-usual for the organic intelligence staff of the affected units and fall outside the scope of the 'phase-zero' considerations presented in this article.

[iv] PM&C CT Review, 23 Feb 15, p22

combine security agencies into the Home Affairs portfolio.[v] In part, this decision will assist with the planning and integration of the CT effort, which is hampered by differing threat environments across the Commonwealth, inconsistent security agency capabilities, and inter-agency jurisdictional issues. So there is a natural synergy between the Government's CT requirements and Defence's organisational strengths. This does not mean the ADF takes the lead on any operational CT response – far from it – but the ADF's skill at raising and training capabilities, developing doctrine, conducting complex multi-agency planning, and supporting cross-jurisdictional operations can be harnessed to support the national security community.

This opportunity is particularly significant to AUSTINT, as any ADF contribution - prior to a major incident- is likely to be intelligence-led. The whole-of-government CT effort requires cross-jurisdictional battlespace awareness, effective intelligence coordination and planning, and, potentially, niche intelligence capability contributions – all of which are AUSTINT's raison *d'etre*.

As a core function, AUSTINT evaluates the strategic, operational and tactical threat environments in order to understand the battlespace. The career pathway for AUSTINT personnel sees them appointed to roles across this spectrum, which serves to ingrain a broad analytical perspective.[vi] It is this broad and flexible approach that provides Defence with an organisational strength almost unmatched in the national security community. Civilian national security agencies are defined by narrow roles, functions and jurisdictions; and a consequence of this can be a narrow field-of-view. AUSTINT can assist by helping the CT community to develop a holistic view of the threat.

Defence is also well-placed to support the planning and coordination function for the national security community. For our part, AUSTINT has an extensive and recent body of experience planning and

Nice, France Terror attack.

conducting multi-agency intelligence operations, and those hard-won lessons have been turned into relevant intelligence doctrine.[vii] Just as importantly, AUSTINT personnel work in dedicated planning staffs in agencies such as Joint and Special Operations Command, and Headquarters 1st Division, where the integration of intelligence into operational planning is a daily occurrence. Defence planning staff are accustomed to using JOC's established Requirements and Collection Management function which, despite its shortfalls, is a more mature entity than any enjoyed by the national security community. So we are well placed to support the development of a whole-of-government CT campaign plan, and this effort would be based off doctrine, manning and operational experience which does not exist elsewhere.

There may also be opportunities for AUSTINT capabilities to support a whole-of-government CT campaign directly. Deployed AUSTINT collection, analysis and military liaison functions offshore are already a staple intelligence feed for the CT community, and the quality of these contributions have established a moderate level of credibility with national security agencies.[viii] Of note, AUSTINT's proven ability to conduct effective operational network and systems analysis is not matched anywhere else in the CT community. National security agencies are tremendously effective against specific targets, but lack the processes to achieve that effect

[v] https://www.pm.gov.au/media/2017-07-18/strong-and-secure-australia

[vi] The AUSTINT career profile deliberately appoints Officers to Strategic, Operational, Tactical(Regimental) and Representative postings (including the NIC) in order to broaden their understanding of the functions and requirements of agencies at the various levels.

[vii] SLIPPER, OKRA, PARAPET, SNAVE etc. Results = FATC, ASC, SIE, TNACs, JCITF

[viii] Details removed due classification.

at a macro or systems level, or beyond traditional jurisdictions. AUSTINT also has a proven ability to tailor intelligence product to whole-of-government customers to support law-enforcement effects, as was demonstrated by the conduct of evidence-based operations in Afghanistan.

But in addition to its offshore role, AUSTINT also has a major domestic role to play, which remains largely unexplored or coordinated by Defence and is not widely understood across Government.[ix] With almost 100,000 potential sensors, established security reporting channels, and extensive security intelligence holdings – and as an identified terrorism target [x] – Defence (through DS&VS' security intelligence function) is an excellent source of domestic situational awareness for the CT community. Defence can also help build security agency capability. Opportunities exist for AUSTINT elements – most notably those drawn from 1st Intelligence Battalion – to support the generation of law-enforcement capability through joint training activities. Personnel with specific skills could be seconded to national security agencies to ease the strain on human resources, and provide the benefit of ADF perspective and experience. In a similar vein, members of government security agencies have attended Defence intelligence training courses, and this should continue, as the skills taught work just as well in the domestic threat environment. Overall, these contributions demonstrate that Defence does have a role in what is perceived to be a non-traditional space.

Obstacles and challenges

There are a number of legislative hurdles that have traditionally prevented Defence, and therefore AUSTINT, from operating domestically. Defence contributions in the domestic arena are restricted by provisions of the *Defence Act 1903*, which emphasise the primacy of state governments in a CT response. Part IIIAAA of the Act details the 'call-out' mechanism for Defence when a State authority acknowledges it cannot deal with a 'domestic disturbance'.[xi] Traditionally, Government does not countenance a Defence response outside the bounds of Part IIIAAA, yet this approach fails to acknowledge the contribution that Defence can make prior to a terrorism event.[xii]

Other legislative impediments to an AUSTINT contribution include the privacy and investigative restrictions laid down in the *Intelligence Services Act 2001*, and *ASIO Act 1979*. However, the effects previously described can still be achieved, and the intent of these laws complied with, through the secondment of AUSTINT personnel to national security agencies.

The final obstacle concerns the allocation of scarce AUSTINT resources. Making the case to second AUSTINT personnel to other government agencies in a manner that provides no tangible, short-term benefit to Defence is a hard sell, particularly given the host of other equally significant operational and force generation commitments.[xiii] However the case for an AUSTINT contribution is clear, and the commitment of even a small number of personnel in the right places may have a positive impact on national security that far exceeds the cost.

Conclusion

The whole-of-government response to the burgeoning terror threat requires the sort of complex inter-agency planning and consideration to which Defence is accustomed. AUSTINT stands in a

[ix] Lindt Café Inquest, multiple references, TBI.

[x] For further information, see the Defence Security and Vetting Service (DS&VS) Defence Security Threat Assessment (DSTA) and DS&VS SYINTREP 001/15 on the DSN portal. Also refer ATA 218/2016. For more detailed local security information, refer the DS&VS Regional Threat Supplements.

[xi] Part IIIAAA of the Defence Act establishes a call-out mechanism whereby the Governor-General, on advice of the Commonwealth Government, may authorise the ADF to become involved in the response to a domestic disturbance following a request from a state government. Such authorisation can only be granted if the Prime Minister, Attorney-General and Defence Minister are satisfied that the state is not able to protect itself from the relevant threat of violence.

[xii] p118, para 63 of The Lindt Café Coronial Inquest noted that 'the role of the ADF is not limited to circumstances where it is called out pursuant to Part IIIAAA of the Defence Act'. Defence is currently part of a review into the legislative and policy framework for call-out, and it is the author's hope that a phase-zero intelligence contribution is being considered as part of that effort.

[xiii] https://www.aspistrategist.org.au/strategist-six-mark-binskin/

Lindt Cafè Seige.

unique position - with a range of skills, knowledge and recent operational experience - that can greatly assist our partner security agencies. As demonstrated so tragically in Manchester, London and Victoria in just the last few months alone – the threat is real, and it is going to get worse, but the ADF is in a position to do something about it.

Postscript: The Turnbull Government's July 2017 decision to establish a Home Affairs portfolio presents a prime opportunity for Defence to contribute in the manner discussed in this article. As articulated by the Prime Minister, [xiv] the Home Affairs Department will be the mechanism for providing 'strategic planning, coordination and other support' to a federation of security agencies. By rapidly mobilising some human resources, Defence could assist with the establishment of the fledgling Department, providing the benefit of Defence experience and perspective while serving to normalise Defence's potential contributions to the primary whole-of-government CT authority.

[xiv] https://www.pm.gov.au/media/2017-07-18/strong-and-secure-australia

THE POWER OF IMAGERY

Corporal Dave Eason

The old adage, a picture speaks a thousand words, is never more true than in the battlespace. A well-constructed image can change the battlespace, and how soldiers understand it. Within a small Iraqi town, a Vehicle Born Improvised Explosive Device (VBIED) approached a manned check point. Members of the Iraqi Army successfully completed newly acquired drills to prevent the VBIED – in the process saving their lives. A Major in the Iraqi 9th Div attributed his troop's success to an infographic designed by a deployed Australian Multimedia Technician.

The infographic illustrated a simple but effective set of tactics to confront a VBIED – notably one of the biggest threats in Iraq. The graphic employed imagery to illustrate to inexperienced Iraqi soldiers how to combat VBIEDs. As a direct result of these infographics, and their dissemination by the Iraqi CoC, Iraqi soldiers were no longer abandoning checkpoints for fear of VBIEDs. In its simplest form, the use of images coupled with basic instructions in Arabic, gave inexperienced troops the confidence and skill to confront Daesh. Ultimately, this

Example Taji Products.

infographic will contribute to the defeat of Daesh, and perhaps one of its most powerful weapons.

The above example emphasises infographics are a powerful medium to communicate information.

Consideration for Information Operations should always be given, for it truly is a force multiplier.

CPL David Eason is currently employed as a Multimedia Technician.

Example Taji Products.

CONDUCTING INTELLIGENCE ON UN OPERATIONS: A PERSPECTIVE FROM SOUTH SUDAN

Squadron Leader Claire Pearson

South Sudan has been both born out of, and into conflict. After 40 years of civil war in Sudan that cost millions of lives, the world's newest nation had a mere 18 months to celebrate its newfound status before it dissolved into a civil war of its own. This new conflict has, to date, killed hundreds of thousands, as fractures form along tribal Dinka/Nuer and intra-clanic lines, those supporting and against the embryonic government, and those exploiting the ensuing chaos. The most recent outbreak of violence, which commenced in July 2016, will only compound this sorrow. Further adding to the misery, in February 2017, South Sudan was the first country in six years to be declared as being in famine. Sadly, the UN observed this famine was man-made, and likely avoidable.

Established in 2011 to facilitate the creation of this new nation, United Nations Mission in the Republic of South Sudan (UNMISS)[1] forces are structured with a Force Headquarters (FHQ) (three-star level) in the capital Juba, with four brigade Sector Headquarters, and their respective G2 staff, located across the country.[2] Sector East Headquarters, its two infantry battalions, Military Liaison Officer team and support companies are located in the remote town of Bor, a 45 minute helicopter flight north of Juba. This paper provides an insight into employment on a UN G2 staff. As with all deployments, lessons identified can prove useful in preparing us for the future, refining intelligence practices and codifying training.

IFV responding to armed protestors at Bor UN Camp gate.

The Changing Nature of Intelligence in the UN

The UN intelligence function has evolved in recent years. Historically, the UN has been understandably wary of using the term 'intelligence', opting for 'information' amid concerns from both member states and host nations.[3] Due to an increase in peace

[1] UNMISS is a Chapter VII (Peace Enforcement) mission with a mandate to monitor violations, provide conditions conducive to the provision of humanitarian assistance, and use lethal force where necessary in support of the Protection of Civilians (POC).

[2] The infantry battalions in the Sectors did not have their own G2 staff so the Sector HQ G2 staff provided the intelligence for the whole Sector.

[3] This is in part due to many member states associating intelligence with secret police, with connotations of enhanced interrogation techniques that include methods counter to the Geneva Convention, and wider concerns relating to interference with state sovereignty and misuse of information.

keeping operations in non-permissive environments over the last few decades, and a commensurate level of UN peacekeepers being targeted and killed, the term *intelligence* is becoming more widely accepted.[4] Equally, while the G2 function has traditionally been exclusively focused on supporting force protection, the G2's role has broadened more recently to provide more holistic intelligence support to the mission. In a contemporary UN context, intelligence also supports measures of effectiveness of the mission, and enables the UN to protect civilians.

Despite Australia's involvement in UN operations over the last 70 years, from an intelligence perspective, the ADF's exposure to the UN system has been quite limited. While arguably possessing a robust intelligence capability in East Timor that was not without its challenges, as the lead nation, the ADF could shape the intelligence enterprise to largely reflect Australian and allied doctrine. This was underpinned by intelligence staff that received professional training, and possessed requisite security clearances. More often than not, outside of Australia's immediate region, the ADF's contribution to peacekeeping operations under the auspices of the UN will likely be in lower numbers, with the bulk of the forces originating from countries such as Ethiopia, Pakistan, India, Bangladesh, and Rwanda.[5] Accordingly, with the majority of senior billets allocated to nations that contribute the most troops, Australia and indeed our traditional allies, have limited influence over the composition of Sector and FHQ staff and processes. As such, lessons identified as a G2 in UNMISS are indicative of intelligence challenges Australia will likely face when operating within a UN mission.

Going Back to Basics

While we expect a baseline of intelligence training from Australia's more traditional partners, in the UN environment, trained or qualified G2 staff are

Bor Town.

Sector East G2 Team.

uncommon [6], with language barriers presenting additional complications. This was evident in the UNMISS FHQ where the J2, who was responsible for setting intelligence standards for the wider mission, was a reserve German infantry officer with no previous intelligence experience. Within the Sectors, it was even less likely for peacekeepers to appreciate the full value of intelligence to support decision-making and force protection, with Sector staff mainly from the major UN troop contributing nations (ie the African Union and Indian sub-continent) [7]. Accordingly, it is rare for these individuals to have any

[4] The UN General Assembly's Special Committee on Peacekeeping Operations used the word 'intelligence' for the first time in its 2017 report (which is agreed to be consensus by more than 150 countries, including major troop and police contributing countries).

[5] These countries make up the top five UN troop contributing countries. The highest troop contributing NATO nation is Italy (26th highest troop contributing country) and FVEY nation is the UK (52nd highest).

[6] Australia is one of only a handful of countries in the UN that have dedicated intelligence professionals as part of their military.

[7] Of a Sector Headquarters staff of 32, only 2 members were from western/developed nations (both Australian) with the overwhelming majority of staff from developing nations in Africa and the Indian Sub-continent.

formal intelligence training with often no experience drafting INTREPS, conducting analysis, briefing commanders or even using basic IT systems.[8] In Sector East G2, informal intelligence and IT training led to some success, and a series of basic, thematic and geographic focused rolling PowerPoint briefs and Excel trackers were established. However, we must recognise that in light of the multinational force composition on UN operations, expectations must be tempered by variations in literacy, cultural and gender barriers, staff training, professionalism, and inevitable language barriers.

The Challenge of Collection

Notwithstanding the paucity of G2 staff experience, a wider challenge on UN operations is being reliant on largely Tier 1 and 2 HUMINT [9] of limited veracity, often not corroborated by patrols. Reporting could best be characterised as single source rumours, shaped by the bias of local nationals, and at times the UN members relaying the information. This was the case in Sector East as patrols and their commanders failed to see the value in reporting, often ignoring collection requirements, and at times, creating invalid information to conceal that they were not engaging with the local population. Reports were further clouded by cultural issues, as patrols who adopted an aggressive force posture (weapons at the ready) when engaging with locals in and around schools/churches reported hostile local sentiment toward the UN.

Collection activities were further complicated by the absence of formal guidance from the J2 staff in Juba, and the Department of Peacekeeping Operations (New York), on what was permitted on UN operations. This created the very real potential for an incident, particularly noting the Government of South Sudan was already highly sensitive to any intelligence collection, real or perceived, taking place. [10] With

Local women collect water in Bor Town.

Engaging with local children.

untrained and unqualified intelligence staff allowed to conduct activities up to and including what can only be described as source operations (at times with the encouragement of senior military mission leaders), the risk was acute. This came to a head in Sector East when the visiting FHQ Chief of Operations (an O6 from an African Union nation) was briefed on the collection challenges. His solution: give locals money in exchange for information. When the various risks associated with the UN conducting paid source operations were highlighted, his response was that

[8] The other Sector East G2 staff officers during my tenure were from Rwanda (Infantry), Kenya (Intelligence), Sri Lanka (Infantry), and Bhutan (Infantry).

[9] ADDP 2.0 defines Tier 1 as activities conducted by ADF personnel who do not possess formal specialist training and conduct information collection activities of a non-specific or non-targeted nature from human sources. This includes routine/patrol questioning, and civil-military activities. Tier 2 is defined as activities conducted by ADF personnel who possess base level formal training specific to certain employment or collection requirements. It could be argued that Tier 1 and 2 HUMINT is routinely conducted on UN operations.

[10] This sensitivity was most acutely demonstrated during the armed incursion of Australia House (the former ADF accommodation compound in Juba) and temporary detention of an ADF member after local government officials observed the member using binoculars.

instead of money, the G2 staff could use 'payment in kind' – that is, provide locals with alcohol, cigarettes and phone cards. In this instance, the Sector East G2 cell viewed such comments as suggestions rather than direction. However, it is possible other Sectors conducted paid source operations without an endorsed mandate, or appropriate training.

With a heavy reliance on rudimentary HUMINT collection, and an absence of more advanced technical collection capabilities, restricted access and permissiveness within the host country presented significant challenges. Host nations often impede UN peacekeepers to conceal human rights violations, or only consent to UN involvement through fear of further sanctions. In UNMISS, this translated to frequent Status of Force Agreement (SOFA) violations. This included routine roadblocks, impeding freedom of movement; overly bureaucratic measures to inhibit Dynamic Air Patrols; refusing to allow the UN to use UAVs [11] ; and preventing UNMISS from taking hand held imagery. These restrictions had critical implications during the July 2016 crisis, hampering already limited intelligence efforts.[12] G2 staff were unable to confirm local, and unverifiable, media reports that tens of thousands of White Army militia were moving toward the UN compound in Bor. [13] The government's refusal to permit UN rotary wing operations during the crisis (presumably out of concern the UN would use them to observe movements of SPLA forces), made seemingly simple tasks such as confirming the movement of 1000s of militia or IDPs, near impossible.[14] Unless the UN applies greater pressure on countries to comply with the SOFA, restrictions on access to information will undoubtedly be an enduring challenge faced by G2 staff on future UN operations.

With UN peacekeeping patrols having exceptionally limited reach across the AOR [15] and host nation

Engaging with SPLA LO during crsis.

Engaging with local IDP children.

[11] In the last five years, the UN has started using UAVs in missions such as MONUSCO (Democratic Republic of Congo).

[12] The 2016 July crisis followed a fragile peace in South Sudan with clashes breaking out in Juba between the SPLA (government) and SPLA-iO (government "in opposition"). These Juba clashes triggered militias, the SPLA and SPLA-iO mobilising in other parts of the country. In addition to the death of South Sudanese civilians and military members, the clashes resulted in the death of two UN (Chinese) peacekeepers.

[13] While the reported number of White Army militia may appear inflated, it did align with the number of forces involved in attacks on Bor during the 2013/14 crisis. The UN FOB was a key focal point for the White Army due to concerns their Nuer tribesmen in the UN IDP camp would become a target.

[14] A similar situation occurred where the G2 staff were unable to report the number of Ethiopian forces that entered South Sudan (initially without permission) following the abduction of over 100 Ethiopian children by South Sudanese tribesmen.

[15] The Sector East AOR is 122,581 km. Put into perspective, this is 10 times the size of Australia's AOR in Uruzgan, Afghanistan. With two FOBs in Sector East (Bor and Pibor), routine Short Duration Patrols were conducted in less than ten percent of the Sector. Less frequent Long Duration Patrols covered an additional 15 percent of the AOR (weather dependant) with the remaining 75% of the AOR unpatrolled with exception of an occasional Dynamic Air Patrol, reliant on local militias providing authorisation for flight safety.

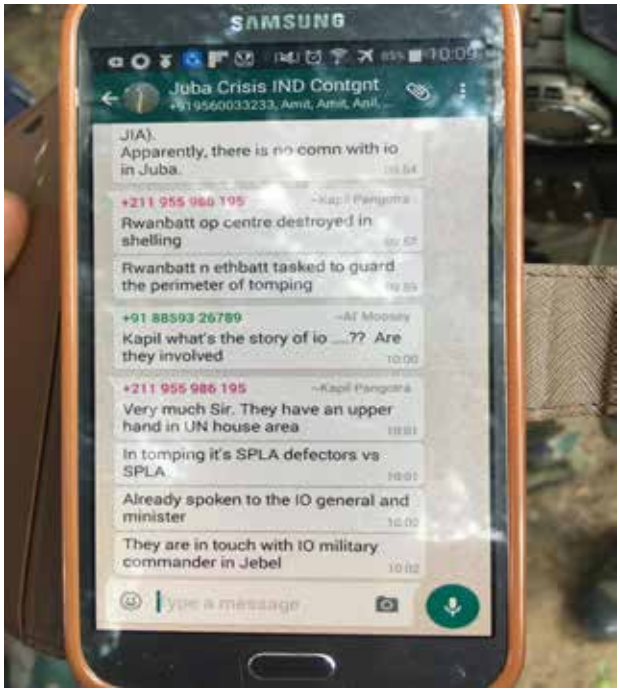
restrictions in effect, NGOs that had extensive reach in the Sector such as Médecins Sans Frontières and 'Blue UN' [16] would appear to be a wealth of information. However, with reporting from civilian agencies fed through the civilian UN Information Officer [17], an interesting phenomenon became evident: UN civilian staff exhibited an entrenched suspicion of sharing reporting with uniformed channels. This reservation was, in part, out of concern that this would jeopardise an NGOs' ability to garner acceptance from the host nation, but also due to a deep seated mistrust of the uniformed peacekeepers' intent and competencies. This refusal to share reporting with military peacekeepers was exacerbated by the UN Information Officers', who viewed their exclusive access to NGO reporting, and briefing senior UN civilians on a unique line of reporting, as a way of guaranteeing employment within the UN system. Anecdotally, other uniformed peacekeepers have identified this same phenomenon on other missions, signifying that this practice could be common across other UN operations.

When Communications Fail

While mission specific, the systemic failure in UNMISS to communicate and share information across the broader mission created issues with reporting between Sectors and FHQ stove piped at all levels. Sectors were unable to posture themselves appropriately to detect key indicators of destablisation in their own AOR. In a country where the peace process was exceptionally fragile, a seemingly isolated attack on an IDP camp had the potential to rapidly reignite tensions across the country.[18] This was evident during the July 2016 crisis where very limited reporting of the crisis in Juba was released by FHQ J2 staff, despite wider implications such as the mobilisation of the White Army militia. Accordingly, in a crisis, personal relationships and networks became essential as formal mechanisms broke down. Unexpectedly, an

Bor IDP camp next to Bor UN Camp.

unofficial rolling operations log maintained by Indian civilian, contractor and military members across South Sudan via *WhatsApp*, became a most useful line of reporting. This unique approach demonstrated that in the absence of formal communication chains, novel "work arounds" should not be discounted, and are often invaluable.



The WhatsApp Feed.

[16] Blue UN is a term that refers to aid organisations owned by the UN such as World Food Program, UNHCR and UNICEF.

[17] Information Officers ostensibly provide a similar function to the G2/J2 in analysing reporting from civilian channels to report on the situation within the country, reporting up through UN civilian channels. They do not inform on force protection and are the key point of contact when engaging with NGOs on reporting.

[18] A challenge in most contemporary operations is the rapid transfer of information by civilians and warring factions through mobile phones/ text messaging. A crisis in one region can be rapidly communicated across an entire country promoting rapid escalation of violence across an AOR, faster than a peacekeeping force can counter through strategic messaging/PSYOPS.

The Unexpected (and Surprisingly Rewarding) Duties

UN deployments present a number of challenges, both professionally as an intelligence officer, and personally. There remains entrenched bias among peers and superiors, particularly in relation to the participation of women in the military. However, this did present the opportunity to contest assumptions on a daily basis (at times with the necessary backing of the Australian Contingent Commander). An added cultural bias that a uniformed woman should automatically become the Gender Advisor, created an unanticipated opportunity. Through being the Sector East Gender Advisor, it was possible to obtain a new insight into operations that personally had been dismissed previously; this being that a gender perspective was an essential part of the peace process and a combat (and intelligence) enabler. Gender Advisors play a critical function in providing recommendations on patrol composition, how peacekeepers access and engage with the female population, and ensure military actions do not have an indirect adverse effect on a particular gender. Engagement with 'the other 50%' of the population is critical for two reasons. Firstly, it ensures peacekeepers access to the female population who were, through their obvious vulnerabilities in conflict, an essential indicator and early warning sign to when the security situation was deteriorating. Secondly, it had an essential role in long-term mission success as significant evidence ties a nation's ability to resolve conflict to how women are engaged in the peacemaking process.[19] As such, while the role as Gender Advisor was assigned on the incorrect assumption that only a woman could provide such policy advice, it offered a significant personal and professional learning opportunity.

In closing, when deploying as a G2 on UN operations, there are unique complexities that are not generally encountered on other operations, due to the operating environment, the UN system, training of personnel, a potential absence of clear country lead or standards. Realistic expectations and innovative approaches in tackling the role are required to enhance the mission. However individuals, and the ADF collectively, can make a significant impact on operations, providing trained and professional intelligence staff to the UN. From what was, to date, the ADF's most remote intelligence deployment, I would offer the following takeaways:

Bor Town.

Routine armed robbery outside Bor UN camp.

1. **Remember, it is business, not personal**. Resilience is arguably a necessity to operate in challenging circumstances that mirror neither our doctrine nor at times, our values. Potential dislocation from a larger ADF contingent makes this even more essential.

2. **Keep it simple**. Turn to your basic training and establish simple practices that can be replicated by staff that have no intelligence background, limited English skills and potentially no experience using IT. If an INTLOG or SIGACT tracker cannot be maintained by other G2 staff while you are on leave or after you redeploy, forget about it/simplify further.

3. **Knowledge management is key**. Expect no cogent system for managing information, and no software to support data retrieval. Make knowledge management a priority early, establishing simple ways your staff can find and maintain information, such as: personality 'Baseball cards', town JIPOEs and rolling briefs.

4. **Your team isn't going anywhere, so get your trainer hat on**. Educate your commander and their principle staff on how an intelligence professional can effectively contribute to mission effects, but within limitations. You will have little ability to influence the composition of your team. The chances of your team (particularly at the Sector level) having representation from our standard partner nations is rare. With 12 months the standard length of deployment for most countries, the sooner you can enable your cell, the better the outcome.

5. **Target patrol Commanders; make their patrol report a priority to them**. With a heavy reliance on patrols and Military Liaison Officers to fill your collection requirements, you need to sell the importance of good reporting to the commanders. Simplify requirements, and potentially run tutorials on drafting effective patrol reports.

6. **Remain flexible**. It is difficult to prepare for the various permutations of personnel, expertise, local and UN specific obstacles you may encounter - no deployment experience will be the same. The added overlay of unique and unanticipated roles means flexibility is key to delivering the best effect.

Working with local girls.


Local children.


Engaging with local principal.

SELECTION AND TRAINING IN COMBAT INTELLIGENCE

Major James Ellis-Smith

'I need to be able to trust you. As a combat officer, I am going to listen to what you are saying and know that the next thing I am going to be doing will be to be putting my life and the life of my men on the line executing this. Ultimately I know you aren't going to be next to me when it happens; whether I listen to your advice or not will depend on whether I believe you are as invested in this as I am. I need to believe that you understand what it is that I am going to be doing'

Major Micheal Henderson

The success of intelligence support to operations is defined by its relevance and impact on decision making. Within AUSTINT and in our current training paradigm, the strength of analysis is the only well defined metric of performance. Analysis alone cannot achieve relevance and impact - analysis only enables the combat intelligence officer to *know*. Influence – the ability to directly affect the plans and decisions using that information - is critical. Understanding this cultural dynamic is an important first step in establishing selection processes and training that will better enable AUSTINT to support operations.

Intelligence, Combat and Command Culture

The defining characteristic of combat – and where it is differentiated than any other environment in which intelligence is practiced – is that combat is inherently contested. The decision making process occurs in a deliberate contest between multiple actors seeking to defeat or destroy each other. Decisions

are often made quickly and the ramifications of those decisions are inevitably serious. The realities of combat, and the actions of an enemy force, mean that planners and commanders are often compelled to make decisions and conduct operations, regardless of the input of the intelligence officer. In the absence of sound intelligence, a commander makes the decision based on intuition, experience and tactical assessment as a foundation for assessment of enemy action. Thus, while intelligence (and fundamentally, the intelligence officer) exists to enhance plans and decisions, it must ultimately be accepted that the intelligence staff and function is only essential to *good* plans and decisions.

While some factors that contribute to flawed decisions are inevitable – friction, deception and limited time – other factors are innately preventable - a lack of timely and accurate intelligence, flawed assumptions, and the unconscious bias of commanders and planners. The combat intelligence officer's fundamental role is to continually enhance plans and decisions by challenging and overcoming both the inevitable, and preventable factors; firstly acting as an advocate for the enemy plan, but also inculcating commanders with sounds intelligence that will inform their quick decision making process. The intelligence officer is therefore continually seeking to guide the decisions and plans – both deliberate and rapid - as close to objectively 'right' as possible.

In practice, this means that the combat intelligence officer maintains something of an adversarial relationship with planners and commanders. The combat intelligence officer must not only provide accurate intelligence, but they must also be prepared to continually challenge the decision making process. In addition, the intelligence officer must work to subtly inform and shape command understanding of the threat environment, so that it is inherent to their instinctive assessment of the fight. In this relationship, the challenge for the combat intelligence officer is in both gaining the information necessary to inform the best decision possible, but also using that information – actively working to ensure that it is incorporated into the decision making process at all levels – and on occasion, against resistance. Analysis alone cannot achieve this - analysis only enables the

combat intelligence officer to know. Influence – their ability to directly affect the plans and decisions using that information - is critical.

The adversarial nature of the relationship between intelligence and command can be challenging, and it can be difficult to appreciate the obligation experienced by commanders to make decisions. A common response is to argue that it is a failure of command if plans or decisions are not influenced by sound intelligence. Intelligence staff might argue that their analysis is good, but that the commanders and planners do not appreciate it's value, or that the commander's direction was poor; that the commander is overbearing, obtuse or disinterested, or 'doesn't like intelligence'. Proving 'worth' in combat intelligence is difficult, because the most significant impact of good combat intelligence comes in this continual and innate improvement of plans and decisions. Influence that enhances plans and decisions is intangible. 'Good' intelligence officers can be recognised by commanders and staff, but it remains difficult for either Intelligence staff or commanders to precisely quantify that effect.

Clearly defining what analysis and influence are – and how they are distinct – is therefore critically important.

Analysis

The ability to source, collate and synthesise information, and identify those elements of information that are most reliable, and of the highest utility.

Influence

This incorporates some specific and acquired skills, such as, tactics, knowledge of operational concepts and an understanding of military planning methods - but it is mostly dictated by experiential or innate skills and traits. These include: persuasive and engaging verbal communication, the ability to identify and understand organisational culture, and the ability to generate rapport. Influence can be characterised with three key traits.

Credibility

Being trusted and believed is critical to the military intelligence community and its importance is already reinforced to intelligence trainees. This incorporates a range of personal traits such as bearing, confidence, combat effectiveness, fitness and general military skills.

Authority

This comes from the specific skills and knowledge, taught or accumulated – that convince the commander and planner that the intelligence officer's input to the plan is worthwhile. These include an understanding of the planning and decision making process itself; when planners require specific inputs; and what is possible in plans and operations; in other words an understanding of tactics and operational theory. Authority also requires that the intelligence officer understands their own core role - managing intelligence capabilities, how to task them effectively and where information can be gained.

Rapport

Finally, influence is strongly affected by rapport, which incorporates personal traits, like emotional intelligence: the ability to conform to organisational culture; communication skills, and the general ability to build effective relationships with others, particularly planners and commanders.

Integrating *Influence* in Training and Selection

Influence is a specific trait, developed over time, and is typically aligned with rank as a readily recognised metric of experience and qualifications. Not all individuals have an intuitive capacity for credibility, authority and rapport, but these traits can be selected for through the existing process for course nominations, performance reporting and assessment and enhanced through focussed professional development. The intelligence training and development continuum should be designed

to incrementally expose analysts to influence fundamentals after a period of time consolidating their baseline analytical skills. In the combat intelligence context, this would see initial training focussed on analytical skills, evolving over the course of the analyst's career to increasingly teach and assess tactics, operational concepts, planning, and organisational culture.

As competition for more senior positions increases, a combination of course evaluations, deliberate assessment boards and workplace performance evaluation could be used to select individuals demonstrating influence traits, who would then be promoted. By this stage of selection, all personnel would have been afforded the opportunity to refine or develop influence traits. Those personnel deemed unable to proceed past the established development gateways would reach a terminal rank, but could be retained and employed within specialist roles.

Operational Impacts

Incorporating influence traits in the selection and training process would allow for a re-allocation of scarce resources within the Intelligence capability, and enhanced operational effects. Career management agencies, in consultation with AUSTINT and combat unit stakeholders, should consider appointing more senior, or those subject to specific selection criteria aligned to influence traits, to fill Intelligence roles at the Battle Group level and in Brigade staff, increasing performance expectations of staff in these positions. The intelligence function could then move toward a 'high performance, limited numbers' approach to manning at the tactical level, where intelligence staff are deliberately trained, selected and promoted on the basis of their ability to perform independently, and with limited organic support.

Complementing this, would be more effective use of reach back intelligence support for tactical intelligence operations forward. Efficient manning of tactical intelligence cells would mean that more positions for junior staff could be made available in operational, strategic or 'reach-back' functions, where analysts could be afforded the chance for development, as well as gaining an understanding of the strategic and operational context to tactical actions. These analysts could be utilised more flexibly and could be employed against real time operational requirements, trained and developed in the work place by more senior intelligence staff. This would provide them unique experience that could enhance planning and decision making at the tactical level in future postings.

Conclusion

This paper has sought to outline the fundamentals of command culture and military intelligence practice, and the necessary individual traits required for success across a range of intelligence roles. Specifically, this paper has sought to outline the distinction between analysis and influence as core intelligence traits. In a variety of combinations and proportional balance, analysis and influence are the twin foundations of success in a combat intelligence officer. Understanding this - and making the necessary adjustments selection, training and appointment of intelligence officers - provides a foundation for intelligence and organisational culture that improves the decision making of combat commanders and planners.

WHAT DOES LEADERSHIP LOOK LIKE IN INTELLIGENCE CORPS, AND SHOULD IT BE ANY DIFFERENT TO LEADERSHIP ACROSS THE ARMY?

Major Nichola Doxford

When our Captains are trained to be Company 2ICs and our Majors are trained to be OCs – shouldn't leading small teams be a breeze? This short paper is designed to be informal and get readers to reflect on their own leadership, and how it could be improved.

Intelligence Corps is interesting when compared to the 'standard' Army model of sections, platoons, companies (or squadrons) and battalions (or regiments). The Corps has a traditionally shallow structure, and often operates individually or in cells/ teams which are small in size, large in responsibility, and heavy in rank for their relative size – such as S2 cells and fusion cells. The home unit of the Corps is the Intelligence Battalion, however even there you find small cells and small companies. Ranks from sergeant to lieutenant colonel leading teams of less than 15 people tends to be the norm rather than an anomaly in the Corps.

Another interesting facet of the Corps is the requirement for both officers and soldiers to be able to do the same core job – intelligence analysis and assessment – and sometimes even the same specialist job. This can lead to a dynamic where leaders may get tied up in the 'doing' of the work rather than the direction, control and management of the capability. Other Corps generally don't suffer from this issue as their soldiers have training that the officers don't receive (i.e. an ammo tech being commanded by a RAAOC officer), and thus officers are forced to deal with overall capabilities rather than do the work themselves. Gone are the days

when the officers and SNCOs were by default, the smartest or most skilful person in the room by virtue of rank. Increasing diversity in recruitment, and an increase in education levels in the work force means we have a corps of soldiers with multiple degrees, Masters degrees, PhDs and multiple languages under their belt. But, that doesn't mean that officers and SNCOs are incapable of leading effectively!

Given those two characteristics of the Corps – should leadership be exercised any differently than in the wider Army? I don't think so, and I think we need to go back to leadership basics to understand why, and to identify the areas where every leader in the Corps can do a health check of their own performance.

At the team level, there are three key tasks for leaders and they are: set direction, build the team and manage the team.

Set direction

Two frequent complaints heard within the Corps are: direction is not clearly articulated, or direction changes too frequently. Members of a team need to understand what they are working towards, and why. It is a leader's job to define the **long-term goals of the team**, and to outline the path towards those goals, including delegation of responsibilities between team members, and the timeframe in which the goals needs to be achieved. This requires good communication – preferably verbal followed up by written where appropriate. It also requires regular checks that the team is on the right path, at the right stage and performing at the right level. The achievement of goals assists with building a positive dynamic in a team – more on this later.

Build the team

A good team is one that is maximised in terms of its productivity and interaction. It is a leader's job to ensure that members are considered both from an individual and a team perspective. Individuals need to be understood for their strengths and weaknesses, their background and experience, and their future potential. Understanding individuals does not mean putting the needs of the individual above the needs of the team, but balancing the two and clearly communicating that balance. An individual who is understood and appreciated for what they bring will integrate with a team in a positive manner and improve the team dynamic. A high performing team will have morale and an identity (or *esprit de corps*) that has been built, usually through shared experiences, and the successful achievement of team goals. It is the leader's responsibility to make the opportunities to build the team's dynamic and identity.

Other complaints heard frequently within the Corps are: team members or team leaders change too frequently, and there is no mentoring by leaders. Mentoring is another key activity conducted by a leader which builds the team. Mentoring is knowing the individual, understanding their personal long-term goals, and then guiding them on how to achieve those goals through career choices, positive changes to their behaviours and giving them opportunities to grow. There are both formal and informal ways of doing this, and it is up to the leader and the individual to decide what they prefer.

Manage the team

The last two complaints I intend on addressing are: team leaders aren't planning long-term and are reacting to too many "5m targets", and back-briefs are not occurring.

Management plays a large role in leadership, and it could be said that if you can't manage then you can't lead. Managing a team is inherently interrelated in the two points above, and cannot be done if the leader is busy doing the work of the team. The key tasks of management are planning, organising and controlling. A leader needs to plan the path for the team to achieve their goals, and organise the team in such a way that they get there. They need to provide **direction and control** to the team, clearly and unambiguously. Management involves prioritisation, expectation management, goal-setting, feedback, direction, back-briefs both up and down the chain, resource management (particularly time) and administration. Team leaders are an important conduit between individuals and the organisational leaders, and need to balance requirements of the two. A team leader should know the capability of their team and their limits and convey that to organisational leaders.

These points should not be new to anyone – they are drawn directly from *LWD 0-2 Leadership*. But are we doing them, or are we letting some fall by the wayside? Leaders will vary in quality, no doubt. There are characteristics to great leaders that can't be drawn from doctrine or be taught, particularly things like charisma and emotional intelligence. But the points above are the basics for all leaders. Take five minutes (or more) and critically analyse whether or not you are doing these things as well as you could be. Engage with your team to see whether they have understood the direction of the team. Watch your team and see if you could do anything to help build them up. Do these basics, make some mistakes, learn about yourself and your team, become better leaders for the Corps.

THE GATEWAY TO ANALYSIS

Major Troy E. Mitchell, USMC

From the dawn of time, intelligence professionals and their adversaries have consumed information for analysis from publicly available means, obtaining knowledge and understanding about one another. Effectively navigating the seas of open-sources allows the intelligence professional to better understand physical and human factors in the operational environment to satisfy information and intelligence requirements.

During the reformation of the U.S. intelligence community, the Open Source Office was formed to "ensure efficient and effective use of open-source information and analysis" (Director of National Intelligence, 2006). Yet analysts continue to analyze and produce intelligence on secure and classified systems vice polling open-source information to steer their data mining efforts. As such, analysts lack the knowledge of where to look within the Internet, which results in starting from where they are most comfortable due to time constrained environments, as well as the barriers to exchanging information between the three classified systems.

When data mining, most analysts underestimate the utility of the various academic and government affiliated think-tanks. More times than not, their analysis is equivalent, if not better, than items found on the DSN and DINet. These sites should serve as the starting point for research and data mining prior to navigating classified networks. They provide insight to national strategy and interests enabling a focused effort supporting the intelligence community and military commanders. Quality Open Source research, reaching beyond the reported events via various news agencies, provides a fundamental understanding of why events occur within a given society. Another popular means of receiving

information from these sites are through podcasts. Since many intelligence professionals are auditory learners, this medium of reception may support enhanced comprehension.

As with other intelligence disciplines, OSINT enables a "cueing and redundancy" collection strategy. For example, when transiting to and from work, listening to the "BBC World Service: Global News" podcast could cue the analyst to global security threats, anticipating emerging intelligence priorities in the workplace. This cues the analyst to focus their research, mining relevant news agencies and think-tanks for more detailed analysis. As the analysts poll multiple news sites, social media, think-tanks, etc. on the same topic, they practice redundancy as they are "using several same-discipline assets to

cover the same target" (Ibid). By sourcing multiple sites, the analyst derive an unbiased opinion, and create an assessment defining the crux of the threat characteristics, terrain, weather, and civil consideration.

A conduit grossly under examined is social media. Social media provides a cultural perspective for why and how events unfold, as illustrated during the Arab Spring. These uprisings saw the use of cell phones, social media, and text messaging as organizing tools, along with "cross-pollination among activists in neighboring countries, and the involvement of international media" (Kilcullen, 2013, 32), which highlighted that the world's newly urban populations are highly connected and networked. Similarly, during the Mumbai attacks in 2008, a team of attackers, led by members of the Pakistani Inter-Service Intelligence (ISI), monitored the siege using cell phones to track Twitter feeds, internet reports, and Indian and international news broadcasts (Agrawal et al, 2011, 33-43).

The adoption of video cameras as a weapon of war has been aided by the technological changes that define the Web 2.0 era. The vastness and openness of the YouTube platform defies efforts to control content, which allows the site to have strategic significance in the competition for influence. Abu Musab al-Zarqawi was a proponent of the YouTube war in Iraq, which extended to other affiliates of the Islamic State through lessons learned methodologies. Through this medium, insurgents reach an unprecedented array of audiences with radical messages and intensely anti-western propaganda (Forest, 2009, 30-32). By accessing various forms of violent extremist and other organization's media, intelligence analysts shape a narrative conducive of plausible courses of action, and network analysis affiliated with the entity's capability and capacity.

Al-Shabaab thoroughly exploited Twitter's capabilities during the Westgate Mall attack that occurred on September 21, 2013. Al-Shabaab has utilized the social media website since the entrance of the Kenyan military in southern Somalia in October 2011. However, during the siege, the insurgent group's media department provided a continuous stream of updates and commentary, which revealed how the organization values tweeting, particularly in English, to draw the attention of the world's media outlets (Anzalone, 2013, 3). By generating over 730,000 tweets (Card et al, 2013), Al-Shabaab created a counter-narrative that painted the siege as a response to the greater suffering endured by those inside Somalia. By comparing the proclaimed counter-narrative with the capabilities of the organization, analysts have the opportunity to combine visual and written text to analyze, with trend analysis of the organization over time. Based on previous events by the organization and the current circumstances, analysts can assist planners and decision-makers with plausible outcomes and residual effects associated with dismantling a threatening entity.

One potential conduit of information to enable planning is entities involved in crisis mapping, such as the Harvard Humanitarian Initiative (HHI). The organization launched in 2007 to "examine the impact of crisis mapping, geospatial and crowd sourcing technologies to prepare, mitigate, and respond to emergencies" (Harvard Humanitarian Institute, 2013). Crisis mapping is the real-time gathering, display and analysis of data during a crisis, usually a natural disaster or social/political conflict (violence, elections, etc.) (Crisismappers, 2013). Crisis mapping projects allow large numbers of people, including the public and crisis responders, to contribute information either remotely, or from the site of the crisis to support humanitarian assistance and disaster relief.

Crisis mapping became apparent during the 7.0 magnitude earthquake that struck Port-au-Prince, Haiti in 2010. The destruction caused by the earthquake resulted in collapsed housing and government buildings. As the world raced to support Haiti, there was a gap in data to enable assessing the damage, and planning for a response. Many intelligence analysts fled to classified systems as opposed to the internet to attempt to fill that gap. These analysts did not know where to begin their research, even though CNN continually updated their website. After a large-scale disaster, there is always an effort to collect, analyze and distill critical information required to facilitate humanitarian aid, and while the Haiti disaster became the first time those affected by the disaster issued pleas for assistance through social media and mobile technologies, the solution was crowd-sourced

on social media. Thousands of ordinary citizens mobilized to aggregate, translate, and plot these pleas on maps, and to organize technical efforts to support the disaster response. In one case, hundreds of geospatial information systems experts used fresh satellite imagery to rebuild missing maps of Haiti, and to plot a picture of the changed reality on the ground. This work—done through OpenStreetMap—became an essential element of the response, providing much of the street-level mapping data that was used for logistics and camp management (Chan & Crowley, 2011, 8). Through understanding where to focus and what tools and applications are available to all-source analysts, the productivity of intelligence production enabling operations substantially increases governmental response efforts leading to opportunities of achieving effects driven operations in compressed contingency response efforts.

OSINT serves as an effective tool if the collection managers and analysts creatively utilize the asset to enable analysis and production. By commencing analytical products on the DRN, analysts have the ability to disseminate and share products to various first responders and non-governmental organizations. By merging academic databases and government affiliated think-tanks, analysts deepen their knowledge, providing a solid foundation for analyzing alarming events. The answers are not always on classified domains, but these domains should serve to augment the analytical research that was sparked via intelligence collaborated classified production efforts.

Major Troy E. Mitchell, USMC is the J2 Exchange Officer at the Amphibious Task Group. Major Mitchell possesses a Doctorate in Strategic Security. He has served as a reconnaissance and intelligence officer on multiple ARG/MEUs and combat theaters.

The appendices to this paper are available from the HOC Cell (AUSTINT) SharePoint site located on the DRN. http://drnet/Army/AUSTINT/Pages/Welcome.aspx

REFERENCES

Agrawal, M., Oh, O., & Rao, H. (2011, Sepember). Information Control and Terrorism: Tracking the Mumbai Terrorist Attack through Twitter. *Information Systems Frontiers*, 13, 33-43.

Anzalone, C. (2013, October). The Nairobi Attack and Al-Shabab's Media Strategy. *The Sentinel*, 6(10), 1-6.

Card, B., MacKinnon, J., & Meier, P. (2013, November 18). #Westgate Tweets: A Detailed Study in Information Forensics. Harvard Humanitarian Institute. Retrieved from http://irevolution.files.wordpress.com/2013/11/westgate-analysis-in-info-forensics.pdf

Chan, J. & Crowley, J. (2011). Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies. Harvard Humanitarian Institute. Retrieved from http://hhi.harvard.edu/sites/default/files/publications/publications%20-%20crisis%20mapping%20-%20disaster%202.0.pdf

Citrenbaum, G. & Hall, M. (2012). *Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments*. Santa Barbara: Praeger Security International.

Crisismappers (2013). What is crisis mapping? Retrieved from http://crisismappers.net

Director of National Intelligence. (2006, July 11). *Intelligence Community Directive Number 301: National Open Source Enterprise*. Office of the Director of National Intelligence. Retrieved from https://www.fas.org/irp/dni/icd/icd-301.pdf

Forest, J. (2012). *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas*. Westport: Praeger Security International.

Gray, A. (1988). Global Intelligence Challenges in the 1990's. *American Intelligence Journal*, Winter 1989-1990, 37-41. Retrieved from http://oss.net/dynamaster/file_archive/041103/e0bf2d-2f6a4730a0845a01de675660f5/USMC-1993 07%20General%20Al%20Gray%20on%20Global%20Intelligence%20Challenges.pdf

Harvard Humanitarian Institute (2013). Crisis Mapping and Early Warning. Retrieved from http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning

Joint Chief of Staff. (2007, June 22). *Joint Publication 2-0: Joint Intelligence*. Department of Defense, B-5—B-6.

Kilcullen, D. (2013). *Out of the Mountains: The Coming Age of the Urban Guerilla*. New York: Oxford University Press.

United States Marine Corps (2004, July 30). MCWP 2-2: MAGTF Intelligence Collection. Department of Defense.

DEFICIENCIES IN IET TRAINING WHEN WORKING IN THE COMBAT BRIGADE

Corporal Nathan McGowan

This essay is written to provide an understanding of the differences between what is taught at the Defence Force School of Intelligence, and how it relates to the work completed in a Combat Brigade Intelligence Cell, in particular during the 2017 Joint Land Series – or 'Road to Hamel'.

I completed my intelligence Initial Employment Training (IET) course in June 2016 and Subject 4 for Corporal in November 2016. Since graduation, I have worked in the HQ 3rd Brigade S2 Cell, and in 2017 supported Exercises Preliminary Brolga, Carbon Brolga, Silicon Brolga, Brolga Strike and Exercise Talisman Sabre. Based on this experience, I believe there are three main deficiencies in the IET training program that create significant gaps in the Combat Brigade S2 Cell. These are: understanding ISR, writing INTREPS/INTSUMS, and the way we are taught to make assessments.

Understanding ISR

There are no formal lessons on the IET course that teach intelligence analysts how to conduct ISR, or maintain an ISR matrix. The ISR component is only taught on the Subject 4 for Corporal course. Understanding ISR is a key component of the

combat intelligence analyst's role, particularly if they are working in the S25 cell. During IET course, the extent of ISR planning taught was limited to NAI and TAI development as a part of the IPB process. We were not taught where and how the NAI/TAI fitted into the conduct of operations or linked back to further IPB. The main function of the S25 is focussed on IPB and ISR planning. This leaves a deficiency in trainees being posted to combat units who require a great deal of extra training in order to enable the S25 function in the field environment.

The requirement for ISR training for IET graduates is critical in enabling the intelligence analysts to interact with and support the planning staff. However, due to the lack of skills provided during basic training, intelligence analysts posted to a combat unit are under-skilled and struggle to assist in the development of the ISR plan. Education on ADF ISR assets was not adequately provided through IETs and meant the junior analysts who work as part of a brigade planning team are unable to provide timely and effective advice when requested. The knowledge some intelligence analysts have developed is based on incidental learning from discussions with senior intelligence staff, and the time dedicated by liaison officers from specific capabilities.

There needs to be an ISR component taught during the IET course in order to effectively prepare analysts for marching into their unit, especially a Combat Brigade. Without this training, analysts struggle to provide the required support to their unit's S25 cell, particularly when there are manning pressures across the Brigade's intelligence staff.

Report Writing

The lessons regarding INTSUMs and INTREPs taught at DFSI are also not entirely relevant to the role of a combat intelligence analyst. At DFSI, too much focus is placed on the formatting and grammar within the reports, and whilst this is important for products made up and circulated in barracks, it is not ideal in a foundation warfighting environment. The INTREPs we utilised on exercise were intended to be a bottom line up front (BLUF) report: using the format of 'At,

At, What? So What? What Next?'. However, at DFSI this format was never taught, even though it is pertinent to an analyst's role in the combat intelligence environment. This abridged format places a greater focus on assessment rather than facts which is another aspect that was lacking in the lessons on report writing during the IET course.

Assessment Development

Whilst assessments are taught and critiqued at DFSI, they are not done so in a way that helps analysts prepare effectively for the workplace. Most analysts straight out of IETs have to learn on exercise, and whilst this is the way of the army, these assessments, if incorrect, negatively affect the Brigade's operations, and the cohesion and productiveness of the S2 cell. Based on what I learned on the 2017 Joint Land Series, I believe more time should be focused on improving assessments within the school environment where mistakes can be corrected without consequence. Intelligence assessments in support of Brigade operations need to be timely, accurate and succinct in order to enable rapid communication across the digital mediums they are transmitted on.

Lessons regarding writing of the INTSUM should also include a greater emphasis on the collation of reporting, the identification of patterns, and whether the information is trending towards an assessed course of action, or a change in the battlespace that is not consistent with previous assessments. Again, there is too much emphasis placed on proper formatting and grammar instead of understanding and analysing the information received and relating that to the previous assessments made as part of the IPB.

On the IET course, the focus of assessments was based on a 'what has happened'. This teaching looks at 'what' has happened, then 'how' it has happened, but not really 'why' it happened. This way sees an intelligence analyst look purely at the micro event in their initial assessment instead of situating the event as part of the wider picture. This has the potential to send an analyst down the wrong track. During my time at 3 Bde we have been taught to reverse the assessment process and start with 'why' the event/activity has occurred to better understand the 'what' and 'how'. This process allows you to rapidly understand the event in context, and most importantly, to have a solid understanding of the 'what next?'. On IET course we were also taught to obscure the source of the reporting by using terms like 'secret reporting indicates'. This does not work in the Combat Brigade as commanders like to have faith in the source of information. I found that by starting with the specific source, and the date/time of the report, commanders and staff had greater faith in both the reporting and my assessments.

In conclusion, based on my experience on the 2017 Joint Land Series, I have found that intelligence analysts feel under-skilled when they are posted to a combat unit if they have not conducted the Subject 4 for Corporal immediately after completion of the IET course. This is due to the ISR component being left of the IET course. Having the ISR phase moved back into the IET course, subsequent to the IPB lessons, will allow trainees to be able to have a sound understanding of the collection phase of the intelligence cycle, and how it fits in as part of the IPB. It will also assist analysts to work in the S25 cell without requiring re-training or continuous guidance. Furthermore, combat intelligence analysts find it hard to effectively generate INTREPs and INTSUMs due to teaching being limited to formatting and grammar. The lessons on how to make assessment are explained only briefly and do not relate well to how analysts should conduct their assessments in the workplace, specifically in a combat intelligence role.

THE EMPLOYMENT OF DIGITAL SYSTEMS IN SUPPORT OF THE S2 FUNCTION IN FOUNDATION WARFIGHTING

Lance Corporal Peter Herd, Sergeant Lauren Thurlow and Corporal Katie Twomey

An effective technological system that communicates across all levels of command is imperative to providing effective intelligence support and information sharing capabilities in support of Joint Land Combat. This was highlighted during the 3 Brigade readying phase, in particular, during EX TALISMAN SABRE 2017. This essay will outline the advantages of digital systems in enabling an effective intelligence sharing capability, and also the challenges faced when technology fails to fulfil this core function. This essay will highlight the issues of the digital age in supporting the intelligence function, as well as to recommend means and methods to counter these problems for future exercises and operations.

The advantages of increased technology usage in intelligence processes are vast. The current digital system used is the Battlespace Management System (BMS), which is an excellent tool for enabling the operator access to a vast range of analytical functions. These functions include the ability to rapidly plot enemy actions to accurate grid references and measure weapon ranges to form assessments on likely anticipated enemy dispositions. The distance measurement tools are particularly useful in quickly determining the range of enemy weapon systems from own troops to provide early warning to commanders. The program also enables 3D imagery (MCOO) to provide an understanding of the terrain to aid in the

development of COAs. This makes it an effective tool in forming assessments on possible enemy defensive positions, as well as artillery positions, ambush locations, observation posts, engagement areas and withdrawal routes. The program also enables multiple maps to be loaded so the operator can view the terrain in depth.

However, a shortfall identified in the program is that maps must be loaded prior to deployment. Once deployed, there are difficulties in uploading additional maps, limiting the capacity for a greater

understanding of the terrain. This example was experienced during EX TALISMAN SABRE 17, when commanders requested further maps in specific areas to be uploaded, which was not possible. A similar situation was experienced with the overlay function. The system allows for separate overlays to be constructed and edited in an isolated fashion that can be later introduced, allowing the users to have a greater geospatial appreciation of an asset and its function within the battlespace. This is particularly useful when a new element is introduced or separate hypothesis require to be constructed in order to support situational awareness, targeting or the planning function. During EX TALISMAN SABRE 17, due to the vast number of consoles logged onto BMS, the system should not have supported more than 20 overlays, but was at one point operating more than 32. This significantly undermined system performance, and led to 'crashes' at inopportune times. Even though the S2 cell was allocated eight overlays even this restricted the Headquarters in its ability to graphically represent several incidents, threats and opportunities as well as the ISR plan, enemy COAs etc. The program is an effective analytical tool; however, as with every technological system, there are shortfalls that come with the advantages.

The program has potential to be an effective communication sharing system to provide early warning to Battlegroups and to disseminate information. However, in its current form, the program does not have a message function suitable for distributing information as required by Intelligence Analysts. This problem includes the restricted size of the message, the need for an appropriate and consistent delivery time, and a simple and effective notification of receipt or acknowledgement service. Although there are multiple ways to send messages, many of these have limitations on the amount of characters, and the priority given to the message's transmission. Although some messaging options were more expedient than others, the amount of detail able to be conveyed was limited. As a result,

the analyst was forced to abbreviate messages, often relaying only the most pertinent information and assessment rather than additional factual detail. Conversely, the message functions that have more characters were slow in passing through the system traffic, which was unsuitable for relaying important information. It is imperative that a system is developed which enables the wide distribution of detailed messages quickly, to inform commanders of situation updates. Until this time, analysts will be limited in their capacity to conduct their intended role to the standard required.

Throughout the majority of EX TALISMAN SABRE 2017, the Brigade intelligence cells encountered connectivity issues with the digital information sharing system. As a result, this stalled effective communication to and from the Battlegroups, delaying the provision of analysis of the battlespace. To mitigate the disruption in communications, the intelligence watchkeepers were forced to ensure that messages were relayed via alternate means, which in itself was problematic, as each Battlegroup communicated through different means. This resulted in Intelligence staff sending messages through multiple means, and often without certainty that messages were even successfully reaching the Battlegroups. Additionally, the different communication methods were often operational at different times, forcing the analysts to attempt to distribute messages using up to four/five different means. This created significant duplication of effort and inefficiency for the watchkeeper. Instead of being able to focus on understanding the threat picture to enable staff planning, the Intelligence cell was consumed with relaying messages to the Battlegroups multiple times over to ensure that situational awareness was maintained across the Brigade. This activity was long and cumbersome in an environment that is often time sensitive. On EX TALISMAN SABRE 17, the communication between the S2 and S6 function was frequent. The messaging problem was related to the number of consoles utilising the BMS and as a result, many other avenues were investigated to effectively communicate across the Battlespace.

Once messages are received at a console a window appears on the screen, notifying the user of the message. This function is excellent to immediately inform the operator. However, if the operator is conducting a time sensitive task, or closes that window for other reasons, the message is filed away in a over complicated message filing system which can be difficult to find at a later stage, and can lead to messages getting lost. The multiple options to handle the messages can also be confusing to infrequent users, leading to messages being mishandled. The message alert function is very useful to inform the user of 'unhandled' information; however, upon raising messages again, the user is limited to reading one line of the message, which can be frustrating to operators.

The other tools we utilised included the internal Mission Secret Network communication or 'chat' program called "Transverse". The display constitutes single or a series of windows, each presenting a different chat room. Each message is conveyed with its time and the sender's callsign, followed by the intended message. This enables multiple chat rooms to be established with immediate communications between multiple users. During EX TALISMAN SABRE 17, this function was excellent as the S2 cell could receive up to date dialogue and interact when required. This was particularly useful during live feeds from UAS platforms conducting ISR, enabling up to date information as well as the ability for the S2 Cell to interact with the operators of the asset.

We also employed the digital message system enabled through High Frequency means called 'TAC chat'. This system is a laptop console connected to an AN/PRC 150 and displays a simple text window showing the time of a message and its intended recipient. This is a very simple system that is easy to use with minimal training, and produces clear error messages when communications are interrupted or not received. This style of system is similar to Transverse and it would be ideal if it could be operated in a similar manner, and combined into one system, reducing the number of consoles that an operator is required to monitor.

Despite the obvious problems and frustrations resulting from the duplicated efforts, there were benefits to the issues faced by the intelligence cell. The disruption to message traffic forced the Intelligence Cell to be adaptable in their processes and to seek ways in which to overcome these problems to enable the continuation of timely intelligence to support the Brigade. When enemy

tracks failed to synchronise across terminals, the cell was forced to rely on the hard copy maps and talc overlays we had maintained. Additionally, due to the constraints of physical space inside the vehicle which restricted analysts from sharing computer terminals, handwritten logs to used to manage the data from enemy SIGACTS. Despite this return to 'old school' methods, the Intelligence cell was able to constantly monitor the enemy situation and maintain situational awareness when technology failed.

A vital lesson can be learned from this experience. In an age of continuous technological advancement, there is the risk of over reliance on technology to provide us the skills and means to manage information and intelligence. Regardless of the vast capabilities that technology is able to provide, we must be prepared for when these systems fail. This means being adaptable in applying our core skills using hard copy maps, pens, and whatever tools we can rapidly develop to make the intelligence processes as fast as possible. Ingrained knowledge of the operational area, weapon systems, the terrain and the enemy strengths and weakness are undoubtedly the best means of overcoming these problems when technology fails. The more we know about our enemy and the operational environment without resorting to notes or historical data, the more quickly we can form assessments of future enemy intentions.

The use of technology to disseminate information also does not negate the importance of face to face communication between the Brigade HQ staff. BMS was employed by 3 Brigade during EX TALISMAN SABRE 17 and has proved itself as a useful tool for battle tracking and providing basic situational awareness on the current operational picture. However, clear and frequent face to face communication between Intelligence and Operations staff is imperative to interpret the battlespace and what it means overall, linking the tactical, operational and strategic reporting through graphical representations. Without frequent dialogue to discuss historical data and the current threat picture, the ability to form accurate assessments of future enemy intentions cannot be successfully achieved. Intelligence Analysts must establish good relationships and maintain frequent discussions with Operations and BOS experts to ensure that the most accurate assessments can be developed.

The digital age in which we live is constantly changing with advancements in technology and communication means, both inside the military and in the civilian world. Although technology provides the potential tools to make intelligence processes easier, it is no substitute for core intelligence skills and an in-depth knowledge and understanding of the enemy. Even though we can develop multiple systems to communicate, there is a limit to the number of problem solving plains that a human being can operate on at once. If a simple to operate, communication interface can be developed, the Intelligence Analyst will have more time at their disposal for in-depth and accurate analysis.

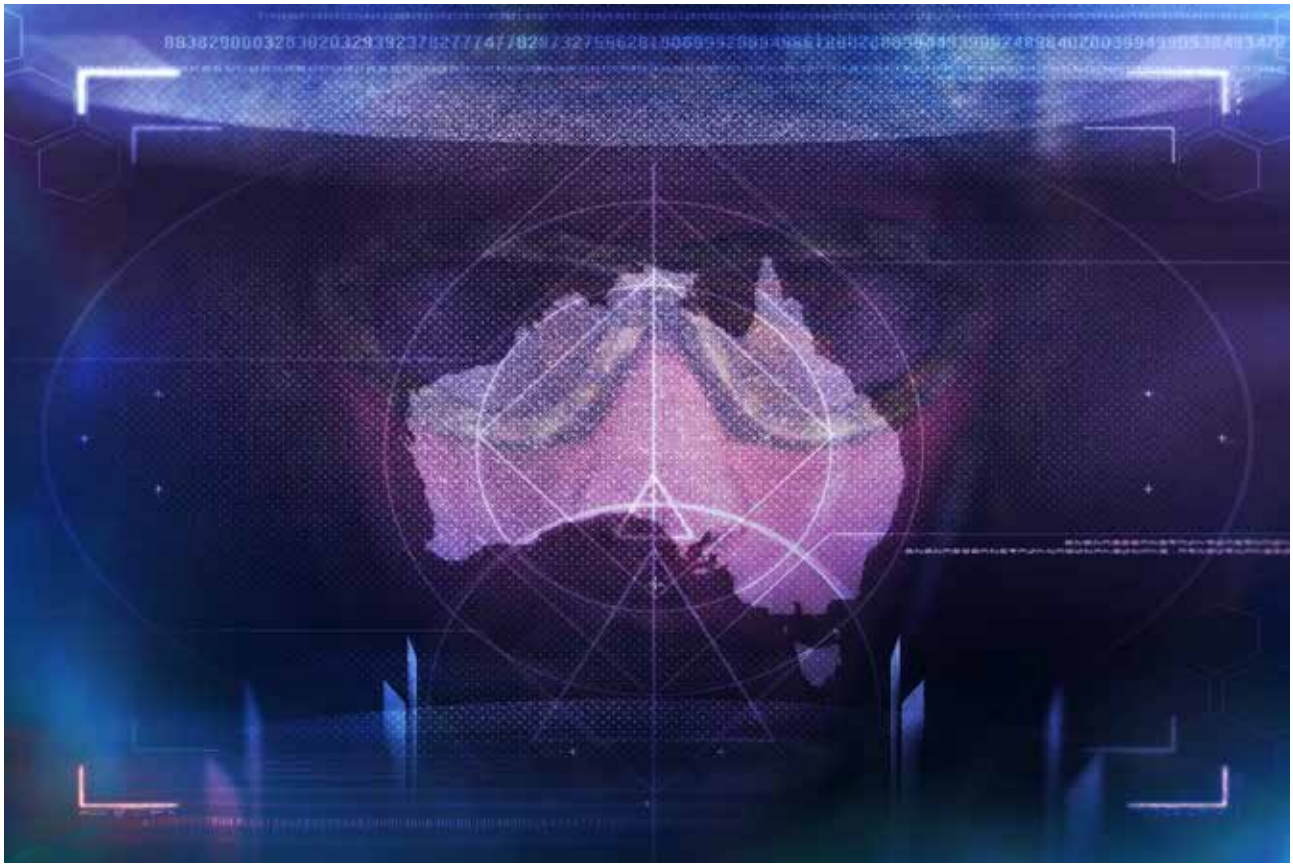
Despite all of the advantages technology and ICT systems has to offer, Intelligence Analysts must be prepared to use hard copy maps and tangible resources to support operations in the event that technology fails. Our reliance on technology to think for us reinforces the need to practice intelligence processes without technology, so we remain capable of providing intelligence support when we are denied access to technological systems. Similarly, we must maintain face to face communication to uphold effective working relationships and to ensure that the greatest situational awareness of the operational environment is shared.

In short, technology is great when it works. When it fails, go old school!.

AUSTRALIAN INTELLIGENCE CORPS: COORDINATING TECHNOLOGICAL REQUIREMENTS

Lieutenant Colonel Arran Hassell

In a world in which approximately 3.7Bn people – of the estimated 7.5Bn global population (49.6%) – are internet users[1] (2.8Bn people (37%) are Social Media Users)[2] ; nano, robotic and computer technologies are exponentially improving every year[3]; and the largest global militaries are considering how to incorporate artificial intelligence into their warfighting functions, we need to seriously ask ourselves: does the Australian Intelligence Corps (AUSTINT) have the technology (collection, analysis and dissemination tools), manning structures, employment specifications, training and processes it needs to



[1] Internet World Stats, World Internet Usage and Population Statistics, www.internetworldstats.com/stats.htm, 25 Mar 2017

[2] Smart Insights, Global Social Media Research Summary 2017, www.smartinsights.com/social-media-marketing/social-media-strategy/new-blobal-social-media-research/, 27 Apr 2017

[3] The Emerging Future, Human Intuitive Perspective of Technological Advancement in Fifty Years, www.theemergingfuture.com/speed-technological-advancement.htm

operate in this information rich environment that is the modern battlespace? Arguably, it does not.

After 18 years of continual operations, AUSTINT Corps still does not have access to fundamental computing tools such as a common and standarised data repository. We do not have automated tools that can access data from all Defence data repositories for use by analysts in disparate locations. We don't have advanced analytic tools that make sense of large volumes of data. We don't have standardised and centralised training on data input and data retrieval in and out of common data repositories. We do not have TS connectivity at all levels of command across Army, let alone a common TS video-teleconferencing capability. We don't have social media exploitation tools. We have not fully developed processes, nor a training regime, for tracking, reporting and managing red forces on battle management systems. We don't have a concept for how we will contribute to Intelligence Mission Data required for modern Defence capabilities. This is to say nothing of how we could use artificial intelligence in the collection and processing of information. Whilst many individuals in AHQ and units are developing solutions to many of these technology issues, AUSTINT Corps does not have a coordinated Corps plan for technology remediation that would range from acquisition through usage in units, to training and changes to employment specifications.

Since 2015, the Australian Intelligence Corps' leadership's main collective focus has appropriately been on remediating our Corps' shortage of personnel. Hollowness remains an ongoing issue of importance, requiring final resolution; however, much has been done much to address this and cultural concerns to a point whereby our Corps leaders may soon be in a position to refocus their collective attention to the next issue of collective concern. I would proffer that the next issue of concern is our technology needs. Like the Corps hollowness issue, this issue would benefit from a whole of capability approach; whereby Corps leadership gains an understanding of the need, prioritises capability requirements, understands the risks and proactively and collectively moves towards holistic solutions.

Acknowledging that money and personnel are finite, prioritising expenditure and staff effort become important. The key three technology related areas that I consider require immediate attention above all others (in priority order) for our analytic/all source capability (our base line capability) are: a common

data repository, advanced analytics tools, and social media exploitation software. These three items are commercially available now. Our analysts need these tools now. This, of course, is a simplistic view, not blurred by the realities of acquisition cycles, foreign military sales hurdles, contract negotiations, or staff work requirements.

However, as a Corps there are things we can all do to better enable faster acquisition of such capabilities. We need to better understand and accept risk. As a Corps and as individuals, we often want the perfect solution and are ready to critique concepts and equipment if it is not exactly what we think we need. With technology developing and changing rapidly, the moment we think we know what we need is the moment that available technologies change and are no longer exactly what we think we need, so we don't progress purchases. We need to accept risk in accepting products which are not top of the line but do the vast majority of what we need from the tool. When looking at data repositories and advanced analytics for example, the US Department of Defence's Distributed Common Ground System (DCGS), Palantir's Metropolis, and Northrop Grumman's eCore all offer advanced analytic tools and limited data repositories that would meet our Corps' needs. However, none of these systems are perfect and we have focused on testing them to try to get a system that meets our detailed requirements. I would suggest that we can no longer afford to spend additional time in attempting to purchase the perfect tool. We need to risk money and risk a perfect outcome so that at least we have a tool, even if it is not the tool that can do everything, exactly as we want. An imperfect tool is better than no tool at all; our current situation. Additionally, our personnel will make any tool work. If the tools don't work to our requirements then we can seek industry modifications. We can no longer leave our analysts without these fundamental tools; it would be akin to having infantry soldiers without rifles and body armour.

Gaining the hardware and software we need is only part of the challenge. When we gain a data repository, there will be a requirement to input and retrieve data into and out of the repository on an ongoing basis. We will need a dedicated element of the intelligence staff responsible for data management. In a deployed or domestic all source cell looking at live issues, data management will be a full-time job. We will therefore need to review our employment specifications and our training of our soldiers to incorporate data management as a principle task. Similarly, we need to develop a common approach for data management of threat capabilities on battle management systems. We need to develop a standardised procedure for how our Corps manages the threat picture, and who within the Corps is responsible for the threat Common Operating Picture management. Finally, we then need to incorporate these skills into foundation training.

The three greatest procedural challenges related to technological advances that I consider we face and need Corps coordination are: structuring our workforce and amending employment specifications to specify who is responsible within the intelligence cell for the management of data; developing common procedures for the management of data and data repositories as well as threat pictures on battle management systems; and training our workforce to make them more capable of storing, accessing, understanding, analysing and managing all data at their disposal.

With or without this technology, our people will continue to product excellent intelligence to help commanders understand the battlespace and ultimately win. However, our people will be more effective if enabled with better computing and technology-based tools, as well as employment specifications, procedures and training required to operate these tools. A centralised Corps plan would enable consistency across disparate corps elements and ensure we are keeping up with technological advances, worlds best practice and commanders' requirements. This is our Corps' next greatest collective challenge. If we are to continue our Corp' successes in the coming years, we need to undertake a technological advance as a collective, working together to get the best outcome for our Corps and Army.

COMBAT COUNTERINTELLIGENCE: REGAINING THE INITIATIVE

Captain Gerard Hinchliffe

I have no means of ascertaining the truth.

Robert E. Lee [1]

Introduction

Defining the current role of counterintelligence (CI) in the Australian Army's combat operations is a difficult task. The practice of CI by the Australian Army is often 'templated' and passive in nature, offering basic protection of friendly force information for the relevant commander. Less consideration is given to the offensive opportunities against threat intelligence collection assets and so the priority of intelligence staff work is quickly passed to other requirements. Effective combat CI should seek to undermine the threat intelligence cycle, finding ways to confuse and delay the threat commander and their intelligence staff. Effective combat CI must also understand the vulnerabilities of the threat intelligence system and subsequently coordinate friendly operational effects to target these weaknesses. The Australian Army already holds the means to conduct combat CI and with adjustments to tactics and mindsets, CI operations can be conducted in a more proactive manner.

This brief essay aims to discuss the current and potential role of combat CI within the Australian Army. Firstly, observations will be drawn on the current condition of combat CI, followed by a review of current CI doctrine. This examination will demonstrate the need for clear procedures to conduct effective combat CI. Finally, an alignment of combat CI elements will be suggested to demonstrate the potential future for CI in the Australian Army. Overall, this essay will advocate an adjustment in the way the Australian Army currently practices CI and the conceivable benefits that would arise from a review of current combat CI procedures.

[1] Lee, R. in Lathrop, C. 2004, The Literary Spy, Yale University Press, New Haven

Opining Combat CI

The current state of CI in the Australian Army stems from an identity crisis at the tactical level where it is observed as passive or defensive measures drawn from the CI estimate. A combined effort between the intelligence cell and the information operations (IO) officer, CI is often viewed as an administrative task or staff duty conducted solely at the start of an operation – not a key analytical task to support operational planning. Current practice is derived from a lack of understanding for the need of specific CI planning and analysis to target the threat intelligence system.

The confusion over CI lies partly with AUSTINT personnel. Preliminary training in CI often focuses solely on the CI estimate and the role of CI in protecting friendly force information. Further study in the area is relegated to on-the-job training and experience gained within combat units or formations. If the mindset from initial or basic training is not changed through experience in these tactical organisations, AUSTINT members are likely to continue applying CI solely in its defensive form.

Compounding this situation is the fact that most defence and military commentary focuses on strategic level or civilian CI activities. Anecdotes on espionage and static surveillance during the Cold War fill many CI pieces in academic writing. Combat CI is also discussed little within AUSTINT, let alone within the Australian Army or Australian Defence Force (ADF). CI is not only required at the tactical level, it is critical to protecting the entire intelligence collection chain from the ground up. Most other armies understand this and the lack of a centralised CI capability in the Australian Army is testament to this fact. The opportunity to affect adversary intelligence operations whilst protecting our own is routinely missed due to the existing patchwork of non-specific CI training, procedures and practice. The first step to remedying this situation lies in the identification and definition of combat CI for Australian Army operations.

Defining Combat CI

The keystone doctrine for ADF counterintelligence, *ADDP 2.1 Counterintelligence*, (ADDP 2.1) succinctly defines CI as '*activities that identify, assess, monitor and counter the threat posed by hostile intelligence collection*' [2]. The separate concepts of security, field security and security intelligence are also defined to highlight the difference between CI (identification and countering intelligence threats) and security (countering overall threat activities). The concept of CI is also broken down to highlight the various offensive and defensive CI measures available to ADF elements. The non-exhaustive list of tasks provides a greater understanding of the spectrum of CI measures potentially available in planning and conducting ADF tactical operations. Tasks ranging from blocking (physical locks and handling procedures) [3] and destruction (physically destroying an enemy intelligence asset) [4] draw upon manoeuvre task verbs to achieve corresponding CI effects in the intelligence environment.

As the overarching ADF document on CI, the ADDP 2.1 does not provide extensive detail on practice, leaving the implementation of combat CI to the respective services. Currently, combat counterintelligence measures are scattered across several publications in Australian Army doctrine, the most recognisable being *LWP-G 3-2-2 Deception*. There is no central combat CI publication for the Australian Army, though one is in the process of being drafted. The most coherent guidance on

[2] *Australian Defence Doctrine Publication 2.1 Counterintelligence, 2nd edition*, page 1-2, para 1.7.
[3] *Australian Defence Doctrine Publication 2.1 Counterintelligence, 2nd edition*, page 1-4, para 1.19(d).
[4] *Australian Defence Doctrine Publication 2.1 Counterintelligence, 2nd edition*, page 1-4, para 1.19(l).

CI in Australian Army doctrine is found in *LWD 2-1 Intelligence Staff Duties* (LWD 2-1). In this publication, Australian Army CI is defined as '*a series of synchronised activities across the battlespace… designed to protect essential friendly force information through the disruption, degradation and denial of adversary ISR* (intelligence, surveillance and reconnaissance) *systems*' [5]. This sufficiently aligns with ADF CI doctrine but the LWD 2-1 is similarly not a procedural publication and details to implement CI at the tactical level are not provided.

This situation goes some way to explaining why there is confusion on CI in the tactical sphere; whilst the overarching term is defined, the activities and procedures that constitute CI specific to the Australian Army remain vague. Ownership over the planning and execution of individual activities needs to be clearly defined to ensure they are conducted and coordinated effectively. The contemporary operating environment facing the Australian Army requires combat CI to be assessed in terms of tactical effects available to a commander. Boilerplate CI estimates to conduct offensive and defensive combat CI will not sufficiently deter the intelligence collection threat presented by a smart and adaptive enemy. To achieve more efficient targeting of these threat intelligence systems, the capability of Australian Army CI assets need to be coordinated accordingly.

Designing CI

The ADF requires its constituent services to conduct CI to '*counter threats through offensive measures aimed at reducing the threat and defensive measures to reduce vulnerability to the threat*' [6] . To that end, the Australian Army depends on intelligence cells to create CI products from analysis conducted during the intelligence preparation of the battlespace (IPB) process. Familiar outputs such as courses of action, situation templates and named areas of interest (NAIs) can be analysed with respect to CI. NAIs over people, places and information systems identify inputs for the CI estimate and plan. In order to generate CI effects, the relevant S2X or J2X is critical in advocating for the effect, asset and coordination

of effort. In turn, the CI plan can be 'operationalised' when assets are ordered tasks to achieve the required CI effects.

The assets that may be involved are varied as the effects discussed earlier and can be applied in both kinetic and non-kinetic manners. The effects of 'inoculate' or 'educate' may be provided by military police or intelligence staff briefings prior to deployments or when establishing secure facilities. The effects of 'degrade' or 'deceive' may be achieved by light electronic warfare teams reducing reconnaissance communication nets or providing false information on friendly force sizes or locations. The effect of 'destroy' may be achieved by the kinetic engagement of threat ISR assets such as mounted reconnaissance or unmanned aerial vehicles (UAVs). The overall affect of such measures is that both the quantity and quality of information collected by threat ISR systems will be influenced or limited - to the detriment of the threat commander's decision-making process.

These examples demonstrate that defensive CI operations will mainly require the efforts of intelligence and security cells but offensive CI operations will need the efforts of electronic warfare assets, ISR platforms and strike capabilities to target the passage and quality of information delivered to the threat intelligence commander. The tactical assets mentioned above exist within the Australian Army order of battle and are growing in capability. The 2016 Defence White Paper makes clear the need for greater ISR capabilities within the Australian Army and looks to procure, amongst others, armed medium-altitude UAVs to potentially expedite the

[5] *Land Warfare Doctrine 2-1 Intelligence Staff Duties 2013,* page 6-1.

[6] *Australian Defence Doctrine Publication 2.1 Counterintelligence, 2nd edition,* page 1-3, para 1.15.

detection and engagement of potential targets [7]. Of note, however, is that these assets are rarely perceived in terms of combat CI. The employment of these assets for CI purposes relies on the development of a wider combat CI mindset amongst planning and operations staff. The implementation of both defensive and offensive CI measures actions using ISR, C2 and manoeuvre elements requires liaison between the S2X/J2X and operations officers, especially when managing the use of ever-scarce assets.

Aligning CI

Aligning the doctrine, methods and assets used to conduct combat CI is not a simple task. Neither is it insurmountable. Firstly, aligning Australian Army counterintelligence doctrine with the ADDP 2.1 would be beneficial to not only Army knowledge and training but to interoperability with other services. The recent update of the *LWP-G 2-2 Intelligence Surveillance and Reconnaissance* and its nesting within the wider ADDP framework provides a working example of how Australian Army ISR fits into the wider ADF ISR effort. Future Australian Army CI doctrine must do the same and demonstrate how the Australian Army CI plan can assist the wider ADF CI effort outlined in ADDP 2.1. Without this guidance, CI efforts at the tactical level may be created in isolation and be potentially detrimental to the conduct of joint operations.

Secondly, there needs to be greater ownership of the combat CI process within the relevant staff. The brigade must implement the CI plans developed by joint or divisional headquarters and provide clear direction through to the respective battalions and companies. Manning constraints will always play their part in the allocation of tasks but the role of CI must be given greater consideration when forming a headquarters. CI estimates must be more proactive in identifying the offensive measures available to friendly forces and intelligence staff need to become more cognisant of the employment requirements of friendly assets to conduct CI activities.

Finally, there needs to be a greater acceptance and awareness of operations staff to the need to conduct offensive combat CI activities. If combat CI measures remain purely as intelligence actions, there will be limited ability to conduct such operations. If operations staff are involved early in the planning cycle and the severity of the threat outlined clearly, the fusion of intelligence and operations planning will be able to conduct effective CI activities. This effort can also be extended to the training environment. As Australian Army training at the battlegroup and brigade level increasingly involves RAAF and RAN personnel, counterintelligence efforts can be aligned and honed during key training activities throughout the training calendar. This is critical in the ISR effort where assets from all three services can provide valuable information in both the planning and operation of CI activities.

Conclusion

Since its inception, the Australian Army has been deployed to locations exposed to the intelligence operations of foreign services. Even when conducting activities in Australia, there will be threats that seek to learn any or all aspects of Australian Army combat operations. The ability and effectiveness of the Australian Army to oppose these intelligence and operational threats is dependent on the alignment of common doctrine, thorough CI estimates, creative planning, and efficient operations.

The recent collection trends identified in popular military commentary on 'hybrid warfare' or 'gray zone conflict' clearly demonstrate the flexibility and adaptability of adversary intelligence collectors within current conflict zones. To maintain combat effectiveness, the Australian Army needs to train to counter the type of intelligence threats it faces on the modern battlefield. Properly aligned combat CI activities will not only create more effective combat plans for manoeuvre elements but better protected plans for the entire operational force. The ability to confront and engage intelligence threats is already in the grasp of the Australian Army. Restructuring doctrine, coordinating existing assets and adjusting mindsets will allow for the development of combat CI that the Australian Army requires in the years to come.

[7] *2016 Defence White Paper,* page 98, para 4.55.

CULTURAL COMPETENCE AND ADAPTIVE LINGUISTIC CAPABILITY IN ADF HUMINT SOURCE OPERATIONS

Captain S

> *"Cultural competence is a set of congruent behaviours, attitudes, and policies that come together in a system, agency or among professionals and enable that system, agency or those professions to work effectively in cross-cultural situations".*
>
> Cross et al 1989

For some time, a range of Government and non-Governmental organisations have been acknowledging the importance of 'Cultural Competence' or 'Cultural Proficiency' in their service delivery and practitioner training. This has been particularly prominent in healthcare and social services as well as law enforcement and the criminal justice system.

This article will argue that elements of Cultural Competence and related aspects such as effective linguist capability are integral to HUMINT in general and Source Operations in particular. The article will then suggest how this can be better incorporated into both specialist and continuation training and how linguist support to the capability can be enhanced to avoid 'Cultural Fouls' and missed collection opportunities.

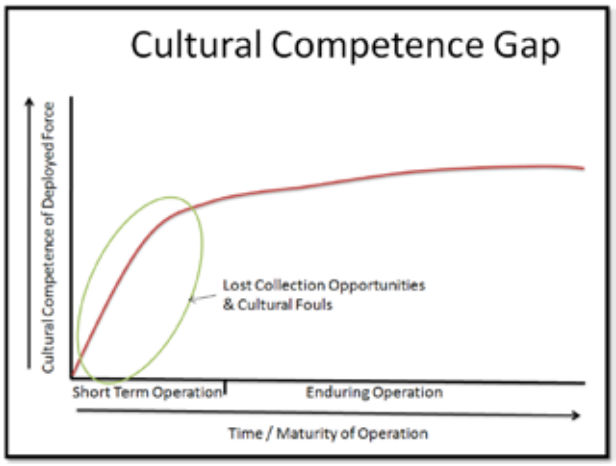
As Source Operations is a HUMINT discipline it is explicit that human interaction is central to the capability. Throughout the selection, training, certification and employment of a Defence Source Operator (DSO), interpersonal skills are assessed and scrutinised. However almost all of this scrutiny is conducted in a cultural and linguistic vacuum. With the exception of one week of invaluable training in the use of an interpreter, all meetings are conducted between Australians, and in English. Training activities are almost exclusively conducted domestically, with a domestic simulated source network. Yet ADF HUMINT almost exclusively run sources who are foreign nationals, in an overseas operational theatre, who either do not speak English, or speak it as a second, third, or fourth language.

Less visible than the linguistic barrier is the difference in world view shaped by culture. Understanding source motivation is a critical component to effective Source Operations, but the world view of a 42 year old father of three from Brisbane is inherently different to their counterpart from Kandahar, Dili, Mogadishu, or Aleppo. Everything from sense of humour, to honour, duty, loyalty and loss of face can vary widely when

you factor in such aspects as religion, educational, exposure to violence, and long standing cultural norms. After such huge efforts during training to fine tune DSOs to pull the right strings on Australian role players, little preparation is given for re-tuning this skill set to a source who may be Pashtun, Dinka, Arab or Melanesian. This cultural gap is currently addressed inadequately by a few mandatory pre-deployment 'Culture briefs' unsuited to Source Ops – no other formal preparation is given. Once in theatre DSOs learn 'on the job' and their most effective training in the local culture is the mistakes and missed opportunities of the first few months of their deployment. This is hardly ideal. Imagine a medical team deploying to an area with exotic and unfamiliar tropical diseases, who then learn 'on the job', so that after the mistakes on the first dozen patients they can begin effective treatment.

What is even more damaging, and can delay the adaptive process for DSOs, is that they are left unaware of how significantly different the subtleties of human interaction are from culture to culture. Whilst some DSOs will be able to draw upon lessons learnt on previous deployments or through other experience, some leave their training unaware that people in different cultures lie and deceive in different ways about different things for different reasons. Psychologists are divided as to the extent of the impact of culture on such fundamental aspects of human interaction, but recent experience in Afghanistan starkly demonstrates that the cultural gap can be huge. When an Australian is offended by a joke at their expense they may just laugh it off or immediately express their displeasure, whereas in many cases Afghan soldiers have brooded upon the offence and decided it required a violent and fatal response. This occurs even when days earlier he considered the Coalition Soldier a good friend. This is inexplicable to a Western mind and seems erratic, unstable and duplicitous. An Afghan man's shame, honour, and personal goals can all be significantly different to what a 'Westerner' might expect. DSOs need to firstly be aware that all preconceptions and templated solutions need to be reassessed for each deployment. Secondly, they need specific preparation for that environment, so that they are amongst the most culturally attuned personnel deployed. This is often the case by the end of their deployment, but it should be the case at the beginning as well.

Compounding the issues of different perceptions across cultures are the complexities of language use and our linguistic capability. As mentioned before, during DSO training the source's exact words are often scrutinised for ambiguity and meaning. Yet upon deployment the availability and quality of



interpreters can be so poor that the most subtle question is mangled into something with potentially different implications. Two major issues impact the availability of good linguist support. First is the requirement to have interpreters who are security vetted. Second is the availability of linguist support in the specific language being used – including the appropriate dialect for that region and ethnic group. Ideally, a Field HUMINT Team (FHT) would deploy with sufficient ADF personnel trained in the local language to a standard high enough to replicate local language skills. This is highly unrealistic even in regions in which Australia has been militarily involved for decades. The result is that FHTs are forced to rely upon a limited number of contracted linguists provided by commercial companies, who can source native speakers from diaspora populations in the western world. Inevitably these individuals are in high demand, so are both expensive and scarce. Complex conversational plans, operational security, and unspoken signals require a high level of synergy. In many cases the contracted interpreters are an excellent asset, and are both hard working and capable, however this is far from guaranteed. As a limited resource they are often overworked, spending

excessive time working with sources. This has a cumulative impact on their operational effectiveness: A fatigued or disinterested contracted interpreter is unlikely to deliver the close cooperation required. Additionally, interpreters can learn far more about the HUMINT network and tradecraft than is prudent for security.

So how does a small, specialised capability increase cultural competence and build a linguist support system which can be effective in unforeseen future operations?

Training Cultural Competence

DSO training needs to incorporate two distinct elements to achieve Cultural Competence. The first is to teach DSOs a generic understanding of cultural relativity and the challenges this can produce in Source Operations. Such insight is currently delivered only in an ad hoc manner via informal vignettes from instructors' personal experiences. This should be formalised into a dedicated component of Source Operator training. A pre-course study pack could include historical cases of lessons learnt during Source Operations and the complexity of cross cultural communication. Whilst this will be nested in specific examples it will demonstrate the relativity of our world view. This can be reinforced during the course by amending some role player parts to include certain cultural issues and requirements. For example, one serial could include an otherwise placid Source taking offence over something very minor, which then requires the trainee to apologise and identify how to rebuild rapport. This integration of cultural nuance should be continued during internal unit training, and enhanced with external presentations and study on relevant religious and cultural beliefs in likely areas for deployment.

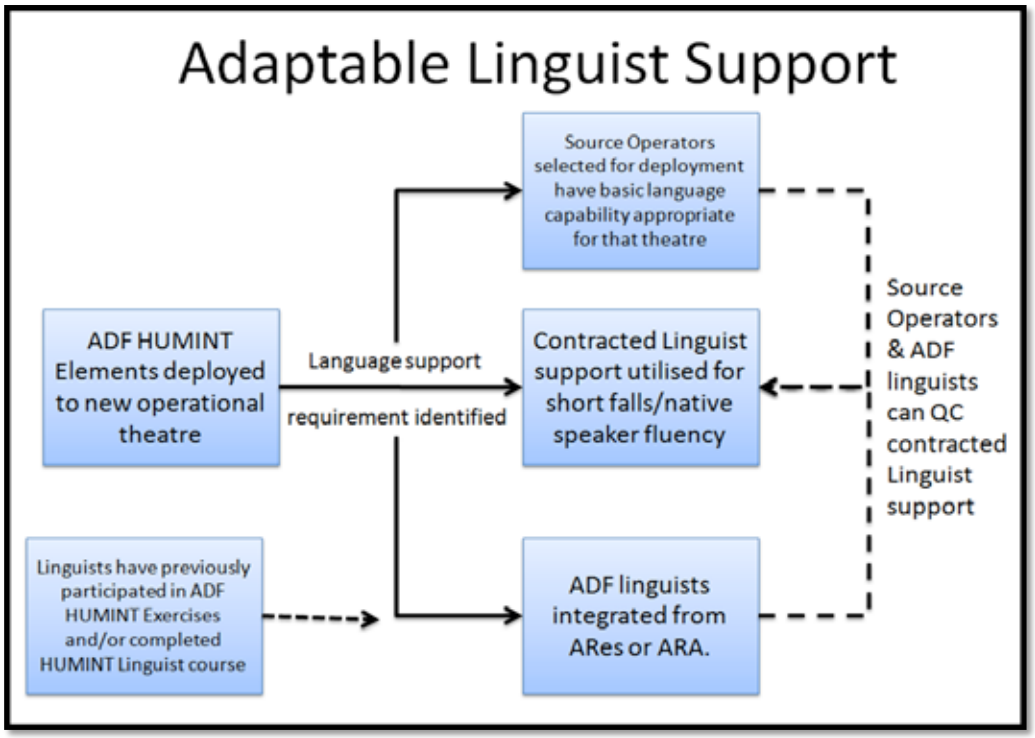
Notwithstanding the security challenges, it would be invaluable to conduct unit training exercises in friendly countries where a cultural difference would be inherent in the training activity. The physical and human terrain would offer unique challenges and demonstrate the need to understand your environment as quickly as possible.

The second element is to deliver effective pre-deployment cultural training to make FHT members amongst the most culturally attuned personnel on the deployment. This should exploit both academic experts and analysts within Defence to produce, as a minimum, a study pack on generic cultural issues in that region, external lectures or engagement opportunities with diaspora communities in Australia (with suitable pretext) and a tailored, funded reading and resource list. This is every bit as relevant as reading into the current reporting in theatre, as it provides the broader context within which that reporting is being produced.

Building adaptable Linguist Support for ADF HUMINT

More complex is the provision of appropriate and agile linguist support. The best way to achieve this is also one of the most difficult – develop military linguist resources tailored to HUMINT operations. As it is not viable to maintain a huge cadre of full time linguists, some risk must be taken in predicting which languages will be required based on Australia's strategic collection priorities and anticipated areas of involvement. These languages should form the basis for a two tier approach to linguist capability. Following the example of 2nd Commando Regiment, every Source Operator should be supported to develop their basic language skills, based on individual aptitude and operational requirements (most likely languages in Australia's region, and in the Middle East). This requires direction, funding and time. Access to high quality self-paced learning programmes such as Rosetta Stone could complement university evening courses, for example those offered by the University of Queensland, or bespoke intensive courses at Defence School of Languages would deepen linguist ability. Finally, dedicated periods of time would be allocated to support learning, with operators held accountable for their progress. Even if all this effort allows Australia to deploy just two Source Operators to a new operational theatre with a basic understanding of the local language, that is of huge significance for the quality of the Source network that will subsequently be produced. The importance of language as a rapport building tool is immeasurable and even a relatively small vocabulary will allow the first rotation of HUMINT personnel to understand the local

situation much more quickly. It will also allow those first operators to quality check their interpreters. Often the first allocation of contracted interpreters are of hugely variable quality, as urgency and the chaotic operational environment results in some unsuitable individuals being hired.



The second tier of linguist support would be a cadre of dedicated ADF linguists possessing a high degree of fluency in one or more of the target languages. Existing linguists could be captured on a database for use by HUMINT elements both on operations and in training (languages are already recorded on PMKeys). In order to ensure these linguists were optimised to support HUMINT operations, a short specialist course could be created to ensure those likely to support HUMINT had a basic understanding of HUMINT processes, requirements and considerations. The linguist's inclusion in exercises would serve a double purpose – it would enhance the ability of the linguists to support Source Operations, and would train DSOs to work through interpreters. However, what would greatly enhance this capability is the targeted recruiting of a reservist linguist capability. Currently HUMINT reservist capability is significantly undermanned and consists primarily of ex-Regular personnel. These unfilled reserve positions could be filled with linguist support personnel, recruited via University Regiments, targeting students studying appropriate foreign languages at University. By advertising the financial benefits of having languages recognised in the ADF, appropriate candidates may be enticed to Corps transfer to AUST INT Corps Reserves and sit within the ADF HUMINT capability.

These suggested changes to both cultural training and linguist capability are small and relatively cheap by comparison to the cost of other intelligence collection capabilities. They are however, significant in enabling the ADF to increase the quality of HUMINT reporting in the crucial early period of an ADF operation – particularly for contingency forces (CONFE). The biggest barrier to their effective implementation is the current limitation in manpower and training time available within the ADF HUMINT capability. It is therefore necessary to balance the importance of understanding the Human Terrain and the importance of other training ADF HUMINT are currently committed to.

What is clear is that as the world continues to be unpredictable and volatile, the need for ADF Commanders to understand complex Human Terrain will remain pivotal. ADF HUMINT's cultural and linguistic competence is a key factor in that ability to understand complex environments, across a range of operations, from short term humanitarian support through to long term warlike operations.

PELUANG EMAS (A GOLDEN OPPORTUNITY): S2 CELL IN MALAYSIA

Captain Timothy Dubber

In 2016 rotations commenced for a S2 cell based at the Royal Malaysian Air Force (RMAF) Base – Butterworth, Penang. This element would focus on providing force protection to the Army staff based in Penang, and act as a declared intelligence presence in Malaysia. The support was to be provided both to the 2/30th Training Group (2/30 TRG GP), one of the Direct Command Units of HQ 1st Division / Deployable Joint Force Headquarters (HQ 1 Div/ DJFHQ), and to the Rifle Company Butterworth (RCB) rotations. With the capability beginning to find its feet, it would appear that a good opportunity exists to review how the integration of the new S2 cell is progressing, as well as to highlight the good training and work done by AUSTINT soldiers in one of Australia's longest standing overseas commitments.

2/30 TRG GP is the small, permanent Army cadre staff posted to Royal Malaysian Air Force Base, Butterworth. Its role is to command RCB, and to train them to directed levels of foundation warfighting in South East Asia, while contributing to Army's international engagement plan in the region. While the RCB is generally based on a sub-unit from a combat or combat support arm, its manning

Enemy party for RCB Exercise.

provides for a number of essential combat service support elements, whose role is to provide specialist support to both RCB and to HQ 2/30 TRG GP. The newly raised S2 cell slots into this ORBAT, to provide intelligence support to both these customers.

The S2 cell rotation itself deploys as a part of the RCB rotation, with the soldiers currently supplied from1st Int Bn, or HQ 1 Div/DJFHQ, and concentrated at HQ 1 Div/DJFHQ before deployment. When in country, this small cell is under the command of CO 2/30 TRG GP, and the technical control of the J23 in HQ 1 Div/DJFHQ. This year, working in the J23 cell, I was fortunate enough to not only work with the S2 cell, but also to visit them in country, and gain a better understanding of the role that the capability is playing in Malaysia.

When I spoke with CO 2/30 TG about his perspective on the S2 cell, he first and foremost identified the importance of the S2 cell in helping him understand, and monitor the real world situation in Malaysia:

> *"While the JNCO can be tasked to support RCB's training outcomes - development of threat scenarios and provision of intelligence briefing are but two examples that come to mind - the real benefit lies in the provision of real time intelligence support to CO 2/30 TRG GP, and his staff. Despite its relative stability and prosperity, Malaysia's ethnic diversity represents potential fault lines that can, and are, exploited by various political groups who seek to increase their influence and power base. In addition, it is well known that the Malaysian authorities are paying particular attention to the movement of foreign jihadists, and home grown extremists. Regular update briefings to both 2/30 and RCB staff are an essential way of maintaining situational awareness in a dynamic environment. Furthermore, while the intelligence analyst is just one enthusiastic JNCO on the ground, for CO 2/30 TRG GP, he or she is analogous to the spokesperson for a large government department, or corporate organisation: behind the person giving the briefing is a huge, unseen collection of experts who gather the data, sift through the product and provide the analysis."*

One of the key reasons for the development of the S2 cell rotation was to provide an opportunity for young AUSTINT soldiers to conduct combat and security intelligence, in direct support of an ADF contingent overseas, in a unique environment. I was also able to talk to the S2 from RCB 117, CPL M, and get his opinion on the benefit gained from the rotation:

> *"The opportunity provided to a JNCO to be in a live S2 role is excellent as it develops the capability and personal skills, whilst in that position. The exposure to working in an international environment is something that cannot be simulated in exercises in Australia, and is therefore very important. The real world experience has been extremely beneficial to increasing my understanding and effectiveness as an analyst."*

The first rotation consisted of two AUSTINT Analysts. However in the next rotation this was changed to include one analyst, and one geospatial technician (GEOTECH). The CO had several examples of the utility of the GEOTECH in country:

> *"Like his analyst colleague, the geotech's efforts can be prioritised towards either support to HQ 2/30 TRG GP, or the RCB. In the latter case, the products that can be produced to support training are invaluable, whether they be accurate traces of jungle patrol routes, or detailed overlays in support of long road moves. Similarly, the GEOTECH can be used to support 2/30 TRG GP exercise planning, both locally in Malaysia, and wider afield in Singapore or Thailand. The degree of support that can be provided is only limited by the amount of time that one individual can devote over a three month deployment."*

SPR B, the GEOTECH for RCB 117, was able to provide his perspective on the utility and need for geospatial support in Malaysia:

> *"Adding Geospatial Intelligence (GEOINT) support to the RCB rotation program is a good example of Army resources going to where they are needed. For years, RCB has been using a number of antiquated maps over training areas that desperately need updating. By deploying experienced*

Geospatial Technicians, that can identify and remedy shortfalls in data and topographical products, Army is ensuring that RCB planners and troops have the best available information moving forward.

Working with RCB117 and 2/30 TRG GP has had its challenges, but overall it has been a greatly rewarding experience. Admittedly, there have been a lot of products that require updating, and some areas that were so out-of-date, it was easier to start from scratch, so the workload has been high. However, it is very rewarding to have made a product, and also be in proximity to these areas, so that you can go out with your handheld GPS and capture more data or ground-truth information that you collected from other means."

Further to their other in-barracks tasks, the S2 cell has also been working closely with the RCB Military Police (MP) detachment, Australian Defence Force Investigative Service (ADFIS) Warrant Officer, and 19 Squadron Force Protection Flight (FPF). The increased communication between these elements has allowed for a greater level of understanding between the different security stakeholders on RMAF Base Butterworth. WO2 A, the ADFIS WO collocated at RMAF Butterworth expressed his opinions about the newfound relationship:

"Time and circumstance has seen the components morph into the current configurations. The MPs and S2 Cell members are either CPL or PTE, and tend to gravitate towards the ADFIS WO for support and guidance. Whilst the ADFIS WO has no command and control over the MPs or S2 members, he provides valuable technical control and advice to the MPs, and support and guidance to S2 members if required. This helps to mitigate the issue of continuity of information caused by the three monthly rotations.

The OIC FPF and ADFIS have established liaison points of contact which the S2 Cell, and 1 MP members are encouraged to use and maintain these. S2 members provide a valuable resource, and not only to HQ 2/30 TG GP and RCB, but to the overall mission in Malaysia. Together with the MPs, ADFIS and OIC FPF, we have formed what could be best described as a 'Quasi Fusion Team'. The MP detachment provides an important level of force protection for S2 members to conduct their matters.

In the normal course of conducting inquiries and investigations, and the conduct of vice patrols by MPs, valuable sources of information and intelligence are identified and obtained. It is important that this intelligence and information is shared with the necessary agency. It is this understanding and willingness to cooperate that sees ADFIS, MPs, FPF and S2 working closely together at RMAF Base Butterworth to achieve better products and outcomes."

The relationship between HQ 1 DIV/DJFHQ remains an important aspect of the support provided to 2/30 TRG GP and the RCB. This support includes pre-briefing prior to movement into country, the provision of reach-back support during the trip, and the collection of information and lessons post the return to Australia. CPL M also echoed the importance of this support:

"The relationship between S2 cell and DJFHQ is important, and has been effective. Having a meet and greet with the J2 staff is important as it builds the initial relationship and promotes healthy communication. The reach-back service they provide has been appreciated and is highly effective."

However, conducting duties in barracks isn't the only activity that the S2 cell has undertaken, with support to RCB activities throughout Malaysia and even further afield. Of particular importance are the ceremonial activities, which SPR B noted to me:

"A personal highlight of this rotation has been the opportunity to join in the commemoration of ANZAC Day at Hellfire Pass and the Kanchanaburi War Cemetery in Thailand. The dawn service at Hellfire Pass was especially moving; to have so many people who have travelled so far to stand together in silence for the memory of those who died, was an emotional and unforgettable experience."

So far, the rotations have provided an excellent opportunity for AUSTINT soldiers and Geospatial Technicians to conduct training further abroad, in a unique and independent environment. Looking to the future, there are further opportunities to develop both this rotation, and the support that the S2 cell gives to 2/30 TRG GP.

The J2 HQ 1 Div/DJFHQ has been pleased with the performance of our deployed junior staff, and continues to work towards improving opportunities for Army Intelligence professionals to spend time in our Near Region. He knows it is early days for a permanent Intelligence presence with 2/30 TRG GP, and believes that in due course, the rotations may become offset, the team size might grow, and a permanent S2 may be allocated. For this to occur, our continued credible performance, and value adding, is key.

Regardless of future developments, the rotation has been well received in terms of the capability that it brings to the permanent elements posted in country. CO 2/30 TRG GP wanted to reinforce the importance of the current rotation in Malaysia:

> *"The provision of a dedicated S2 Cell in support of 2/30 TRG GP and RCB is a significant capability enhancement. Their ability to reach back and draw on the resources of DJFHQ and 1 Int Bn, along with the wider Defence intelligence community is an important development in 2/30 TRG GP's ability to deliver optimal training to RCB while sustaining a broad understanding of a complex and ever-shifting strategic environment in the heart of South East Asia."*

And looking at the issue from the soldier's point of view, CPL M's comment on the value of the rotation is illuminating:

> *"RCB has been a rewarding and worthwhile deployment that provided opportunities for personal and professional development, established good working relationships with people from other units and trades, and also left enough time to see some of the sights and have some fun."*

Overall, the RCB S2 cell position is an excellent opportunity for any JNCO or soldier, whether analyst or GEOTECH. As the rotation matures, these positions should become available to a wider audience, and soldiers should be volunteering for an extremely beneficial career developmental opportunity.

S2 Staff providing an IPB brief in country.

RUSSIA AND THE INFORMATION WAR

Warrant Officer 2 Donna Herbert

> *"If the 20th century was defined by the battle for freedom of information and against censorship, the 21st century will be defined by malevolent actors, states or corporations, abusing the right to freedom of information."* [i]
>
> Vasily Gatov

The West exhibits a persistent concern for Russian provocations and information weaponisation. We are experiencing a shift in the digital era from active or passive proponents of mass communication and information accessibility, to being willing or unwilling participants in a new epoch. In an era of pervasive information, the age of information overload has emerged. [ii] The difficulty we now face is distinguishing between accurate and inaccurate information in an over-saturated information environment. [iii] This essay will argue that Russia has taken advantage of the contemporary information environment to emerge as the key player in information warfare.

[i] Vasily Gatov is a Russian media analyst cited in Pomerantsev, P., Weiss, M. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Interpreter, Institute of Modern Russia, New York. Retrieved from http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/

[ii] Sean S. Costigan and Jake Perry, *Cyberspaces and Global Affairs*, revised ed. (Burlington, VT: Ashgate, 2013), p. 319 cited in Chad W. Fitzgerald & Aaron F. Brantly (2107) Subverting Reality: The Role of Propaganda in the 21st Century Intelligence, International Journal of Intelligence and CounterIntelligence, 30:2, 215-240, Retrieved from http://dx.doi.org/10.1080/08850607.2017.1263528

[iii] Chad W. Fitzgerald & Aaron F. Brantly (2107) *Subverting Reality: The Role of Propaganda in the 21st Century Intelligence*, International Journal of Intelligence and CounterIntelligence, 30:2, 215-240, Retrieved from http://dx.doi.org/10.1080/08850607.2017.1263528

'Information warfare' no longer pertains only to those seeking to understand and control the information environment for military advantage. In a new context, it can be applied to corporate or organisational environments, with phrases such as 'digital wars', 'cyber wars' and 'cyber attacks' now being widely used. [iv] As a result, commercial companies and social media platforms are increasing their efforts to identify and prevent the misuse of their information ecosystems and platforms. A recent Facebook Security release stated, "We have had to expand our security focus from traditional abusive behavior, such as account hacking, malware, spam and financial scams, to include more subtle and insidious forms of misuse, including attempts to manipulate civic discourse and deceive people." [v] Facebook identified targeted data collection; content creation (seeding stories or disinformation via online fake personas), and false amplification (for example, astroturfing, defined as coordinated activity by inauthentic accounts), to be their primary focus for tracking and response within the information ecosystem. [vi] This increased level of defensive and offensive measures to protect social media platforms and corporate entities poses a challenge to those seeking to influence, pervert or invade existing information ecosystems. Despite this, the use of the internet, in particular social media, presents huge opportunities for state and non-state actors to support an information war.

Advances in the technology that enables our use of information is also shaping the way we perceive conflicts. The use of information by state and non-state actors to achieve effects in the operational environment feature prominently in approaches such as network-centric warfare, 4th generation warfare, or asymmetric warfare. [vii] The concept of 'hybrid warfare' [viii] is being offered as a new 'war winning' strategy that makes coordinated use of both military (use of force) and non-military (irregular tactics, criminal disorder, terrorist acts etc.) to achieve synergistic effects in the physical and psychological dimensions of conflict. [ix] It has been argued that hybrid warfare 'combines' two indirect approaches to war that are at odds; one designed to shorten, and one to lengthen a conflict. [x] In the aftermath of Russia's successful use of non-military instruments– information in particular– during the annexation of Crimea, followed by events in the Ukraine, it was suggested that Russia's new approach to warfare is hybrid. [xi] The Kremlin's weaponisation of information, culture and money appears to be an integral part of its vision for 21st-century 'hybrid' or 'non-linear' war; the essence of which is to wage war without ever announcing it officially. [xii] However, this thought process is flawed; all wars are hybrid to an extent, and the use of information, ergo propaganda, is really nothing new.

The propaganda battle between the Bolshevik 'Red Army' and British forces during the Russian Civil War employed tactics applicable to the conduct of information warfare today. The combination of mass leaflet drops, a deluge of pamphlets, and infiltration by agents seeding discontent amongst fighting

---

[iv] Ibid.

[v] Weedon, J., Nuland, W. and Stamos, A. (2017) *Information Operations and Facebook*, ver1.0. Facebook.

[vi] Ibid.

[vii] Renz, B,. Smith, H. (2016). *Russia and Hybrid Warfare – Going Beyond the Label*, Aleksanteri Papers 1/2016, Kikimora Publications at the Aleksanteri Institute, University of Helsinki, Finland. Retrieved from https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/10549/ap_1_2016.pdf?sequence=1

[viii] The hybrid concept was outlined in 2007 by a former US Marine officer, Frank Hoffman, as an operational approach that provided an analytical construct which could explain the success achieved by comparatively weak opponents such as a non-state actor like the Taliban against vastly superior militaries as discussed in Renz, B,. Smith, H. (2016). *Russia and Hybrid Warfare – Going Beyond the Label*, Aleksanteri Papers 1/2016, Kikimora Publications at the Aleksanteri Institute, University of Helsinki, Finland. Retrieved from https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/10549/ap_1_2016.pdf?sequence=1

[ix] Ibid.

[x] Scheipers, S. *Winning wars without battles: hybrid warfare and other "indirect" approaches in the history of strategic thought*'. Cited in Renz, B., Smith, H. (2016). *Russia and Hybrid Warfare – Going Beyond the Label*, Aleksanteri Papers 1/2016, Kikimora Publications at the Aleksanteri Institute, University of Helsinki, Finland. Retrieved from https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/10549/ap_1_2016.pdf?sequence=1

[xi] Ibid.

[xii] Pomerantsev, P., Weiss, M. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Interpreter, Institute of Modern Russia, New York. Retrieved from http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/

elements and the population, led to the need to replace the entire British force with fresh soldiers 'inoculated' against Bolshevik messaging [xiii] Bolshevik propaganda was so successful it influenced the decision-making at the highest level of British government, culminating in the eventual removal of the British forces. This shaped the course of the intervention, whilst atrocities conducted by British forces facing withdrawal only reinforced Bolshevik narratives. [xiv] Volume, mass media, perseverance, control of the narrative, and tailored messaging amplifying existing fears or emotions presented a winning formula.

> *"Who controls the past," ran the Party slogan, "controls the future: who controls the present controls the past."*
>
> Orwell, G. 1949. 1984

Modern Russian propaganda has developed in unison with the changing information environment. Russian techniques are not revolutionary in the sense of they are not something new and different, but they have embraced the contemporary information environment. The use of the internet and social media, along with state-sponsored national and international news channels allows for high volume, high tempo messaging, and determines those first narratives which set the conditions for the dominate narrative. In the Ukraine context, it has been suggested that independent information lost out to mass propaganda where the main objective was to mobilise the population in support of an expansionist campaign. [xv] First impressions are resilient; individuals are more likely to accept the first information received, even when faced with conflicting messages. Experimental psychology literature suggests that, all other things being equal, messages received in greater volume and from more sources will be more persuasive. [xvi]

This presents a huge obstacle for Western capabilities which are slow to respond, seem to be adopting a 'less is more' targeted approach, and remain cautious in their employment of offensive methods to compete with the noise. To understand how huge an obstacle this is for the West, you need only consider the reports of Russian internet troll factories, [xvii] fake news, and disinformation that inundate Western media. Trolls manage multiple fake accounts with daily quotas for posts on news articles, often with simplistic sentiments such as, "Putin makes Obama look stupid and weak". [xviii] Likewise, you need only watch the Russian foreign-language television channel RT (Russia Today) to receive anti-Western, anti-US sentiment. On the surface this channel appears professional; however once you scratch beneath the surface you detect something more sinister. Simply put, this is not for a Russian audience. Most of the programs are in English, or have English subtitles. The main message on programs such as 'Watching the Hawks' (anti-US content and themes) and 'The Divide' (anti-capitalism slant) is, "the US is engaged in a self-interested and ruthless bid for world domination, and that by implication anything that Russia, or any other country, can do to resist this is commendable and justified." [xix]

The simplicity of Russian propaganda appears to be its strength, and its weakness. It is repetitive and predictable; employing the tactics of: dismiss the critic, distort the facts, distract from the main issue,

[xiii] Lockley, A. (2003). Propaganda and the first cold war in North Russia, 1918-1919, History Today, 53(9). Retrieved from https://search.proquest.com/military/docview/202816210/B6B72EE759AE46EBPQ/1?accountid=10479.

[xiv] Ibid.

[xv] Ibid.

[xvi] Ibid.

[xvii] The New York Times reported on a the rise of Russian troll factories, in particular one based in St. Pertersburg known as the 'Internet Research Agency' which is said to employ hundreds of personnel posting pro-Kremlin propaganda online under fake identities. Chen, A. (2015). The Agency. *The New York Times*, 02 June 2015. Cited in Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia, Connections: The Quarterly Journal, 15(1). Retrieved from https://search.proquest.com/military/docview/1776776849/29F01C46179E4659PQ/96?accountid=10479

[xviii] Sindelar, D. (2014). *Inside Russia's Disinformation Campaign*. Defence One. Retrieved from http://www.defenseone.com/technology/2014/08/inside-russias-disinformation-campaign/91286/.

[xix] Lucas, E., Nimmo, B. (2015). Information Warfare: What Is It and How to Win It? Centre for European Policy Analysis, *INFOWAR*, Paper No. 1, November 2015. Retrieved from https://pdfs.semanticscholar.org/1032/80b245e9444f262f716cbd27953de952b261.pdf

and dismay the audience. [xx] Some have suggested that rather than trying to block, refute or undermine the propaganda, focus instead on countering its objectives; increasing, or turning down, the flow of persuasive information, and start to compete. [xxi] Other recommendations include the creation of an agreed set of regulations and ratings for media–such as Transparency International's Corruption Perception Index–to set benchmarks for disinformation and bias, along with targeting of networks and influencers; or crowd-sourced investigations, [xxii] but the reality is that responses to Russia's information war may be imperceptible amongst the noise.

The contemporary information environment is pervasive, and the exploitation of information ecosystems by those seeking to influence public discourse is ongoing. The recent conflicts in Crimea and Ukraine have seen commentators label the Russian approach to warfare as 'hybrid', with the use of information being a key component. Russian propaganda techniques are, however nothing new. Russia's use of high volume, mass media and those first narratives, along with developments in the information environment, allows us to draw parallels to a future worthy of an Orwell novel. Russia's use of disinformation and propaganda is presenting a challenge for the West whose hesitance to employ offensive measures on scale sees them fail to compete. Solutions such as the application of rules to govern transparency, or simply targeting influencers may be viable options; however Russia is clearly wining the information war.

[xx] Ibid.

[xxi] Paul, C., Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model, Why It Might Work and Options to Counter It*, RAND Corporation. Retrieved from http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

[xxii] Pomerantsev, P., Weiss, M. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Interpreter, Institute of Modern Russia, New York. Retrieved from http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/

JOINT TARGETING IN IRAQ AND SYRIA: OPERATION INHERENT RESOLVE 2016

Major Karen Hunter

The deliberate joint targeting enterprise for Combined Joint Task Force Operation Inherent Resolve (CJTF-OIR), the US led operation to militarily defeat ISIL in Iraq and Syria, was fundamentally based on the US targeting doctrine outlined in CJCSI 3370.01B. This article will explain how this process was employed between mid 2016 and early 2017.

Before explaining the process, a few key facts need to be understood:

1. The deliberate targeting process outlined below refers to targeting of infrastructure and facilities, not High Value Individuals (HVI). Each identified target facility had to be functionally characterised as serving a military purpose for ISIL, and that striking it – even in the absence of enemy presence – would have an effect on ISIL capability.
2. This process was for deliberate targets only. Every deliberate target within the Combined Joint Operational Area (CJOA) was required to be processed through the CJTF-OIR CJ2 target cell (CJ2T). Dynamic targeting was managed through the Combined Air Operations Command (CAOC).
3. The purpose of the CJTF-OIR deliberate targeting enterprise was to present targets to the CJTF-OIR Deputy Commander (DCOM) at the Joint Targeting Coordination Board (JTCB), to be approved as valid military targets and added to the Restricted Target List (RTL). Once on the RTL, the CAOC would conduct Advanced Target Development (ATD) in preparation for Joint Integrated Prioritised Target List (JIPTL) approval, meeting any specified restrictions. Restrictions included strike window recommendations or mitigations for collateral concerns, and all targets in Iraq required Iraqi government approval. Once approved and on the JIPTL, the target could be scheduled for strike.

The CJTF-OIR targeting process (figure 1), is rooted in doctrine and was designed to provide indicative timings for target approvals. It is this diagram which will form the basis of the discussion.

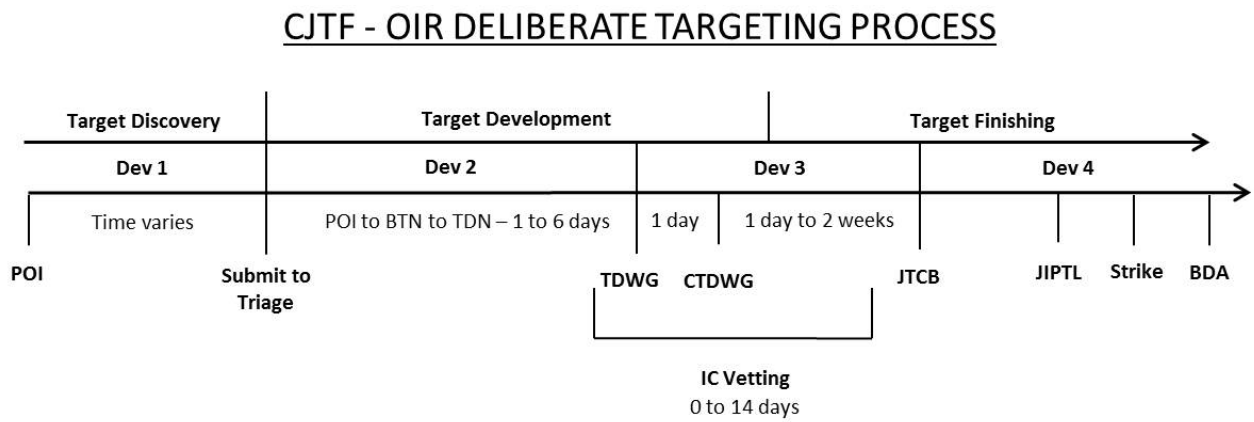


Figure 1: The CJTF-OIR Deliberate Targeting Process.

Target Discovery

There were over 25 target development organisations globally, from participating coalition nations and component commands. Each of these organisations was conducting target discovery to identify Places of Interest (POI) for further development. As soon as a POI reached the minimum reporting standards IAW the CJTF-OIR Targeting Directive, the POI could be submitted to CJ2T Triage for target development.

Target Development

Once submitted to Triage, the target developer would continue to research and develop the target while Modernized Integrated Database (MIDB) was updated, BE numbers [i] and ISIL O-suffix [ii] identifiers created, and target materials produced. The Triage team consisted of fires and intelligence personnel, and would assist the Target Developer in completing the requirements for Basic Target Development (BTD) (figure 2).

	Target Type				
Target Development Element	**Facility**	**Individual**	**Virtual**	**Equipment**	**Organization**
Identification	BE & O-Suffix	EID	EID	EID	Unit ID/EID
Location	GEOCOORDS	GEOCOORDS, Last known location	IP address, GEOCOORD, Last known location	GEOCOORDS, Last know location	
Function	Category Code	Function Code			
Significance	Facility Significance Remark	Target Significance Remark			
Facility Description	Facility Description Remark	Not applicable to these target types			

Figure 2: Basic Target Development (CJCSI 3370.01B).

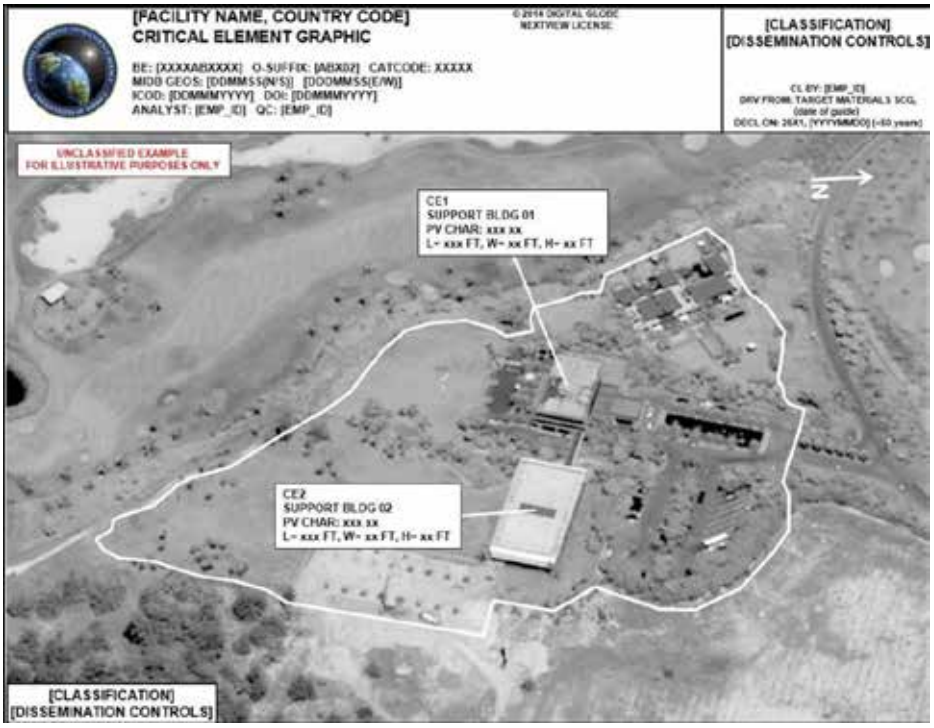


Figure 3: An example image of a Critical Element Graphic (CJCSI 3370.01B).

[i] The BE number is the unique target identification number for a facility of installation within MIDB.

[ii] The O-suffix is a five-character alphanumeric code within MIDB. An "ISIL O –suffix" identified the facility as being associated with ISIL.

Once MIDB entries were updated and target materials created (such as the Critical Element Graphic at figure 3), the target developer would produce a Target Development Nomination (TDN) in the Target Pack format (established by CJ2T and based on Intermediate Target Development as per figure 4) to meet the minimum requirements of:

1. **Target Description**. A detailed description of the target, such as the size and construct of the facility, including all structures within the installation outline, access points, fencing etc.
2. **Target Function and Categorisation**. The description of the target's former function (and if it was a CAT I or CAT II facility [iii]), current ISIL military function (including secondary and tertiary functions as required), and how long the facility had been under ISIL control.
3. **Target Significance**. An analysis of the level of significance of the target to the enemy system.
4. **Expectation**. An assessment of how and through which methods targeting of the facility would affect the target system, and an assessment on how long it would take the enemy to recover from the loss of this facility.
5. **Intelligence Gain Loss**. An assessment of the intelligence gain or loss to be expected if the facility was targeted.
6. **Critical Elements**. An explanation of each critical element of the facility, to include physical structures within the installation, as well as equipment, materials or personnel that were critical to the military function of the target.

	Target Type				
Target Development Element	**Facility**	**Individual**	**Virtual**	**Equipment**	**Organization**
Significance (continued)	Target Significance: Addresses the target's effect to the target system	Completed during basic target development			
Target Description	Describes recognizable attributes of the target entity				
Characterization	Elaborates on assigned category/functional code(s)				
Expectation	Describes why engaging the target entity should affect the target system.				
Elements	Those elements necessary for the target to perform its primary function				
Source Documentation	List of source data, to include serial numbers of associated reports.				
Collateral Damage Considerations	Describes collateral concerns, environmental or population density concerns in the area surrounding the target entity, and second and third order effects on infrastructure and other non-physical entities				
Intelligence Gain and Loss	Describes potential intelligence gains or losses resulting from affecting a target.				

Figure 4: Intermediate Target Development (CJCSI 3370.01B).

[iii] Categories of no-strike facilities, i.e. hospital, school, mosque is considered CAT I, other civilian infrastructure such as businesses, houses, bridges is considered CAT II.

7. **Collateral Damage and LOAC Concerns**. A list of collateral considerations and LOAC considerations (as required) within a 500m radius of the target to assist with ATD. This included items such as the potential for chemicals onsite, and the need for a plume analysis and risks to civilian infrastructure and non-combatants.

8. **Assessment of Pattern of Life / Pattern of Activity**. As assessment on when the facility was being used, who frequented it and the surrounding area (combatants and / or non-combatants), what they were doing, and any other observables at the target indicate support for the military purpose and its significance.

The timeline for this phase to be complete would vary (the minimum was one to six days as per figure 1), and a target was considered to have "passed" Triage when they had a completed TDN to the minimum standard ready for the Target Development Working Group (TDWG) and Coalition TDWG (CTDWG).

The TDWG was a working group held at the Secret FVEY level, although it could be elevated and the audience limited as required for sensitive targets. The CTDWG was a repeat of the TDWG conducted the next day at the Secret IRKS [iv] level, to include all participating nations. The WGs were conducted through global video conferencing four to five times a week, and included component commands, their subordinate commands, strategic organisations from coalition nations, and members from CJTF-OIR representing other directorates.

The target remained the responsibility of the target developer up until such time it was briefed at the C/TDWG. At this time, it would be allocated to a member of the Validation Team.

Target Finishing

The Validation Team were Intelligence Analysts who reviewed each target in fine detail, re-plotting coordinates, reading through intelligence reporting, researching additional intelligence reports, identifying gaps, coordinating collection and refining and assessing the target objectively. They provided a level of detachment in reviewing the target developer's assessment and vetted every aspect of a target to prepare it for the JTCB. The goal was to ensure the DCOM had a clear understanding of the risk versus the significance of the target, and knew exactly what risk he was accepting by approving it to the RTL. High-risk targets that were outside of the DCOM's approvals could be referred to the COMD, and if required, higher to the national level.

Intelligence Community (IC) Vetting

When a target was passed through Triage it was also sent to Intelligence Community (IC) vetting. IC vetting allows the US strategic agencies to provide input into target validity. IAW CJCSI 3370.01B, IC vetting is not a compulsory process, although it is desirable. The main issue with IC vetting was the additional time this added to the targeting process, as these organisations worked business hours and took time to respond. This often resulted in tensions due to the requirement to meet operational timelines, especially over public holiday periods. Notably, throughout the course of my deployment the need to obtain IC vetting on every target had diminished. This reduced the number of targets that needed IC review, enabling them to focus their efforts on complex targets that represented an increased strategic risk.

Dev 1 - 4

As a target was developed through the process, it would be classed as Dev 1, 2, 3 or 4 which assigned its priority for ISR collection. Essentially, once a target was presented at the TDWG / CTDWG and assigned to a member of the Validation Team within CJ2T for finishing, it was given priority for collect (at Dev 3) against target development theatre lines to verify the intelligence and determine the pattern of life (PoL) on and around the target facility. Once a target had been presented at the JTCB, if further collection was required the target would be classified Dev 4, which was the highest priority.

[iv] IRKS is the releaseability for OIR and includes all coalition nations.

ATD, Strike and Battle Damage Assessment (BDA)

Once a target was approved to the RTL, the CAOC would conduct ATD and present the target with Joint Desired Point of Impact (JDPI) and Collateral Damage Estimation (CDE) to the DCOM at the JTCB. It was at this stage the target was approved to the JIPTL for strike. Post-strike, Phase 1 and 2 BDA would be conducted to determine whether re-strike was required. The Validation Team provided intelligence analysis support throughout the ATD process (primarily for intelligence override to assist in accurate CDE) and provided intelligence support re-strike recommendations as required.

Conclusion

The targeting process outlined provides a basic overview of the deliberate joint targeting enterprise employed for CJTF-OIR over mid 2016 – early 2017. Whilst this process reflects the doctrine outlined in CJCSI3370.01B, each operation will have different requirements which align the doctrinal process to suit specific operational risks, authorities and requirements. Indeed the process as outlined here evolved prior to, during and after my deployment as the operation developed, the enemy adapted and different personalities took command. Despite this, the broad process and concepts have been established and proven effective over time and are likely to form the basis of future joint targeting operations.

Major Hunter was embedded with CJTF-OIR, CJ2-T, as the Senior Targeting Analyst, over Jul 2016 – Jan 2017, providing intelligence support to all Deliberate Targeting in Iraq and Syria.

CHALLENGES TO DELIBERATE JOINT TARGETING OF ISIL

Major Karen Hunter

Deliberate targeting against ISIL for Operation Inherent Resolve (OIR), whose boundaries extend beyond Australia's own Operation Okra, presented a number of challenges. This discussion will address a number of the key challenges that targeting in this environment presented over July 2016 – January 2017, a time of significant change across the Combined Joint Operations Area (CJOA).

The four areas to be examined are: the fact that targeting operations commenced without a clear understanding of the target systems; ISIL abuse of civilians and civilian infrastructure for military purpose; ISR and limited ground forces; and the evolution of operations. However, before exploring these challenges it is critical to understand what was occurring operationally at this time.

Background

Over this time period, ISIL was on the back foot, particularly after barely contesting for the city of Fallujah against Iraqi Security Forces in late May 2016. Over the following seven months in Iraq, the Tigris River Valley was cleared to Mosul (excluding a pocket near Hawijah), significant gains were made in the Euphrates River Valley, and after months of

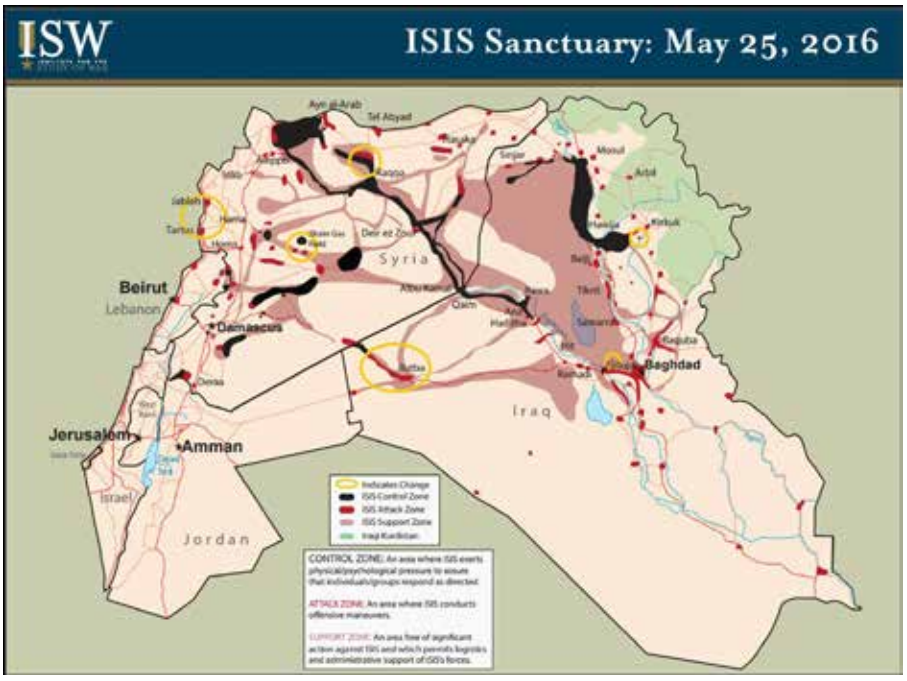


Figure 1: ISIS Sanctuary map 25 May 2016 [i]

[i] Imaged source from: http://www.understandingwar.org/backgrounder/isis-sanctuary-map-may-25-2016.

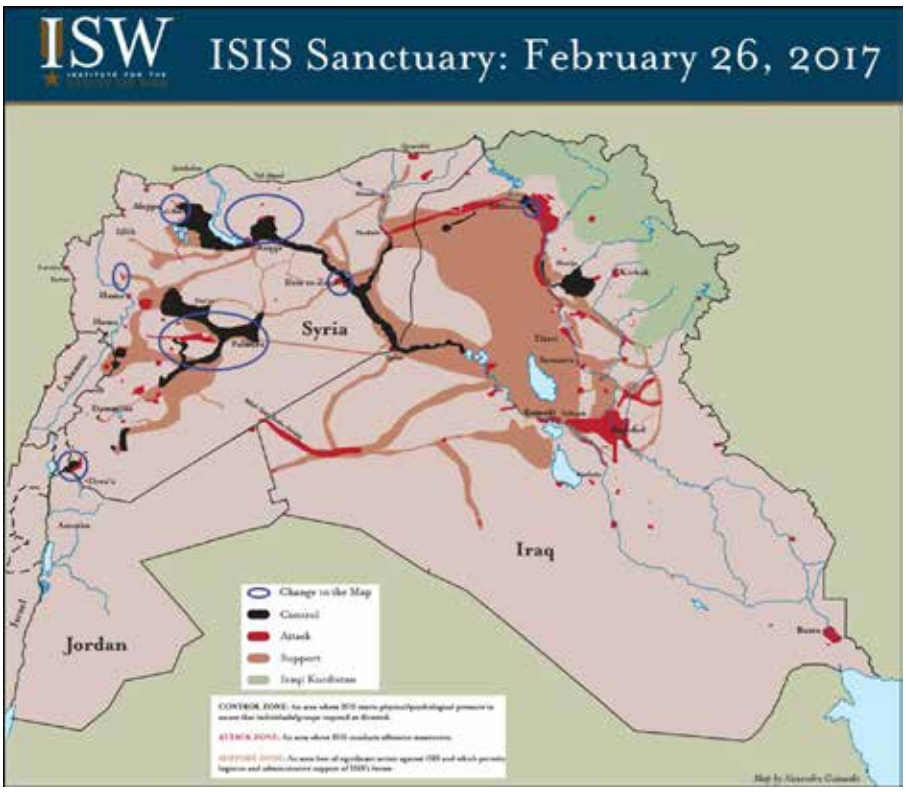


Figure 2: ISIS Sanctuary map 26 February 2017 [ii]

fighting, East Mosul was cleared. In Syria over the same time frame, ISIL had lost control of all territory along the Turkish border, significantly impacting the freedom of movement of international fighters and their black-market logistic supply. They also lost Manbij and were in a losing battle for al-Bab. The Syrian Democratic Force was effectively clearing the avenues of approach north and west of Raqqah. It is against this backdrop that analysts globally were trying to understand ISIL's changing target systems in order to develop targets to support operations.

Playing catch up in understanding the target system

An ongoing difficultly in the targeting enterprise was that targeting of ISIL commenced in late 2014 without a clear understanding of their target systems. This made attempts at Phase 3 Battle Damage Assessment (BDA) [iii], and accurate and detailed analysis on the impact of targeting operations almost impossible. No Target Systems Analysis (TSA) [iv] was conducted prior to the commencement of operations, and as a result, no Joint Integrated Prioritised Target List (JIPTL) was available and ready for the rapid deployment. This was described by AVM Steve Roberton to an Air Power Seminar given in Canberra in April 2015, when discussing the speed at which the all–air power, ADF task group deployed in October 2014:

There was no 'Op Plan' that they pulled off the shelf with, 'Here's your list of 2,000 JIPTL targets. . .' That doesn't exist. That's being built as we move along. . [v]

[ii] Image sourced from: http://www.understandingwar.org/backgrounder/isis-sanctuary-map-february-26-2017

[iii] BDA is composed of a physical damage assessment phase (Phase 1), functional damage assessment phase (Phase 2), and target system assessment phase (Phase 3). Phase 3 BDA provides an assessment of the overall impact and effectiveness against the enemy's target system relative to operational objectives. (Joint Publication 2-01.1, Joint Tactics, Techniques and Procedures for Intelligence Support to Targeting, 9 January 2003)

[iv] "*TSA is an important prerequisite to identifying and developing enemy target entities. It is used to identify, describe, understand, and document adversary target systems in a way that breaks the system down into components, and may describe key target entities. It explains the functional, spatial/geographic and temporal relationships between system components and other target systems*." (CJCSI3370.01B, Target Development Standards, 6 May 2016)

[v] Operation OKRA – A Commander's Perspective by Air Commodore Steve Roberton, An Air Power Seminar given at Canberra on 15 April 2015, retrieved on 15/08/17 from http://www.sldinfo.com/wp-content/uploads/2016/04/OpOKRA_Transcript.pdf

By the end of 2015, a concerted effort had been made by coalition nations to produce TSAs on ISIL's various target systems in an attempt to play catch up. Throughout 2016, these were produced by reach-back organisations, who adopted a "micro" TSA approach, applying analytical rigour to one aspect of ISIL's operating systems, often researching in a specific geographic location (e.g. ISIL's logistics system in Ninawa Province or ISIL Military C2 in Raqqa). Whilst these micro TSA's provided invaluable depth of analysis to support targeting, the lack of detailed analysis of ISIL's start- state prior to targeting will remain a hurdle in our understanding of ISIL into the future.

Over 2015 and into 2016, it was clear that the coalition was having an effect on ISIL, and the success of air operations was apparent as ISIL began to lose territory and control. However, as their territory shrank and the "easy" targets evaporated, not understanding how their systems operated, and how they had evolved due to our targeting efforts, impacted our capacity to find new significant targets. This combined with their propensity to hide in dense urban areas among non-combatants, and extensive use of tunnelling, made deliberate targeting difficult.

ISIL appropriation of civilian facilities for military purposes

Despite attempting to establish itself as a quasi-state, ISIL is a non-state actor who has appropriated civilian infrastructure to fulfil its military purpose. Essentially, every potential target was categorised as either a CAT I or CAT II [vi] protected facility, and had to be established as a valid military target. For example, ISIL may have taken control of a mechanic garage to build VBIEDs, so this previously CAT II facility was now serving a military purpose and could be approved as a valid military target. To complicate this, ISIL may have continued to allow this facility to service civilian vehicles through business hours, and employed the garage as a VBIED workshop at night; meaning the facility was considered "dual-use" serving both its original civilian function alongside its appropriated military function. Dual-use targets could still be legally engaged with mitigation options that required detailed intelligence support to identify strike options and avoid non-combatant casualties.

Another challenge was the fact ISIL combatants co-located their family members, including children and infants, with facilities serving a military purpose. Overt signs of domestic and civilian activity, such as the blatant exploitation of children playing within an ISIL military installation, whether that be a headquarters, logistics and operations centres, IED facilitation or chemical weapons factory. Whilst such actions did not prevent it being approved by the Restricted Target list (RTL) as a valid military target, the intelligence required to support lethal targeting to mitigate for the presence of non-combatants was immense. Sometimes it was just not feasible to develop appropriate mitigations that aligned with the target significance and risk acceptance. The level of intelligence support required to have confidence in what was happening inside a facility relied heavily on ISR, which presented another challenge.

ISR and the impacts of limited ground forces

> *Air/land coordination is a most important aspect about this campaign that's being conducted. It is all about the fact that we don't have our people—US, Coalition people— on the ground, in the fight* [vii]

In the early phases of this conflict, ISIL maintained strict control over territory it had captured. This meant access into ISIL territory was limited, even for partnered ground forces. Additionally, ISR options were significantly less than what many in the coalition were accustomed to, compounded by a lack of ground forces. For deliberate targeting, the need to know what was happening inside a facility meant a

[vi] Categories of no-strike facilities, i.e. hospital, school, mosque is considered CAT I, other civilian infrastructure such as businesses, houses, bridges is considered CAT II.

[vii] Operation OKRA – A Commander's Perspective by Air Commodore Steve Roberton, An Air Power Seminar given at Canberra on 15 April 2015, retrieved on 15/08/17 from http://www.sldinfo.com/wp-content/uploads/2016/04/OpOKRA_Transcript.pdf

dependence on quality HUMINT. Obtaining HUMINT that was reliable and could be verified, especially for ISIL-dominated regional areas, was particularly difficult.

Over 2016, ISR capabilities operating in the CJOA increased along with our 'boots on the ground', and this seemed to match pace with ISIL's reduced footprint. Where ISIL flags had unashamedly stood attached to buildings as they flaunted their military activities, they now often disguised facilities with indications of civilian presence, and increased the use of tunnelling. As our partnered forces pushed deeper into ISIL territory and boundaries changed, the shift from an air dominant campaign to a ground campaign accelerated.

A changing operation

The criticality of joint operations was not more apparent than in this conflict. The speed with which coalition air forces were able to ramp up operations, deploy and start targeting ISIL was remarkable. After over a year of acceleration in forces and territory growth, by June 2014 when ISIL claimed Mosul, the rest of the world came to realise action was now desperately needed. With their arrogance at peak levels, ISIL were often failed to conceal their activities, and targeting of ISIL's military appropriated bases commenced. Initially, the Combined Air Operations Command (CAOC) area of operations (AO) covered large swathes of countryside due to the size of enemy controlled territory. But by mid-2016, changes to the ground footprint, as ISIL territory contracted, saw the campaign evolve from an air dominant campaign to an increased ground force focus. This translated into an increased need to ensure targeting operations were supporting the ground manoeuvre commander's plan. Pressure on the CAOC to maintain the "drumbeat" (a regular and consistent pace of targeting to keep pressure on ISIL) with targets becoming fewer and more difficult to find, a shrinking AO, and restrictions due to the ground manoeuvre plan created tension in the targeting enterprise. The coalition air forces were victims of their own success and restrictions on their freedom of action took some adjustment, as CJFLCC and CJSOTF took command of areas previously part of the CAOC AO.

As the pace of ground force manoeuvre increased, and with fierce fighting in Mosul into January 2017, the CJTF-OIR Commander started to push target authorities, and risk acceptance for deliberate targets, down to the 2-Star component commanders. Despite being a natural progression of the operation, such changes in authorities do require perspective adjustment from those who lose some of their responsibilities (or absorb new ones). This transition was a combination of the commander's leadership style, but also a reflection of the campaign shift from a joint / air dominance focus, to a greater need to let the armies lead the mission with air force now in a supporting role. By this stage, as our ground forces took control of greater territory, our increased ISR and access provided better verification of intelligence and reduced some of the risk. Also, by giving subordinate commands increased authorities, the CJTF-OIR Commander facilitated the increasing momentum of ground forces, which was essential as we transitioned to a point in the campaign where ISIL's military defeat was increasingly certain.

Conclusion

The four challenges discussed here are, in many ways, unique to the time period specified, however can also be viewed as enduring challenges for OIR and echo issues faced in other conflicts. Each of these challenges could be considered individually in more depth; however this discussion does provide an overview and allows some insight into the CJTF-OIR Joint Targeting enterprise.

ISR & IO DOCTRINE

Major Holley and Captain Barrett

"But that doesn't make any sense."

Anon.

Doctrine is one of the least fashionable areas of our professional life, yet one of the most discussed. Generally across Army you hear that doctrine is either 'out of date' or exists 'only for courses' and it bears no reflection on 'how we do it in our unit'. However, we in our Corps are unique in our approach and acceptance of doctrine; not only does it guide us on courses, like other Corps, but we use it nearly every day in the barracks and deployed workplace to provide us a framework and protections. This causes us to be actively 'on-board' with its creation, amendment and updating, resulting in the ISR&IO doctrine portfolio being the most current portfolio in the Army Doctrine Library. However, regardless of our standing in the doctrine community it does not see us resting on our laurels, more can always be done.

The state of play

The ISR&IO Doctrine portfolio covers 13 separate publications across both the Application (LWD) and Procedural (LWP) Levels. These publication are required to be reviewed and where necessary rewritten every five years. Until recently, the timeframe required to review and rewrite a publication was extensive and unworkable for the workplace. This was recognised by the Land Doctrine Centre and the Army Doctrine Publication Model was implemented. Under this model, the four phases of publication production (review, assessment, development and production) have been drastically reduced from the historical two year plus timeframe, to just 276 days (normally less for ISR&IO publications). The ISR&IO Doctrine portfolio is funded to maintain a working throughput of between three to five publications per financial year. However currently, we are experiencing a surge and have eight publications in various stages of the model; four in Draft (being rewritten), three in Final Draft (rewrite completed and undergoing a formal edit) and one in Interim (rewritten and released for workplace use; however, undergoing final editing and publishing).

Case Study: Adversary Doctrine

With the acknowledgement that Army adversarial doctrine (Musorian Armed Forces - LWP-G 7-5-1 and LWP-G 7-5-2) has remained stagnant for an unacceptable number of years (nine and seven years respectively), DG TRADOC directed that a new adversarial publication be written. This new Musorian publication; LWP-G 7-5-5, replaces both LWP-G 7-5-1 and LWP-G 7-5-2 and provides near peer, peer and peer plus (emerging) adversary forces fielding the complete range of modern weaponry and equipment. Although the new publication has condensed the existing two publications into a single publication, this has not been at the expense of tactics or procedures. Instead, the chaff has been the minute detail of individual defensive position construction techniques, duplication across chapters and moving the adversary into modern mobile mechanised formations (yes gone are the three to four man threat groups; unless they are dismounted recon). This new publication is currently in the final edit and publishing process and should be available via Doctrine on-line later this year.

However, the future of the MAF as the adversarial doctrine in Army is dim. Commencing next year, the MAF will be replaced by the DATE (Decisive Action

Training Environment) adversary. DATE is a US Army threat force concept that is aligned to real world scenarios and is also currently fielded by the UK and Canadian Armies. It too is originated in the near peer, peer and peer plus adversary threat forces construct. Currently DATE is only employed internationally in the wider Army exercise arena, with the ADF being the first to employ DATE in the 'School House' training environment. This has resulted in the new LWP-G 7-5-5 publication commencing a second rewrite to enable it to sit subordinate to DATE as the 'DATE Adversary TTPs'. This inclusion of DATE TTPs has been positively received by the international DATE community.

DATE for the Army means that they will only have a single adversary force from Kapooka, through their career courses and throughout their Army exercise lives. For the Intelligence Professional it means you only have to learn and understand new equipment capabilities and limitations. The underpinning TTPs will remain widely untouched since your heady days on your career courses at DFSI, DIntTC or SMI (for the really mature members).

Future developments in Doctrine

With the knowledge that the printed publication has declined as the viable medium, the Land Doctrine Centre has been examining ways to modernise doctrine through improved technology and 'bringing doctrine to life' in the information age. Currently three lines of development are being examined simultaneously: The first line of development is the creation of 'live' publications through enhanced authoring capabilities enabling amendments and updates in days and weeks; rather than months and years. The second area is for a marriage between text and full motion video, with a selected few publications are currently being utilised as test beds to replace pages of text with embedded video. For the ISR&IO portfolio this is the future with 11 publications identified to be upgraded. The final line of development is increasing the presence of doctrine on social media and the creation of *The Cove*. The Land Doctrine Centre has been steadily increasing the presence of doctrine on social media; announcing the release of doctrine, providing updates on ongoing doctrine modernisation initiatives and advising users how they can contribute to the development of doctrine. While *The Cove* (www.cove.org.au) is a professional development network for Army that is managed by Forces Command and accessed from outside of the Defence Protected Network. *The Cove* provides access to all unclassified doctrine and unclassified reading material, while providing an opportunity for readers to contribute to the development of doctrine through the use of an online collaboration tool that promotes discussion and professional discourse.

As radical as it sounds, the next generation of trainees may be able to conduct training and assessment serials through Virtual Reality systems, utilising full motion video publications on smart devices. This may be a distance from where we currently stand; however, there is no harm in keeping an open mind to potential technical improvements in the drafting and delivery of doctrine to Intelligence Corps members.

The ISR&IO Doctrine Team looks forward to continue to provide up to date doctrine to you in the second half of 2017.

And remember; Doctrine is not a dirty word.

‘A SPAN OF YEARS’ CAPTAIN VICTOR EDGAR LEDERER, AUSTRALIAN INTELLIGENCE CORPS 1942-1945 [1]

Lieutenant Colonel Glenn Wahlert

Vale Vic Lederer, who passed away in Canberra on 22 May 2017, aged 102.

A rare event occurred in Canberra in August 2016 when the Chief of Army, LTGEN Angus Campbell, and RSM-A, Don Spinks, presented replacement medals to the oldest known member of the Australian Intelligence Corps, CAPT Victor Lederer. Vic, who celebrated his 102nd birthday two months later, considered it ‘the best day of my life’. And what a life it has been so far.

Born in the United Kingdom two months after the start of the First World War, he was the son of an Englishwoman and a successful Austrian businessman who imported British cotton into Europe. However his father was also a reserve officer in an Austrian infantry regiment and was soon recalled to join his unit. Vic remained in the United Kingdom with his maternal grandmother throughout the war, and was finally reunited with his parents in Germany in late 1918. Schooled in Saxony, by his seventh birthday he could speak Dutch, English, German and French.

Vic has a clear memory of Hitler’s rise to power in the early 1930s and the Nazi ‘thugs’. His father, fearing for his son, arranged a job for Vic in England in the cotton industry. ‘You see, Nazi Germany wasn’t very good for my health as, unbeknown to me at the time, my father was born Jewish.’ Having no interest in the cotton industry, Vic was impressed by a book on Australia. ‘The clean air, open spaces and my love of horses is what made it for me.’ In 1937 Vic migrated to Australia and worked as a stockman and timber cutter in the Northern Territory.

Photo: CPL Max Bree, Defence PR.

When war broke out Vic was working in Sydney. ‘I was not going to stand by and watch while Hitler took over the world,’ he said. He enlisted in the 2nd AIF as a private in June 1940, but it was not long before his fluency in German attracted the attention of No. 4 Special Wireless Section, an electronic warfare intercept unit. Acting as a translator, Vic supported the Australian Army’s operations against the German, Italian and Vichy French forces in North

[i] This article is based on several interviews with Mr Lederer in July and August 2016, and his unpublished manuscript, A Span of Years, held by the Australian War Memorial (MSS1155).

Africa and Lebanon. 'My job was to listen to the enemy radio nets and read signals intercepts. Much of it was encrypted, but German aircrew used plain text. There was one chap in particular whose voice I always recognised, and through him and his pals, I was able to build up a picture of their [organisational] structure by identifying enemy units, locations, commanders and even their objectives in some cases.'

With Japan's entry into the war, Vic's unit returned to Australia and, in April 1942, he and most of the staff of the No. 4 Special Wireless Section were transferred to a new signals intelligence unit known as the Central Bureau. Promoted to sergeant, Vic's new job was initially just to learn Japanese, particularly the Japanese military's Kana code. Within a few months he was assessed as 'proficient', was promoted to lieutenant in the Australian Intelligence Corps, and posted to a forward listening post in Papua New Guinea. 'We were near Wau and close to the Japs. Our job was to focus on the smaller Jap radio nets and build up an Order of Battle of the Jap division nearby, identify their commanders and locations, and try to gain intel on their morale and fighting fitness.'

Captain Vic Lederer, taken in late 1945.

For the rest of 1942, and most of 1943, Vic worked as an intelligence analyst in New Guinea, returning to the Central Bureau's Brisbane office in early 1944 where he used the first cypher machine in Australia. Promoted to captain in March 1944, he was sent on a six-week course at Land Headquarters School of Military Intelligence in Brisbane, prior to moving with the advance element of the Central Bureau to Morotai, Netherlands East Indies (now part of Indonesia's Maluku Islands). Morotai was being developed as a major base to support the liberation of the Philippines, and Vic's role was to monitor Japanese communications. It was here that he had to use his personal sidearm for the first time. 'They told us there were about 200 Japs left on Morotai. It was closer to 3000, and if they [the Japanese] had been better at their jobs I wouldn't be here telling you this,' he said. One night a Japanese raiding party crept into the camp and threw grenades at the tents. 'We all scrambled and I contacted the local American infantry battalion for assistance. When we tracked them down, we threw everything we had at them. Killed them all. No regrets.'

Vic remained in Morotai for most of 1945 to support the Australian-led Borneo Campaign and, on his discharge from the Army, he again used his language skills as an immigration selection officer. Working out of Germany, he screened thousands of Europeans who wanted to come to Australia. 'I'd mix among those waiting for an interview and listen to them taking to each other to identify the Nazis and communists. I did my best to help those that were genuine cases, but I picked the best one for myself.' Vic was referring to a beautiful, young, Lithuanian girl, Tina. They have been married for over 66 years.

In an interview with LTCOL Glenn Wahlert in mid-2016, Vic impressed with his remarkable memory. He could recall key dates and people, and even his Japanese and some Malay, but he could not recall what happened to his medals. The Australian Intelligence Corps' Head of Corps, BRIG Stephen Beaumont, arranged for replacement medals and a small ceremony to present them to him in his family home in Curtin, Canberra. Vic was 'thrilled to bits' to meet both the Chief of Army and Regimental Sergeant Major of the Army. 'What an honour for an old fella like me, who played a very small part in the war,' Vic remarked, displaying the modesty of a generation of men and women to whom we owe so much.

LTCOL Glenn Wahlert is an ARes historian with the Army History Unit and is currently researching the history of the Australian Intelligence Corps. He is keen to hear from both past and serving members to record their stories. He can be contacted at ggwahlert@bigpond.com

WHO WERE THE AIF'S INTELLIGENCE OFFICERS?

Lieutenant Colonel Glenn Wahlert

On the declaration of war in August 1914, no specialist Army intelligence service existed in Australia.[1] However, members of the Australian Imperial Force (AIF) did perform intelligence functions on the staff of infantry and light horse units and formation headquarters. In addition, as the war progressed, Australians were employed in an increasingly wider range of intelligence roles with the corps heavy artillery, flying squadrons and intelligence police, and attached to the British Intelligence Corps at General Headquarters. In September 1917, for example, there were over 100 intelligence officer positions within I and II ANZAC Corps.[2]

Recent research to identify those who served in the AIF in an intelligence role between 1914 and 1918 uncovered almost 100 names. Of these, 89 had served as intelligence officers (IOs). [3] The existing records of these IOs were then examined in an attempt to draw some conclusions as to who these individuals were, [4] how they trained, and how they compared with their contemporaries in the AIF. [5]

Who were they?

Of those in the group examined, 58% enlisted as soldiers, while the remainder either transferred their Militia commission to the AIF, or were offered a commission due to previous service or level of education. They represented an educated workforce, with a large percentage of both officers and enlisted men either having a degree, or studying for one on enlistment.

Regardless of their enlistment rank, around half were employed in white collar occupations, with students or teachers the most numerous. [6] The next most common occupation for soldiers was clerk (23%), a trade that appears to have been well regarded in the intelligence field. The average age of the IO group on enlistment was 25 years; 70% were born in Australia, with the remainder primarily from the United Kingdom (with one New Zealander and one born in India) and 15% were fluent in French, German or both.

How typical were they of the AIF?

The profile of the average IO varies from the typical AIF enlistee in a number of ways. First, IOs were slightly older at 25 years, while the average age of members of the first AIF convoy was 21 years, although this increased as the war progressed. [7] The IOs who enlisted as private soldiers included a larger percentage (48%) of white collar occupations than their contemporaries in the AIF, who were mainly blue collar workers. [8] However, the officer IO recruits were similar to their fellow officers, apart from the fact that there was a higher proportion of students and teachers among the IOs.

Captain George Meysey Hammond, MC and Bar, MM, was the IO of 28th Battalion. The sling supporting his useless left arm can be seen in this image, as well as his 'unique' cap (AWM A03367).

The most notable difference between the IOs who enlisted as soldiers and their contemporaries in the AIF was their rapid promotion through the ranks and commissioning. Many of the soldiers selected for intelligence work, and eventual promotion to IO, were exceptional men. George Meysey Hammond, for example, enlisted aged 21 in February 1915 as a private in the 28th

Battalion. Unlike his peers in intelligence, Hammond had worked as a labourer, merchant seaman and postal worker before enlisting and had no previous military service. However his martial and leadership abilities were quickly recognised as he was promoted to corporal while still in training in Perth, and to sergeant soon after joining his unit in Egypt. At Gallipoli, he distinguished himself as a battalion scout under command of the battalion IO, and was awarded the Military Medal.

Wounded in the fighting around Pozières in July 1916, Hammond was commissioned as a 2nd lieutenant on return to his unit from hospital, and immediately became involved in the fighting on the Somme. Wounded again, he lost the use of his left arm, and his Medical Board recommended his discharge. However, the Board agreed to permit him to rejoin his unit provided he remained out of the fighting. Consequently, his commanding officer appointed him battalion IO. Admired by his men as fearless, he could never keep away from the action and, as the battalion IO at Polygon Wood, part of the Third Battle of Ypres in September 1917, he moved forward with the first wave. The citation for the Military Cross he won in this action reads in part:

As the Intelligence Officer, he went forward with the advance party and secured much valuable information. Though only having the use of one arm, he captured a score of prisoners single-handed. He was fearless in the extreme. [9]

Described as 'tall and rather thin, with an exceptionally deep voice', there is no doubt that he was an also an extremely brave, if unconventional, soldier. 'His speech was studded with nautical expressions, and his cap and clothing were freakish and sometimes disreputable.' [10] Hammond went on to command an infantry company and was killed in action at Morlancourt in mid-1918.

George Meysey Hammond followed one of two career paths for junior officers who spent time in an intelligence role. The first, as exemplified by Hammond, was a posting as an IO in a unit or formation headquarters, in part to learn the duties of a staff officer, before moving back to a combat sub-unit. The other, which was far less common, was the specialist who was 'streamed' into a progression of intelligence positions throughout the war. This was the course followed by Major John Rogers. Rogers was among the first to join the AIF on the declaration of war as a 19-year-old private soldier in the 6th Battalion. Like Hammond, Rogers rose rapidly through the ranks, reaching Company Sergeant Major at Gallipoli in July 1915, then Platoon Commander and, by March 1916, had been appointed the battalion's IO.

John Rogers enlisted in the AIF as a private soldier in 1914 and became Blamey's trusted IO in both World Wars (AHU image).

John Rogers went on to serve as an IO on a brigade headquarters, as a General Staff Officer Grade 3 Intelligence (GSO3 Int) with Headquarters 1 Division, and finally as Brigadier Blamey's Intelligence Officer in Headquarters Australian Corps. In a testimonial written by Blamey in 1922, he commended Rogers for his: *…lucid mind and great capacity for taking pains with everything that he undertook. … His bright personality, personal courage and readiness to undertake any task won him great popularity …* [11]

By the war's end, Rogers had been awarded a Military Cross while battalion IO, and was Mentioned in Despatches for his detailed planning of operations as GSO 3 Int at 1 Division. At Blamey's request he served again in the Second World War in several intelligence roles, including the Director of Military Intelligence as a brigadier.

How were they trained?

Initially, the AIF simply provided 'on-the-job' training for its IOs, but when it moved to France in early 1916 they were exposed to a wide range of British schools covering numerous specialist skills, including intelligence. Whenever out of the line, brigade or divisional headquarters would arrange two-week courses for their IOs and intelligence staff. John Rogers recalled attending a 'brief but oft-remembered Staff Course run by Colonel Blamey', commenting that Blamey's teachings were as valuable and applicable in peace as they were in

war, covering, 'such matters as the analysis of a problem and logical methods of dealing with it.' [12] Army and corps-level courses also ran throughout the year. For example, an army intelligence school was established at Harrow School, England, and conducted eight-week courses primarily to prepare officers for divisional and corps intelligence staff positions. The training ended with the interrogation of German prisoners of war in England. [13]

There were no formal selection criteria for those seeking appointments as IOs in the AIF. Indeed, sometimes selection was simply a matter of circumstance, as it was for George Meysey Hammond, or an evident talent for detailed planning, as in John Rogers' case. Others found their way into an intelligence role because they possessed specialist skills, such as ex-police officers who were seconded to the ANZAC or Australian Corps Intelligence Police, or those fluent in French or German who were regularly detached to General Headquarters. What is clear, however, is that, as the war continued, and commanders gained a better understanding of just what intelligence was and how it should be employed, men of proven intellect and ability were handpicked for IO positions, some moving up through the intelligence network from battalion to brigade or division, and even up to corps headquarters. Many of these men formed the basis of the Australian Intelligence Corps when it was re-raised in October 1939. [14]

ENDNOTES

1 The Australian Intelligence Corps had been disbanded in June 1914 and its staff absorbed into the intelligence sections of each of the Military Districts.

2 This included 60 battalions, 15 brigades, five divisional headquarters and the intelligence staff of I and II ANZAC Corps. While an establishment for brigade intelligence officers (IOs) was not approved until early 1918, it was common practice for a junior officer to be detached from a battalion to serve as the brigade IO. See AWM25 423/24, Intelligence – In the Field 1915-19.

3 For the purpose of this article, an IO appointment is defined as having intelligence matters as the primary duty. Such appointments included unit and formation IOs and General Staff Officers Grade 3 (GSO3) on divisional and corps headquarters.

4 Of the 89 officers identified, the National Archives of Australia (NAA) held 53 personnel files. The discrepancy is most likely due to the fact that some of the officers were attached to the AIF from the British Army, with other missing files possibly the result of the misspelling of names or the fact that the files were simply misplaced.

5 For a statistical analysis of those who served in the AIF, see Jean Bou and Peter Dennis, *The Australian Imperial Force: The Centenary History of Australia in the Great War*, Vol. 5, Oxford University Press, Melbourne, 2016.

6 Some 48% of soldiers were white collar workers (50% of officers) and 24% were either teachers or students on enlistment (32% of officers).

7 Ibid., pp. 75–78.

8 Ibid., p. 82. Throughout the war white collar occupations, such as accountants, bank clerks, etc., remained well represented, although labourers and other working class occupations tended to dominate.

9 Personnel file, Meysey George Hammond, NAA. See also AWM personal notes at: https://www.awm.gov.au/images/collection/pdf/RCDIG1068587--16-.pdf

10 A.J. Sweeting, 'George Meysey Hammond, (1892–1918), *Australian Dictionary of Biography*, Vol. 9, Melbourne University Press, 1983.

11 Judy Thomson, *Winning with Intelligence: A Biography of John David Rogers*, Australian Military History Publications, Sydney, 2000, p. 60.

12 Ibid., p. 63.

13 See, for example, AWM4 32/2/11; see also Second Army, Instructions for Intelligence Duties, at: http://cdm15942.contentdm.oclc.org/cdm/compoundobject/collection/p15942coll107/id/116/show/47

14 On 18 October 1939 the Governor-General signed a series of Statutory Rules amending Australian Military Regulations. The amendments included the re-raising of the Australian Intelligence Corps and listed its precedence as below 'Australian Tank Corps' and above 'Australian Army Chaplains' Department'.

QUEENSLAND VOLUNTEER BRIGADE: INTELLIGENCE CORPS 1878-1880

Mr Lindsay Wilson

In the 1870s tensions broke out between the predominately Muslim Ottoman Empire and Western Europe focussed in mistreatment of Christians in the Balkans. In 1876, a series of military actions, including the Royal Navy sailing up the Dardanelles to Constantinople, led to Eastern Europe allied against Austria, Britain and France.

Uncomfortable in their relative isolation, noting the tiny presence of the Royal Navy in the region and poor state of their land defences, the Australian colonies engaged Britain for advice. In August 1877, Colonel Sir William Jervois and Lieutenant Colonel Peter Scratchley inspected the defences of Queensland. They considered the long coastline of Queensland, dispersed settlements and developing resources as an invitation for an enemy incursion to push foreign imperial agenda in times of heightened tension. They identified that information for defence planning in Queensland was virtually non-existent.

In Scratchley's report to the Queensland Government was the recommendation for '… attaching to the Headquarters Staff of a small body of officers and men, to form an Intelligence Corps, who will undertake in time of peace the preparation of accurate plans of the country between Brisbane and the sea coast, and between the other large towns in the north and the sea. In time of war they would be required to perform the duties of scouts, guides, orderlies, and escorts, and would cooperate with the mounted police in harassing an enemy who attempted to advance upon Brisbane–most of the men should be thorough horsemen, possessing a good eye for country.' [i]

Consequently, Joseph Adams was appointed as Captain in command of the 'Intelligence Corps', Queensland Volunteer Brigade on 26 October 1878. [ii] As a property valuer in civilian life, Adams was a logical choice and he apparently set out to develop a capability. Given the nature of part time soldiering, there is no surprises in Scratchley's third progress report of February 1879 wherein: '… Captain Adams, the Intelligence Officer, has been requested to prepare military plans of the surrounding country, showing the roads and principal features; for at present no plans whatever exist, and the want of them would be seriously felt in time of war. Captain Adams has under taken to procure the necessary volunteer assistance to enable him to proceed with the work. He requires a suitable room, which I have no doubt it will be possible to find in some Government building.' [iii]

Joseph Adams in the uniform of a Lieutenant Colonel of the Queensland Defence Force. The image probably dates from early 1900s when he was awarded the Colonial Auxiliary Forces Officers' Decoration for long service.

One activity known to have been undertaken by Adams was to set in motion practices to improve communications between forward forces and headquarters. At the annual Volunteer Encampment at Eagle Farm in 1879 he was responsible for the establishment of a telegraph link back to Government House at the Domain in Brisbane. A feature of that encampment was heavy rain and boggy conditions at the low-lying race course where the encampment was held. The telegraph operator

Joseph Adams in the uniform of a Lieutenant Colonel of the Queensland Defence Force. The image probably dates from early 1900s when he was awarded the Colonial Auxiliary Forces Officers' Decoration for long service.

working for Adams was Gunner Edwin Welsby of No 1 Battery, Queensland Volunteer Artillery. Shortly after the encampment Gunner Welsby died, attributed by the press, to the effects of exposure during the encampment. He was accorded a military funeral and interred at Toowong Cemetery. [iv]

In July 1880, Adams was promoted to Major and had gained the assistance of Captain George Weale [v] , a surveyor in civilian life and Adjutant 2nd Queensland Regiment (Toowoomba). However, the Intelligence Corps was short lived as Adams and Weale were posted to the Headquarters Staff in September 1880. There is no further mention of the Intelligence Corps in Queensland records.

Adams went on to serve in a range of logistic support roles until his retirement in 1891. Weale, was mentioned in the local press for courage is helping supress a fire at Toowoomba in January 1881. [vi] He did conduct survey work at the Toowoomba rifle range in 1881. [vii] He left military service and died of dysentery in outback Queensland in 1886. [viii]

It is likely that Adams and Weale were unable to meet the challenge set down by Scratchley. Part-time service and the reluctance of colonial government to spend on the military is likely to have prevented real progress. In hindsight, it is likely that Scratchley did not appreciate what was readily available in the various departments of the Queensland Government. The Crown Land's Office was active in surveying and publishing maps of Queensland. A typical notice in the Queensland Government Gazette of the time stipulated: '… public officers are hereby required to afford … the fullest information possible, and permit … access at all reasonable times to maps, plans, and other public documents …' for public interests. [ix]

The development of the fortifications at Lytton established a military presence in the very area that Scratchley was concerned about. His thinking on scouting in wartime was reasonable, but there were horsed troops in the colony and would later develop into the capable Queensland Mounted Infantry. By 1880, published discussions by officers of the colonial military were demonstrating a clear understanding of potential incursion routes. [x] It is a reasonable assessment that Scratchley's recommendations were unnecessary. The first topographic map produced for the Colonial Government in Queensland was prepared in 1886 by Lieutenant Edward Cave Owen (at right) from the Defence Force. This map covered the township of Fort Lytton and adjacent country. [x] The demise of the Intelligence Corps was not detrimental and the Queensland Defence Force soldiered on until absorbed by the Federal forces on 1 January 1901.

ENDNOTES

[i] *The Brisbane Courier*, 3 August 1878 p.5 and *The Queenslander* 10 August 1878, p. 604

[ii] Joseph Hodgson Adams. Late British 72nd Regiment of Foot. Staff Sergeant 1 Coy, QVB 1867. Second Lieutenant No 1 Company, 23 February 1870. Captain 21 February 1877. Captain in command of the Intelligence Corps, Queensland Volunteer Brigade, 26 October 1878. Noted in The Week 12 June 1880 for leading locals fighting a fire at a house in the Valley, cited as being in the 'Intelligence Corps'. Major Intelligence Corps 30 July 1880. Staff 24 September 1880. He served in a range of staff appointments and was placed on the Retired List 6 March 1891.

[iii] *The Queenslander*, 22 February 1879, p. 245.

[iv] *The Brisbane Courier* 9 May 1879

[v] George Telford Weale. Appointed Lieutenant, 8 Coy, QVB 7 April 1876, vice Baxter. Captain 2 Queenslanders 30 July 1880. Transferred to Intelligence Corps 30 July 1880. Transferred to Staff 24 September 1880. Captain QDF 1885, seniority 30 July 1880. Unattached List QDF 24 February 1885. Died 1886.

[vi] *Toowoomba Chronicle and Darling Downs General Advertiser* 25 January 1881, p. 3.

[vii] *The Brisbane Courier* 5 February 1881, p. 6

[viii] *Toowoomba Chronicle and Darling Downs General Advertiser*, Saturday, June 12, 1886

[ix] *Queensland Government Gazette* 1880, p. 360. The Crown Lands Office had an active survey and mapping function, which would have been available for Defence purposes in time of war.

[x] The Brisbane Courier 28 July 1880, p. 3.

[xi] Queensland Government at https://www.qld.gov.au/recreation/arts/heritage/museum-of-lands/topographic-maps/

BOOK REVIEWS

The Peril of Incrementalism: A Call to Read 'Dereliction of Duty'

Reviewed by Lieutenant Colonel Ping Han Chua

It is indeed an uncommon occasion in history when a theorist is able to apply their teachings directly to the field of expertise. International development experts watch with semi-morbid fascination as Ashraf Ghani, who co-authored the book 'Fixing Failed States' with Clare Lockhart, struggles to bring institutional renewal and stamp out corruption after his election as President of Afghanistan.

In the same way, those who study military strategy and civil-military relationships relished the appointment of LTGEN H.R. McMaster as the US National Security Advisor in the Trump Administration. Those who have followed McMaster's career are familiar with his intellect, direct nature and operational experience (he commanded the US 3rd Armoured Cavalry Regiment in Ninewah Province, Iraq, in 2005).

President Trump's appointment of McMaster prompted me to pull '***Dereliction of Duty: Lyndon Johnson, Robert McNamara, the Joint Chiefs of Staff, and the Lies That Led to Vietnam***' off my bookshelf. It is an adaptation of McMaster's PhD thesis and has earnt a reputation as a dense and incisive study of this important period in modern US history. McMaster's dissection of the decision-making and political dynamics of the Kennedy and Johnson administrations is impressive in its detail and lucidity. His research brings to life the day-to-day machinations of national strategy, and his analysis and conclusions are a damning indictment of the hubris and deception within the political and military echelons. It is a book that deserves to be read by military professionals, civil servants and political leaders. 'Dereliction of Duty' is not so much a history book, but a moral story.

At its heart, 'Dereliction of Duty' is an exploration of how military strategy, when pursued as a consensus-building exercise to walk a middle course, can result in failure and the disastrous loss of lives and treasure. McMaster builds a compelling story of deliberate deceit, concealment, self-censorship and compromise amongst the President, his national security staff and the Joint Chiefs. The book deals with the three years in which the US 'sleep-walked' into a massive commitment to Vietnam without a clear set of strategic goals. When McMaster lays out the US approach of gradually 'ramping up' its military response to the communist regime in North Vietnam, one gets the sense of strategy applied like a dining room light dimmer switch. Then-Secretary of Defense Robert McNamara was under the dangerous illusion that the use of force - once ratcheted up - could be easily dialled back. To him and others in the US Administration, war could be operated like a system based on rational cost-benefit calculation.

'You Fight the War You Have - Not the War You Want'

President Johnson is laid with primary, overarching responsibility for the massive US commitment to

Vietnam. After replacing the assassinated John Kennedy, LBJ was fixated on his 'Great Society' platform of social justice and civil rights in the US. Ironically, he saw the brewing conflict in Vietnam as a side-show that needed to be prevented from detracting from his domestic agenda. Every political decision for the Vietnam problem was thus cast in this light; LBJ acceded to McNamara's gradual approach and deliberately attempted to conceal or deceive the public as to the growing scale of US involvement.

The gradual approach was in fact the means of getting the US knee-deep into Vietnam; it had the exact opposite result that LBJ intended. McNamara, deeply influenced by the successful management of the Cuban missile crisis, mistakenly assumed that precise military actions by the US would result in predictable responses from the North Vietnamese leaders. This 'strategic messaging through the use of force' elicited the wrong or opposite reaction: instead of deterring the Communists from subverting South Vietnam, early US bombings spurred the North Vietnamese to increase the pace of their takeover campaign. [1] The graduated force strategy might be excusable were it not for a Pentagon war game that correctly predicted the results of such a strategy: a cycle of escalation and force commitments from which the North Vietnamese or the US could pull back. The war game was disregarded.

'Dereliction of Duty' thus casts the Vietnam problem in a light that is very familiar to us - how does a nation fight a war of limited objectives? When national survival is not at stake, how does a country avoid committing far more than any potential benefit that might be gained? The call of the book is to avoid the alluring myth of doing the minimum, rather than doing what might be required. In the early stages, the Administration faced a fork in the road of abandoning the decrepit South Vietnamese government, or making a full-blown military commitment to try and defeat the Communists with overwhelming force. Instead the consensus-based, middle path ensured the US defaulted to the latter choice, but long after any reasonable prospect of political victory had passed.

This disastrous incremental approach was aided and abetted by the mis-matched, and sometimes toxic and dysfunctional relationship between the President and national security staff, and the Joint Chiefs. [2] Once again, LBJ's fixation on his domestic agenda, and maintaining a facade of unity, shaped everyone else in the strategic apparatus. The Joint Chiefs, who advocated a 'massive response', were themselves riven by inter service rivalry, and willingly supported smaller initial deployments in the hope that the President would authorise larger deployments later. McNamara's graduated approach came undone when incremental military actions and troop commitments became a self-perpetuating logic, to the point where the US found itself 'owning' the war.

Given the dire warnings contained in the book, one cannot help but think how HR McMaster, as the US President's 'point man' for coordinating national security strategy, would heed his own writing. While it is oft said that 'information without influence is useless', the book also teaches that influence that is prized over good information is immoral and can invite catastrophe. 'Dereliction of Duty' warns against the effects of over-reliance on a close, like-minded circle of advisors.

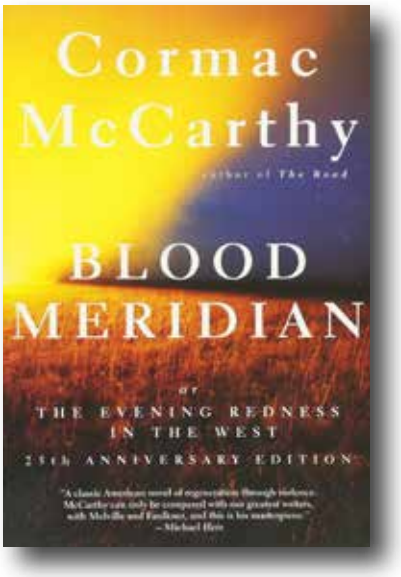
It is unclear where McMaster lies in the pantheon of those who exert influence on President Trump. One can hope that the US strategy on intractable problems such as defeating global violent extremist ideologies, and the North Korean nuclear game does not result in that nation once again 'sleep walking' into an untenable situation. For the rest of us, this is a book that deserves to be read.

[1] Separately, the idea of military force as messaging is very well handled in another excellent book 'War from the Ground Up' by Emile Simpson.

[2] In fact, McMaster's acerbic description of the most senior military commanders of that period prompted a US general to remark that 'McMaster would one day make a good colonel'!

Blood Meridian or The Evening Redness in the West

Reviewed by Warrant Officer 2 Anthony Knowlton



Author: Cormac McCarthy
Publisher: Knopf Doubleday Publishing Group

Blood Meridian is a dense, violent, anti-Western that is challenging both thematically and grammatically. Despite this, it rewards the determined reader with a vivid, intensely well-researched portrayal of the United States – Mexico borderlands during the mid – 1800s.

Written in 1985 by American author Cormac McCarthy, it has been hailed as a literary masterpiece, and one of the great, modern American novels. Despite being a confronting tale, the ugliness of the content is balanced by the lyricism of the narrative voice.

Central to the narrative are the twin figures of 'the kid' and Judge Holden. The book documents their shared experiences as part of a historical group of bounty hunters known as the Glanton gang.

The kid begins as the *everyman*. A nondescript teenager of inauspicious beginnings, he is the avatar through which the author asks us to consider the increasingly chaotic and gruesome events that unfold. His ignorance (and thereby relative innocence) is contrasted against Judge Holden, the physically massive, highly educated anti-hero. The Judge's attitude is summed up in his description of war:

> *"War was always here. Before man was, war waited for him. The ultimate trade awaiting its ultimate practitioner."*

In this statement, the Judge appears to surrender himself to war as a preternatural force, indulging of his own depravity as an exercise of fate. Here the author challenges a key assumption of the nature of violence and humanity - by portraying the most powerful, educated character in the novel as the one most capable of deliberate brutality. The author denies the reader access to the characters' inner monologues. By doing this, he allows us to exercise critical judgement of their actions, and thus reflect on the following questions:

What is murder during war?

Is humankind ultimately destructive?

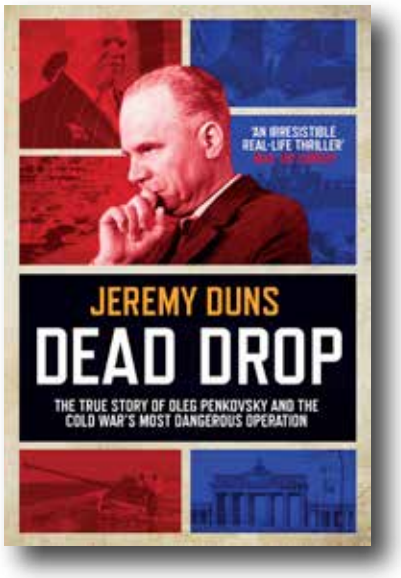
And most importantly…

> *Should we demonise our foe? And in doing so, do we create a creeping justification for unnecessary brutality, for the sake of 'sending a message'?*

The novel satirises the Western genre, presenting both the Glanton gang, and the Native American tribes they hunt, as equally capable of extreme violence. It is an essential read for anyone interested in ethics, and in exploring the moral rules of warfare in non-state conflicts.

Dead Drop: The True Story of Oleg Penkovsky and the Cold War's Most Dangerous Operation

Reviewed by Sergeant Robert McMinn



Author: Jeremy Duns
Publisher: Simon & Schuster UK

Oleg Penkovsky, codenamed HERO was a colonel with Soviet Military Intelligence (GRU) during the late 1950s and early 1960s, who informed the United Kingdom and the United States about the Soviet emplacement of missiles in Cuba. The story of his cooperation with MI6 and the CIA is commonly known, and has been the inspiration for many spy-fiction novelists, including Jeremy Duns. However, the circumstances that led to his discovery by the KGB, and his subsequent arrest, still remains a mystery.

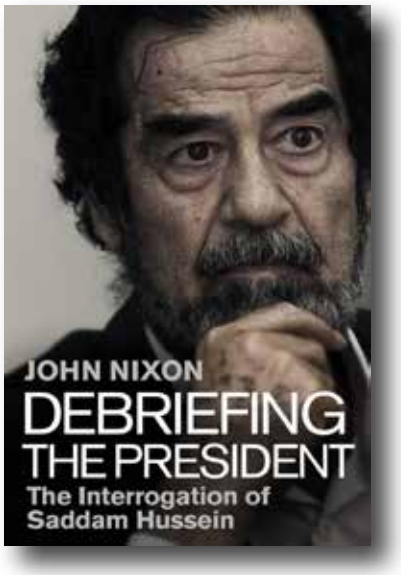
Dead Drop is the author's first non-fiction spy novel, which aims to provide the reader with an insight into the high stakes, high drama world of espionage during the Cold War era, while attempting to uncover how, and when, the KGB identified him as a traitor. *Dead Drop* is a very thorough and entertaining account into one of the most important double agents during the Cold War.

I found it impossible to put the book down; this was due to both my interest into the topic, but mostly the writing style of the author. Duns' background as a spy-fiction writer immersed me in the in the lives of Penkovski, and all who were involved in the handling of his collection operations against the Soviet Union. I felt the tension associated with every meeting, and exchange of information, and as someone that is not source operations qualified, it provided me with an appreciation into some of the tradecraft used, and the complexities of running a source, especially during the Cold War.

I would recommend this book to anyone who is interested in espionage in the Cold War era. The Penkovski case was the inspiration for spy-fiction novel, *The Russia House* by John le Carré, so if you are familiar with it, you should also read *Dead Drop*.

Debriefing the President: The Interrogation of Saddam Hussein

Reviewed by Private Brihannan Carr



Author: John Nixon
Publisher: Blue Rider Press

Debriefing the President is an intriguing account of one senior CIA leadership analyst's experience conducting prolonged interrogation of Iraqi President Saddam Hussein. Nixon was deemed an expert on Hussein, and spent three years attempting to learn every detail of the Iraqi President's life prior to his trial and subsequent execution.

Nixon was required to conduct an official ID of Saddam Hussein relying on scars, tattoos and a set of specific questions that only Hussein himself could answer. Once it was confirmed the US military forces had in fact captured the elusive Saddam Hussein, Nixon conducted the first ever prolonged interrogation on the Iraqi President.

Nixon describes Saddam as, "tough, shrewd and manipulative" and stated that "he (Saddam) was a ruthless dictator who, at times, made decisions that plunged his region into chaos and bloodshed."

Despite this, *Debriefing the President* makes you wonder if the Iraq War was worth it. You find yourself asking the question, would US and coalition forces currently be fighting the enemy we now face if Saddam Hussein had remained in power? The book presents Hussein in a way that considers his actions and approaches of leadership and acquiesces that he may have been capable of maintaining a balance between the Shia and Sunni communities, notwithstanding his cruel and inhumane approaches.

Nixon believes, like many others, that the US effort to capture Saddam was misguided, and came at a high price. Nixon states, "in hindsight, the thought of having Saddam Hussein in power seems almost comforting in comparison with the awful events and wasted effort of America's brave young men and women in uniform, not to mention the $3 trillion dollars and still counting we have spent to build a new Iraq."

No Silver Bullets: The Perception and Promise of Norms in Cyberspace

Reviewed by Captain Travis Hoffman

International Cyber Norms: Legal, Policy and Industry Perspectives

Anna-Maria Osula and Henry Rõigas (Eds)

NATO Cyber Defence Centre of Excellence (CCDCOE), 255 pp.

Available online at: https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html

One might be forgiven for believing the hype - a scan of contemporary cyberspace-focused media holds that "norms" are the panacea for the internet's ills, promising to transform it from a "wild, wild, West" to a true global commons. [1] This, however, is where the consensus ends, with the diverse range of perspectives among stakeholders and the nascent nature of cyberspace generating uncertainty and tension in any subsequent discussion.

International Cyber Norms: Legal, Policy and Industry Perspectives clarifies this quagmire - it abstains from proffering solutions and aims instead at a better understanding of the topic. [2] Having emerged from a series of CCDCOE workshops throughout 2014-2015, the piece's diverse authorship represents a microcosm of the phenomena it addresses, namely norm formation for cyberspace. [3] The book exceeds its namesake promise, not only detailing stakeholder perspectives, but proffering sound meta-analyses of these views and the very nature of norms. While the book as a whole serves as an effective introduction to the field, individual chapters lose little by being read in isolation.

The book's scope ought to be commended and is achieved without significant sacrifice in its analytical depth. Its consistent terminological clarity and overall coherence are impressive in light of this breadth and depth; there is early acknowledgement of the potential for ambiguity and a concerted effort to

[1] A. Chowdhry, *Obama looks to avoid cyber arms race*, Federal Computer Week, Sep 06 2016, available online at URL: https://fcw.com/articles/2016/09/06/obama-putin-cyber.aspx; B. Obama, *2016 G20 Summit Closing Address*, Speech, 5 Sept 2016, available online at URL: https://www.youtube.com/watch?v=mkFHCQRJMg4; B. Wilkins, *President Obama Warns of 'cyber arms race' with Russia*, Digital Journal, 7 Sept 2016, available online at URL: http://www.digitaljournal.com/news/politics/president-obama-wants-to-prevent-cyber-weapons-arms-race/article/474196; C. Krauthammer, *Column: Norms of international behaviour have run off the rails*, Fredericksburg, Sept 10 2016, available online at URL: http://www.fredericksburg.com/opinion/columns/column-norms-of-international-behavior-have-run-off-the-rails/article_97dc77df-80c3-557d-896c-4ef2cebee327.html; F. Hanson, *What the G20 can do to advance cyber norms*, The Interpreter, The Lowy Institute, 24 Aug 2016, available online at URL: http://www.lowyinterpreter.org/post/2016/08/24/What-the-G20-can-do-to-advance-cyber-norms.aspx.

[2] A.M. Osula, H. Rõigas (Eds), *International Cyber Norms: Legal, Policy and Industry Perspectives*, NATO CCD COE Publications, Tallinn, 2016, available online at URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf.

[3] NATO CCD COE, *International Cyber Norms, Legal, Policy and Industry Perspectives*, NATO CCD COE Website Library, 2016, available online at URL: https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html.

mitigate this throughout. [4] Specialised terminology is explained well when required, such as the Chapters 2 and 3, elaboration of legal *patois*, the Chapter 5 elucidation of international relations parlance and the nuanced interpretations of regional conceptions of contested terminology in Chapters 3, 6 and 9 especially. [5]

The diverse range of contributors inevitably generates tension within the book, such as the stark contrast between the normative advocacy among the industry perspectives late in the book, and its otherwise clinically objective tone. [6] This blemish, however, is countervailed by perspectives throughout the book, most notably Prof Austin's prescient admonishment against moral rectitude in normative analysis. [7] His treatment of China's national security motivations also effectively straddles theory and practice, an approach not applied uniformly throughout the book. An occasionally academically solipsist approach, evident in Chapter 6's inventory of Estonia's approach, Chapter 10's single-minded advocacy for technological integrity and Chapter 11's effusive proposal for a cyber-security ontology, while meeting the intents of the chapters, detracts from the book's overall readability. [8]

The book serves as a microcosm of norm formation in cyberspace, in that it contains many disparate voices. While the book admirably answers many questions, it perhaps more importantly raises many more, much like all developments in the field that it seeks to describe. In doing so, the book reveals its greatest strength; it leaves the reader with the distinct impression that for both scholars and practitioners in the field of cybersecurity governance, there are no silver bullets.

[4] AA.M. Osula, H. Rõigas, 'Introduction' in A.M. Osula, H. Rõigas (Eds), op. cit., pp.11-22.

[5] M.N. Schmitt & L Vihul, 'The Nature of International Law Cyber Norms' in A.M. Osula & H. Rõigas (Eds), op. cit., pp.23-48; S. Watts, 'Cyber Law Development and the United States Law of War Manual' in A.M. Osula & H. Rõigas (Eds), op. cit., pp.49-64; T. Erskine & M. Carr, 'Beyond 'Quasi-Norms': The Challenges and Potential of Engaging With Norms in Cyberspace' in A.M. Osula & H. Rõigas (Eds), op. cit., pp.87-110; M Kaljurand, 'United Nations Group of Government Experts: The Estonian Perspective' in A.M. Osula & H. Rõigas (Eds), op. cit., pp.111-128; G. Austin, 'International Legal Norms in Cyberspace: Evolution of China's National Security Motivations' in A.M. Osula & H. Rõigas (Eds), op. cit., pp.171-202.

[6] I. Chintzes & S. Alam, 'Technological Integrity and the Role of Industry in Emerging Cyber Norms' in A.M. Osula & H. Rõigas (Eds), op. cit., pp.203-220.

[7] G. Austin, op. cit., p.172.

[8] M. Kaljurand, op cit.; I. Chintzes & S. Alam, op. cit.; C. Vishik, M. Matsubara & A. Plonk, 'Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms', in A.M. Osula & H. Rõigas (Eds), op. cit., pp.221-242.

TRAINING AWARDS AND PRIZES

Royal Military College Award Recipients

LT Robert Campbell (Session 1 2017). *Queens Medal, NZ Army Chief of Army Prize*, awarded to the graduate with the most consistent effective performance in leadership positions, *Thales Australia Prize* awarded to the graduate achieving highest aggregate marks in all Military Skills and Field Leadership Assessments, and the *Australian Intelligence Corps Prize* awarded to the overall best performing graduate allocated to the Corps.

LT Hannah Ryall (Session 2 2016). *The Australian Intelligence Corps Prize.*

LT Emma Randall (Session 1 2016). *RMC Trophy*, awarded to the most proficient female graduate at Physical Training, and the *Australian Intelligence Corps Prize*.

LT James Harvey (Session 1 2016). *NZ Army Chief of Army Prize*.

LT Brayden Joy (Session 1 2016). *The Major Robert Morrison Prize*, awarded to the graduate who has demonstrated, during their time at RMC, consistent oratory skills, including delivery of oral orders, public speaking and debating.

Defence Force School of Intelligence Prizes

Initial Employment Training

Session 25:
TPR Nathan McGowan, *Student of Merit*
CPL Ben Howson, *Academic Award*

Lieutenant Robert Campbell receiving the Queens Medal, NZ Army Chief of Army Prize, from the Australian Minister of Defence, the Honourable Marise Payne.

Session 26:
TPR Jon Murcott, *Student of Merit*

Session 27:
LCPL James Leask, *Student of Merit*
PTE Mathew Johnson, *Academic Award*

Session 28:
PTE Nicola Karakatsanis, *Student of Merit*
PTE Oscar Morgain, *Academic Award*

Session 29:
SGT Matthew Raymer, *Student of Merit*
TPR Callum Brunn, *Academic Award*

Regimental Officers Basic Course

Session 14:
CAPT Joshua Copland, *Student of Merit*
LT Tai-Li Hafon, *Academic Award*

Army