



Issue 3, Number 1
2015

Salus Journal

A peer-reviewed, open access journal for topics concerning
law enforcement, national security, and emergency management

Published by
Charles Sturt University
Australia
ISSN 2202-5677



Issue 3, Number 1, 2015

www.salusjournal.com

Published by

Charles Sturt University
Australian Graduate School of Policing and
Security
PO Box 168
Manly, New South Wales, Australia, 1655

ISSN 2202-5677

Advisory Board

Associate Professor Nicholas O'Brien (Chair)
Professor Simon Bronitt
Professor Ross Chambers
Professor Mick Keelty AO, APM
Mr Warwick Jones, BA MDefStudies

Editor-in-Chief

Dr Henry Prunckun
Charles Sturt University, Sydney

Assistant Editor

Ms Kellie Smyth, BA, MAppAnth, GradCert
(LearnTeach in HigherEd)

Web Editor

Mr Patrick McKenzie

Editorial Board—Associate Editors

Dr Jeremy G Carter
Indiana University-Purdue University
Dr Anna Corbo Crehan
Charles Sturt University, Canberra
Dr Ruth Delaforce
Griffith University, Queensland

Dr Garth den Heyer
New Zealand Police

Associate Professor Michael Eburn
Australian National University, Canberra

Dr Victoria Herrington
Australian Institute of Police Management

Dr Valerie Ingham
Charles Sturt University, Canberra

Dr Stephen Loftus
Oakland University, Michigan

Dr Stephen Marrin
James Madison University, Virginia

Dr David A McEntire
University of North Texas

Professor Alida Merlo
Indiana University of Pennsylvania

Dr Alexey D. Muraviev
Curtin University, Perth, Western Australia

Dr Maid Pajevic
*College 'Logos Center' Mostar,
Bosnia-Herzegovina*

Associate Professor Felix Patrikeeff
University of Adelaide, South Australia

Dr Tim Prenzler
Griffith University, Queensland

Dr Suzanna Ramirez
University of Queensland

Dr Susan Robinson
Charles Sturt University, Canberra

Dr Rick Sarre
University of South Australia

Professor Emeritus Joseph Scanlon
Carleton University, Ottawa Canada

Dr Brian Sengstock
University of the Sunshine Coast, Queensland

Mr Jason-Leigh Striegher, MA
Charles Sturt University, Sydney

Dr Patrick F. Walsh
Charles Sturt University, Sydney

Dr Grant Wardlaw
Australian National University, Canberra

Dr Troy Whitford
Charles Sturt University, New South Wales

Salus Journal

Issue 3, Number 1

2015

Contents

Analytical Essay

- Raising New Zealand's Terrorism Threat Level:
Is Transparency Important in National Security?**
Richard Shortt 1

Research Articles

- The Hidden Advantage in Shoot/Don't Shoot
Simulation Exercise for Police Recruit Training**
Amanda Davies 16
- First Principles of Intelligence Analysis:
Theorising a Model for Secret Research**
Henry Prunckun 31

Book Reviews

- Applied Thinking for Intelligence Analysis: A Guide for Practitioners***
Trista M. Bailey 48
- Police Leadership and Management***
Alan Beckley 51

Licensing

All material published in *Salus Journal* is published under a Creative Commons License. Under this licence you are free to copy and distribute the essays, articles, and reviews under the following conditions: 1) you give attribution to the author(s); 2) the essays, articles, and reviews are not used for commercial purposes without written permission of the author(s); 3) that you do not alter, transform, or build upon the essays, articles, or reviews; and 4) further distribution is based on the "share-alike" principle.

Analytical Essay

RAISING NEW ZEALAND'S TERRORISM THREAT LEVEL: IS TRANSPARENCY IMPORTANT IN NATIONAL SECURITY?

Richard Shortt*

In mid-October 2014, ten years after the New Zealand Government confirmed the establishment of a Combined Threat Assessment Group (CTAG) to advise it on a range of potential threats, the prime minister announced, for the first time, the raising of New Zealand's domestic terrorism threat level. Unfortunately, the assessment that gave rise to the threat level's change (or a version of it) was not made public. Therefore, how were New Zealanders or others expected to properly understand the environment giving rise to the threat changes, and to judge whether the assessors got the setting right. This paper argues increased public transparency is appropriate when additional security measures resulting from a change in threat perception impact citizens' lives and cost taxpayers more money. In presenting this argument, the paper briefly describes the role of threat assessments and how threat levels are set. In the absence of a public version of New Zealand's threat assessment giving a cohesive, concise and transparent outline of the threat environment, the paper presents publicly available information from well-informed high office holders to see if that provides alternative and suitable transparency. Finally, the paper compares New Zealand's terrorism threat assessment transparency processes with those of four countries with similar characteristics to New Zealand to see if alternative models of public transparency are available for consideration.

Keywords: New Zealand, threat assessment, risk analysis, counterterrorism, national security assessment

INTRODUCTION

In mid-October 2014 the New Zealand prime minister confirmed that the country's terrorism threat level had been raised from Very Low to Low (Watkins, 2014). That change signalled that threat assessors and senior bureaucrats agreed that the potential for a terrorist attack in New Zealand had moved from being considered "unlikely" to "possible, but is not expected" (New

* Corresponding author: rshortt@csu.edu.au

Zealand Government, n.d.), a subtle change one might suggest.¹ Subsequent statements by both the New Zealand prime minister and the director of the New Zealand Security Intelligence Service (NZSIS) (Key, 2014; Young, 2014) in early November 2014 provided an opportunity—unusual in New Zealand’s case—to assess the newly confirmed level against the rhetoric of two well-informed high office holders. The opportunity for comparison was defined as unusual given New Zealand does not publish a public version of its threat assessments,² and because this was the first time the Government had publicly released the country’s threat level (IS sparks terror law tightening, 2014) in the decade since it instituted the Combined Threat Assessment Group (CTAG) to provide such advice (Clark, 2004).

Since the events of September 11, 2001 in the United States, and the subsequent wars fought in Afghanistan and Iraq, the world is a more security conscious place (Archer, 2005, p. 398; Pickering, McCulloch & Wright-Neville, 2008, p. 1). That consciousness permeates to countries that once considered themselves geographically remote from such issues, like New Zealand for example (Clark, H. 2002). Now, informed by a range of media sources—including social media—that present news from around the globe as events unfold, citizens are arguably more conscious of threats through this regular delivery of “focusing event” (Birkland, 2004, p. 181) linked stories. Alongside the increasingly well-informed citizenry, governments, including that of New Zealand, are claiming they are now amenable to their national security sectors being more transparent regarding the efforts they take on behalf of citizens (Bushnell & Wilson, 2014, p. 15; Fisher, 2014b).

In general terms, public agency transparency has been linked to increased trust in government, and trust in government has been linked to greater citizen satisfaction and economic prosperity (Ayres & Braithwaite 1992, Levi & Stoker 2000, Fukuyama 1995, Inglehart 1999, and Putnam 2000, as cited in Grimmeliikhuijsen, 2009, p. 174). Taking the issue of transparency’s value further, O’Neill (in Moore, 2014, pp. 131–132) is quoted as saying that “[s]ome claim that it is the ‘key to better governance’, to stemming corruption and to accountability.” If O’Neill—and those she paraphrases—are correct, then New Zealand, having slipped from first equal to second place in the 2014 Corruption Perceptions Index (Transparency International, 2015) may well be interested in reclaiming its previous top ranking.³

In New Zealand's particular case, its intelligence institutions had suffered damage to their levels of public trust and confidence as a result of the leaking of intelligence by Chelsea Manning and Edward Snowden, and domestic revelations of the Government Communications Security Bureau exceeding its legal mandate while assisting New Zealand Police (Fisher 2014a; New Zealand Intelligence Community, 2015). The move towards greater national security transparency (Fisher, 2014b) was, unsurprisingly, confirmed as an attempt to build and strengthen public trust in the efforts of the security and intelligence communities (Bushnell & Wilson, 2014, p. 15; Fisher, 2014b).

Therefore, it was noticeable that when New Zealand lifted its terrorism threat level no publicly transparent rationale for the change was provided by the agencies responsible. Despite there being an apparent acceptance of the value of increased transparency (Bushnell & Wilson, 2014, p. 15; New Zealand Intelligence Community, 2015), when it came to an issue resulting in heightened security activity, law changes and additional expending of seven million dollars of tax-payer funds on the security intelligence service (Key, 2014), there was limited official explanation as to why.

In examining the issue of New Zealand's threat assessments and transparency, this paper discusses the role threat levels play in the security environment and describes how they are determined. The paper then presents the only publicly available commentary on what caused the changes to New Zealand's threat level and asks the rhetorical question: Are they a suitable replacement for publication of an official and transparent rationale for the threat level change? The paper discusses the publicly available information provided by four Scandinavian countries that share similar characteristics to New Zealand. In doing so the paper argues that the Norwegian policy of transparently providing such information is an alternative policy model that New Zealand could consider, particularly if it is serious about transparency and trust being important issues for the national security sector, which it appears to be (Fisher, 2014b; New Zealand Intelligence Community, 2015). The paper is not a detailed or methodical comparison of threat assessment techniques, decisions or security environments.

THE THREAT ASSESSMENT PROCESS

Before considering the transparency of the change to New Zealand's threat level, it is useful to outline what a threat assessment is and how a level is determined.

Threat levels by themselves are blunt instruments, irrespective of how well nuanced they are or should be, and only ever provide one piece of a multi-piece “jigsaw.” The jigsaw, or to use its technical name “risk analysis” (Prunckun, 2015, p. 283), is a more complex process and requires additional inputs before it can advise on what protective security actions need to be taken in response to a change in threat perception (Prunckun, 2015, p. 300–301). A need for additional protective security action will, in all likelihood, result in tax-payer funded activities such as increased access controls to particular premises and places, a more visible security presence in public spaces and increased government agency planning and focus on events and people of concern (2015, p. 283). Therefore, heightened public interest (and associated accountability) can be expected when a decision is taken to change a threat level to a higher setting.

As an input to the risk analysis jigsaw, threat assessment seeks to determine the levels of intent and capability residing in those who may seek to cause harm (Prunckun, 2015, p. 284–285) and to report that through reference to a series of pre-defined level statements. Detected threats fall into one of two categories: general threats or specific threats. A general threat arises from events occurring in the wider environment—such as the rise of the Islamic State (IS—also referred to by various commentators in this paper as ISIL and ISIS) and its call to jihad—which have or are likely to have an impact on the environment being assessed (i.e. New Zealand’s domestic security environment).

Alternatively, a specific threat is where information is available identifying a particular person (or group) as having both the intent and capability to carry out an attack on a particular target (or targets), or where a particular event or person has been mentioned directly by someone seeking to cause them harm. It could be argued that general threats are, by their nature, more commonly encountered than specific threats. General threats, therefore, give rise to a range of prevention focused security activities (such as access controls to symbolic buildings and pre-boarding airport security screening procedures), while specific threats give rise to more focused actions, which can include visible acts by security and law enforcement agencies such as the execution of search warrants, the arrest of suspects or the provision (or increase) of personal protection measures that include deployment of protection officers and alternative travel security (e.g. motorcades).

In essence, threat assessment is, arguably, a combination of art and science. The art is the skill required of the threat assessors to process a wide

variety of information from various sources (sometimes referred to as intelligence) and to make analytical determinations about what it all means. While the science aspect is the threat formula used (Intent + Capability = Threat) combined with the assessment techniques and methods employed by the assessors to provide rigour to the process (Prunckun, 2015, pp. 283–302). The threat assessment process is designed to be devoid of political input in order to allow an unbiased and well-analysed product to emerge that can be factored into risk assessment processes by decision-makers—both bureaucratic and political (Department of the Prime Minister and Cabinet, 2014, p.12; Prunckun, 2015, p. 300–301).

WHAT NECESSITATED THE CHANGE IN NEW ZEALAND’S THREAT LEVEL?

The most recent iteration of the New Zealand terrorism threat assessment process (at the time of this writing) resulted in the upward movement of the threat level to the Low setting. Unfortunately, as mentioned earlier, New Zealand does not provide a public version of the contents of its threat assessment, therefore, it was not possible to understand the detailed context that led to that decision. Instead, as the *New Zealand Herald* editorial of 6 November 2014 (New Zealand Herald, 2014) stated “The public has to trust him [the prime minister] on this. ...only the Prime Minister and his closest advisers are able to assess the evidence collected by the intelligence agencies.” An accurate statement, up to a point. Subsequent to the public announcement of the threat level change the New Zealand prime minister and the director of the NZSIS (the organisation’s chief executive) made public statements which touched on the terrorist threat, therefore, it was possible to review those utterances to determine if they provided a cohesive, concise and transparent explanation for the adjusted threat level.

The first public comment on the threat level came from the prime minister on 13 October 2014, when he mentioned the level raising (IS sparks terror law tightening, 2014). Amongst other things, he was quoted as saying “We are also aware of people within New Zealand who have a desire to travel and fight for the Islamic State of Iraq and Levant [ISIL] ...” He was reported as having gone on to say “...there was a growing risk to New Zealand from foreign fighters looking to leave or to return” Subsequently in a speech about national security, delivered on 5 November 2014 (Key, 2014), Prime Minister Key stated “ISIL’s ability to motivate Islamist radicals, as well as its growth, ambition, resources

and methods, make it a brutal threat, not only to stability in the Middle East, but regionally and locally.”

The prime minister went on to outline how the ISIL threat was relevant to New Zealand. He confirmed that ISIL had been “successful in recruiting New Zealanders,” with between 30 and 40 people “of concern” being added to government security lists. He also confirmed ISIL supporters have had their passports cancelled and were, therefore, unable to leave New Zealand to pursue their extremist desires, and he stated that “it is important to note that there are individuals here who are attracted to carrying out domestic attacks of the type we have seen prevented in Australia and recently take place in Canada.” The prime minister acknowledged that those prevented from travelling “are a distinct threat to our safety and security. People who are prevented from performing terrorist acts abroad can turn their minds to terrorist acts at home ...” (Key, 2014).

The second commentaries of relevance came from of a media interview with the director of the NZSIS via the subsequent articles published on 1 November 2014 (Young, 2014; Watkins, 2014). In Young’s item the director was quoted as saying “What [ISIS] is doing is they are sending out this material which is awful, it’s all on the internet ... urges people to do small-scale attacks that are not complicated, that don’t require planning, that don’t require anything fancy, nothing more than a knife or a car or something you light a fire with ... All that that [sic] was needed was intent. Capability was not difficult to put together ...” (Young, 2014).

In a different media item following the same interview, also published on 1 November 2014, the director was reported to have said “the threat is real – and closer to home than any of us realise. This is actually what I think about, all of the time” (Watkins, 2014). Watkins—the journalist reporting the story—went on to describe how the director had a “thick pile of ISIS propaganda material” and how she (the director) read aloud from one manual published by ISIS. The passage stated “Every Muslim should get out of his house, find a crusader and kill him. It is important that the killing becomes attributed to patrons of the Islamic State who have obeyed its leadership ... One should not complicate the attacks by involving other parties, purchasing complex materials, or communicating with weak-hearted individuals” (Watkins, 2014). Watkins reported that when she questioned the director further about the material and its impact on New Zealander’s, the director advised, “There are people who we know are interested in these kinds of acts” (Watkins, 2014).

The Watkins story went on to provide some insight into who those “people” might be when it mentioned events in the city of Auckland where:

...the spotlight has fallen on a mosque in Avondale where there have been sensational claims that a former teacher, Sheikh Abu Abdullah, encouraged his followers to ‘jihad’ against infidels. Two men who attended his classes had their passports cancelled before they could board a plane to Syria. (Watkins, 2014)

To summarise the comments from the prime minister (from two separate sources) and the director of NZSIS (from a further two separate—but linked sources), clearly there was a general (possibly verging on a specific) threat in New Zealand arising from ISIS’s propaganda which had been effective in radicalising and/or motivating a small number of people to adopt ISIS’s ideology. Furthermore, the propaganda, spread via the internet, continued to influence the New Zealand adherents and contained a call to ‘jihad’ through the perpetration of small-scale, easily executed, attacks.

Unfortunately, the propaganda also warned the adherents to avoid some of the means by which—it can be assumed—security and law enforcement agencies come to learn of planned attacks, namely: communicating with others, forming groups, or purchasing equipment. The jihad call by ISIS was by its nature a general threat—albeit containing specific advice—recommending surprise and simplicity. Examples of its implementation elsewhere in the world (at the time of writing) included: the almost fatal knife attack on two Australian police officers, the fatal car and gun attacks on soldiers and civilians in Canada, and the almost fatal hatchet attack on four American police officers.

So, do the statements from two of New Zealand’s most well-informed commentators on the terrorist threat serve to provide the cohesive, concise and transparent rationale for the threat level raise? Furthermore, do the statements also provide the transparency of New Zealand’s national security community (Bushnell & Wilson, 2014, p. 15; Fisher, 2014b) that is sought in order to instil public trust? Those are clearly questions this paper cannot answer, they are questions that the New Zealand public and national security community need to consider and ultimately answer. However, it is argued that a political statement from the prime minister—about a review focusing on foreign fighters (Key, 2014)—which mentioned the threat level in conjunction with that context, and a media interview by the director of NZSIS about the role of the country’s security service—who touched on the terrorism threat in a general way during the

piece—do not equate to a cohesive, concise and transparent statement of the factors that caused threat assessors and senior bureaucrats to make the change they did.

It is further argued that to achieve a cohesive, concise and transparent statement an official public version of the New Zealand threat assessment was needed, released by one (or jointly by both) of the organisations with lead-agency responsibility for terrorism under New Zealand's National Security System (Department of the Prime Minister and Cabinet, 2011, p. 25). The agencies responsible are the New Zealand Security Intelligence Service and the New Zealand Police (2011, p. 25). The rationale for suggesting an official release, hosted on a government agency website (or multiple government agency websites), is that the information from the prime minister and director had to be gathered from four separate sources over a span of 24 days.

Clearly, the information provided by the prime minister and director was capable of being publicly released. Therefore, what prevented it from being released in the form of a public version of the New Zealand Threat Assessment? If it had, then that assessment would have originated from an authoritative source—potentially a terrorism lead-agency (or agencies), would have been linked to one date, and would no doubt have been preserved for future reference via a link (or links) on a government agency website. Such a release process, it is contended, would have gone a long way towards achieving a cohesive, concise and transparent presentation of New Zealand's threat environment and why it was necessary to raise the terrorism threat level. The transparency would have then contributed towards the development of trust in the government agencies concerned as desired (Bushnell & Wilson, 2014, p. 15; Fisher, 2014b), and as demonstrated by Grimmelikhuijsen (2009).

Some commentators or scholars may argue that such a release process is not possible as threat assessment documents often contain classified information (from domestic, and possibly foreign, intelligence and security agencies), and/or material that identified individuals or groups and thereby may breach their privacy, or which would provide a tactical advantage to those giving rise to the threat. Those arguments are essentially correct, however, it is possible to provide a “declassified” version of a threat assessment, or specific and precise commentary on the factors giving rise to a change in threat level, without reference to classified, private or tactically advantageous information.

OTHER COUNTRIES APPROACHES TO THREAT AWARENESS

Elsewhere in the world, countries which share similar characteristics to New Zealand (size, population, GDP, and spend on security) (Shortt, n.d.) do provide public versions of, or commentary regarding, their threat assessments. In particular, Scandinavian countries—two with multi-agency threat assessment entities similar to New Zealand’s CTAG (Persson, 2013, p. 8)—provide the opportunity to view both their current threat level and the rationale behind them by either publishing a public version of the assessment, or specific comments on them, via security agency websites.

In Norway the threat level was set in 2010 at “likely” (that Norway will be threatened by or hit with an act of terror in the next 12 months) and has not shifted recently (Norway: Terror Threat or Attack on Nation 'Likely', 2014). The Norwegian authorities linked their threat level to the fact that Norway was going to send troops to help train Iraqi security forces. Incidentally, New Zealand made a similar decision in November 2014 (Trevett, 2014). The publicly available English language version of the 2014 Norwegian annual threat assessment (Norwegian Police Security Service, 2014) provided detailed background on the threat environment in Norway and outlined a number of different threats associated with the country. The assessment was accessible through the security service’s website. While no information could be located detailing the Norwegian threat levels and their definitions, it was interesting to note in the Norwegian assessment a statement about why the document was published and what relevance it had to risk management:

The threat assessment is intended for the Norwegian public, in order to provide information on expected developments in the threat picture. It is also intended for enterprises that need an up-to-date threat assessment for their long-term risk management. The value of the assessment therefore depends on the users’ knowledge of risk management and their ability to reduce their own vulnerability. (Norwegian Police Security Service, 2014, p. 1)

For Sweden, the threat level concerning terrorism was raised in 2010 from “Low” to “Elevated” (Swedish military raises terror threat level, 2012; Swedish Security Service, 2010.). The Swedes set and maintained that level based on a general threat situation and not because of any specific threat (Swedish military raises terror threat level, 2012; Swedish Security Service, 2010). The Swedish Security Service did not publish a public version of the threat assessment, but

provided an eight paragraph explanation of the shift on their website (Swedish Security Service, 2010). Sweden use a five level threat scale, consisting of: No threat, Low threat, Elevated threat, High threat and Extreme threat, which is also published on the security service's website (Swedish Security Service, 2010).

Denmark's threat level (as at January 2014) remained at "Significant" driven by a general threat given rise to by the country's "foreign and security policies ... along with the Cartoon Case ..." (Center for Terror Analysis, 2014). The Danish Center for Terror Analysis (CTA) not only published a public version of the national threat assessment via its website, but has also published other similar documents (in Danish and English language versions) including one titled: "The threat from solo terrorism and lone wolf terrorism" (Center for Terror Analysis, 2011) which appeared quite pertinent to the newly evident threat posed by IS's call to jihad using simple means. No information, however, could be located detailing the Danish threat levels.

And finally, in Finland the threat level was published on the security service's website as "Low", with the caveat that:

...the threat of violent acts perpetrated by radical Islamists without any external guidance has increased both in Finland and elsewhere in Europe. ... Because the threat has become more complex, assessing its level and targets has become more difficult. In Finland, there are targets representing other states and religious interests as well as international events under increased threat from terrorist organisations and radical individuals. (Finnish Security Intelligence Service, n.d.)

The threat level and caveat were contained in a three-paragraph statement on a webpage published by the Finnish Security Intelligence Service. No information could be located detailing the Finnish threat levels or definitions.

The brief overview above identifies that two of the Scandinavian countries (Norway and Denmark) published substantive documents containing the rationale for the setting of their terrorism (and other) threat levels, while the other two countries (Sweden and Finland) published short statements on their security service websites. Clearly, the Norwegian and Danish policy of publication sets them ahead of New Zealand in the transparency stakes with its non-publication policy. Sweden and Finland, with the short online statements about their levels and why they were set thus, could also be argued to be ahead

of New Zealand in transparency, given none of the official New Zealand government agency websites visited provided any information about the current terrorism threat level or the rationale for it.

CONCLUSION

Despite New Zealand's acknowledged need for a more transparent, and therefore trusted, intelligence community the country has not adopted that approach when it comes to explaining why the country's threat level needed to rise. The role of explaining was instead left to a political actor and a chief executive through tangential commentaries. In a world that is arguably more threat conscious as a consequence of a decade of counter-terrorism action, warfare and media reporting, the lack of an authoritative source was quite noticeable.

While some commentators may argue that releasing such information will compromise rather than enhance security, Scandinavia's approach—Norway and Denmark's in particular—to the issue show that cohesive, concise and transparent awareness can be achieved. Furthermore, Norway provided a clear justification for their approach, seeing it as the appropriate means of informing the public and private sectors so both could adjust their risk management thinking. In these times of governmental fiscal constraint, heightened threat anxiety and expenditure of additional tax-payer funds on preventative security measures, it is argued New Zealand's non-transparent threat assessment publication policy needs reviewing, with the Scandinavian countries of Norway and Denmark providing useful alternative approaches for consideration.

NOTES

1. New Zealand uses a set of six levels to assess the potential of a terrorist attack: Negligible (very unlikely), Very Low (unlikely), Low (possible, but not expected), Medium (feasible and could well occur), High (likely) and Extreme (activity is expected imminently). (New Zealand Government, n.d.)
2. On 11 November 2014, a search was completed of the following New Zealand Government websites looking for a public version of the New Zealand threat assessment: www.nzsis.govt.nz, www.dpmc.govt.nz, www.police.govt.nz and www.intelligencecommunity.govt.nz. A general Internet search was also undertaken using the *Google* search engine and the terms: New Zealand AND threat assessment/terrorism/threat. The New Zealand threat assessment document, or official commentary on it—beyond the commentary referred to in this paper—could not be found.

3. Interestingly, New Zealand was beaten for first place in the corruption index as least corrupt nation by a Scandinavian country—Denmark. Third, fourth and fifth places in the index were occupied by Finland, Sweden and Norway—three other Scandinavian countries.

REFERENCES

- ABC News. "Norway: Terror Threat or Attack on Nation 'Likely'." <http://abcnews.go.com/International/wireStory/norway-terror-threat-attack-26698414> (accessed 10 November 2014)
- Bushnell, P., & Wilson, G. (2014). *Performance Improvement Framework: Review of the agencies in the core New Zealand Intelligence Community (NZIC)*. Wellington: State Services Commission.
- Center for Terror Analysis. (2011). *The threat from solo and lone wolf terrorism*, https://www.pet.dk/English/~media/Engelsk/the_threat_from_solo_terrorism_and_lone_wolf_terrorism_-_engelsk_version_pdf.ashx. (accessed 7 November 2014)
- Center for Terror Analysis. (2014). *Assessment of the Terror Threat to Denmark*. <https://www.pet.dk/~media/Engelsk/VTD%20NTV%20UK/20140124FINALVTDENGELSKpdf.ashx>. (accessed 7 November 2014)
- Clark, H. (2002). *Address to Symposium on World Terrorism*. <http://www.beehive.govt.nz/speeches>. (accessed 14 March 2013)
- Clark, H. (2004). Threat assessment group established. <http://www.beehive.govt.nz/node/21889> (accessed 14 March 2013)
- Committee of the Intelligence Services. (2010). *Beretning om udvalgets virksomhed (Report on its operations)*. http://www.folketingstidende.dk/RIPdf/samling/20101/BeretningAlmenArt/20101_BER_2.pdf. (accessed 12 June 2014)
- Department of the Prime Minister and Cabinet. (2011). *New Zealand's National Security System*. <http://www.dpmc.govt.nz/sites/all/files/publications/national-security-system.pdf>. (accessed 25 September 2013)
- Department of the Prime Minister and Cabinet, N. Z. (2014). *Annual Report for the Year Ending 30 June 2014*. Wellington: Department of the Prime Minister and Cabinet.

- Finnish Security Intelligence Service. (n.d.). *Terrorist Threat Assessment*.
<https://www.poliisi.fi/poliisi/supo60/home.nsf/pages/B67B6ACE2A5F08D1C22579B40028B50A?opendocument> (accessed 6 November 2014)
- Fisher, D. (2014a, 2 July 2014). “Hugh Change Needed to Intelligence Services,” *New Zealand Herald*.
- Fisher, D. (2014b, 9 December 2014). Why NZ spy chiefs can no longer get away with saying 'we can neither confirm or deny', *New Zealand Herald*.
http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11371394 (accessed 11 December 2014)
- Grimmelikhuijsen, S. (2009). Do transparent government agencies strengthen trust? *Information Polity*, 14, 173–186. doi: 10.3233/IP-2009-0175
- IS Sparks Terror Law Tightening. (2014, 13.10.2014). *Stuff.co.nz*.
<http://www.stuff.co.nz/national/politics/10609621/IS-sparks-terror-law-tightening> (accessed 7 November 2014)
- Key, J. (2014). *Speech to NZ Institute of International Affairs*.
<http://www.beehive.govt.nz/speech/speech-nz-institute-international-affairs-0>. (accessed 11 November 2014)
- Moore, M. (2014). “RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework.” *The Political Quarterly*, 85(2), 131–132.
- New Zealand Government. (n.d.). *Threat Level Definition*.
http://www.beehive.govt.nz/sites/all/files/Threat_Levels.pdf. (accessed 11 November 2014)
- New Zealand Herald. (2014, 06.11.2014). “Solid Evidence of Terror Links Vital before Passports Held.”
http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11353880 (accessed 11 November 2014)
- New Zealand Intelligence Community. (2015). “Protecting and Advancing Our National Security.” <http://nzic.govt.nz/about-us/securing-new-zealands-future/> (accessed 19 January 2015)
- Norwegian Police Security Service. (2014). *Annual Threat Assessment 2014*.
www.pst.no/media/70068/NTV_2014_engelsk.pdf. (accessed 11 November 2014)

- Persson, G. (2013). "Fusion Centres—Lessons Learned." *A Study of Coordination Functions for Intelligence and Security Services* (pp. 1–40). Stockholm: Swedish National Defence College.
- Pickering, S., McCulloch, J., & Wright-Neville, D. (2008). *Counter-Terrorism Policing: Community, Cohesion and Security*. New York: Springer.
- Prunckun, H. (2015). *Scientific Methods of inquiry for Intelligence Analysis, Second Edition*. Lanham: Rowman & Littlefield.
- State Services Commission.. (2007). *All-of-Government Brand Policy and Guidelines*. <http://www.ssc.govt.nz/sites/all/files/a-o-g-policy-and-guidelines.pdf>. (accessed 14 October 2013)
- Shortt, R. (n.d.). *Intelligence Meets Enforcement: Heartache or Harmony in Responding to "Wicked Issues" such as Transnational Criminality?* Dissertation in progress, Charles Sturt University, Australia
- Swedish military raises terror threat level.
<http://www.thelocal.se/20120604/41242> (accessed 6 November 2014)
- Swedish Security Service. (2010). Changed Threat Level.
<http://www.sakerhetspolisen.se/en/swedish-security-service/about-us/current-events/news/2010-10-01-changed-threat-level.html> (accessed 6 November 2014)
- Transparency International. (2015). 2014 Corruption Perceptions Index.
<http://www.transparency.org/cpi2014/results> (accessed 20 January 2015)
- Trevett, C. (2014). Isis deployment won't end in combat like SAS in Afghanistan: Brownlee
http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=1135452 6 (accessed 7 November 2014)
- Watkins, T. (2014). The new terror threat.
<http://www.stuff.co.nz/national/politics/10687081/The-new-terror-threat> (accessed 11 November 2014)
- Young, A. (2014, 1.11.2014). We're about security not spying: SIS chief, *New Zealand Herald*. Retrieved from
http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=1135136 8 (accessed 11 November 2014)

ABOUT THE AUTHOR

Richard Shortt is a former national security policy advisor in the Department of the Prime Minister and Cabinet, New Zealand (2003–2005). He was the manager of the Combined Threat Assessment Group (CTAG) in New Zealand between 2005 and 2008. Mr. Shortt holds a Master of Public Management degree from Victoria University, Wellington, New Zealand, and is currently a PhD candidate at Charles Sturt University studying the relationships between intelligence and law enforcement agencies.

- o O o -

Research Article

THE HIDDEN ADVANTAGE IN SHOOT/DON'T SHOOT SIMULATION EXERCISES FOR POLICE RECRUIT TRAINING

Amanda Davies[†]

During the past thirty-five years, developments in computer-related technology have been providing increasingly more sophisticated simulation alternatives for training law enforcement officers. Such developments have leveraged on the back of progress achieved in the aviation, military and medical professions as law enforcement educators seek to address the challenges of training for high-risk, high-stakes professional environments. While globally, simulation based learning exercises are at the forefront in use-of-force training with firearms for police recruits there is limited published research which views the influence of these exercises on operational practice through the lens of the police recruit as they engage with the demands of their volatile, unpredictable workplace. This paper discusses a case study of a cohort of 372 police recruits whose police academy education program included participation in simulation based learning exercises centred on decision making in use-of-force. The pivotal inclusion in the study was the opportunity for the police recruits to reflect on the influence of the simulation exercise experience from an operational perspective. The study revealed an unvoiced advantage—while trainers are focussing on the amount of ammunition used, the marksmanship accuracy, and the justification for the use-of-force, the students are unconsciously building a repertoire of realistic experiences as a reference library for the moment of decision in real life shoot/don't shoot incidents.

Keywords: Police use-of-force, firearms simulation training, police recruit training, law enforcement simulation technology, weapons training

INTRODUCTION

Recent global events involving police use of firearms highlights the often confusing, complex and high risk situations armed police officers find themselves in. Consequently, developing an understanding of the way police officers are trained to make decisions and act or react in such situations

[†] Corresponding author: adavies@csu.edu.au

influences their operational practice is important. Simulation training for armed police officers is an area that needs closer examination and understanding for its influence on the decisions taken by police officers when faced with life or death decisions.

The use of simulation for use-of-force and firearms training both in law enforcement and the military has been in place for several decades, initially their use was concerned with skill development and assessment in the use of firearms (Copay & Charles, 2001; C.O. Dillion, 1972; Dorering, 1980; Edholm, 1978; Griffith 2009; Knight, 2007; Morrison & Shave, 2002; Olsen, 2004; Pinizzotto, Kern, & Davis, 2004; Weiss & Davis, 2002). More recently an emerging trend to utilise technology-supported simulations for more holistic training has been evidenced. This move to incorporate additional aspects of training and assessment with firearms skill development ranges from a combination of firearms skills to the use of communications to resolve an incident (Gillis, 1999). Furthermore, inclusive in this progress is an escalation to the assessment of verbal communication skills to defensive tactics (Hodge, 2003).

The clamour by high-tech experts to service the expectations for law enforcement simulation technology has led to the development of a number of well-regarded use-of-force simulation products entering the market place. As reported by Griffith (2009), and Nowicki (2009), those products which accommodated learning opportunities which extended beyond the traditional firearms range experience to placing the officer in an environment which re-creates as many of the environmental conditions that exist in their operational domain, such as the public street, are gaining popularity with educators.

The momentum in the technology arena driven by the demand from law enforcement agencies with responsibility for preparing recruit officers for operational duty has seen the development of virtual high fidelity, interactive, shootout environments (Andrews International, 2011; Wollert, Burnett, Sizemore & Balash; 2014). These developments have not changed the priority of situating marksmanship as the number one focus for many law enforcement agencies. As Johnson (2013) writes in discussing firearms training for FBI agents:

The thing that jumps out at you from the (shooting incident) research is that if we're not preparing agents to get off three to four rounds at a target between 0 and 3 yards, then we're not preparing them for what is likely to happen in the real world," says FBI training instructor Larry "Pogo" Akin.

Developing an understanding of whether experience in a simulation exercise and the subsequent perception and prediction of level of skills and knowledge is ultimately evidenced in the field and what impact simulation exercises have on the transfer of learning to professional practice for police officers is hampered in this under-published area.

Firstly, in the main published research in this domain concentrates on the training environment. The seminal work of Helsen and Starkes (1999) in this arena is centred on understanding how prepared the recruit officer feels for the use-of-force decisions inherent in police work. Similarly contained within the training environment is the research reported by Scharr (2001) and the comprehensive report on Canadian law enforcement agencies use-of-force simulations developed by Bennell and Jones (2004). The responses from participants in each of the simulation exercise research reports pertained to their perception of the influence of the simulation exercises during training and to predicting their level of confidence for decision making in future professional practice.

The second restriction is premised on protecting the commercial intelligence of the technology companies developing high tech use-of-force simulation products.

While there is a growing body of literature which examines use-of-force by police officers from many perspectives (see Alpert & Dunham, 2010; Dymond, 2014; Klahm & Tiller, 2010; Willits, & Nowacki, 2014) Klahm, Frank & Liederbach (2014) acknowledge the limited available literature published in this field:

Historically researchers have lamented the lack of available data to fully explore police use of force. Police agencies have been reluctant to disclose information, especially when the data include descriptions of violent acts committed by police. At the same time, data that describe behaviors that occur on the other end of the continuum-verbal commands, threats, and other nonviolent acts—are not typically collected on official records (p.558).

There is however, an emerging trend for articles discussing use of force simulations to be publically available on the internet (see PoliceOne.com). The study reported here focuses on the relationship between use-of-force simulations in training to application in the field and is consistent with the suggestion by

Dymond (2014) that research on specific areas related to use-of-force has the potential to inform more widely:

This article aims both to assist practitioners in providing an overview of the state of knowledge pertaining to Taser in the UK and to assist academics by using this review to highlight broader gaps in the literature on Taser and indeed, on use of force more generally (p.165).

CASE STUDY

To contextualise the police recruits' reflection on the influence of the use-of-force simulation experience it is valuable to provide the background to the case study. This case study included a cohort of 372 police students undertaking weapons (including Glock pistol firearms) and tactics training as a part of their academy based studies prior to deployment as operational probationary constables. Included in the weapons and tactics training program is participation in a VirTra use-of-force simulation exercise. The VirTra simulation training product provides five screens and a 300-degree immersive training platform.

The judgemental use-of-force training mode supplies a library of realistic scenarios with an audio system and transducers simulating sounds and movement. The participant officer/s step onto a platform surrounded by the screens, onto which the high definition video is played. In this study the participants utilised a replica gas fired Glock pistol and OC spray (oleoresin capsicum which irritates the eyes and causes tears and pain).

The threat-fire element with return fire was not utilised in the study. The simulation scenario is operated by an instructor who has the ability to change the response from the screen characters dependent on the actions of the officer. In the spirit of ethical disclosure, the author advises that the work reported here is independent of any relationship with the manufacturer of the VirTra equipment or its representatives.

At the time of participating in the VirTra simulation, the police recruits had completed two fourteen week sessions of academy studies inclusive of firearms marksmanship and weapon less control tactics in preparation for commencing twelve months as a probationary constable.

DATA COLLECTION

The case study participants were invited to complete a pre-simulation questionnaire which focussed on understanding their previous experience with firearm usage, and their level of confidence to undertake the VirTra use-of-force simulation exercise/s. The pre-simulation questionnaire also focussed on understanding the factors the participants considered would affect their decision making in the scenario. Immediately following the police recruit's participation in the simulation exercise they were invited to complete a post-simulation questionnaire. The post-simulation questionnaire provided an opportunity for the participants to reflect on their simulation experience, emotionally, physically and from a learning perspective. In particular reflecting on how confident they felt that the decision/s they made in the simulation were correct and the rationale for their perspective. Further the questionnaire sought to identify the factors which impacted on the participants' decision making during the simulation exercise.

Following a three to four month period post-simulation exercise participation the case study VirTra participants were invited to participate in an interview. The purpose of the interview was to develop an understanding of the influence of the VirTra simulation experience on the operational practice of the cohort who were now operational field based probationary constables.

The data presented in this paper is drawn from the researcher's previous doctoral research project. In this regard, time constraints did not allow for an exploration of longer term influences of the simulation experience on the participants' operational policing practice. During the study period there was not the opportunity to include a control group who undertook the police recruit training program without participating in the VirTra simulation.

Including police recruits in the study who had previously undertaken the police recruit training program without participating in the VirTra was of concern due to the lapse of time since their Academy studies. At the time of this study those non-VirTra participant officers would have been field based for more than three years and their perception of initial citizen/police interactions potentially clouded/contaminated by their length of operational experience. The focus of the study was to understand the role of judgemental use-of-force simulations in police training programs and there may be an avenue for future research in this field which addresses limitations of this study.

SETTING THE SCENE

Central to validation of the suggestion that experience in a use-of-force VirTra style simulation offers advantages beyond the mechanics of marksmanship which are transferred to the participants' real world of policing is to firstly understand the participants' simulation experience.

In this case study the post-simulation questionnaire included questions designed to elicit an understanding of the sense of realism the participants felt in the simulation scenario based exercises. The data as presented in Table 1 suggests 71% of the participants considered the VirTra simulation scenarios made them feel as if they were at the scene in relation time.

Table 1—Level of realism experienced by VirTra participants (n=372).

Question 2: “The VirTra simulation scenarios made me feel as if I were actually at the scene in real time.”	Very strongly agree	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	Very Strongly Disagree
	53 (14.2%)	87 (23.4%)	126 (33.9%)	46 (12.4%)	38 (10.2%)	9 (2.4%)	13 (3.5%)

Of the remaining 28.5%, 12.4% were undecided and 16.2% disagreed. In analysis of further data collected in this study the reasons offered for participants not feeling as if they were at a real scene included: a view of the simulation as a game as they identified themselves as serious video game players; a lack of understanding as to the mechanics of how the simulation exercises operate; and lack of preparation for participation in the simulation exercise and some participants experienced technical malfunction of the simulation environment (split screens, audio and visual misaligned).

To build a holistic understanding of the experience of the participants in the simulation as it pertains to their field based reflections, it is important to consider the data in Table 1 with that presented in Table 2. Table 2 presents the cohort response in relation to the opportunity to apply decision making skills during their participation in the VirTra simulation exercise. Here 92.2% of the participants agreed they had opportunity to apply their decision making skills in

the scenario. The implication here is that while 16.1% of the cohort did not agree the VirTra scenario felt real only 2.9% considered they were not able to apply decision making skills in the scenario.

Table 2—Opportunity to provide decision-making skills in VirTra simulation (n=372).

Question 4: “The VirTra simulation scenarios provided an opportunity for me to apply my decision-making skills.”	Very strongly agree	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	Very Strongly Disagree
	98 (26.3%)	132 (35.5%)	113 (30.4%)	18 (4.9%)	5 (1.3%)	3 (0.8%)	3 (0.8%)

The cohort responses to the post-simulation question: “I felt completely immersed and focused on the VirTra simulation scenarios,” similarly suggest that while there were participants who considered the VirTra simulation exercise did not make them feel as if they were actually at the scene in real time this did not necessarily preclude them from feeling immersed and engaged with the simulation scenario. As Table 3 indicates, 76.3% of the cohort agreed they were immersed and engaged, 12% were undecided and 10.5% disagreed.

Table 3—Sense of immersion and engagement in the VirTra simulation (n=367)

Question 3: “I felt completely immersed and focused on the VirTra simulation scenarios.”	Very Strongly Agree	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	Very Strongly Disagree
	61 (16.6%)	96 (26%)	124 (33.7%)	47 (12%)	24 (6.5%)	8 (2.1%)	7 (1.9%)

POTENTIAL FIELD BASED INFLUENCE OF USE-OF-FORCE SIMULATION EXPERIENCE

Combining the perception of the case study participants sense of their engagement with the use-of-force simulation exercises with their perception of the how the experience will impact on their field based operational practice provides the platform from which latter discussion will be premised.

Question 16 of the post-simulation questionnaire captured the participants' perception of how they viewed the potential influence of the VirTra simulation experience on the participants' future operational practice. As indicated in Table 4, a total of 321 responses were recorded for the question and these were grouped according to similar descriptors. The responses indicated that 97.6% of respondents anticipated that their experience in the VirTra simulation would have a positive effect on their future policing practice. Here the participants have identified the potential reliance on the VirTra experience as a reference point for their field based decision making.

OPERATIONAL BASED REALITY OF THE INFLUENCE OF USE-OF-FORCE SIMULATION EXPERIENCE

An important consideration which permeates the discussion of the VirTra participants' experience in the simulation, their transfer of learning to operational practice and their perspectives on the reality of the simulation scenario and environment is that these novice learners have a limited repertoire of similar experiences as reference points to which to turn when confronted with real situations. Their experience in the simulation exercise becomes their point of reference.

Professor Crego, a lead in simulation design for police education, suggests that simulations have the capacity to expose novices to experiences which are impossible to create in the training environment. Furthermore, the suggestion by Crego that simulations provide a significant "experiential element enriching the stock of experience (1996, p.84) to aid in recognition-primed decision-making (Crego, 1996; Flin & Arbutnot, 2002; Flin & Slaven, 1996) resonates with the learning experience articulated by the participants in this case study. This notion of building a reference point from their use-of-force simulation experience is evidenced in the comments presented in Table 5. Here participants commented on the value to their learning achieved by participation in the use-of-force simulation.

Table 4—Areas of policing practice perceived to be influenced by simulation experience.

Question 16: “How do you expect participating in the VirTra simulation will influence your future policing practice in the field?” (n=321)		
Area of Impact	No. of responses	Examples of Responses
Increased confidence	72	“By participating in the VirTra scenarios I have more confidence while in the field” “more confidence on the job”
Improved decision-making	70	“It will improve my decisions” “make better decisions” “help make decisions” “better decision-making, quick thinking; it will improve and test my decision-making skills”
Increased preparedness for real situations	46	“make me more aware of what can happen on the street” “it will give me knowledge of what might occur in the field” “more prepared for real world”
Increased awareness of types of situations and context for decision-making	33	“Better understanding of what is required and expected in certain circumstances” “what to expect in real life”
Increased experience and exposure	22	“Exposure and confidence” “guide us in the choice/decisions we will have to make”
Improved decision-making under stress	17	“It will help greatly with my decision-making under stress, shooting in limited time” “helps to build confidence and how to deal with and handle stressful situations”
Positive impact for the future	15	“In a positive manner; allow me to be more prepared”
Improved reaction time	4	“Will hopefully build up muscle memory so in times of duress I can react quickly and efficiently”
Allows opportunity to relate back to it from the field	4	“Gives me a base I could rely on to get me through situations” “the VirTra gives the student police officer a more realistic idea of the real world, it develops the student to learn from mistakes”
Limited or none	8	“Not sure yet as I am wrapped up in VirTra not being real” “don’t know yet as haven’t been faced with situations but hope that it would help me make the right decision” “not sure how it will affect”

Noteworthy are the comments presented in Table 5, Row G where a direct connection between the value placed on the learning achieved from the use-of-force simulation experience at the time and how this view has changed once the participant had operational experience and realised the value of the simulation experience.

Table 5—Value of VirTra Experience

Participant	Scenario	Valuable	Examples of Rationale Given
a	Homeless man	Absolutely	“The sense of someone coming towards you, had never been put in the situation ... it was totally foreign, you have to react quickly”
b	Warehouse	Definitely	“Encompassed everything you do before going to the field puts it all into perspective”
c	Warehouse	Yes	“Teaches you to scan a lot more ... not to get complacent”
d	Warehouse	Pretty good	“Made you see what was happening in real life”
e	Warehouse	Yes	“I found that for situations that are stressful and we would never be able to have the experience of until it happens at work I thought it was really great”
f	Domestic	Yes	“It was a valuable learning experience to give practice to deal with people who are aggressive and how to use your appointments”
g	Domestic	At the time, no, now I know better	“At the time I didn’t get it because I had never been faced with anything like that before, my natural instinct was to go with my hands and grab him [POI], now I know better and would use communication and use my voice to manage the situation”

A further data source in this case study which underpins the notion of the use-of-force simulation providing/building a reference point for inexperienced police officers is evidenced in the comments provided during field based interviews with the participants who had completed three to four months operational

experience. A sample of the comments are presented in Table 6. It is worthy of note that in these comments there are direct references to the use of the simulation experience as a reference point at the time of making decisions in real time operational situations.

Table 6 presents responses to two post-simulation field based interview questions. Combining the presentation of these responses assisted in collating emerging themes related to the role of the use-of-force simulation experience in operational decision making for the probationary constables.

Table 6—The role of the use-of-force simulation experience on real time operational decision making.

Interview Question 9: “Following your experience in the field in making decisions about the use of your firearm, can you tell me how the simulation training experience affected your decision-making in those incidents?”	
Interview Question 10: “Were you aware at the time of the incident in the field of reflecting on your experience in the simulation unit? How did this impact on your decision in the field? Please explain.”	
Preparation for the unexpected	“The main thing I got out was to be prepared for the unexpected” (P.3) “What I did in the real situation was made sure I was very aware of what was going on and all of the possibilities, just like in the simulation” (P.1) “Made me realize I have to keep sharp and be aware of what is going on around me ... so in the field incident I stayed focused on what was going on around me” (P.13) “In my field job I was going into the unexpected, just like the man on the mobile phone in the simulation, it made me continue to be aware of expecting the unexpected” (P.6)
Heightened awareness of unpredictability	“You might let one thing go but you have to keep thinking about everything else because you don’t know what will happen next, I learnt this from the simulation” (P.9) “Being aware that there is the possibility of a weapon being produced in any situation and how quickly tiny jobs can escalate” (P.6)
Ability to make decisions quickly	“The simulation taught me to consider quickly, you don’t want to shoot the wrong person” (P.3) “In the field it happens so quickly, just like the simulation” (P.1) “The simulation taught me how important it is to react in time, make the decision in time” (P.6)
Confidence in knowledge of use-of-force justifications	“I was less concerned about the firing, because I had prior experience of that, this for me was more about the justifications for use of the firearm in the field” (P.11) “The simulation experience heightened my awareness of the use of appointments and understanding when justified to use it” (P.6)

DISCUSSION AND CONCLUSION

Due to the intrinsic nature of police work, coupled with increasing national and international threats and the duty to protect life and property, it is acknowledged that no two policing response incidents will be identical, although there can be core similarities. These normally revolve around such problems as resolving and managing the threat to people's safety. The learning value of the use-of-force simulation experience for training police recruits therefore cannot be underestimated for its influence in building the library of experience, albeit virtual.

This is more important as a police officer steps into a world of high risk where confidence in making timely and accurate decisions is paramount. As the newly deployed constables' policing career extends, the library of situations in which they have applied their use-of-force decision making skills will expand and provide further guidance and reference to aid them at each new situation.

The evidence in this case study indicates that the key transferred influence from participation in a use-of-force simulation exercise is centred on building their personal reference point for times of crisis. By doing so, when faced with situations that demand high level decision making, officers will be equipped to make appropriate decisions in potential life or death situations. The value of an evidenced based approach to use-of-force education initiatives is highlighted by Klahm & Tiller (2010) in summarising:

...organizational policy, in theory, should be predicated on empirical research. As such, it is imperative that we fully understand the nature and extent of police use-of-force as well as the factors related to its use. Only then can training protocols be tailored to its appropriate use and policy formulated to instruct officers when they can and should use force (p.214).

REFERENCES

- Alpert, G.P. & Dunham, R.G. (2010). "Policy and Training Recommendations Related to Police Use of CEDs: Overview of Findings from a Comprehensive National Study." *Police Quarterly*, 13, 235–259.
- Andrews International. (2011). *Andrews International Training Center*. Retrieved 17 September 2011, from www.andrewsinternational.com

- Bennell, C., & Jones, N. J. (2004). *The Effectiveness of Use-Of-Force Simulation Training Final Report*. Toronto, Canada: Carleton University.
- Copay, A. G., & Charles, M. T. (2001). "Handgun Shooting Accuracy in Low Light Conditions." *Policing: An International Journal of Police Strategies & Management*, 24(4), 595–604.
- Crego, J. (1996). *Critical Incident Management Engendering Experience through Simulation* (unpublished doctoral dissertation). Technology, Information, Management and Economics Institute, Graduate School, University of Salford, Manchester, England.
- Dillon, C.O. (1972). Training Films Test Police Firearms Use. *Law and Order*, 20(7), 38–43.
- Doering, R.D. (1980). A Simulator System for Tactical Training of Police Under Fire. *The Police Chief*, 47(10), 25–28.
- Dymond, A. (2014). "The Flaw in the Taser Debate is the Taser Debate: What do We Know about Taser in the UK, and How Significant are the Gaps in Our Knowledge?" *Policing A Journal of Policy and Practice*, 8 (2), 165–173.
- Edholm, P. (1978). "Realism in Firearms Training." *Law & Order*, 26(10), 30–32, 34–35, 45.
- Flin, R., & Arbuthnot, K. (Eds.). (2002). *Incident Command: Tales from the Hot Seat*. Aldershot, United Kingdom: Ashgate.
- Flin, R., & Slaven, G. (1996). "Personality and Emergency Command Ability." *Disaster Prevention and Management*, 5(1), 40–46.
- Gillis, G. (1999). "Verbalization and Firearms Training: The Missing Step." *Police*, September, 44–47.
- Griffith, D. (2009). "Virtual Reality Training. *Police Magazine*, 33(4), 33–37.
- Helsen, W.F., & Starkes, J.L. (1999). "A New Training Approach to Complex Decision Making for Police Officers in Potentially Dangerous Interventions. *Journal of Criminal Justice*, 27(5), 395–410.
- Johnson, K. (2013). "FBI Focuses Firearms Training on Close-Quarters Combat. *USA TODAY*. Retrieved from <http://www.usatoday.com/story/news/2013/01/fbi-firearms-training/181105/>

- Klaham IV, C.F., & Tillyer, R. (2010). "Understanding Police Use of Force: A Review of the Evidence." *Southwest Journal of Criminal Justice*, 7(2), 214-239.
- Knight, D.A. (2007). "Perfect Practice Makes Perfect." *FBI Law Enforcement Bulletin*, 76(6), 1, 7.
- Morrison, G.B., & Shave, P.L. (2002). "Firearms Training and the Smaller Department." *The Police Chief*, June, 17–24.
- Nowicki, E. (2009). "Firearms Training Trends." *Law and Order*, 57(1), 15–16.
- Olsen, D. (2004). "Strategies for Safer Weapons Training and Use." *Law Enforcement Technology*, January, 52–60.
- Pinizzotto, A.J., Kern, H. A., & Davis, E. F. (2004). "One Shot Drops: Surviving the Myth." *FBI Law Enforcement Bulletin*, 73(10), 14–21.
- Hardesty, K.(2013). "Maximising Use-of-Force Simulators in Law Enforcement Training." <http://PoliceOne.com/policeproducts/training>. Accessed 20 October 2014.
- Scharr, T.M. (2001). "Interactive Video Training for Firearms Safety." *Federal Probation*, 65(2).
- Weiss, J., & Davis, M. (2002). Safe Simulation Training. *Law & Order*, 50(6), 83–86.
- Willits, D.W., & Nowacki, J.S. (2014). "Police Organisation and Deadly Force: An Examination of Variation Across Large and Small Cities." *Policing and Society*, 24(1), 63-80.
- Wollert, T.N.; Burnett, R.; Sizemore, E., & Balash, D. (2014). "The Cutting Edge: Practical Firearms Training While Saving Ammo." Accessed 23 October 2014 www.teamorlando.org/the-cutting-edge-practical-firearms-training-while-saving-ammo

ETHICS STATEMENT

I confirm that the results of this study are independent of any relationship with the manufacturer of the VirTra equipment or its representatives.

ABOUT THE AUTHOR

Dr Amanda Davies is Course Director for the Associate Degree in Policing Practice at the School of Policing, Charles Sturt University, Australia. Her research specialisation is in communication skills for the professions and technology as it applies to police training and education. Dr Davies has published papers on the role of simulation in police training programs, including the e-simulation environment. She holds a Master of Education degree and in 2013 completed her dissertation for the degree of Doctor of Philosophy, which explored the impact of simulation based learning exercises on the development of decision making skills and professional identity in operational policing.

- o O o -

Research Article

FIRST PRINCIPLES OF INTELLIGENCE ANALYSIS: THEORISING A MODEL FOR SECRET RESEARCH

Henry Prunckun[‡]

Leveraging off of the author's previously published research, this paper advances a set of *first principles* for a paradigm on intelligence analysis. The study used a grounded theory approach to explain a theoretical framework about "secret research." Data were collected by means of a survey of the subject literature on intelligence, and thematic analysis was used to develop the theory's propositions from these unstructured (i.e. qualitative) data. The resulting theory is a system of propositions that is *coexistent* rather than being *sequential*. The theory's six propositions state that intelligence research is: 1) conducted in secret, 2) identified within the intelligence cycle process so that data collection and analysis can be problem focused. In this regard, intelligence analysis can be 3) offensive as well as 4) defensive, but 5) it must be timely, and 6) its findings need to be defensible. The proposition of defensibility comprises seven research methodological axioms: 1) data must be valid and 2) reliable, and when possible, the research methods employed should use: 3) randomness, 4) experimental design; 5) pre- and post-tests, 6) inferential statistical tests, and 7) multiple measures of observing the data.

Keywords: Intelligence theory, analytic theory, theory development, first principles, theorising, secret research, intelligence research

BACKGROUND

One could start the discussion of first principles by posing the question, "Why should we be concerned with intelligence?" The answer is simple—because intelligence enables individuals and organisations who seek to exercise control over particular situations. In this sense, control equates to power. As Marrin (2007: 828) states, there needs only be two factors for intelligence to

[‡] Corresponding author: c/o Australian Graduate School of Policing and Security, P.O. Box 168, Manly, New South Wales, Australia, 1655.

exist: “power and competition.” Cohen (1975: 41–42) in his classic treatment of the study of power writes:

Power is sought because without power the security and even the ability of [one] to continue to exist is generally decreased. Without power, [one] has no ability to deter another . . . from actions whose consequences threaten the vital interests of the former. Without power [one] cannot cause another . . . to do that which the former desires but which the latter desires not to do. Power is sought because the more power that [one] has, the greater is the number of [his or her] available options. The more options available to [one], the greater [his or her] security. The greater [his or her] security, the better off [he or she is]. [He or she is] more secure in [his or her] life and in the enjoyment of [his or her] private property.

Intelligence is, therefore, not a form of clairvoyance used to predict the future but a science based on sound quantitative and qualitative research methods adapted largely from the social and behavioral sciences (as well as the humanities and other academic disciplines). But as Lowenthal (2009: 6) points out: “Intelligence is not about truth. If something were known to be true, states would not need intelligence agencies to collect the information or analyse it. . . . [So,] we should think of intelligence as a proximate reality . . . [Intelligence agencies] can rarely be assured that even their best and most considered analysis is true. Their goals are intelligence products that are reliable, unbiased, and honest (that is, free from politicisation).” In this regard, intelligence enables the analyst to present solutions or options to decision makers based on defensible conclusions.

But at this juncture it should be noted that such conclusions are not absolute, and there will always be some level of probability or uncertainty involved with presenting intelligence findings (i.e. proximate reality). Nevertheless, uncertainty can be reduced and conclusion limits further defined so decision makers understand the boundaries. This must be contrasted with making decisions based on “a hunch,” “instinct,” “luck,” “gut feel,” “belief,” “faith,” “trust,” or “hope.” So, conducting intelligence research is like shining of a light into a dark place.

Having said that, the word *intelligence* conjures up assorted notions of spying and espionage, secrets, and the world of exotic gadgetry. Yet to others, the word *intelligence* is closely associated with the Orwellian concept of Big Brother—a world of hardball politics and an uncompromising quest for

influence. To some degree, intelligence work is associated with these concepts. But here the study of intelligence is approached from the focus of the analytic methods that turn information into intelligence. This process is based on methods used in applied research rather than the James Bond-like devices used by cinema heroes or in the authoritarian oppression exercised by some of the world's police states.

RATIONALE

First Principles

In the post–September 11, 2001 world, analysts have searched for scholarly material to help them develop their analytic skills as well as assist them understand the theoretical base on which the craft of intelligence research is founded. This paper advances a theory of secret research—intelligence analysis—which is founded on what is argued to be the discipline's *first principles*.

First principles refers to the fundamental concepts on which a theory rests. This theory can be applied to the various types of intelligence practice: national security, military, law enforcement, business, and private sector intelligence (i.e. that is, intelligence activities practiced by operatives/organisations other than law enforcement, national security, or the military).

This paper expands the results of my previous study of the issue which were published in *Scientific Methods of Inquiry for Intelligence Analysis, 2nd edition* (Prunckun, 2015: 2–15). This paper extends those findings by constructing a more integrated theory of intelligence analysis. It demonstrates how observations of the various disciplines associated with intelligence analytics can be unified into a single broad theoretical framework. This theoretical model contributes to the debate by putting forward a consolidated view of secret research in the form of a set of *first principles*.

PROBLEM IN CONTEXT

It has been argued that that information is the unrefined, raw material used to produce finished, focused intelligence. Without information, intelligence could not exist. But trying to define information is difficult but not impossible. Information is like gravity and electricity, as it cannot be defined by tangible examples. Nevertheless, its properties can be observed and described, thus enabling improvement in the analytic methods that produce intelligence. The

problem hard sciences face in trying to define gravity and electricity has never prevented engineers from designing and building applications that involve these phenomena. Therefore, a lack of a physical variable does not prevent analysts from producing intelligence from what we call *information*.

It is safe to say that every facet of our lives, whether central or incidental, is in some way related to information. We rely on an alarm clock to wake us in the morning, the newspaper to tell us what is happening in the world beyond the end of our street, the radio to alert us if rain is expected, an array of indicator lights and meters on our car's dashboard to tell us about the car's performance as we drive to work, traffic lights and signs to alert us to road conditions, and on we could go until the clock tells us it's time to lay our work aside and to go off to sleep.

Individuals, organisations, and indeed whole societies owe their survival to information. The concept of community is only possible because of our ability to collect, store, retrieve, and transfer information from one person or body corporate to another. The more complex our society, the more it necessitates the conversion of information into intelligence.

VARIABLES DEFINED

There are many definitions of *intelligence* and this appears to have given rise to some scholars asserting that there is no agreed position on what it means. This is simply not the case. Although there may be as many definitions as there are intelligence scholars, the differences amount to mere word smithing. This is because the various definitions in circulation have commonality that can be narrowed to four meanings.

Dictionaries use what is referred to as an "order of definitions" in cases where there are multiple definitions. They order the definitions by synchronic semantic analysis to clarify the different meanings. Taking this approach for the many uses of the term *intelligence* that appear in the subject literature can be deduced to mean:

1. Actions or processes used to produce knowledge (Prunckun, 2015);
2. The body of knowledge thereby produced (Schroeder, 1983);

3. Organisations that deal in knowledge, e.g., an intelligence agency (Walsh, 2011); and
4. The reports and briefings produced for decision makers in the process or by such organisations (Andrew, et al., 2009: 1).

However, it is axiomatic that these four meanings take place in the context of secrecy. Otherwise, these definitions could apply to other forms of research. Moreover, in this paper, intelligence as a process (i.e. definition 1 above) is categorised by the different functions it performs. *Knowledge* in the context of intelligence equates to *insight*, or viewed another way, the ability to *reduce uncertainty*. Insight (in other words, *advantage*), and therefore, certainty, offers mankind the ability to make decisions that enable civilizations to take better control over the “unknown.” But it should be noted that insights are not produced through mystic rituals; insights are produced through processes based on sound quantitative and qualitative research methods that culminate in *defensible conclusions*. In this sense insights relate to *probability* and/or *prediction*. Expressed as an equation, intelligence could be shown as:

$$(\text{secrecy} (\text{information} + \text{analysis} = \text{intelligence} \therefore \text{insight} \Rightarrow \text{reduces uncertainty}))$$

The elements of this equation will be discussed shortly in relation to the grounded theory of intelligence.

INTELLIGENCE AS A PROCESS

The intelligence process is a series of procedures or steps, forming what has been traditionally termed the *intelligence cycle*. In recent years the term *intelligence process* has gain popularity over intelligence cycle as it has been recognised that it is not really a cycle *per se*, but a process. Nonetheless, this cycle, or process, is initiated by a decision maker who poses a question or requests advice. This is termed an *intelligence requirement* (in some intelligence agencies, such as the military, this is referred to as *essential elements of intelligence*—EEI). The intelligence requirements are forwarded to an intelligence agency and the cycle begins.

I argue that the intelligence process consists of seven steps (see figure 1). Some scholars may contend that this process could be defined in few steps (by consolidating some), or more steps (by expanding particular steps). Nevertheless, my view is that the seven I outline accurately describe the process

without abbreviating what is entailed, or unnecessarily increasing the phases by adding further detail. The first five steps focus on converting raw data¹ into intelligence:

1. Direction setting (i.e., problem formulation and planning);
2. Information collection;
3. Data collation;
4. Data manipulation and processing; and
5. Data analysis.

This resulting intelligence is then treated with two further steps:

6. Report writing; and
7. Dissemination to decision makers (which would include provision for feedback).

Depending upon the initial intelligence requirements (e.g., the research objective), a single “loop” may be sufficient to complete the intelligence research project and provide the decision maker with the insight sought. However, in practice, further data may need to be collected with the cycle beginning again, or the cycle may have two or more tasks being performed at once and may double back before advancing again. For instance, once the research question has been formulated and the data collection plan devised, an outline of the report may begin, and as the more readily available pieces of information flow in, a database or spreadsheet may have been constructed and the data collated.

Furthermore, even before all the data are received, some preliminary analysis may be carried out, and depending upon the results (e.g. at the collation stage which some analysts view as low grade analysis), further information may be requested (e.g., if by chance these results show the data would be inadequate to answer the research question or a serious limitation noted). This would mean that the data collection plan is revised and field operatives called on to gather more or different data, and so on.

As long as a specific intelligence operation is being conducted, the analytic process will be continuous—forming a cycle. As new information is being collected and collated, other data will be manipulated and analysed. The

resulting outcomes will be disseminated for either immediate use and/or used to set new collection goals.

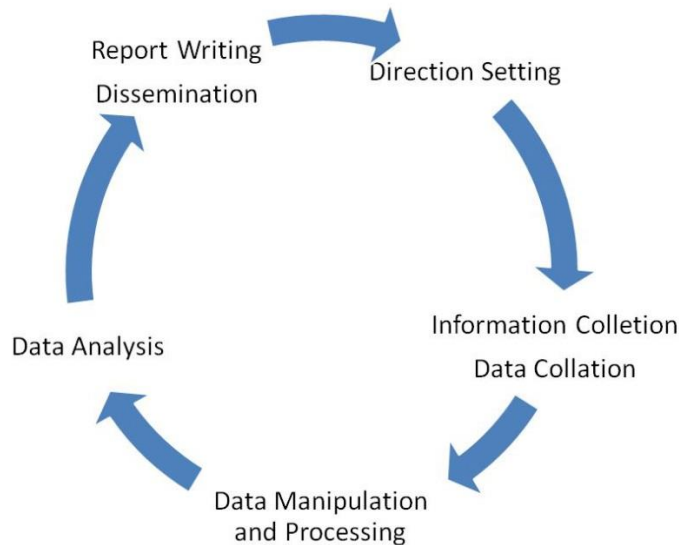


Figure 1—The intelligence process.

The dissemination of the intelligence product can take a variety of forms. Take for instance the case of business intelligence—it could be a background history on a company or one of its executives, a diagram of a company’s office layout, identification of new projects being researched, a prediction on the intended release of a new product, staff salaries, the classification and number of personnel on a company’s payroll, and the like.

The intelligence cycle is not unique to intelligence research but has parallels with research cycles in academic disciplines—*open research* (Prunckun, 1996: 70–72). For instance, the research cycle that is used in applied social research shares the same pattern:

- Establish a plan for information collection and carry out initial field work;
- Observe, discuss and collect data;
- Analyse the data and write the report; and

- Distribute the report and gather feedback that can be used to formulate further disseminate strategies.

INTELLIGENCE ANALYSIS THEORY

Why should we know about the theory of intelligence analysis if we can define it, and once defined, recognise intelligence in any of its four meanings? Because theory offers both scholars and practitioners the ability to understand how and why intelligence is what it is, and does what it does. Without a theory it is difficult to posit a view about an intelligence related phenomenon and then test that hypothesis through empirical observations to see if the results support the hypothesis, or reject it.

Although scholars have called for a theory of intelligence for decades, unfortunately until 2009 the literature was, I would argue, largely devoid of such theorising. Gill, Marrin and Phythian (2009) published an anthology of papers that addressed this “missing” intelligence theory issue to some extent, as did Marrin’s (2007) paper on a general theory of analytic responsibilities. Amongst the collection of essays by Gill, Marrin and Phythian (2009) were treatments by key opinion leaders such as professors David Kahn, Michael Warner, and Jennifer Sims. Although there are other scholars who have discussed the issue elsewhere in the subject literature (Walsh, 2011: 295–298), these researchers were, arguably, at the time of this writing in the forefront of the debate. However, surveying the theories advanced in Gill, Marrin and Phythian (2009) edited volume, it is evident that there is little consensus between the papers and nothing I would call an integrated theory of intelligence analysis. Nonetheless, these scholars are to be commended for progressing the debate by contributing to the discourse.

Given this situation, I responded to Walsh’s (2011: 295) call to build theory so that it might “...contribute further to developing the discipline of intelligence.” I saw this as an opportunity to provide an integrated theoretical framework that consolidates empirical findings and well-understood insights from the subject literature. This paper suggests such a theory; and like Marrin’s (2007) “general theory” of analytic responsibilities, one that is not military- or national security-centric. This is because the world of intelligence is no longer able to operate in such a neatly defined parameter. The post-9/11 world is vastly different to the siloed operations that were hallmarks of the Cold War. Present intelligence research projects can stride several categories of intelligence work—

for instance, law enforcement issues may impact on national security or military issues in the form of, say, espionage, terrorism, or the trafficking in arms, drugs and people, or a range of cyber-crimes. These issue may also impact on business (business intelligence) and private sector organisations (e.g. NGOs operating in developing countries).

GROUNDNED THEORY OF INTELLIGENCE RESEARCH

A *grounded theory* methodology, which I used to develop a complementary theory of counterintelligence,² was applied to observations made by surveying the intelligence subject literature. Grounded theory is an inductive process that examines data and constructs theory from the ideas and concepts that are collated into categories (Bell, 2009; Charmaz, 2009). The analysis of these data (i.e. the survey of the subject literature) formed the basis for the resulting theory of intelligence analysis.

My theory of intelligence analysis has its roots in the four definitions that were put at the beginning of this paper. There may be many other definitions of intelligence due to the fact that some scholars disagree with certain semantic constructions of “this-or-that” definition, it was, nonetheless, still possible to extract the core meaning from these various definitions in the subject literature. The results was the four unencumbered definitions presented above. These “conditions” therefore become the foundation on which I rested the theory. Reiterating these definitions, they are:

1. Actions or processes used to produce knowledge;
2. The body of knowledge thereby produced;
3. Organisations that deal in knowledge;
4. The reports and briefings produced for decision makers in the process or by such organisations; and
5. The fifth condition is that is required in order for intelligence research to occur in any or all of the four preceding definitions is that there needs to be some incorporation of secrecy.

Theoretical Framework

Having surveyed the subject literature and collated various research concepts and ideas into categories, it became apparent that there were six propositions that explained the various definitions of intelligence. This forms a system of

propositional units—a theory. These propositions consistent and integrated, and state that intelligence is driven by decision-makers' priorities so that they can respond to the need to project power in the face of competition/adversity (Marrin, 2007: 831). Each of the propositional units relates to the others in a relationship that is *coexistent* as opposed to being a set of *sequential* units. This means that all propositions need to be present for intelligence research to exist, but one proposition does not need to follow the other (they simply need to be present): 1) intelligence requirements need to be identified within the intelligence cycle process so that data collection and analysis is problem focused. This intelligence research can be either 2) defensive or it can be 3) offensive, and that intelligence needs to be 4) timely, as well as it needs to be 5) defensible. In terms of the last proposition, it comprises seven research methodological axioms—i.e. premises that are evident and accepted on face value.

Proposition 1—Secrecy is Provided via Counterintelligence

If the fifth condition discussed in the section above is not present, *intelligence research* then becomes *open research*. This is because the *knowledge* that is produced in either enterprise—intelligence or research—results in knowledge. It could be argued that knowledge leads to insight, and insight results in reducing uncertainty in decision making, but unless secrecy is involved, it is merely research. Having said that, secrecy will be context driven—what is secret for one agency may not be for another, or it may not be in a certain situation. The equation expressed earlier in this paper presents a logical model for the theory of intelligence:

$$(secrecy (information + analysis = intelligence \therefore insight \Rightarrow reduces uncertainty))$$

Expressed in narrative form intelligence theory might go something like this: Under the veil of secrecy—provided through the counterintelligence function³ (Prunckun, 2012)—analysts obtain information and analyse it. This process results in intelligence (knowledge) and therefore provides insight to decision makers (reports and/or briefings), which in turn reduces uncertainty. This takes place within an organisation (or unit within an organisation, etc.) that's role is to engage in intelligence (secret research).

If the requirement for secrecy is removed from the model, we can see how it transforms intelligence into research. By way of example, take the case of an open research project being conducted by, say, clinicians and researchers who

are exploring treatments for some of the more common forms of arthritis. Using the intelligence model just discussed, it can be seen that all the principles apply—analysts (researchers) obtain information and analyse it. This results in knowledge and therefore provides insights to decision makers (in this case, the development of a suitable drug), which in turn reduces uncertainty (that is, it gives certainty to manufacturing or other processes involved in the drug's effectiveness and/or production). But what is different is the use of counterintelligence to provide secrecy. This makes research *open research*—anyone could, potentially, access this information (or at least in a limited form of circulation as per, perhaps, a “private policy,” if conducted under the auspices of some organisation, but certainly not in a classified way as per intelligence). Open research (or as it is sometimes termed, *open science*, which includes social and behavioural sciences as well as the humanities) makes data, methods, and research findings accessible to the inquiring public.

In contrast, if some level of counterintelligence (secrecy) is applied, the research now becomes intelligence—in this example, *business intelligence*, to place it in the correct typological classification. Not all aspects need to be secrets, but the literature suggests at least one. Comparing this supposed case of drug research to military analysts who might be researching a question about the development of a new weapons system by an unfriendly nation. In the course of their inquiries they may access open source information—say, the *curricula vitae* of certain academics in that nation who are known to be experts in the particular technology needed to develop such a weapons system. Clearly, these data are freely available via the universities websites that employ them; but the fact that the research project is secret, the methods of analysis are classified, and other aspects of the endeavour are undisclosed, makes this *intelligence*.

Proposition 2—Intelligence Requirements, Data Collection and Analysis

The literature suggests that defining intelligence requirements (or essential elements of intelligence) is driven by decision-makers, yet some scholars posit that analysts must not be reactive and should drive the process of identifying topics, issues or problems that need examining (Marrin, 2007: 831). This theory of intelligence analysis puts forward the view that it cannot be one or the other; intelligence analysis must be flexible enough to accommodate both. For example, in a private intelligence setting where an organisation's concerns are narrowly focused, the decision-maker model may be valid. Whereas in a national security or law enforcement context, a hybrid model where decision-

makers set priorities is combined with analysts who advance questions that might need addressing. By perusing a flexible model for setting intelligence requirements (whether they are strategic, operational or tactical), subsequent data collection and analysis will be problem focused.

Proposition 3—Defensive Intelligence

Defensive intelligence is concerned with providing decision makers with insights into how to deal with threats, vulnerabilities, and risks. Defensive intelligence is applicable to five typological classifications discussed earlier—national security, military, law enforcement, business, and private sector intelligence. Defensive intelligence can be concerned with several related aspects of defense—for example these might include: prevention, preparation, mitigation, damage control/response, and recovery (and perhaps other areas).

Proposition 4—Offensive Intelligence

If intelligence research is not used defensively, it can be used in an offensive capacity. Intelligence can be used to assist decision makers plan offensive missions. A simple example is that of targeting in the military. Targeting analysts use intelligence to task military assets so they can damage or destroy enemy capabilities; provide advice for immediate fire or manoeuvre; or to support of deep offensive operations. Examples of the application of offensive intelligence to other intelligence typological classifications are conceivable. Offensive intelligence might include estimative or strategic intelligence because these categories of research projects concern themselves with outmanoeuvring emerging threats.⁴

Proposition 5—Timely

In order for intelligence to be useful, it must be provide in a timely fashion. If an intelligence report or briefing is not provided to decision makers on time, it is *prima facie* that the insights cannot be used. *Timely* may also include the notion of *continuous*—which is applicable in cases where an event is unfolding and updated intelligence is needed on a regular basic.

Proposition 6—Defensible Conclusions

Defensibility takes into account several factors. These include the need for the analytic process that produces intelligence to be transparent and replicable. Transparency means transparent to those who are within the defined circle of trust, not transparent to anyone outside that circle.

The reason for transparency is to allow those reading the reports, or receiving the briefings, to understand the methodological thinking. In academia this is known as reproducibility of results. But to do so would be most unusual, nevertheless what is likely is that a process of assessment will be carried out in the same vein when an academic research report is peer-reviewed for methodological soundness. Reproducibility underscores the fact that intelligence is based on the same research first principles as other types of applied research (barring the element of secrecy)—that is, the use of the scientific method of inquiry, which is based on sound quantitative and qualitative research methods (Prunckun, 2015).

Some scholars refer to this as *auditable*. But regardless of whatever term is used, replication means that, say, the reader of an intelligence report can understand the collection methods, collation and analysis techniques used (and understand why these were selected), and be able to derive similar conclusions as the analyst did from the study's findings. It is not to say that the next time the intelligence cycle is repeated that the same findings will be produced—it means that if the same data and methods used to arrive at the position articulated in the report were employed, it would be reasonable to expect similar results.

Even though the environment in which intelligence operates is dynamic, it does not stand in the way of the concept of replication. Applied social research is analogously the same—rarely does an issue under investigation remain static. There are numerous independent variables in any research question that can be added, removed, or changed. This applies to intelligence research too.

If transparency and the ability to replicate an intelligence study are present, then the findings are able to be “defended.” Integrity tied to this factor are the concepts of relevancy and accuracy—these are concepts often discussed in relation to intelligence research reports. The argument concerning these concepts is that if the proposition of defensible is maintained, by default, these two factors are also catered for, but it requires a set of axioms to help explain the reasoning behind it.

To achieve relevancy and accuracy in intelligence research output, a metaphoric potpourri of related research design considerations needs to be adhered to. These axioms suggest superior methodological design, and with these comes a more robust defence. Not all of the following axioms may apply to every intelligence research project, but as axioms they provide superior methodological design (Thyer, 1989):

Axiom 1—Data must show a high degree of internal validity;

Axiom 2—Assessment methods for dependant variables must show a high degree of reliability;

Axiom 3—Random sampling will prove better to more error prone sampling techniques;

Axiom 4—Experimental designs should be used when possible;

Axiom 5—Pre- and post-test are better than post-test only studies;

Axiom 6—Use of inferential statistical tests are superior to qualitative assessments/impressions only; and

Axiom 7—Multiple measures for observing the issue under investigation are more desirable to single measure approaches.

DISCUSSION

Why does it matter that we have a theory of intelligence research? Because theory allows us to test propositions—questions about, say, the efficacy of certain intelligence approaches, or operational methods, or procedural practices, as well as other issues facing the profession. For instance, it allows us to test the effectiveness of intelligence concerns in terms of outcomes, outputs, and processes. As Walsh (2011: 295–297) put it, it allows the development of the discipline of intelligence.

So what would intelligence scholars and practitioners test with such a theory? Well, prominent amongst the list of possible responses is the so-called phenomena of *intelligence failures*. For example, research questions that evaluate how intelligence agencies prioritise, task, and/or resource research into developing issues (strategic problems) versus current issues (tactical targets), and how these tensions might result in an “intelligence failure.” Take for instance the now ill-famed example of weapons of mass destruction where, “[President] Bush turned to [CIA Director] Tenet. ‘I’ve been told all this intelligence about

WMD and this is the best we've got?' . . . Tenet rose up, threw his arms in the air. 'It's a slam dunk case!'.⁵

Using this theory, other research questions can be formulated and tested. Findings of such empirical studies—ones based on valid and reliable data—can then guide good research practice. In sum, this theory of secret research could not be described as being conceptually dense, but nevertheless it is one that articulates the six coexistent propositions that explain why intelligence research is performed as it is, or where it is not, as it should be.

Perhaps other intelligence scholars will refine this theory so that the theoretical framework that underpins the craft of secret research is even better understood. "All being well, one would anticipate that, in the fullness of time, this and other yet to be articulated [intelligence research] theories will spawn better policy options. These policy options will therefore be based on defensible conclusions that are grounded in empirical research." (Prunckun, 2012: 48)

NOTES

1. *Raw information* is sometimes referred to as *unassessed intelligence*.
2. In 2011–2012 I advanced a theory of counterintelligence. I saw it as a way to fill the void in the subject literature that had existed for decades. My paper on this issue, along with the method I used, was published in progressively revised versions in the following publications: *American Intelligence Journal* (Volume 29, Number 2, December 2011, pp. 6–15), Hank Prunckun, *Counterintelligence Theory and Practice* (Lanham, MD: Rowman & Littlefield, 2012), and Henry Prunckun, "Extending the Theoretical Structure of Intelligence to Counterintelligence," *Salus Journal*, Vol. 2, No. 2, June 2014, 31–49.
3. Space in this paper limits my discussion of counterintelligence. I suggest that scholars who are interested in this intelligence function see Hank Prunckun, *Counterintelligence Theory and Practice* (Lanham, MD: Rowman & Littlefield, 2012) for a more detailed discussion.
4. Acknowledging that counterintelligence can also have an offensive focus and therefore could be included in this discussion (see Prunckun, 2012).
5. Former CIA Director George Tenet's reported reply to then-President George W. Bush regarding his question about the threat posed by Iraq. Quote as cited in Woodward (2004: 249).

REFERENCES

- Andrew, Christopher; Aldrich, Richard; and Wark, Wesley (2009). *Secret Intelligence: A Reader*. London: Routledge.
- Bell, David C. (2009). *Constructing Social Theory*. Lanham, MD: Rowman & Littlefield.
- Charmaz, Kathy (2009). *Constructing Grounded Theory*. Los Angeles; Sage.
- Cohen, Ira S. (1975). *Realpolitik: Theory and Practice*. Encino, CA: Dickenson Publishing.
- Gill, Peter; Marrin, Stephen; and Phythian, Mark, editors (2009). *Intelligence Theory: Key Questions and Debates*. New York: Routledge.
- Lowenthal, Mark M. (2009). *Intelligence: From Secrets to Policy*, fourth edition. Washington, DC: CQ Press.
- Merrin, Stephen (2007). "Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities," in *Intelligence and National Security*, Vol. 22, No. 1.
- Morris, William, editor (1971). *The American Heritage Dictionary for the English Language*. Boston: American Heritage Publishing Co. and Houghton Mifflin Company.
- Prunckun, Henry (1996). "The Intelligence Analyst as Social Scientist: A Comparison of Research Methods." *Police Studies*, Vol. 19, No. 3.
- Prunckun, Hank (2012). *Counterintelligence Theory and Practice*. Lanham, MD: Rowman & Littlefield.
- Prunckun, Hank (2015). *Scientific Methods of Inquiry for Intelligence Analysis, 2nd edition*. Lanham, MD: Rowman & Littlefield.
- Schroeder, Terry L. (1983). *Intelligence Specialist 3 & 2, vol. 1*. Washington, DC: Naval Education and Training Program Development Center.
- Thyer, Bruce (1989). "First Principles of Practice Research." *British Journal of Social Work*, Vol. 19.
- Walsh, Patrick F. (2011). *Intelligence and Intelligence Analysis*. London: Routledge.
- Woodward, Bob (2004). *Plan of Attack*. London: Simon & Schuster

ACKNOWLEDGMENT

I would like to thank the three reviewers for their comments and advice.

ABOUT THE AUTHOR

Dr Henry Prunckun, BSc, MSocSc, PhD, is Associate Professor of Applied Research at the Australian Graduate School of Policing and Security. He specialises in the study of transnational crime—espionage, terrorism, drugs and arms trafficking, as well as cyber-crime. He is the author of numerous reviews, articles, chapters, and books, including, *Scientific Methods of Inquiry for Intelligence Analysis, 2nd edition* (Rowman & Littlefield, 2015), *How to Undertake Surveillance and Reconnaissance* (Pen & Sword Books, 2015), *Intelligence and Private Investigation* (Charles C. Thomas, 2013), and *Counterintelligence Theory and Practice* (Rowman & Littlefield, 2012). He is the winner of two literature awards and a professional service award from the International Association of Law Enforcement Intelligence Analysts. He has served in a number of strategic research and tactical intelligence capacities within the criminal justice system during his twenty-eight year operational career, including almost five years as a senior counterterrorism policy analyst during the Global War on Terror.

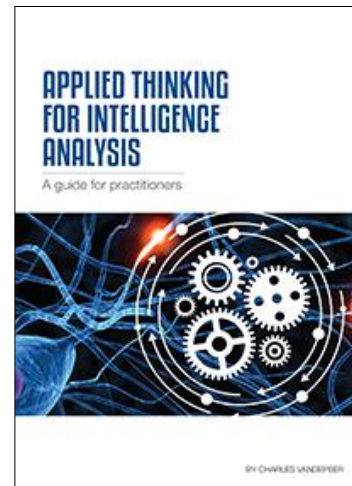
- o O o -

Book Review

Applied Thinking for Intelligence Analysis: A Guide for Practitioners

by Charles Vandeppeer, PhD
Air Power Development Centre, Department of
Defence, Canberra, Australia
2014, 106 pages
ISBN 13: 9781925062045

Reviewed by Trista M. Bailey



Intelligence analysis is a process that requires a distinctive set of problem-solving skills accompanied by the ability to be self-critical. As a profession, it demands precise judgement on problems that are often dynamic, people-based and future-orientated. An intelligence analyst is expected by the customer to provide a conclusive product that is tangible, well informed and credible. *Applied Thinking for Intelligence Analysis: A Guide for Practitioners* is designed to empower the junior intelligence analyst with an easy to understand conceptual toolkit. Rather than be intimidated by the challenge of uncertainty and the abundance of information in today's so-called information age, author Dr Charles Vandeppeer encourages the junior analyst to embrace the unknown and take comfort in what one doesn't know.

Vandeppeer has drawn on the work of several scholars and academic sources in the fields of social science, psychology and critical thinking; producing what is a very clever and intentionally cultivated framework and foundation for the training of a junior analyst. The length of the guide should not fool one into assuming a lack of content or depth—this book provides not only an introduction to analytical techniques and the problems and limitations an analyst may come to face in the future, but also stimulates a new means of

critical thinking with an attempt to cultivate self-reflection and auto-critique within the methodological process.

The progression of concepts discussed use easy to understand terminology, making this book both a fantastic foundational tool for analysis training and also a useful reference book for senior analysts. Positive and negative aspects of the analytical process are identified, linking both understanding and identification of potential limitations within the analysis process. By situating intelligence analysis within context and by detailing the expectations of intelligence analysis with a working and tangible definition, Vandeppeer empowers the analyst with an identified fundamental purpose.

Through the use of a tangible definition of intelligence analysis, reasoning behind the identification of problems, limitations and bias are introduced. The concept of the ‘problem’ is defined, providing grounding for justification on potential limitations, including time and research, evidence and the cognitive bias of the human condition. The chapter “Knowledge, Information and Evidence” identifies the difference between deductive, inductive and abductive reasoning, as well as describing the difference between diagnostic, negative and the absence of evidence. Vandeppeer furthers the concept of self-reflection by explaining concepts such as intuition and other sub-conscious by-products produced by the analysis process that the analyst may face.

Concepts such as language are discussed, including the use of analogies and metaphors within verbal and written product on an audience, including the elements of expertise, prediction and surprise, allowing a junior analyst to question predispositions and presumptions they may have about their own analytical ability. Contrasting concepts are also explained, such as the relationship between prediction (forecasting the future) and retrodiction (making a prediction about the past). For the intelligence analyst, complexity and uncertainty are part of an ongoing process. Vandeppeer brings attention to the influence of the work and social environment on the analyst through ideas on conformity and teamwork, including expectations of the corporate line and also the tendency of analysts to defend past assessments rather than to be open to the idea of producing a falsifiable product.

Aside from identifying limitations and problems, Vandeppeer offers solutions through critical thinking techniques such as backcasting, mindmapping, nominal group technique, pre-mortem analysis and indicators of change in an

attempt to avoid unintended consequences and assumptions within the analysis process. In the chapter, “Mindsets, Cognitive Biases and Arguments,” Vandeppeer identifies the negative by-products of the analytical process. Even though these are inescapable as they are part human element of the process itself, it is key to be aware of them—rationally and consciously thinking of their identification and how to counter these limitations as they develop, in an effort to avoid or minimise them.

Dr Vandeppeer concludes with the concept of unfinished intelligence; although a final product of analysis and assessment is produced in a formal brief or report, intelligence may never be finished. As someone with a rich background of expertise in intelligence throughout a military career, Vandeppeer describes the process to be one that is liberating and empowering—the process itself as the challenge of what an analyst can tangibly produce despite many limitations. It is important to be self-confident in the production of assessments; however, it is of more importance to have humility in reconsidering assessments in light of new information. Assessments are always open to be falsifiable in an age where intelligence is likely to change. Awareness and applied thinking are keys to good intelligence.

ABOUT THE REVIEWER

Trista M. Bailey, BA, MIR, is an officer-in-training in the Royal Australian Air Force (RAAF). She completed her undergraduate degree at the University of Melbourne with majors in Political Science and Cultural Studies. She holds a Master of International Relations degree with the completion of a minor thesis in the field of Strategic and Security Studies; *Australia’s Strategic Paradox: Balancing the Autonomy/Dependency Dichotomy with the Prescriptive Doctrine of “Self-Reliance.”* Ms Bailey’s academic interests include foreign affairs, strategic and security issues, defence policy doctrine, and threat analysis.

- o O o -

Book Review

Police Leadership and Management

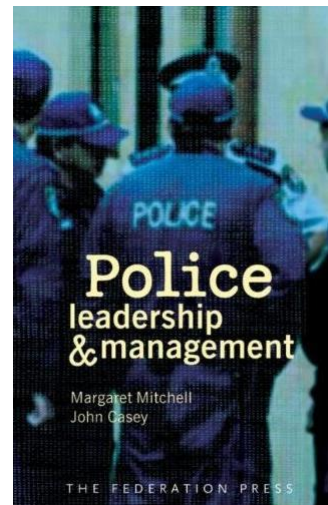
by Margaret Mitchell and John Casey (editors)

Federation Press, Sydney

2007, 290 pages

ISBN 9781862876491

Reviewed by Alan Beckley



The Mitchell and Casey text contains eighteen chapters written by leading police researchers and commentators; and is regarded by many academic tutors as indispensable learning for post-graduate students. The editors have chosen the chapter authors well as they are well-researched and leading authorities in the policing and law enforcement field in Australia. There are three parts to the book, which are all related to aspects of police leadership and management: the changing contexts of operational police work; developing the profession of policing; and managing relationships in policing.

The first section of the book examines changing law, partnership policing, private sector policing, managing intelligence, evidence-based policy and practice and investigative interviewing. These somewhat disparate subjects are linked and cross-referenced on occasions by the authors, but they seem to the strategic reader to be uncoordinated, and by no means comprehensive.

It is true that they all contain changing contexts, but some of the subject matter, such as managing intelligence, was in every-day use in military circles even before police forces were invented, although admittedly, there have been recent developments. Though the authors do not claim exhaustive coverage of the subject of operational police work, the reader might expect to see other contemporary subjects such as internet crime or transnational crime, which do appear briefly in section three. Having criticised the first section for its coverage, it should be noted that the contributors have covered their specialist

subject areas well, particularly identifying the relevant issues for the attention and benefit of police managers and leaders.

The middle part of the book gathers subjects around police professionalism and here the authors seem to have achieved greater coverage of the subject. The long-term on-going, but painstakingly slow, progress towards professionalisation of the police service is assiduously tracked in chapter eight. In this chapter there is a good section to remind readers of the onerous requirements of a professional body; the police service in Australia (as in most other countries in the world) is some way off being able to lay claim to those requirements, not least a nationally-recognised body of knowledge (see chapter thirteen) and clearly defined professional standards, let alone continuous professional development requirements.

Leadership development and accredited training is correctly identified as a way forward along with police ethics, integrity and effective accountability. Performance management systems are described but are under-developed in the police service in Australia following various government requirements of “managing by objectives” and “public service management,” most of which was found not to be effective in this context.

Police organisations will need a serious examination of themselves to identify areas for improvement in their approaches towards organisational justice in human resource management systems to promote fairness, staff well-being and equity within their agencies to optimise staff engagement and quality of service standards. Three chapters in this section discuss these matters and it would have been useful to police managers to identify the overall effect of neglect in these areas to the detriment of professionalising the police. Chapter eleven specifically examines the independent oversight of the police, which is very relevant to the profession of policing, but content overlaps and duplicates some of the information in chapter ten which focuses on police integrity. Both chapters accurately portray the situation of police accountability in Australia but they fail to move the subject on and into developments for the future.

Part three of the book moves into managing relationships in policing. The reviewer was surprised to find this section was all about *external* relationships rather than *internal* relationships in policing; however there are some useful chapters here on how to manage the news media, consultation with the public, policing indigenous communities and the issues relating to international policing.

These factors may or may not personally affect the individual police manager or leader, but it is important to be aware of them as potential issues; however, these three final chapters are relatively rather short and although setting out the facts, they are light on solutions.

The latter sentence could, in fact, summarise the content of the whole book but that is what makes it so useful to police academics and tutors: assignments can be set for the unsuspecting student to assimilate information from the text and then compile their own findings, conclusions and recommendations in the form of an essay. Therefore, the book leaves the thinking and reflection where it should lie; with the student of policing. However, the book is also useful to the non-practitioner researcher as a reference source. Although a few years have passed since its publication, it still holds relevance and is recommended.

ABOUT THE REVIEWER

Alan Beckley is Evaluation Manager and Adjunct Fellow at University of Western Sydney. He is a graduate of FBI National Academy where he trained while serving as a police officer in the United Kingdom. He is currently completing the degree of Doctor of Philosophy in the area of human rights and ethical standards in policing at the University of Western Sydney.

- o O o -

Call for Papers

Salus Journal is a peer-reviewed open access journal for the publication on law enforcement and security issues as well as research findings and discussion papers regarding emergency management and public safety. *Salus Journal* seeks to contribute to practice by inspiring discussion through an interdisciplinary approach.

We invite submissions of articles of between 3,000 and 5,000 words for double-blind peer-review that:

- focus on issues that have an impact on criminal justice, law enforcement, national security, or emergency management;
- engage with contemporary topical practice issues; or
- add to the understanding of complex management conundrums.

Submissions can use either qualitative or quantitative approaches, including studies that employ the use of exploratory or holistic approaches. The journal also accepts discussion papers, critical essays, and analytical papers as long as a clear position is stated and the argument is grounded in sound practice, or the subject literature.

Book Reviews

Salus Journal also accepts book reviews of around 750 words. Reviews should go beyond the descriptive account of the book's contents. Reviews that discuss the implications of the book's message for practice or policy are sought for inclusion in future editions. Books can be either newly published or vintage editions where the book's thesis can be applied to a current situation or in an emerging context.

Submission Process

Visit the journal's submissions page to see a copy of the author guidelines and a summary of the refereeing process:

www.salusjournal.com/submissions