



Volume 4, Number 2
2016

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



Volume 4, Number 2, 2016

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 APM, AO
Mr Warwick Jones, BA MDefStudies

Editor-in-Chief

Dr Henry Prunckun
Charles Sturt University, Sydney

Assistant Editor

Ms Kellie Smyth, BA, MAPAnth, 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
Dr Victoria Herrington
Australian Institute of Police Management
Dr Valerie Ingham
Charles Sturt University, Canberra
Dr Stephen Marrin
James Madison University, Virginia
Dr Alida Merlo
Indiana University of Pennsylvania
Dr Alexey D. Muraviev
Curtin University, Perth, Western Australia
Dr Maid Pajevic
*College 'Logos Center' Mostar,
Bosnia-Herzegovina*
Dr 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
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

Volume 4, Number 2

2016

Contents

Essays

- Ten “Big Bangs” in Theory and Practice that Have Made a Difference to Australian Policing in the Last Three Decades**
Rick Sarre 1
- Cybersecurity Risks: Are they Inflated?**
Petr Chrapavy 19
- Closing the Cybersecurity Skills Gap**
Rebecca Vogel 32
- “We’re the Ones that Stand Up and Tell You the Truth”:
Necessity of Ethical Intelligence Services**
Nathan J. Phillips 47

Research Article

- The Paradox of Fiction and Terrorism’s Overshadowing of
Organised Crime as a Law Enforcement Concern**
Henry Prunckun 62

Book Review

- Branding Terror: The Logotypes and Iconography of
Insurgent Groups and Terrorist Organizations***
Christian Luc Carnus 82

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.

TEN “BIG BANGS” IN THEORY AND PRACTICE THAT HAVE MADE A DIFFERENCE TO AUSTRALIAN POLICING IN THE LAST THREE DECADES

Rick Sarre*

ABSTRACT

This paper discusses what could be considered the top ten innovations that have occurred in policing in the last thirty years. The intent is to focus attention on how practice could be further inspired by additional innovation. The innovations are discussed here as “Big Bangs” as a way of drawing attention to the significant impact they have had on policing, in the same way that the cosmological Big Bang was an important watershed event in the universe’s existence. These ten policing innovations ushered in, it is argued, a new mindset, pattern or trend, and they affected Australian policing profoundly; although many had their roots in other settings long before Australian policy-makers implemented them.

Keywords: police research, innovation, policy-making, criminology

BACKGROUND

Each of the ten “Big Bangs” that follow ushered in a new mindset, pattern or trend in policing practice. Each has significantly changed the way in which policing is now conducted in Australia. Some have been very successful; others less so. This paper looks back over the last thirty years and discusses these themes and trends in the context of their policy implications and practice ramifications.

There are some caveats and criteria that need to be mentioned at the outset. Not all of the Big Bangs have undergone evaluations as such (for example, it is difficult to evaluate *community policing* as a concept), but each has emerged from theoretical development. Not all of the Big Bangs have led to effective implementation, as there is a well-recognised disconnect between a good idea and a legislative or policy response (Sarre, 2011). The innovations discussed here are not considered from a cost-benefit perspective either, because that would involve an econometric exercise of substantial proportions. Finally, there has been no

* Corresponding author: rick.sarre@unisa.edu.au

attempt to rank these developments in order of importance. They are presented here to stimulate discussion and, hopefully, to inspire further policy development.

1. GENDER DIVERSITY IN POLICE RECRUITMENT

It is axiomatic that gender diversity is essential to the employment landscape in Australia. Police ranks, however, have been dominated by men for most of Australia's history. The first appointments of women as police in Australia were made in 1915, initially in New South Wales and then in South Australia. But progress was slow. A political force advocating their recruitment was a loose coalition of women's groups called the *women police movement* (Prenzler, 2015). Women's charitable and political organisations lobbied for a specialist group within the police to deal more effectively with women and girls caught-up in welfare institutions and consequently the criminal justice system. Somewhat surprisingly, it was not until 1961, when the Northern Territory adopted this policy, that all Australian jurisdictions were finally employing female officers.

For much of their history, Australian police forces were workplaces characterised by white males of Anglo-Saxon heritage; recruitment was based on onerous height and weight restrictions that were subsequently shown to be unrelated to the work that police perform (Prenzler, 2015). Antagonism to women in the ranks was intense: in 1971 only 1.8% of police officers in Australia were female. That rate had risen to 15.2% by 1994 and it currently stands at around 25%, although the clustering is mainly at the lower and not senior ranks. From a policy point of view, this can be seen as a less-than-optimal integration outcome (Prenzler & Sinclair, 2013, p.129).

The 25% mark has been brought about by an admirable and visible commitment to gender equity in the last three decades, driven by a legislative imperative for equal opportunity. Indeed, in South Australia, Commissioner Grant Stevens announced in December 2015 his intention to implement a 50/50 gender recruitment strategy that would be aimed at increasing female officer numbers. Australian police departments now tout exemplary human resource management policies, with increasing efforts to become flexible and so-called "family friendly workplaces" (Prenzler, Fleming & King, 2010).

All of the old recruitment criteria, which focused on strength and height and thus discriminated heavily against women are gradually being replaced by selection criteria that are focused on education, trainability, long-term health (including mental health) prospects, communication and problem-solving skills

(Prenzler, 2015; Robinson, 2015). However, more needs to be done. Gender discrimination still occurs. The *Report of the Victorian Equal Opportunity and Human Rights Commission* released in December 2015 (EO & HRC, 2015) found Victoria Police had a culture of cover-up, unlawful acts and unreported sexual discrimination and harassment cases. The report was most uncomplimentary, suggesting commissioners should keep a watching brief on these issues if further improvement is to be gained.

2. EMBRACING DIVERSION: PUSHING OFFENDERS OUT OF THE JUSTICE SYSTEM AT THE EARLIEST OPPORTUNITY

Given the evidence that the probability of an offender returning to the juvenile courts increases as the number of appearances of that offender increases (Cunneen & White, 2002, p.78), police have been at the forefront of policy reforms designed to promote diversionary options at the earliest opportunity. If police are embracing diversionary practices, it becomes less likely that young persons, especially Indigenous young persons (Blandford & Sarre, 2009), will continue into the formal criminal justice processes.

A number of types of diversions are relevant here: informal cautions (used for minor offences and, generally, first time offenders), formal cautions (used for those cases that are assessed as minor by the investigating officer), diversions of offenders into the specialist courts (such as drug courts, mental health courts, and family violence courts) (Daly & Proietti-Scifoni, 2011) and family conferences (which can be convened as an alternative to the juvenile courts). This last option emerged in the late-1980s upon the realisation that reintegration of young offenders was more likely to occur if interactions with them occurred *outside* of the justice system.

Relevant cases (usually referred by police, but can be court referred) are those typically where victims are involved or where the offender has committed the offence before. A family conference is a mediated forum that identifies and attempts to resolve the problems that may have precipitated the offending behaviour. Conferences usually lead to undertakings by the offender, examples of which include attending a drugs and alcohol information session, attending anger management counselling, writing letters of apology to a victim, making payments of compensation, and doing community service.

An evaluation in Canberra twenty-five years ago showed reductions in violence for youths (less than thirty years of age) when they were randomly

assigned to a conference rather than court. In the first two years after arrest, violent offenders who participated in conferences had about 50% less reoffending than those who went to court (Sherman & Strang, 2007). Another study showed reductions of 15–20% in re-offending across different offence types regardless of the gender, criminal history, age and Aboriginality of the offenders (Luke & Lind, 2002).

While evidence of the overall effectiveness of conferencing has been less convincing in recent times (Smith & Weatherburn, 2012; Sherman, Strang, Mayo-Wilson, Woods & Ariel, 2015, p.20), the evidence does suggest a somewhat positive trend. Daly (2000) found high levels of victim satisfaction with conferencing and concluded that restorative justice programs work at least as well as court-based responses, and, interestingly, at no more cost. Police support for conferencing and other diversionary practices remains strong, thus giving these diversionary approaches continued buoyancy. From a policy perspective, the question that now presents is: What innovations can criminologists propose that might take these developments to the next level?

3. COMMUNITY POLICING: POLICING WITH THE CONSENT OF THE COMMUNITY

In the 1980s policy-makers turned to what has become known as *community policing*. This is policing that places a key emphasis on foot patrols (“beat” policing) and community service, not unlike the roles played by peace-keepers of the pre-industrial era. Most importantly, community policing shifted the philosophy away from faster reactive measures towards proactive models of operation that are developed after a process of community consultation. That is, in a system of community policing, citizens provide the grass roots information about policing needs along with the resources that they have, and the police provide the personnel and the hardware to carry out the tasks required. Therefore, it is a joint, and theoretically, equal operation. Community policing is designed not only to prevent criminal activity, but to reduce the conditions under which deviant behaviour is encouraged.

The story of the last thirty years of community policing has brought mixed reviews. Fundamental to the notion of community policing is shared functions and mutual cooperation, and that was never really going to happen (Weisburd, McElroy and Hardyman, 1989). Indeed, it may not be appropriate at all to shift

power from the police to the community in the way envisaged by those promoting the model (Sarre, 1996).

However, the idea of systematising community involvement in crime reduction was ground-breaking. This innovation has withstood the test of time in so far as there has not been a wholesale retreat by Australian police to anything like the reactive models that were used prior to the 1980s. But new questions have arisen: How can policing now adapt this model to social media, portable communication devices and a generation that is not only socially active, but geographically mobile?

4. PROBLEM-SOLVING AND INTELLIGENCE-LED POLICING

Until the current generation of policing, police typically patrolled at random, waited for distress calls and responded accordingly when they came. Under this traditional reactive model, police responded to calls that were not only treated in isolation, but considered closed when the case was solved or filed.

Problem-solving policing, by contrast, de-emphasised random patrolling, and sought-out precipitating factors, which, if eliminated, had the tendency to stop or at least to limit the anti-social conduct that otherwise might have occurred.

Problem-solving policing, and the allied approach of intelligence-led policing, is consistent with the view that not all crime and disorder problems are the same, nor are the neighbourhoods and communities in which they occur the same. A problem-oriented strategy attempts to collate incidents together in order to describe the larger picture (Prenzler & Sarre, 2015). This has the spin-off effect of police being able to avoid political pressure to task resources to certain crimes at the expense of others because the former may carry some emotional, but not material, community concern.

Examples might include a domestic violence strategy that attempts to tailor police responses in accordance with what is known of the occupants of a house, namely whether there is a history of violence or a firearm on the premises. A community with a history of racial victimisation may benefit from a policing strategy that endeavours to root-out acts of racism. Such approaches have the potential to identify and ameliorate conditions that would otherwise require repeated police mobilisations and thus prevent the wastage of valuable policing resources (Moore, 1992).

Intelligence-based models have demonstrated their worth, and police are supportive of them. Nonetheless, new questions for police commanders arise when it comes to addressing crimes that span national security and domestic policing. For it is here that the police potentially risk tarnishing their image with community claims of political interference, the violation of civil liberties, and the abuse of (secret) powers associated with intelligence work.

5. FORMING POLICING PARTNERSHIPS WITH THE COMMUNITY

In the last thirty years in policing there has been a noteworthy shift away from police assuming sole responsibility for the maintenance of public order towards a model that sees police enjoining others to form partnerships with them (Dixon, 2005, p.5). Police have developed alliances with groups and professionals who focus not only upon social and economic stability (such as teachers, social workers, employment personnel and recreation officers), but also with those who advocate and advance more specific crime prevention programs (such as the Australian Crime Prevention Council).

The emphasis here is on non-police resources being brought to bear on local security problems. The popular Neighbourhood Watch program immediately comes to mind. More generally, there are various courses and programs that teach crime prevention through environmental design (CPTED). The focus of CPTED is on opportunity to reduce crime through public surveillance and target hardening.

These partnerships now extend to a large pool of personnel who look like police, but who are not. Indeed, there has been a dramatic growth in the private security industry since its identification over three decades ago as a key player in policing and security (Shearing & Stenning, 1983). Indeed, a citizen, when moving around the community in daily life, is far more likely to be directed, challenged or searched by a private security officer than by a police officer.

Private providers of security are now an indispensable part of the policing landscape. They engage in investigations, take witness statements, inspect bags, detain suspected shoplifters, monitor detention centres and court precincts, patrol shopping centres, and serve in crowd control operations around sporting and other community events. Indeed, private security has been described as “the primary protective resource” in modern society (Pastor, 2003, p.44).

Moreover, international research has found that private security directly contributes to reductions in criminal victimisation, albeit with a widening gap

world-wide between victimisation of the rich and poor relative to their ability to afford security staff and devices (van Dijk, 2008, pp.129ff). The result has been increased government regulation, although its ability to do anything more than attempt to keep disreputable applicants out of the industry has been mixed (Prenzler & Sarre, 2008).

Associated with this trend is what has been referred to as *third party policing*, a term that acknowledges the role played by businesses, property owners and inspectors working for government and non-government agencies to engage in policing activities that are not directed by police (Mazerolle & Ransley, 2006). The overall result is a *pluralisation* of social control mechanisms of which state-run police forces are simply a part, albeit a crucial one (Prenzler & Sarre, 2006).

The important part of this is that, while the relationships between public and private operatives are still very much in a fluid state (Sarre & Prenzler, 2000), police are, for the most part, accepting of the partnership role played by non-police (Prenzler & Sarre, 2007). It is a mutually convenient arrangement, but can it usefully be extended further? And if so, in what ways?

6. REINFORCING THE IMPORTANCE OF POLICE PROCEDURAL FAIRNESS

According to the growing body of research on this subject, people are more likely to obey the law if they consider that the police are behaving “legitimately,” that is, in a procedurally fair manner (Tyler, 2006). Findings from studies examining the association between police legitimacy and compliance with the law suggest that the former (fair and just processes, along with respectful treatment of individuals) is fundamental to achieving the latter (Tyler, 2003). Where police appear neutral and unbiased, and their decisions are perceived as objective, the perceptions of fairness are enhanced (Tyler & Lind, 1992). Moreover, when people view the law and enforcers of the law as acting lawfully and being procedurally fair, they are more likely to defer to rules and to police decisions, and to self-regulate (Tyler & Fagan, 2008). Policing becomes less problematic in such an environment.

These findings are supported by the fifth *European Social Survey* that was recently conducted across twenty-eight countries. The study found that trust in police procedural justice is the strongest and most consistent predictor of a “felt obligation to obey,” the association being positive and significant in relation to all

countries for which a dataset became available in 2012 (Hough, Jackson & Bradford, 2013).

Barkworth & Murphy (2015, p.270) reported the same thing here in Australia.

Procedural justice appears to be consistently important for influencing both emotional reactions and compliance [with the law and the police] ... By engaging with the public in a polite, respectful, and empathetic manner, police officers will be able to reduce negative sentiments and emotion directed at them, thereby increasing people's willingness to comply with them both immediately and in the future.

Research has also shown that procedural justice is an important predictor of victims' satisfaction with the criminal justice system (Murphy & Barkworth, 2014). Moreover, tailoring the way police speak to drivers during routine encounters (such as random breath testing) can have significant implications for police-community relations (Mazerolle, Bennett, Antrobus, Eggs, & Martin, 2015; Mazerolle, Bates, Bennett, White, Ferris & Antrobus, 2015).

Legitimacy theory has justifiably captured a great deal of attention in research circles. The fruitful research in this field continues apace, and with good reason, for it flies in the face of the commonly expressed lay view that if police were given more latitude to ignore the rules, then the community would become more law-abiding. The "Dirty Harry" style of policing is exposed by this research as counter-productive (Klockars, 1980). If we are to advance developments in this area, criminologists and police commanders should be working together to design ways to facilitate its implementation.

7. ESTABLISHING AN EVALUATIVE (EXPERIMENTAL) BASE AND MAPPING THAT INFORMATION

Beginning in the 1980s, an evaluative (experimental) police research base began to be maintained and consolidated. We now know a lot more about the effectiveness of all aspects of police work because we have been testing the theories, evaluating the data, measuring outcomes, and mapping the geography of crime and its enforcement (Legrand & Bronitt, 2012).

Research into *hot spot* policing specifically, and crime mapping, generally, has revealed that crime tends to cluster in geographical areas (Chainey & Ratcliffe, 2005; Weisburd & McEwen, 1998) and that deploying police as a result of knowing these data can have benefits. Resource allocations can now be better determined by time and place considerations that give rise to efficiencies.

Australia's statistical database has grown exponentially, too. Until twenty years ago was there no effort being made to standardise Australian crime and justice statistics. That has all changed. The Australian Bureau of Statistics now hosts a number of databases, including police data (reported crimes and victimization rates), as does the Australian Institute of Criminology (soon to be located within the Australian Crime Commission), which manages a range of datasets including the Indigenous Justice Clearing House, deaths in custody statistics, homicide statistics, drug use monitoring data, cybercrime and deception offences, victims of crime and violent crime, and firearm monitoring. The Productivity Commission now has entire sections devoted to police resources, police numbers, and public confidence in policing amongst other things (Steering Committee, 2014).

Police regularly conduct internal reviews and establish their own evaluative bases using the data available; for example, the Australian Federal Police has an international deployment group with its own design and evaluation team. Since 1995 the Australian Institute of Police Management has been an integral part of police research and education in this country. We now know a great deal more on the best forums for police accountability, too, an important driver of public confidence in Australia (Prenzler, 2000). The information age is with us. Policing has benefited enormously from it. The nature of experimental research is such that it is ever-ready to push forward. The question is: What new horizons should criminologists be focusing on now?

8. SPECIAL POLICING OF DIVERSE COMMUNITIES AS A BADGE OF HONOUR

Police have made remarkable steps in the recent past towards recognising that some groups in society have special policing needs. Officers have tried to tailor their responses accordingly. The two special needs groups that should be mentioned here are Indigenous Australians, and Australians who identify as either lesbian, gay, bisexual, transgender, intersex, or queer (LGBTIQ).

There is little doubt that the experiences of Indigenous peoples in their relationships with police has been, and often continues to be, qualitatively different from those of non-Indigenous Australians (Johnston, 1991). This arises in contemporary Australian society primarily through two main factors: a frontier war colonial heritage, and two hundred years of social construction of Indigenous peoples as inferior. These constructions continue to provide the context in which

contemporary police decision-making occurs (Cunneen, 2001, p.128). Even today the high numbers of Aboriginal and Torres Strait Islander peoples coming into police custody continue to grow. Indeed, while Aboriginal and Torres Strait Islanders (ATSI) constitute 2% of the Australian population, those who identify as ATSI currently constitute 25% of Australia's prisoner population (Australian Bureau of Statistics, 2015), a policy failure of the highest order.

Nevertheless, there has been a concerted effort by Australian police to address the malaise. There has been a deliberate drive to recruit Indigenous police officers, a policy in keeping with the spirit of the recommendations of the 1991 Royal Commission into Aboriginal Deaths in Custody (Johnston, 1991; Kamira, 2001, pp.79–81), and Indigenous police women especially (Fleming, Prenzler & Ransley, 2013). There has also been widespread implementation of training in cross-cultural sensitivities in police academies, in concert, again, with the 1991 recommendations and designed to eradicate any police racism that may still persist.

Other initiatives include police support for Indigenous-run policing patrols (Blagg & Valuri, 2002). Similarly-structured Aboriginal Community Patrols began through funding by the New South Wales Attorney-General's Department's Indigenous Justice Strategy (Sarre & Sparrow, 2002). The appearance two decades ago of Aboriginal courts in Australia now make it more likely that those on bail will appear in person for hearings and thus be less likely to be ordered to custodial remands (Cultural and Indigenous Research Centre Australia, 2013).

Police liaison officers have been tasked to incorporate into their duties the raising of confidence in police in the LGBTIQ communities such that they are more likely to report victimization. South Australia Police, for example, presently has a liaison arrangement with the Department for Communities and Social Inclusion to implement the 2014–2016 *South Australian Strategy for the Inclusion of Lesbian, Gay, Bisexual, Transgender, Intersex and Queer People*. Considering the well-recognised antipathy shown by police two generations ago towards gay men, the change has been remarkable. But what are the next steps that need to be taken in order to refine special needs policing?

9. REVOLUTIONISING TECHNOLOGIES

Police surveillance capacity is now at a level never before seen, not just the new equipment available to police, but the cheap surveillance equipment now available to the public who regularly share data with police to assist them with their inquiries. True, these devices have been around for a considerable time: there has been CCTV

targeting crime in Australia for decades (for example, see Sutton & Wilson, 2003), but there are now ever-increasing opportunities for portable surveillance technologies to be incorporated into daily police routines (Chan, Doran, Brereton, & Legosz, 2001).

The use of body-mounted cameras by police officers designed to protect them in their work is now commonplace. The relatively low cost associated with fitting officers with vehicle-mounted cameras that provide CCTV surveillance in real time via mobile connectivity makes this a viable (and cost effective) choice for governments. There are two drivers of this trend: the availability of the technology at a price that is more affordable than it was a decade ago, and a global culture of fear and distrust which have provided surveillance practices with legitimacy as unexceptional tools of social order (Sarre, 2014).

Police are also the beneficiaries of technological advances in data extraction and retention, especially in so far as they have been identified as crucial tools in anti-terrorism strategies. True, the jury is still out regarding the ability of these strategies to fulfil these needs (Sarre, 2015), but police have adopted confidently the instruments of innovative data surveillance.

It should be mentioned that there is a growing concern that the use of these technologies has the potential to undermine public confidence in police. This can happen in one of three ways. The first two relate to content on the Internet: police may be filmed doing things that they ought not be doing while they are on duty (one can immediately think of the Rodney King beating) (Kearon, 2013, p.418) or may contribute to their own reputational damage in the public eye by their off-duty and inappropriate use of social media (Goldsmith, 2014). The third comes from the technology itself: police will continue to take the brunt of public criticism that they are simply revenue-raising when using road traffic technology to penalise unsuspecting motorists (Kearon, 2013, p.421).

Government policy-makers, parliamentarians, and the courts alike are searching for the required balance between levels of surveillance that will provide information for the maintenance of security, and the rights of individuals to be free from the prying eyes of agents of the state. On balance, one can form a responsible view that surveillance technologies are more benign than harmful, and that policing policies are finding the required balance. In order to continue to reap the fruits of our free and open society, this is an area ripe for further research. Being crime-free is an ideal goal, but not at the expense of diminishing the community's civil liberties. Where should the line be drawn?

10. CHAMPIONING POLICE EDUCATION OUTSIDE OF THE ACADEMY

There has been a distinct shift in policing education towards an emphasis upon broader educational opportunities for police. This increased focus on tertiary education for police has been driven in part by calls emanating from major reviews and corruption inquiries (Prenzler, Martin, & Sarre, 2010). Indeed, in 1989, the Fitzgerald Inquiry into police corruption located one of the reasons for the dishonesty that had been uncovered in policing in Queensland to be a lack of appropriate education amongst rank and file officers (Fitzgerald, 1989, p.365).

The Commissioner, Tony Fitzgerald, sought to apply the findings of United States research that indicated that broader education outside of the academy generated a greater awareness of the social context of policing, contributed to improved management skills, and produced improvements in communication, negotiation and problem-solving abilities (Carter, Sapp & Stephens, 1989).

The growth of tertiary education for police has been mirrored to a considerable extent by the enormous growth in policing research conducted by university researchers and governmental research bodies (such as the former Australian Institute of Criminology and the NSW Bureau of Crime Statistics and Research). Moreover, in New South Wales and Western Australia, police academies have been integrated with universities, while in other states and territories there is considerable weight given to tertiary education in recruit selection and in framing promotion criteria (Prenzler, Martin, & Sarre, 2010). There is no going back to the days when all education was police academy-based (Trofymowych, 2007/8), although the way forward towards full degree qualifications across the country remains uncertain. Arguably, this is an area of policy development that deserves police commanders' highest priority if we are to continue to make advances in better policing training and practice.

CONCLUSION

These ten Big Bangs, all of which have appeared in the time-frame of less than two generations, have led to major developments in the way in which we do our policing. We should take encouragement from the extent to which police leaders in Australia have become cognisant of the vast and growing tomes of policing literature and have acted upon the findings contained therein. We should take heart from the amount of governmental policy-making that has emerged from the ripening field of police research. The emergent body of knowledge allows us to

be confident that the shifts in policing theory and practice we just discussed will continue to remain influential into the future. All the while, our evaluation methods will need to be sharpened continuously in order to keep abreast of further developments. To borrow a phrase from the current Prime Minister, there has never been a more exciting time to be involved with policing research, education and training in Australia.

NOTE

This is a revised and updated version of a paper that was presented at the National Policing Summit, Melbourne, on 5 August 2015 with the title of: “The Top Ten Innovations that have made a Difference to Policing in Australia.”

ABOUT THE AUTHOR

Dr Rick Sarre, LLB, MA, SJD, is Professor of Law and Criminal Justice and teaches criminology, criminal law, sports law and media law in the School of Law at the University of South Australia. He was educated in Adelaide, Iowa, Ontario, and Canberra, and in 2015 was awarded the Juris Doctor (Honoris Causa) from Umea University, Sweden, in recognition of his contributions to the law. He currently serves as the President of the Australian and New Zealand Society of Criminology. His current research is in the fields of bail reform, restorative justice, and surveillance science, law and practice.

REFERENCES

- Australian Bureau of Statistics (2015). *Corrective Services, Australia*, March Quarter Cat. No. 4512.0. ABS, Canberra.
- Barkworth, J. & Murphy, K. (2015). “Procedural Justice Policing and Citizen Compliance Behaviour: The Importance of Emotion.” *Psychology, Crime and Law*, 2(3), 254–273.
- Blagg, H. & Valuri, G. (2002). *Profiling Night Patrol Services in Australia*. Report of a Research Project for National Crime Prevention and ATSIC (Aboriginal and Torres Strait Islander Commission).
- Blandford, J. & Sarre, R. (2009). “Policing in South Australia’s remote and rural communities: preliminary observations from a novel police diversionary strategy for young Indigenous offenders.” *Police Practice and Research: An International Journal*, 10(3), 187–197.

- Carter, D.L., Sapp, A.D. & Stephens, D.W. (1989). *The State of Police Education: Policy Direction for the 21st Century*. Washington DC: Police Executive Research Forum.
- Chainey, S. & Ratcliffe, J. (2005). *GIS and Crime Mapping*. Hoboken, NJ: Wiley.
- Chan, J., Doran, S., Brereton, D., Legosz, M. (2001). *E-policing: The Impact of Information Technology on Police Practices*. Brisbane: Queensland Criminal Justice Commission.
- Cultural and Indigenous Research Centre Australia (2013). *Evaluation of Indigenous Justice Programs, Project A: Aboriginal and Torres Strait Islander Sentencing Courts and Conferences*. Final report, Canberra: Commonwealth Attorney-General's Department.
- Cunneen, C. (2001). *Conflict, Politics and Crime: Aboriginal Communities and the Police*, Crows Nest, NSW: Allen and Unwin.
- Cunneen, C. & White, R. (2002). *Juvenile Justice: Youth and Crime in Australia*. South Melbourne, Victoria: Oxford University Press.
- Daly, K. (2000). "Restorative Justice in Diverse and Unequal Societies." *Law in Context Special Issue*, 17(1), 167–190.
- Daly, K. & Proietti-Scifoni, G. (2011). "Reparation and restoration" in M. Tonry (ed), *Oxford Handbook of Crime and Criminal Justice*, Oxford University Press, New York, (pp 207–253.)
- Dixon, D. (2005). "Why Don't the Police Stop Crime?" *The Australian and New Zealand Journal of Criminology*, 8(1), 4–24.
- EO & HRC (2015). *Independent review into sex discrimination and sexual harassment, including predatory behaviour, in Victoria Police*, Victorian Equal Opportunity and Human Rights Commission.
- Fitzgerald, T. (1989). *Report of a Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct Pursuant to Orders in Council*. Brisbane: Queensland Government Printer.
- Fleming, S., Prenzler, T., & Ransley, J. (2013). "The Status of Indigenous women in policing: A Queensland case study." *Current Issues in Criminal Justice*, 24(3), 357–374.

- Goldsmith, A. (2014). "Disgracebook policing: social media and the rise of police indiscretion." *Policing and Society*, 25(3), 249–267.
- Hough, M., Jackson, J. and Bradford, B. (2013). "Legitimacy, Trust and Compliance: An Empirical Test of Procedural Justice Theory Using the European Social Survey." In J. Tankebe and A. Liebling (eds), *Legitimacy and Criminal Justice: An International Exploration*. Oxford, UK: Oxford University Press.
- Johnston E. (1991). *Report of the Royal Commission into Aboriginal Deaths in Custody*. Canberra: AGPS.
- Kamira, J. (2001). "Indigenous Participation in Policing." In M. Enders & B. Dupont (eds) *Policing The Lucky Country*, Sydney: Hawkins Press (pp.70–82).
- Kearon, T. (2013). "Surveillance technologies and the crises of confidence in regulatory agencies." *Criminology and Criminal Justice*, 13(4), 415–430.
- Klockars, C. (1980). "The Dirty Harry Problem." *The Annals of the American Academy of Political and Social Science*, November, 452, 33–47.
- Legrand, T. & Bronitt, S. (2012). "Policing to a different beat: measuring police performance." In T. Prenzler (ed), *Policing and Security in Practice: Challenges and Achievements*. Houndmills, Hampshire: Palgrave-Macmillan (pp.1–19).
- Luke, G. & Lind, B. (2002). "Reducing Juvenile Crime." *Crime and Justice Bulletin* 69, Sydney: BOCSAR.
- Mazerolle, L. & Ransley, J. (2006). *Third party policing*. Cambridge: Cambridge University Press.
- Mazerolle, L., Bates, L., Bennett, S., White, G., Ferris, J. & Antrobus, E. (2015). "Optimising the length of random breath tests: Results from the Queensland Community Engagement Trial." *Australian and New Zealand Journal of Criminology*, 48(2), 256–276.
- Mazerolle, L., Bennett, S., Antrobus, E., Eggins, E. & Martin, P. (2015). "Enhancing police legitimacy: Results from the Queensland Community Engagement Trial (QCET)," *AIPM Research Focus*, 3(4), 1–8.

- Moore, M.H. (1992). "Problem-solving and Community Policing." In M. Tony & N. Morris (eds), *Crime and Justice: A Review of Research*, 15, Chicago: University of Chicago Press, (pp.99–158).
- Murphy, K. & Barkworth, J. (2014). "Victim Willingness to Report Crime to Police: Does Procedural Justice or Outcome Matter Most?" *Victims & Offenders*, 9(2), 178–204.
- Pastor, J. (2003). *The Privatization of Police in America*. Jefferson, NC: McFarland & Company.
- Prenzler, T. (2000). "Civilian Oversight of Police: A Test of Capture Theory." *British Journal of Criminology*, 40(4), 659–674.
- Prenzler, T. (2015). *One hundred years of women police in Australia*. Brisbane: Australian Academic Press.
- Prenzler, T. & Sarre, R. (2006). "Australia." In T. Jones & T. Newburn (eds), *Plural Policing in Comparative Perspective*. London: Routledge.
- Prenzler, T. & Sarre, R. (2007). "Private Police: Partners or Rivals?" In M. Mitchell & J. Casey (eds), *Police Management and Leadership in Australia*. Sydney: Federation Press.
- Prenzler, T. & Sarre, R. (2008). "Protective Security in Australia: Scandal, media images and reform." *Journal of Policing, Intelligence and Counter Terrorism*, 3(2), 23–37.
- Prenzler, T. & Sarre, R. (2015). "The Police." In H. Hayes and T. Prenzler (eds), *An Introduction to Crime and Criminology*, 4th edition, Frenchs Forest, New South Wales: Pearson Prentice Hall, (pp.272–292).
- Prenzler, T. & Sinclair, G. (2013). "The Status of Women Police Officers: An International Review." *International Journal of Law, Crime and Justice*, 41(2), 115–131.
- Prenzler, T., Fleming, J. & King, A. (2010). "Gender Equity in Australian and New Zealand Policing: A Five Year Review." *International Journal of Police Science and Management*, 12, 584–95.
- Prenzler, T., Martin, K. & Sarre, R. (2010). "Tertiary Education in Security and Policing in Australia." *Asian Journal of Criminology*, 5(1), 1–10.

- Robinson, Susan (2015). "Rethinking Recruitment in Policing in Australia: Can the Continued Use of Masculinised Recruitment Tests and Pass Standards that Limit the Number of Women be Justified?" in *Salus Journal*, Issue 3, No. 2, pp. 34–56.
- Sarre, R. (1996). "The State of Community Based Policing in Australia: Some Emerging Themes." In D. Chappell & P. Wilson, P. (eds), *Australian Policing: Contemporary Issues*. 2nd edition, Sydney: Butterworths, (pp.26–41).
- Sarre, R. (2011). "We get the crime we deserve: Exploring the political disconnect in crime policy." *James Cook University Law Journal*, 18, 144–161.
- Sarre, R. (2014). "The use of surveillance technologies by law enforcement agencies: what are the trends, opportunities and threats?" In E. Pływaczewski (ed), *Current Problems of the Penal Law and Criminology*, Białystok, Poland: Temida Publishing House (pp.755–767).
- Sarre, R. (2015). "Metadata retention: A review of the policy implications for Australians," *Crime, Justice and Social Democracy: Proceedings of the 3rd International Conference*, QUT, 1, 9–17.
- Sarre, R. & Prenzler, T. (2000). "The Relationship Between Police and Private Security: Models and Future Directions." *International Journal of Comparative and Applied Criminal Justice*, 24(1), 91–113.
- Sarre, R. & Sparrow, S. (2002). "Race Relations." In T. Prenzler & J. Ransley (eds), *Police Reform: Building Integrity*. Sydney: Federation Press.
- Shearing, C. & Stenning, P. (1983). *Private Security and Private Justice: The Challenge of the 80s*. Montreal, Canada: Institute for Research on Public Policy.
- Sherman, L. & Strang, H. (2007). *Restorative Justice: The Evidence*, London: The Smith Institute.
- Sherman, L., Strang, H., Mayo-Wilson, E., Woods, D. & Ariel, B. (2015). "Are Restorative Justice Conferences Effective in Reducing Repeat Offending? Findings from a Campbell Systematic Review." *Journal of Quantitative Criminology*, 31(1), 1–24.

- Smith, N. & Weatherburn, D. (2012). "Youth justice conferences versus Children's Court: A comparison of re-offending." *Crime and Justice Bulletin. Contemporary Issues in Crime and Justice, No. 150*. Sydney: NSW Bureau of Crime Statistics and Research.
- Steering Committee (2014). *Police Services*. Canberra: Steering Committee for the Review of Government Service Provision (Productivity Commission).
- Sutton, A. & Wilson, D. (2003). "Open-street CCTV in Australia." *Trends & Issues in Crime and Criminal Justice, No. 271*, 1–6.
- Trofymowych, D. (2007/8). "Police education past and present: Perceptions of Australian police managers and academics." *Flinders Journal of Law Reform, 10*, 419–433.
- Tyler, T. (2003). "Procedural Justice, Legitimacy, and the Effective Rule of Law." *Crime and Justice, 30*, 283–357.
- Tyler, T. (2006). *Why People Obey the Law*. Princeton NJ: Princeton University Press.
- Tyler, T. & Fagan, J. (2008). "Legitimacy and Cooperation: Why do people help the police fight crime in their communities?" *Ohio State Journal of Criminal Law, 6*, 231–275.
- Tyler, T. & Lind, E. (1992). "A Relational Model of Authority in Groups." *Advances in Experimental Social Psychology, 25*, 115–191.
- Van Dijk, J. (2008). *The World of Crime*. Los Angeles, CA: Sage Publications.
- Weisburd, D. & McEwen, T. (eds) (1998). *Crime Mapping and Crime Prevention*. Monsey, NY: Criminal Justice Press.
- Weisburd, D., McElroy, J. and Hardyman, P. (1989). "Maintaining Control in Community Policing." In D. Kenney (ed), *Police and Policing: Contemporary Issues*. New York, NY: Praeger.

- o O o -

CYBERSECURITY RISKS: ARE THEY INFLATED?

Petr Chrapavy[†]

ABSTRACT

With various views being posed on cybersecurity, this paper examines the proposition that cybersecurity risks are inflated. Due to the complexity of the cybersecurity environment, the risks will be dichotomised into two distinct categories—those posed by cybercrime, and those classified as cyber-warfare. In relation to cyber-crime, the paper examines the rise of cyber-crime, its costs, and the views of these factors by “alarmists” and “sceptics.” In relation to cyber-war, the paper sets aside the emotive issue of the consequences and focuses on the likelihood of a catastrophic attack. The paper concludes that the risk of cyber-crime is real, but the sometimes mooted existential threat poses by cyber-war is inflated. The paper argues that it is important for cyber defences to improve in line with the risks, and to do this, researchers need to work across both categories of cybersecurity.

Keywords: cybersecurity, cyber risk, cyber defence, cyber-war, cyber-warfare, cyber-terrorism, hacking

INTRODUCTION

In her summary of the most notorious cyber-attacks in 2015, Zetter (2015) points out a worrying trend in the unrelenting rise of cybercrime: “every year hack attacks seem to get worse—whether in their sophistication, breadth, or sheer brazenness” (para. 1). She illustrates this by listing the most successful attacks against high-profile targets, which ranged from the Internet’s leading adultery website (Ashley Madison), defensive cybersecurity firm (Moscow-based Kaspersky Lab), offensive cybersecurity firm (Italy-based Hacking Team), to US Federal Office of Personal Management. These views are not isolated. But differing opinions are published regularly in the press and academic journals. Therefore, it is timely to review the positions taken by these authors to see if cybersecurity risks are inflated.

[†] Corresponding author: petr@riotsolutions.com.au

CYBERCRIME RISE

Of concern was the revelation that: “Juniper Networks discovered two unauthorised backdoors in its NetScreen firewalls, one of which would allow the unknown hackers to decrypt protected traffic passing through the firm’s VPN/firewall” (para. 1). These devices are used worldwide by both private organisations and government agencies; thus their compromise would have resulted in an unauthorised access to some extremely sensitive information. According to Zetter (2015), what is of particular concern is that the prevailing view in the security community is that a sophisticated adversary is behind at least one of the backdoors; potentially a nation-state (para. 27).

The evidence indicates that, in general, cybercrime has been steadily rising and—despite some notable local and global law enforcement successes, shows no sign of abating (ACSC, 2015). In their first unclassified report, the Australian Cyber Security Centre (ACSC, 2015) claims “the cyber threat to Australian organisations is undeniable, unrelenting and continues to grow” (p. 2). Furthermore, the report states: “if an organisation is connected to the Internet, it is vulnerable. The incidents in the public eye are just the tip of the iceberg” (p. 3). Its key predictions for 2015, the ACSC envisaged a continual increase in the sophistication of cyber-attacks and in the number of “state and cyber criminals with capability” (p. 24). Overall, while the report highlights the high levels of risks, it also includes a warning about possible bias in statistics compiled by the Australian Signals Directorate (ASD) and Computer Emergency Response Team (CERT) Australia. While the ACSC takes cyber-attacks very seriously and considers that “destructive cyber-attacks could be considered equivalent to an armed attack, and therefore, an act of war” (p. 9), it considers such a scenario “unlikely outside a period of significant heightened tension or escalation to conflict with another country” (p. 9).

Only three months after the ACSC report was published there was a cyber-attack on the Bureau of Meteorology (BOM), which can be taken as a confirmation of the ACSC’s prediction. The BOM systems might have to be entirely replaced (Uhlmann, 2015, para. 4), as their complexity, customisation and interconnectivity dependencies mean they cannot simply be shut-down in order to be cleaned. Therefore, the estimates of damage run into hundreds of millions of dollars, supporting the assertion that the risks of targeted cyber-attacks are not exaggerated.

In 2015, the European Cybercrime Centre (EC3) at Europol published *2014 Internet Organised Crime Threat Assessment* that stated: “In general, cybercrime is increasing in scale and impact ... trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage” (Europol, 2014, para. 6). The current report for 2015 shows further evidence that cybercrime is not only continuing to increase, but it is becoming more aggressive (Europol, 2015).

While attackers were previously content with stealth approaches, avoiding confrontation where possible, the analysis points to a growing trend for “direct, confrontational contact between the criminal and the victim, where the victim is put under considerable pressure to comply with the perpetrator’s demands” (Europol, 2015: 62). This suggests risks posed by cyber adversaries, especially organised crime, are not overstated. Moreover, due to the continuing commoditisation of cybercrime methods and techniques, specialised software products and services that are easily accessible to unskilled, entry-level cybercriminals, enable them to “launch attacks of a scale and scope disproportionate to their technical capability and asymmetric in terms of risks, costs and profits” (Europol, 2015: 7).

There is a mature, competitive market for crime-as-a-service products and services, and this creates a force multiplier for many forms of cybercrime (more so in the realm of cyber-dependent crimes than cyber-enabled crimes). Services such as the so-called bulletproof hosting, spam bots, and counter-antivirus, among others, are crucial to enablement of some cybercriminal offences, while not being a direct subject of criminal complaint (Europol, 2015: 63).

In 2015, there was also a marked increase in distributed denial of service (DDoS) attacks, as reported by Akamai Technologies (2015), one of the global content delivery network providers whose platform “regularly transmits between 15%–30% of all Internet traffic” (p. 60). These attacks were sometimes followed by extortion attempts, particularly when the financial and telecommunications industries were targeted (p. 24). The data for the third quarter of 2015 showed increases in attack trends for DDoS metrics when compared to the same quarter of 2014 (a 180% increase in total attacks). One type of DDoS attack particularly stood out: there had been a 462% increase in reflection attacks (p. 5). These utilise (abuse) computing resources of a potentially legitimate third party component to attack the intended victim, which allows the attackers to hide their real identity.

CYBERCRIME COSTS

Data from sources such as the European Union's law enforcement agency (Europol, 2015), Australian Cyber Security Centre (ACSC, 2015), and one of the first studies to estimate the extend of cybercrime revenue (Michigan State University, 2016) indicate that cybercriminals are certainly making vast profits. However, it needs to be noted that accurate estimates of the costs of cybercrime cannot be determined, mainly due to under-reporting and under-recording. Nonetheless, these data show that the economic damages can be substantial. This was also evident in the Ponemon Institute (2015) study of the costs incurred due to cybercrime. The report found that there were notable differences in the total costs of cybercrime among the 252 companies from seven countries that took part in the study. The report's summary stated that, "the US sample reports the highest total average cost at \$15 million and the Russian sample reports the lowest total average cost at \$2.4 million" (p. 2).

Even though the report was a sponsored investigation by Hewlett Packard Enterprise, and not a "independent" academic report, it nevertheless can be seen as a good indicator of the magnitude of the problem. Likewise, Australian data showed the cost of cybercrime was \$3.4 million, though this amount was calculated two months prior to the successful attack against the Bureau of Meteorology systems, which was estimated to have caused hundreds of millions of dollars in damages (Uhlmann, 2015).

Under-reporting and under-recording are allied to the issue of cybercriminal operations going undetected and continuing to operate for years. One example is that of the botnet dubbed *Ponmocup*, which was one of the largest. According to van Dantzig et al. (2015, p.2, para. 2) this botnet was active for "nine consecutive years, [and was] also one of the longest running. Ponmocup [was] rarely noticed though, as the operators take care to keep it operating under the radar." Van Dantzig et al, (2015) found that the botnet's operators used techniques specifically designed to avoid detection by anti-virus software, and both automatic and manual analysis. The report's authors found that "it has infected a cumulative total of more than 15 million unique victims since 2009. At its peak, in July 2011, the botnet consisted of 2.4 million infected systems" (p. 2). While the exact amount of money earned by the botnet operators is not yet known, the authors suggest it is a successful multi-million-dollar business.

ALARMISTS

While security vulnerabilities seem to manifest everywhere on the Internet, it is the most extreme scenarios that are often cited in the media. This is illustrated in the following example from an article by Iyer (2015, para. 1):

With the increase in hacking these days, right from infecting a computer to remotely hacking a car in motion, one may wonder what would happen if a hacker decides to compromise your bionic arm, your pacemaker, or maybe your brain implant. Thanks to some students at the University of South Alabama, we have an answer: You die!

The article refers to attempts by a group of students to exploit security vulnerabilities in a sophisticated what is termed a *wireless patient simulator* product called iStan. Many hospitals use this system “to show and explain medical school students how to carry out procedures without killing people” (Iyer, 2015: para. 4). Within just a few hours the students were able to gain access to most functions of the device and demonstrate that it was susceptible to various types of cybersecurity attacks. According to the director of the simulations program, Mike Jacobs, the students were able to speed-up and slow-down the simulator’s heart rate via its inbuilt pacemaker, and “if it had a defibrillator, which most do, we could have shocked it repeatedly. If it was the intent, we could definitely cause harm to the patient,” Jacobs said. “It’s not just a pacemaker, we could do it with an insulin pump, a number of things that would cause life-threatening injuries or death” (Iyer, 2015: para. 8).

Medical devices are just one type of a spectrum of devices that are being connected to the Internet and now known as the Internet of Things (IoT), or the Internet of Everything (IoE). McAfee Labs (2015) claimed that these sensors, wearables, and other devices exposed themselves, their users, and potentially the entire system they are part of, to new cybersecurity vulnerabilities. Additionally, the report warned “every new product that connects to the Internet faces the full force of today’s [risks], and we have a long way to go to keep up with the speed and complexity of attacks” (p. 21).

From a law enforcement point of view, while the IoT is seen as an emerging risk environment, Europol (2015) stated, “the rising number of smart ‘things,’ including smart homes, smart cars, smart medical devices and even smart weapons are a clear indication of its adoption” (p. 54). It follows that this situation will

extend to challenges for law enforcers because the IoT provides new opportunities for cybercrime (p. 8).

Technologies in the rapidly evolving Smart Home market get media attention, and in general, seem to be susceptible to cybersecurity vulnerabilities and/or exposing users to issues involving breach of privacy. The range of risks is also of concern, as Howard (2015) pointed out: “what if your home is hacked and no longer recognises you? What if a computer virus deactivates your home security system? What if a denial-of-service attack renders useless thousands of smart homes housing our aged?” (p. 13, para. 7). He also draws attention to less frequently mentioned risks of false positives that could be triggered by an attacker or by system malfunction.

Some wearable devices allow the elderly and disabled to push a button that summons medical help. But in the smart home these could be further enhanced so they can trigger other types of alarms for assistance when the sensor determines a need—potentially without the monitored person having to call for help. In case of a false alarm, when this occurs, the medical emergency responders may simply waste a bit of time. However, “when it happens at a societal level,” Howard points out that if “dozens, hundreds, or even thousands of these false alarms are being triggered—the systems in place for initial public safety and health responses may be overwhelmed” (para. 9) and will fail with consequential effects.

Coming back to examples of extreme scenarios in media headlines, Rozenfeld (2015) opens the online article with a somewhat alarmist statement that cybersecurity experts consider: “a widespread cyberattack is likely to occur in the next ten years, possibly causing the theft of tens of billions of dollars’ harm to a nation’s security and capacity to defend itself, or a significant loss of life” (para. 1). However, the article lacks depth of analysis as it only cites the Pew Research Center survey’s results that showed more than 60% of the 1,642 participating experts *thought* such attack was likely, and nearly 40% gave the chance of a major damage from a cyber-attack a low likelihood rating. This split does not indicate general consensus and lacks an evidence base for drawing such conclusions. Besides, there were those experts voicing their concern that the risks are being exaggerated to generate an atmosphere of fear, accordingly this would have the potential to generate profits for those enterprises selling cybersecurity protection services and software products.

SCEPTICS

When considering the likelihood of cybersecurity risks, one needs to be aware of potential bias in reports published by cybersecurity vendors. Yet, some vendors do critically evaluate data and avoid alarmist or sensational tones in their reports. For example, where McAfee (now a subsidiary of Intel Corporation) discuss threats to critical infrastructure, in their *2016 Threats Predictions* report (McAfee Labs, 2015, p. 37):

If we believe the press reports coming from some security vendors, our future has become considerably more uncertain—with targeted attacks aimed at our critical infrastructure. Many of those highly publicised reports came after the 2010 attack by Stuxnet, which caused significant physical damage. However, it took years before a second successful attack against critical infrastructure appeared in the news. With only two publicly recognised instances since 2009, our 2016 predictions about critical infrastructure attacks must acknowledge that they are low-incident, but high-impact events.

The risk of devastating attacks on national infrastructure is discussed by Leyden (2015). He argues cyber-attackers “have never been credited with taking down a power grid. States themselves, which have a lot more resources behind them, have only been credited with a handful of full-on, serious enterprise attacks” (para. 20). He adds that when it comes to the risk of cyber-terror attacks against national power grids, in reality, small animals are more of a danger. He states, “squirrels have more luck sabotaging electrical systems” (para. 22) when compared to hackers because they often chew through electrical cables. He refers to data on *CyberSquirrel1.com* “a site that logs these types of incidents, reckons the rodents have been responsible for 505 such operations. Birds have reached 141, and raccoons 31. Humanity has clocked up just one” (para. 23). Leyden uses this illustration as an overstatement of worst-case scenario risks in response to the UK government’s increased spending on prevention measures. In terms of attacks by rogue states and terror groups, Leyden (2015) argues “there’s no evidence they have the capability and even their motivation to attack systems online is at least open to question” (para. 24).

Even the 23 December 2015 attack that incapacitated parts of the Ukrainian electrical grid for several hours (Goodin, 2016), which was highly likely to have been caused by a malware infection (Lee, Assante & Conway, 2016: 8), should be considered a statistical outlier. According to the US Department of Homeland

Security, “The threat of a damaging or disruptive cyber-attack against the US energy sector is low.” DHS judged that “advanced persistent threat (APT) nation-state cyber actors are targeting US energy sector enterprise networks primarily to conduct cyber *espionage* [not sabotage]” (U.S. DHS, 2016: 2).

CYBERWAR

Discussions about cyber-attacks against national critical infrastructure and their associated activities are termed *cyberwar* (sometimes synonymously referred as *cyber-terrorism*). Schneier (2010) argues cybersecurity risks posed by a wide range of perpetrators had been mislabelled as cyberwar by the media, and that instead, those attacks were probably committed by citizen activists or organised crime. He stated that “we’re not fighting a cyberwar now, and the risks of a cyberwar are no greater than the risks of a ground invasion” (para. 16). Tucker’s (2015) take on the cyberwar rhetoric echoes Schneier’s concerns, opining a worst-case scenario attack against critical infrastructure is a “perennial bogeyman” (para. 11). He stated that many experts consider the likelihood of a surprise attack on civilian infrastructure, aimed to cause severe economic damage and loss of life, is very low. He pointed out the tendency of some parts of the US military to overstate the level of cyber risks. As a case in point, he referred to a testimony by a retired Cyber Command commander before the Senate Armed Services Committee, where the commander considered the danger of a potentially devastating attack as *imminent*. Yet, to date no such attack has occurred.

However, even within the US intelligence community there are some moderate voices not subscribing to some version of a cyber Armageddon, a digital Pearl Harbor, or a cyber 9/11; terms sometimes seen cited in the media. In his strategic assessment of worldwide risks related to cyber-attacks, James Clapper, Director of National Intelligence, reported that “cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact” (Clapper, 2015, p. 1). Nevertheless, despite this concerning trend, the risk of a catastrophic attack against the US, orchestrated by any particular actor, was deemed as unlikely. Instead, the assessment reported that the US intelligence community envisions “an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security” (p. 1).

Five years prior to Clapper’s strategic assessment, the likelihood of cyberwar was already being widely discussed. Stevens (2010) called it an

“increasingly hysterical US debate over cyberwar” (para. 1), claiming that cyberwar has been consistently portrayed to the public as an existential threat. He cited Howard Schmidt, appointed in 2009 to coordinate the development and delivery of national cybersecurity policy, as stating that “the US is not in the midst of a cyberwar” (para. 3), and then contrasts this statement with the claim made by Mike McConnell (at that time vice-president of Booz Allen Hamilton, a major defence contractor), that “the US is fighting a cyberwar today, one it is losing” (para. 4). According to Schmidt (cited in Stevens, 2010), this is inflammatory rhetoric that hides flawed reasoning. Nonetheless, Stevens (2010) added that Schmidt does not represent the view of the whole cybersecurity industry or the US security agencies that may consider “there are simply too many perceived security benefits to information technologies and billions in federal contracts to be made from them” (para. 7).

Not all cyber-attacks require the Internet as a vehicle for delivery of the “payload,” though most adversaries will take advantage of the vast, global connectivity that this network of networks provides. Notwithstanding, the key Internet infrastructure itself can be a potential target in an attack designed to bring the global network down. In an aptly titled section “Fear vs. Reality: Cyber Warfare in the Press and in Reality,” Shein (2013) argued that some worst-case scenarios are fallacies, including the “notion that attackers could take the entire Internet off-line” (para. 50). He concedes that, oddly enough, this scenario is actually conceivable, and cites at that time well-known hacker “Mudge” from the L0pht group, who, when testifying before the US Senate in 1999, stated that his group could shut down the Internet within thirty minutes.

His claim gained further credibility four years later, when researchers found vulnerabilities in one of the key Internet routing protocols. While arguing that it would be technically possible, Mudge posed the question as to why would anyone want to do so—in effect severing their own access to valuable information and resources that could be exploited. According to Shein, “for a cyber warrior to ‘take down’ the Internet makes little sense; it would be like an invading army blowing up a bridge that still lay before them” (para. 51). Similarly, for a nation-state, for example in case of a denial-of-service attack against the entire United States, the backscatter traffic resulting from such an attack would likely overwhelm the rest of the Internet. He cites the economic interdependence of nations as a strong disincentive for such a devastating cyber-attack, and adds that “above all else, the cyber warfare doctrines of all companies with sufficiently

advanced capabilities to perform such an attack would instead dictate that they exploit access to resources, rather than cut off the ability to continue to do so” (para. 52).

CONCLUSION

On balance, the arguments for-and-against the risks posed by *cyber-crime* appear not to be inflated. The general view appears to support that the scale, reach, and impact of crime associated cyber-attacks are genuine. In contrast, the case for *cyberwar* appears to be overstated. This is despite a few notable cases that have occurred, such as the cyber-attack on parts of the Ukrainian power grid. In the main, catastrophic scenarios are still considered as low in likelihood.

Notwithstanding whether the two cybersecurity manifestations discussed here are overstated or not, there is little doubt that the overall risks posed by cyber disruption are a hazard for individuals, organisations, government agencies, and the economies of nations. So, what implications does this have for cybersecurity practice? One thought is that it is important for cyber defences to improve in line with the risks, and to do this, researchers need to work across both categories of cybersecurity regardless of the likelihood of an attack. This is because cyber-related risks are associated with all Internet-based systems and devices. As the Director of National Intelligence advised: “cyber threat[s] cannot be eliminated; rather, cyber risk[s] must be managed” (Clapper, 2015, p. 5). Therefore, risk management is a sensible approach to what can sometimes be a divided discourse of opinion.

ABOUT THE AUTHOR

Petr Chrapavy, Graduate Certificate in Intelligence Analysis, is a member of the Australian Information Security Association (AISA), Institute of Electrical and Electronics Engineers (IEEE), Institute of Instrumentation, Control and Automation (IICA), and Cloud Security Alliance (Australia Chapter). He has over twenty years’ experience in the ICT industry, with the last eleven years spent in various roles dedicated to cybersecurity.

REFERENCES

Akamai Technologies. (December 8, 2015). Q3 2015 State of the Internet – Security Report. *State of the Internet*. Retrieved from <https://www.stateoftheinternet.com/resources-cloud-security-2015-q3-web-security-report.html>

- Australian Cyber Security Centre (ACSC). (2015). *The Australian Cyber Security Centre Threat Report 2015*. Retrieved from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf
- Clapper, J. R. (February 26, 2015). *Statement for the Record Worldwide Threat Assessment of the U.S. IC Before the Senate Armed Services Committee*. Office of the Director of National Intelligence (ODNI). Retrieved from http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf
- van Dantzig, M., Heppener, D., Ruiz, F., Klijnsma, Y., Zheng, Y., de Jong, E., ... Haagsma, L. (November 30, 2015). *Ponmocup. A giant hiding in the shadows*. Retrieved from https://foxitsecurity.files.wordpress.com/2015/12/foxit-whitepaper_ponmocup_1_1.pdf
- Europol. (2014). *The Internet Organised Crime Threat Assessment (IOCTA) 2014*. Retrieved <https://www.europol.europa.eu/iocta/2014/keyfindings.html>
- Europol. (September 30, 2015). *The Internet Organised Crime Threat Assessment (IOCTA) 2015*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf
- Goodin, R. (January 6, 2016). First known hacker-caused power outage signals troubling escalation. In *Ars Technica*. Retrieved from <http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/>
- Howard, E. M. (December 2015). Home, Smart Home. *The Institute*, 39(4). 13.
- Iyer, K. (September 8, 2015). Hackers Turn Off The Pacemaker Of A Simulated Human And Kill It. *TechWorm*. Retrieved from <http://www.techworm.net/2015/09/hackers-turn-off-the-pacemaker-of-a-simulated-human-and-kill-it.html>
- Lee, R. M., Assante, M. J., Conway, T. (March 18, 2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

- Leyden, J. R. (November 24, 2015). Cyber-terror: How real is the threat? Squirrels are more of a danger. *The Register*. Retrieved from http://www.theregister.co.uk/2015/11/24/cyber_terror/
- McAfee Labs. (November 9, 2015). *McAfee Labs 2016 Threats Predictions*. Retrieved from <http://www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf>
- Michigan State University. (February 16, 2016). *Cyber thieves making millions in profits*. Retrieved from <http://msutoday.msu.edu/news/2016/cyber-thieves-making-millions-in-profits/>
- Ponemon Institute. (October, 2015). 2015 Cost of Cyber Crime Study: Global. *Hewlett Packard Enterprise*. Retrieved from <https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf>
- Rozenfeld, M. (March 6, 2015). Should We Fear a Catastrophic Cyberattack? *The Institute*. Retrieved from <http://theinstitute.ieee.org/opinions/question/should-we-fear-a-catastrophic-cyberattack>
- Schmidt, M.N. (Ed). (2013). *Tallinn manual on the international law applicable to cyber warfare*. New York: Cambridge University Press. Retrieved from <https://archive.org/download/TallinnManual/TallinnManual.pdf>
- Schneier, B. (July 7, 2010). The Threat of Cyberwar Has Been Grossly Exaggerated. *Bruce Schneier* [Web log post]. Retrieved from https://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html
- Schneier, B. (March 4, 2015). Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle. *Bruce Schneier* [Web log post]. Retrieved from https://www.schneier.com/essays/archives/2015/03/hacker_or_spy_in_tod.html
- Shein, R. (2013). A Brief Summary of Cyber Warfare. In *Information Security Today*. Retrieved from <http://www.infosectoday.com/Articles/Cyber-Warfare.htm>
- Stevens, T. (March 10, 2010). The US is not at cyberwar. *The Guardian*. Retrieved from <http://www.theguardian.com/commentisfree/2010/mar/09/us-cyberwar-howard-schmidt>

- Tucker, P. (November 3, 2015). *US Still Doesn't Know Who's In Charge of What If Massive Cyber Attack Strikes Nation*. Retrieved from <http://www.defenseone.com/threats/2015/11/us-still-doesnt-know-whos-charge-if-massive-cyber-attack-strikes-nation/123377/>
- Uhlmann, C. (December 3, 2015). "Classified report on Bureau of Meteorology cyber-attack recommends computer system overhaul." *ABC News*. Retrieved from <http://www.abc.net.au/news/2015-12-03/report-on-bom-cyber-attack-recommends-it-overhaul/6997832>
- The U.S. Department of Homeland Security (DHS). (January 27, 2016). Intelligence Assessment: Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector. Retrieved from <https://info.publicintelligence.net/DHS-CyberAttacksEnergySector.pdf>
- Zetter, K. (December 18, 2015). Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors. Retrieved from <https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/>
- Zetter, K. (December 23, 2015). The Year's 11 Biggest Hacks, From Ashley Madison to OPM. In *Wired*. Retrieved from <http://www.wired.com/2015/12/the-years-11-biggest-hacks-from-ashley-madison-to-opm/>

- o O o -

CLOSING THE CYBERSECURITY SKILLS GAP

Rebecca Vogel[‡]

ABSTRACT

The current consensus is that there is a worldwide gap in skills needed for a competent cybersecurity workforce. This skills gap has implications for the national security sector, both public and private. Although the view is that this will take a concerted effort to rectify, it presents an opportunity for IT professionals, university students, and aspirants to take-up jobs in national security—national intelligence as well military and law enforcement intelligence. This paper examines context of the issue, the nature of the cybersecurity skills gap, and some key responses by governments to address the problem. The paper also examines the emerging employment trends, some of the employment challenges, and what these might mean for practice. The paper argues that the imperative is to close the cyber skills gap by taking advantage of the window of opportunity, allowing individuals interested in moving into the cybersecurity field to do so via education and training.

Keywords: cybersecurity skills gap, intelligence, cyber threat

INTRODUCTION

After the attacks of September 11, 2001, the focus on counterterrorism provided the within the national security and law enforcement communities with additional resources. Although the focus on counterterrorism remains, there are, however, other national security issues that have risen in importance, in particularly cybersecurity.

In December 2008, Australia's then-prime minister, Kevin Rudd, delivered Australia's first National Security Statement (NSS) to Parliament. The NSS articulated the security challenges facing Australia and the federal government's principles and priorities in relation to national security policy. Importantly, the 2008 NSS articulated an important move from a narrow national security approach to an all-hazards, whole-of-government approach. Strategically, this all-hazards approach signaled a shift in thinking about what constituted a national security issue. This change of focus away from counterterrorism, encompassed: organised

[‡] Corresponding author: rebecca.vogel@mq.edu.au

crime, transnational crime (including smuggling of people, drugs and arms), border security, regional stability, and cybercrime. Cybersecurity is an overarching concept for hacking, espionage, fraud, and attacks on critical infrastructure. As such, it is now listed as a key risk area for national security by all of the Five Eyes intelligence partners—Australia, Canada, New Zealand, United Kingdom, and the United States.

Traditional crime is increasingly being replicated online through the Internet of Things, therefore enabling criminals to conduct their operations in a covert manner. Organised crime groups, both domestically and internationally, are targeting Australians at an unprecedented rate, with the Australian Crime Commission (ACC) conservatively estimating that serious and organised crime costs Australia \$15 billion every year. Though the actual figure is likely to be much higher (Australian Crime Commission, 2015b).

Cybersecurity has also received higher prominence militarily. In 2010, US Deputy Defense Secretary William Lynn, during a ceremony to officially establish the US Cyber Command at Fort Meade, Maryland, declared that cyberspace was as important a military domain as was land, sea, air and space. In January 2012, the former Director of the FBI, Robert Mueller, testified in congress that he expected the cyber risks were likely to surpass the risk of terrorism to national security (Office of the Inspector General, 2015). James Clapper, the US Director of National Intelligence, testified in congress in February 2016 that as a strategic global threat, “The consequences of innovation and increased reliance on information technology in the next few years on both our society’s way of life in general and how we in the intelligence community specifically perform our mission will probably be far greater in scope and impact than ever” (ODNI, 2016).

The expansion of national security priorities to include a pronounced focus on cybersecurity has necessitated a change in practitioners’ skills (S. Morgan, 2016). The cyber skills that are needed globally include the ability to maintain computer information systems’ security, protect them from intrusions and attempts to steal intellectual property, neutralising hacking, malware, viruses, denial-of-service attacks, and phishing. Cybersecurity professionals often control who has access to information, so they need to be able to plan and administer information security programs and conduct computer forensics as well as penetration testing.

But globally, cybersecurity skills are in short supply (Evans & Reeder, 2010). This claim has implications for the intelligence community—including law

enforcement intelligence—to increase the skills of their practitioners in this area. This is because as national security issues—such as espionage, terrorism, financial crime, business insider threats, drugs and arms trafficking, and organised crime—become more complex with implementation of the Internet of Things (IoT), the intelligence community will need remain strategic in its approach to deal with these issues.

The present cybersecurity skills gap that has been identified in the subject literature (Francis & Ginsberg, 2016; (ISC)², 2015), has implications for security in both the security sector as well as the public sector (S. Morgan, 2016). It follows that this skills gap presents a unique opportunity for IT professionals, university students, and those aspiring to work in the national security industry to become proficient in cybersecurity.

The paper argues that the imperative is to close the cyber skills gap by taking advantage of the window of opportunity, allowing individuals interested in moving into the cybersecurity field to do so via education and training.

CYBERSECURITY SKILLS GAP

The 9/11 shift in national security priorities focused on counterterrorism, but today other national security threats have increased in priority. Examples relating to cybersecurity are plentiful—e.g. Office of Personnel Management, Anthem, IRS, VTech, Ashley Madison—all occurring in one year—2015. Examples where hackers accessed government and private computer systems, at times, exploiting the vulnerabilities in the security architecture provided by subcontractors working with large organisations. The FBI noted a proliferation in cyber economic espionage cases, including DuPont, Lockheed Martin and Valspar (Federal Bureau of Investigation, 2015).

The speed at which cybercrimes such as fraud, online child exploitation, and payment scams are committed requires a twenty-four-hour international response (Interpol, 2016). Confronting the increase in the assessed level of cyber threats, however, is a gaping hole in the cybersecurity workforce, leading to a global shortage of cybersecurity professionals. As far back as 2010, a report by the US Commission on cybersecurity for the Forty-Fourth President described a “human capital crisis in cybersecurity,” saying “there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the Federal government,” citing a need to expand cyber education and build a

certification system involving large private sector companies, universities with cyber programs and federal agencies (Evans & Reeder, 2010).

Further evidence of the talent shortage is the 2013 report from the US Government Accountability Office which showed a vacancy rate of 22% in jobs within the Department of Homeland Security's National Protection and Program Directorate's Office of Cybersecurity and Communications (U.S. Government Accountability Office, 2013). In 2014, a special Parliamentary Select Committee in the United Kingdom's House of Lords predicted a global shortage of "no less than two million cybersecurity professionals" by the year 2017 (Morgan, 2014).

In 2015, the Global Information Security Workforce Study, a global survey of 14,000 information security professionals by (ISC)², found that by 2020, the global shortage would still remain at about 1.5 million ((ISC)², 2015). This aligns with a view from Michael Brown, CEO of Symantec security software, who said demand was expected to rise to six million by 2019, with a projected global shortfall of 1.5 million (Morgan, 2016). Forbes also indicated in a January 2016 article that the cybersecurity market is expected to more than double in size, from \$75 billion in 2015 to \$170 billion by 2020 (Morgan, 2016).

A 2016 Raytheon survey showed the demand for cybersecurity professionals is growing 3.5 times faster than the overall IT job market, and 12 times faster than the total labour market. This imbalance exists while the global economy is ever more dependent on computer networks as the economic engine, and cybersecurity is becoming an increasing national security concern (Raytheon, 2016).

Numerous factors have combined to create a gap between the number of cybersecurity jobs available and the requisite skills to fill these positions (ISACA, 2015). Some of the factors that have contributed to this void include the increased focus on cybersecurity, a dynamic cyber operating context, and a rapidly evolving cyber risk landscape. In 2015, ISACA and RSA surveyed 649 international cybersecurity professionals as to the depth of this skills gap problem. The results showed that 35% of organisations surveyed were unable to fill security jobs despite the fact that 82% expected attacks. What could be considered more worrying was that 52% of these organisations said that less than a quarter of all applicants had the necessary skills for the position (ISACA, 2015). Lastly, a US Bureau of Labor Statistics report stated that in 2015, more than 209,000 US cybersecurity jobs went unfilled, and postings were up 74% over the previous five years (Morgan, 2016).

RESPONSE TO THE CYBERSECURITY SKILLS GAP

In examining the crisis in human capital for the cybersecurity workforce, Fourie et al. (2014) suggested a two pronged approach that encompasses both short-term and strategic solutions. In the short-term, short courses for individuals already in the IT profession, as well as certification for those seeking a credential. For instance, graduate certificate programs (usually completed after one year of study) and graduate diploma programs (two years of study) would allow candidates to gain the necessary skills and transition into cybersecurity roles from other careers. Long-term solutions consist of collaboration between industry, academia and government to run workforce planning exercises with follow-up collaboration to ensure implementation. Fourie et al. (2014) called on academia to collaborate with the private sector to ensure ongoing relevance in the skills being taught; i.e., who could have predicted a decade ago the enormous challenges posed by the “bring your own device” protocols of today.

The responses seen in the Five Eyes intelligence alliance countries indicate an acknowledgement of the critical nature of the need to narrow the cybersecurity skills gap, with policies and strategies aimed at improving cyber skills amongst the national security community. There is a strategic focus within the broader Five Eyes intelligence community on the need to promote computing degrees regarding educational partnerships and increased workforce capability.

Industry and Government Partnerships with Education/Training Providers

One of the first examples of these initiatives was the Cybersecurity Challenge UK; its goal was to increase the number of cybersecurity professionals in the UK. Since 2010, Cybersecurity Challenge UK (a not-for-profit British company) has been running IT security-related competitions, specifically aimed at increasing numbers of people skilled in cyber security, to proactively address the skills shortage in the UK. The Challenge includes national competitions and networking initiatives which help identify those with appropriate IT skills, make them aware of educational and training opportunities, and provide career opportunities in the cybersecurity arena (Raytheon, 2015).

The UK government is also working with academia in developing cybersecurity programs—for example, GCHQ—the UK equivalent to the Australian Signals Directorate (ASD) and the American National Security Agency (NSA)—in 2014 gave its stamp of approval to six specific universities in the UK to train cyber experts to combat rising levels of cybercrime and build resilience in

its digital environment (Perry, 2014). In New Zealand there was the Cybersecurity Strategy (2011) that proposed collaboration with academia to meet the demand for graduates in cybersecurity (Fourie et al., 2014).

In 2012, the National Security Agency launched a Cyber Operations Program at four select universities to augment the cybersecurity curriculum and provide technical training (Gupta, 2012). The program was set-up specifically to train students for intelligence, military, and law enforcement jobs that require skills to operate protective networks against a hostile attack. The program was then expanded in 2014 by the NSA in conjunction with the Department of Homeland Security (DHS) to include 44 institutions designated as National Centers of Academic Excellence in Information Assurance and Cyber Defense. The purpose of the expanded program was to promote higher education in these areas and prepare a growing number of Information Assurance and Cyber Defense professionals to meet the need to reduce vulnerabilities in US networks (National Security Agency/Central Security Service, 2014). In January 2015, President Barack Obama and UK Prime Minister David Cameron delivered a joint statement regarding strengthening cybersecurity cooperation efforts and training in the largest companies, citing the “urgent and growing danger of cyber threats” (The Office of the Press Secretary, 2015).

The approaching “fourth industrial revolution” was the theme for the 2016 World Economic Forum, and a global report entitled, *Amplifying Human Potential* was released at the Forum. The report discussed the digital technologies young workers will need to navigate and the skills they will need. The report reiterated the importance of education—that “through education, there is an unassailable opportunity to prepare everyone for such a change (Infosys, 2016).”

The education system, both at a secondary level and the tertiary level, needs to be directly involved in programs to enhance cybersecurity skills. While the tertiary level appears to be moving in the right direction, in 2014, 64% of high school students in America did not have access to computer science classes or other classes that would help prepare them for a career in cybersecurity (Raytheon, 2014). Industry experts consider that even if schools place a much stronger emphasis on cyber security, it may take up to twenty years for the skills gap to close (Morgan, 2014).

Increased Workforce Capability

In October 2012, the FBI launched its Next Generation Cyber Initiative, which was aimed at enhancing the Bureau's ability to deal with cybersecurity issues. To do this, the FBI sought to hire more computer scientists. While the FBI has made some progress toward this goal, recruitment and retention of qualified candidates is reported to remain a challenge; this is because there are higher salaries offered in private industry (Dunsmuir, 2015). Tellingly, a 2015 audit of the Next Generation Cyber Initiative showed the FBI was not able to hire 52 of the 134 computer scientists it was authorised to recruit, presumably because of the lower wages the Bureau offered (Office of the Inspector General, 2015).

In Australia, the 2013 *Australian National Plan to Combat Cybercrime* identified two key priorities that were intended to strengthen its response to the cybersecurity skills shortage:

- 1) Improving the capacity and capabilities of agencies to address cybercrime, and
- 2) Partnering with industry to tackle the shared problem of cybercrime.

The imperative for cyber capacity and capability was explained in the report, saying, "...law enforcement agencies need to keep pace with evolving technologies if police are to perform their duties in the digital environment (Commonwealth of Australia, 2013). Similarly, the Australian Crime Commission (ACC), Australia's national criminal intelligence agency, in its *National Organised Crime Response Plan 2015–18*, cited the need to:

- 1) progress the priorities set out in the 2013 *Australian National Plan to Combat Cybercrime*, specifically, ...improving the capacity and capability of government agencies, particularly law enforcement, to address cybercrime; and
- 2) develop a technical capability community of interest, comprising a national forum for relevant agencies and organisations to discover and understand the technical capability challenges facing law enforcement agencies nationally that impede investigations into cybercrime and technology-enabled crime, to identify mechanisms to mitigate or address these capability challenges. (Australian Crime Commission, 2015a).

In 2014, the Pentagon announced an initiative that it intended to create a 6,000 strong cyber workforce to defend against threats to American computer networks, citing a challenge to train a cyber workforce, which is expected to run through 2016 (Bottalico, 2014). The US Senate also passed the *Cybersecurity Skills Shortage Bill* in September 2014, granting authority to hire and retain qualified cybersecurity professionals in an expedited manner, pay recruits more competitive salaries, and provide more attractive benefits and incentives (Chabrow, 2014).

Later, in November, 2015, the UK government announced its *National Cybersecurity Plan* (previously known as the National Cybersecurity Programme) (NCSP) to bolster Britain's next generation of cyber security professionals. The plan involved an increase in spending on cybersecurity to £1.9 billion by 2020, and recruiting 1,900 new staff across the three intelligence agencies. The first National Cyber Centre will be established, which will house the UK's first dedicated cyber force. A £20 million competition will be run to open a new Institute of Coding to train cybersecurity students in high-level digital and computer science skills. In quite an innovative move, the plan targets the most talented 14 to 17 year olds, providing them with expert mentors, challenging projects, and summer school to identify and train potential future employees (UK Government, 2015).

EMERGING EMPLOYMENT TRENDS

The US Bureau of Labor Statistics releases a biennial report on the fastest-growing occupations. Its 2013 report indicated that the information-security profession, including cybersecurity professionals, is expected to grow 36.5% by 2022. This profession is one of only twenty occupations with the highest expected percentage change of employment between 2012 and 2020 (Bureau of Labor Statistics, 2014).

Results of research conducted by KPMG are also indicative of the trend toward “upskilling” within the private sector to protect itself against cyber breaches. In 2014, KPMG surveyed 300 senior IT and HR professionals in the UK within organisations of between 500–10,000 staff and found that companies are “increasingly desperate” to in their quest to hire the right cyber people, with 70% admitting their company lacks the ability to assess incoming threats (KPMG, 2014).

There are positive trends being seen in bridging the gap in cybersecurity skills and reasons for optimism. The 2015 ISACA report showed enterprises are beginning to look at cybersecurity as an issue for the business itself, and not just

for the security manager. Security Operations Centres (SOCs) are being implemented, budgets are increasing, and executive support for security programs is more apparent, helping to elevate cybersecurity programs (ISACA, 2015). Another emerging trend in employment practice is to use Cyber Challenge competitions as a means to vet the cybersecurity skills and know-how of prospective employees. The US Cyber Challenge, in partnership with private industry, is creating “mini-challenges” to be piloted in late-2016, which will allow job applicants to demonstrate their cybersecurity abilities and potential employers to evaluate their skills in real-time (Chabrow, 2016).

EMPLOYMENT CHALLENGES

There are challenges surrounding developing and maintaining a robust cybersecurity workforce within the national security community, encapsulated in a 2015 article from *The Times of London*:

Technological skills are at a premium, and the Confederation of British Industry calculates that in three years there will be 600,000 vacant slots for able technological graduates. People who work at GCHQ are on government pay; many could earn far more outside. ‘Cheltenham is not much like San Francisco. If you’re a techie, this might not be the first place you would want to come,’ the head of personnel says (MacIntyre, 2015).

Across the Atlantic, a US report (2016) reiterated similar challenges seen in the Federal Cybersecurity Workforce, namely: 1) demand outstripping supply for cybersecurity professionals, 2) skills gap in cybersecurity positions, and 3) agency strategic workforce plans that do not specifically address cybersecurity workforce needs (Francis & Ginsberg, 2016). Compounding the challenges faced by the cybersecurity skills shortage are those of enticing and retaining the information security experts needed within the National Security space and public sector space more broadly.

The 2014 KPMG survey mentioned earlier indicates a higher “churn” rate for cyber professionals than for IT professionals, and 52% of those IT and HR professionals surveyed agreed there is aggressive headhunting in this field (KPMG, 2014). This presents an obvious challenge to the public sector, as the public sector, with its historically lower salaries, will surely struggle to retain cyber-skilled individuals who can and will be easily headhunted by the private sector, with its much more robust capability to offer attractive pay packages. Private sector entities, including the large Professional Services, Technology and

Financial Services firms, will no doubt increase salaries and compensation packages offered to public sector cybersecurity specialists, effectively cherry picking many of the best potential employees.

A 2015 report by the US Department of Justice highlighted the struggle facing the FBI in attracting computer science recruits, mainly due to low pay (Dunsmuir, 2015). The FBI, responding to the report, said “the cyber workforce challenge runs through the federal government” and that it was necessary to develop “aggressive and innovative recruitment and retention strategies” (Dunsmuir, 2015). An encouraging move to address the pay gap issue was the introduction of US legislation (S.1,691—*Border Patrol Agent Pay Reform Act of 2014*), which incorporated the Department of Homeland Security’s Workforce Recruitment and Retention Act, aimed at mitigating the significant problems of successful retention and recruitment, which was passed in December 2014, enabling qualified recruits to be paid more competitive salaries, benefits and incentives.

IMPLICATIONS FOR PRACTICE

The global cybersecurity skills gap has important implications for the private and public sectors. There is a critical need to address the talent shortage by increasing the number of individuals who have cybersecurity skills. While problematic, this situation presents a unique window of opportunity for those individuals looking to work in the national security community. Current IT professionals, university students and others interested in the cyber domain have abundant opportunities to upskill in cybersecurity areas such as forensic computing, social media exploitation or threat intelligence reporting, and move into this dynamic, growing field.

Numerous government initiatives are in place to address the cyber skills shortage, as well as legislation which will provide the means for the public service to become more competitive in attracting and retaining the best and brightest individuals.

The public service, facing challenges of competition from the private sector in recruitment and personnel retention, will need to innovate and respond in a much more agile way to market forces in order to attract and keep the best cyber personnel. Given the challenges in competing on remuneration, organisations that offer additional benefits on the job, such as ongoing training and professional development, a clear career path within the cybersecurity field, ongoing

engagement with outside stakeholders, vendors and academia, to inform their employees' cybersecurity expertise, will likely have a stronger case for retaining their cybersecurity professionals. These aspects of a strategic workforce planning and retention program will ensure that the next generation of cybersecurity professionals remain engaged in the national security sector to combat the cyber threats of the future.

The implications of the ongoing and growing threat posed by criminal and foreign adversaries are clear for cybersecurity operations and intelligence practice. The gap between the need for individuals highly skilled in cyber and the numbers of cyber-trained intelligence analysts within the National Security and Law Enforcement communities provides a challenge, but also numerous opportunities. Reskilling and upskilling in cyber expertise within the national security community will be important in dealing with dynamic, technically savvy cyber opponents. Creating an agile, skilled cybersecurity workforce is the current challenge. The bottom line is that national security communities will need to invest in their workforce, to improve the cybersecurity capability and capacity of their people through further education and training.

ABOUT THE AUTHOR

Rebecca Vogel, BA, MPICT, Cert HE, is a lecturer in intelligence at the Department of Security Studies and Criminology at Macquarie University, Sydney. Prior to receiving her master's degree, she worked for Dun & Bradstreet as a senior business analyst and fraud investigator assessing high risk businesses. Ms Vogel was also a government licensed private investigator in the US state of Wisconsin. She is a member of the board of the Australian Institute of Professional Intelligence Officers, and the editor of the Institute's journal—the *Journal of the Australian Institute of Professional Intelligence Officers*.

REFERENCES

- (ISC)². (2015). *Global Information Security Workforce Study*. Retrieved from <https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-%28ISC%29%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf>
- Australian Crime Commission. (2015a). *National Organised Crime Response Plan 2015-18*. Retrieved from

- <http://www.ag.gov.au/CrimeAndCorruption/OrganisedCrime/Documents/NationalOrganisedCrimeResponsePlan2015-18.pdf>.
- Australian Crime Commission. (2015b). *Organised Crime in Australia 2015*. Retrieved from <https://www.crimecommission.gov.au/sites/default/files/FINAL-ACC-OCA2015-180515.pdf>.
- Bottalico, B. (2014). Pentagon creating 6,000-strong cyber force. *Maryland Gazette*. Retrieved from http://www.capitalgazette.com/maryland_gazette/news/ph-ac-gn-cyber1001-20141001-story.html
- Bureau of Labor Statistics. (2014). *Occupational Outlook Handbook*. Retrieved from <http://www.bls.gov/ooh/fastest-growing.htm>.
- Chabrow, E. (2014). Senate Passes Cybersecurity Skills Shortage Bill. Retrieved from <http://www.bankinfosecurity.com/senate-passes-cybersecurity-skills-shortage-bill-a-7340/op-1>
- Chabrow, E. (2016). Adapting Cybersecurity Contests as a Recruitment Tool. *Careers Info Security*. Retrieved from <http://www.careersinfosecurity.com/interviews/adapting-cybersecurity-contests-as-recruitment-tool-i-3092>
- Commonwealth of Australia. (2013). *National Plan to Combat Cybercrime*. Retrieved from <https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf>.
- Dunsmuir, L. (2015). The FBI can't hire enough cyber specialists because it doesn't pay enough. *Business Insider*. Retrieved from <http://www.businessinsider.com/r-fbi-understaffed-to-tackle-cyber-threats-says-watchdog-2015-7?IR=T>
- Evans, K., & Reeder, F. (2010). *A Human Capital Crisis in Cybersecurity*. Retrieved from http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf
- Federal Bureau of Investigation. (2015). *Economic Espionage - FBI Launches Nationwide Awareness Campaign*. Retrieved from

- <https://www.fbi.gov/news/stories/2015/july/economic-espionage/economic-espionage>.
- Fourie, L., Pang, S., Kingston, T., Hetteema, H., Watters, P., & Sarrafzadeh, H. (2014). *The global cyber security workforce : an ongoing human capital crisis*.
- Francis, K. A., & Ginsberg, W. (2016). *The Federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security*. Retrieved from <https://fas.org/>.
- Gupta, U. (2012). NSA Launches Cyber Operations Program. Retrieved from <http://www.careersinfosecurity.com/nsa-launches-cyber-operations-program-a-4860>
- Infosys. (2016). *Amplifying Human Potential - Education and Skills for the Fourth Industrial Revolution*. Retrieved from <http://www.experienceinfosys.com/humanpotential>
- Interpol. (2016). *Coordinating Efforts to Better Combat Cybercrime Focus of INTERPOL Working Group*. Retrieved from <http://www.interpol.int/News-and-media/News/2016/N2016-040>.
- ISACA. (2015). *State of Cybersecurity: Implications for 2015 - An ISACA and RSA Conference Survey*. Retrieved from http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf
- KPMG. (2014). 'Hire a hacker to solve a cyber skills crisis' say UK companies [Press release]. Retrieved from <http://www.kpmg.com/uk/en/issuesandinsights/articlespublications/newsreleases/pages/hire-a-hacker-to-solve-cyber-skills-crisis-say-uk-companies.aspx>
- MacIntyre, B. (2015,). GCHQ's secret weapons for tracking enemy terrorists and child abusers. *The Times*. Retrieved from <http://www.theaustralian.com.au/news/world/the-times/gchqs-secret-weapons-for-tracking-enemy-terrorists-and-child-abusers/news-story/a2381cfb3a695272734fcff7f66690a0>
- Morgan, L. (2014). Global Shortage of Two Million Cyber Security Professionals by 2017. *IT Governance*. Retrieved from

- <http://www.itgovernance.co.uk/blog/global-shortage-of-two-million-cyber-security-professionals-by-2017/>
- Morgan, S. (2016). One Million Cybersecurity Job Openings in 2016. *Forbes*. Retrieved from <http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#17a1fb107d27>
- National Security Agency/Central Security Service. (2014). National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD). Retrieved from https://www.nsa.gov/ia/academic_outreach/nat_cae/
- ODNI. (2016). *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee*. Retrieved from <http://www.dni.gov/index.php/newsroom/testimonies/217-congressional-testimonies-2016/1313-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-ic-before-the-senate-armed-services-committee-2016>.
- Office of the Inspector General. (2015). *Audit of the Federal Bureau of Investigation's Implementation of its Next Generation Cyber Initiative*. Retrieved from <https://oig.justice.gov/reports/2015/a1529.pdf>.
- Omand, D., Bartlett, J., & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, 27(6), 801-823. doi:10.1080/02684527.2012.716965
- Perry, K. (2014). GCHQ Endorses New Degrees for Tomorrow's Spooks. *Telegraph*. Retrieved from <http://www.telegraph.co.uk/education/educationnews/11007644/GCHQ-endorses-new-degrees-for-tomorrows-spooks.html>
- Pherson, R. H. (2016). Strategic Foresight - Nine Techniques for Business and Intelligence Analysis. Retrieved from http://www.globalytica.com/wp-content/uploads/2016/03/Strategic-Foresight_Nine-Techniques.pdf
- Raytheon. (2014). *Preparing Millennials to Lead in Cyberspace*. Retrieved from http://www.consumer-action.org/recommended/articles/preparing_millennials_to_lead_in_cyberspace
- Raytheon. (2015). Mission Possible: From Cyber Geeks to Superheroes. Retrieved from http://www.raytheon.co.uk/news/feature/cyber_geeks.html

Raytheon. (2016). Cyber Help Wanted. Retrieved from
<http://www.raytheoncyber.com/news/feature/blog-cyber60-helpwanted.html>

The Office of the Press Secretary, The White House. (2015). Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference [Press release]. Retrieved from
<https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint->

UK Government. (2015). Spending Review and Autumn Statement 2015. Retrieved from <https://www.gov.uk/government/news/chancellor-sets-out-vision-to-protect-britain-against-cyber-threat-in-gchq-speech>

- o O o -

“WE'RE THE ONES THAT STAND UP AND TELL YOU THE TRUTH”: NECESSITY OF ETHICAL INTELLIGENCE SERVICES

Nathan J. Phillips[§]

ABSTRACT

The concept of *ethical intelligence* is sometimes cited as an oxymoron. However, as the ultimate responsibility for intelligence agencies work lies with the government of the day, it is posited that intelligence-related decisions are ethically sound. This is because ethical standards provide the confidence that decisions can be judged fairly, giving governments legitimacy to carrying out what may otherwise be considered questionable activities.

Keywords: Ethical professional behaviour, code of conduct, public accountability, intelligence services, Australian intelligence community, national security

The concept of *ethical intelligence* has long been considered by many as an oxymoron (Bar-Joseph, 2010: 23). However, there exists a flaw in the logic behind such an assumption based on what the concept of what *ethics* means. When interviewed by America's CBS reporter Scott Pelley, former-Director of Central Intelligence, George Tenet stated:

We're the ones that stand up and tell you the truth about when we're wrong. It's a great thing about this government. The only people that ever stand up and tell the truth are who? Intelligence officers. Because our culture is, never break faith with the truth. We'll tell you, you don't have to drag it out of us... Truth matters to us. (Pelley, 2007).

His quote would indicate that ethical behaviour is inherent in intelligence, due to the focus on truth. Yet Goldman's statement that, “‘Truth’ is a goal, yet deception, secrecy and morally troubling compromises are often necessary” (Goldman, 2006:

[§] Corresponding author: nathanjphillips@hotmail.com

x) implies that ethical behaviour is incompatible with the secrecy and deception often associated with intelligence.

Nevertheless, without a working definition of *ethics*, either judgment is presumptuous at best. Furthermore, when intelligence is discussed as a function of a nation state (Herman, 2004: 343), it becomes representative of that government; holding the government accountable for the actions of the function. Therefore, without ethical legitimacy, a government is unlikely to be able to use intelligence agencies with the full support of the general public, risking the choice between public support and effective use of its intelligence services. By losing the capability in favour of public support, a government leaves itself open to concerning threats, both in peacetime and war, and in doing so disregards one of its responsibilities of as a nation—the protection of its citizens. Conversely, a government that is unable to present itself as ethical, risks losing power through public dissatisfaction.

Nonetheless, it is important to recognise that there are other dimensions to intelligence that do not involve national governments; that is, law enforcement intelligence, business intelligence, and private intelligence (e.g. intelligence units of NGOs) (Goldstone, 2008). This paper focuses on national security intelligence that are under the auspices of federal governments.

RATIONALE

A liberal democratic government is answerable to its citizens and as a representation of them, is not unreasonable for those citizens to expect their government to act ethically. It follows that as a function of government, intelligence services should be expected to act ethically. As a result, practices that risk being considered by the public as unethical, such as espionage or telephone/Internet tapping, also risk indicting the government that allowed them, reducing the support given by those they represent. This is made more problematic given that intelligence operations that are, by nature, secret.

This is not to say that intelligence agencies act unethically because they operate in secrecy, but they do act in ways that may be seen by some in the community as unethical because they are not privy to the inner workings of these agencies who are legitimately targeting threats to civil society.

It is posited that if the secret work of intelligence agencies were able to be gauged against a code of conduct in keeping with the public's expectations, yet

worded as aspirational in its crafting (rather than prescriptive), then it might be more difficult to accuse a government of acting inappropriately (and perhaps, illegally) regarding the use of its intelligence agencies.

STATEMENT OF PURPOSE

This paper argues that by carrying-out its work ethically, intelligence agencies are more likely to be seen as beneficial in standing-up for liberal democratic principles by increasing public support. While there are certainly intelligence operations that may seem questionable, having a set of ethical guidelines can be used to justify these actions, whether based on risk of conducting them, or by not conducting them.

To this end, there is support to posit that Australian, as well as the Five Eyes intelligence nation's it works in conjunction with, would benefit from a code of conduct to guide intelligence personnel. What this paper will not discuss is exactly how such a code would be constructed; that is outside the scope of the argument.

INTELLIGENCE AS A FUNCTION OF GOVERNMENT

Intelligence and ethical theory have been compared to Just War Theory in attempts to create a context by which intelligence operations can be held accountable (Prunckun, 2015: 353). While Just War Theory deals with attempts to explain the ethics of both going to war (*jus ad bellum*) and the ethics of actions during war (*jus in bello*) (Quinlan, 2007: 3), Charles Lathrop (2004: 205) argues that intelligence professionals are constantly at war, due to the adversarial nature of intelligence operations, which if accepted, means that *jus in bello* becomes the prominent component.

The use of Just War Theory to address intelligence operations can be problematic due to the lack of open conflict that Just War Theory is designed to address, however its broader purpose is to codify ethical behaviour for events normally considered to be unethical. It is in this sense that it can be used to support ethical intelligence; what is considered ethical in a peacetime environment does not always apply on the battlefield, and similarly, the relatively clear ethical guidelines of normal society are not necessarily appropriate for intelligence organisations. If it is then accepted that intelligence practitioners *are* constantly in a state of war (Gates cited in Lathrop, 2004: 205), then the Clausewitzian tenet that war is a “true political instrument” (Clausewitz, 1976: 87) can be applied, and

as such the way in which a government conducts intelligence operations is likewise an instrument, for which the wielder holds ultimate responsibility.

The concept of governmental responsibility has already featured in the history of the Australian intelligence community (Hope, 1974). Although Justice Hope's Royal Commission on Intelligence and Security (1974) was conducted over forty years ago (at this writing), his statement about Australia requiring high quality and timely intelligence, and acknowledgement that intelligence is still relevant (Hope, 1976: 4). Furthermore, the 1977 decision of then Prime Minister Malcolm Fraser to publically acknowledge the existence of the Australian Secret Intelligence Service (ASIS, 2014), and the 2001 establishment of the same service through legislative means through the *Intelligence Service Act, 2001*, as opposed to through executive order, demonstrate that at times when intelligence was considered most crucial, leaders have made them *more* transparent to the public, and provided *more* government oversight, allowing for *more* external critique.

By bringing the government's primary foreign intelligence service into public knowledge, then transferring the power from prime ministerial control to legislated processes, the government not only took responsibility for what could be argued as the most secretive component of the Australian intelligence community, but it also opened it up to public critique. By being ultimately responsible for the actions of the intelligence services, the government now ensured that there were ethical boundaries by which the intelligence community adhered.

BENEFIT TO GOVERNMENT

There is a tangible benefit to a government that engages in ethical intelligence operations. Although *jus ad bellum* has questionable relevance to intelligence work, *jus in bello* is closer related because it considers the constant (secret) adversarial nature of intelligence operations. Antonia Chayes (2013: 310–311) argues that not only does a government require an ethical declaration of war, but are required to be ethical in victory as well. She points out that the latter is not through any legal requirement, but because of the inherent benefits for being an ethical actor.

Such a stand can only be achieved by applying the principles of *jus in bello*, emphasising ethical conduct during conflict. As such, if it held true that *jus in bello* is relevant to intelligence personnel, then the conclusion that immediately

presents itself is that as a function of a nation state, intelligence operations are of more benefit to the government when they are conducted ethically.

COMPETING THEORIES

Before making a judgment on intelligence activities though, it is necessary to determine an appropriate ethical framework from which to work. Additionally, any professional code of conduct should work towards something; it cannot exist simply for the sake of existing. According to Andrew Abbott (1983: 856), professional codes of ethics exist as recognition of societal obligations. The Australian intelligence community's obligations are to the Commonwealth Government, and therefore any ethical code needs to enable it to meet such obligations. Rather than discuss all existing frameworks, this paper will focus on two in particular: 1) deontological ethics; and 2) utilitarian ethical theory. These are opposing theories, with the deontological approach focussing on justifying the means as a priority, while utilitarianism focussing on the result to determine righteousness.

Deontological Approach

The term *deontological* is derived from *deon*; the Greek for *duty*. In deontological ethics it is through a set of rules that duty is defined. Therefore, the focus for this approach to ethics is based rules rather than the outcome of the rules. As philosopher Immanuel Kant considered the moral code to be, obligatory and universal, disregarding the final outcome as a consideration (Elshtain, 1981: 210). Rather than determine the rules himself though, Kant considered these factors to be a test by which actions can be determined as *good* or *bad*.

If intelligence practitioners were to use a deontological system, it would require treating all information, activities and products by the same set of ethical guidelines, and adhering to them regardless of the outcome. The limitation with this approach was demonstrated when former-US President Bill Clinton decided not to order a strike on Osama bin Laden's location in 2000. President Clinton's decision was based on the possible number of civilian casualties; it could easily be argued that minimising collateral damage could be accepted as a universal rule, however the consequence of not ordering the strike meant that bin Laden was able to lead al-Qaeda in the 9/11 attacks that killed thousands of innocent people (Phythian, 2010: 6).

This theory only has its advantages if a practitioner is unsure of the morality of taken (or avoiding) a particular action, like President Clinton's where, presumably he did not have intelligence that advised him of the threat bin Laden posed alive. However, deontological theory has another weakness in that it requires universal application. So, applying this approach to the 2000 Clinton/bin Laden situation, the minimisation of civilian casualties would have been considered an obligatory rule regardless of the outcome, even if President Clinton had known of the yet to come attacks on the September 11, 2001. That is because deontological ethics would have prevented him from authorising the strike. Additionally, deontological theory's universalism does not allow for adjustment between different settings. Therefore, they are "...applied to all rational, moral members of the community rather than to just some." (Poon and Hoxley, 2010: 263)

The inappropriateness of this approach can be demonstrated by examining the 2013 case where the Australian government was alleged to have eavesdropped on the telephone calls of the Indonesian president's family. If honesty was expected of the Australian intelligence community under this doctrine, then an admission or denial would have been required (based on whichever was accurate). But Australian government policy is not to comment on intelligence operations because any comments could undermine agencies' ability to conduct effective operations. As such, this case is a simple demonstration where the universalism of the virtue of honesty is not appropriate. Therefore, a strict deontological code of ethics would prevent the Australian intelligence agencies to meet their obligations to keep Australians safe.

Utilitarian Approach

In contrast to a deontological approach is the theory of utilitarianism. This philosophy focuses on the outcome as a priority. Under a utilitarianism system, secrecy and deception would pose no barrier to action, provided that the desired outcome was successful. Some may argue that although this system is more applicable to intelligence operations, its application in practice could be used to justify torture, and assassination. It was argued by Stansfield Turner, former Director of the Central Intelligence, that "...the overall test of the ethics of ... intelligence activities ... is whether those approving them feel they could defend their actions before the public if the actions became public" (Turner, 1985: 48), and it is against this Turner Test that utilitarian intelligence operations fail.

By way of example, the inappropriateness of utilitarianism can be seen in this historical case of covert intelligence operations: mercenaries fighting against Italy during World War II fought according to a set of terms, one of which included a licence to rape Italian women (Walzer, 2006: 133–134). While there may have been a necessity to hire mercenaries in accordance with the Turner Test, it is inconceivable that there was a legitimate justification for awarding such a licence.

A more recent example was that of former-US Vice President Dick Cheney whose approach to national security issues post- the 9/11 attacks was the so-called “one percent doctrine”; that is, justifying pre-emptive strikes against any threat that presents a probability of even one percent (Suskind, 2006). Using utilitarian doctrine, the act of first strike could be justified because the intent was to prevent substantial damage to the US—potentially mass US casualties—but without evidence or intelligence to underscore the probability of a future attack, such a doctrine amounts to Orwellian “thought crimes” (Orwell, 1992).

Discussion

The adaptation of one or other of these philosophic approaches appears unworkable for intelligence operations. Even grappling with the thought of constructing a hybrid philosophy does not have instant appeal and so leads one to conclude that there may not be a universal system for intelligence ethics.

Supporters of such claims often focus on asserted universal concerns about mortality and vulnerabilities (Barry, 1998: 20–26), with Barry (1998: 8) stating that “...virtually *any* conception of the good life goes better in the absence of physical injury.” However, this outlook is not consistent with history events. If such a philosophical approach held true, then one could argue that suicide bombers would not exist.

The culture of extremism generally states that one will have had a good life if they die in service to their cause. However, in contrast to Barry’s assertion, this is a retrospective gain. Many cultures, including, but not limited to the Samurai, would prefer suicide over shame as well. Even in modern, Western cultures, the participation in sport and extreme activities, such as sky-diving, imply that people are more than happy to risk injury or death for the purposes of pleasure. Similarly, the idea that an action can be justified by the outcome begs the question *which outcome?* The US Senate Select Committee on Intelligence report on the use of torture by the CIA has been opposed by John Brennan as its Director, who claimed the methods were necessary to defeat the threats, and ultimately the enhanced

interrogation techniques saved lives (Brennan, 2014). However, the report stated in its first two findings that enhanced interrogation techniques were not effective in gaining either intelligence or detainee cooperation, and that the claimed success of such techniques were inaccurate, at times having no impact whatsoever (Senate Select Committee on Intelligence, 2012: 2).

Even giving the enhanced interrogation techniques program the benefit of the doubt, and accepting Brennan's claim, the unintended consequence of questionable practices has led to a lack of faith in the CIA by the US Senate, and arguably by the world public. With regard to long-term consequences, any short-term gains the CIA claimed have led to allegations of torture, and losing some of the CIA's integrity in the eyes of those who determine how much oversight, funding, and independence, the agency should be afforded. These consequences suggest that a utilitarian approach is ambiguous for application to intelligence operations.

Whether agencies look to a rules approach or a consequence-based mode of ethics, there are limitations. A fairly safe conclusion is that intelligence work does not allow for a universal moral compass. This does not mean that achieving an intelligence code of conduct is impossible. Because the Australian intelligence community exists as a function of the Commonwealth Government, it follows that it is the government that needs to establish the code. Logically, this would need constitutional compliance through bipartisan agreement. It is argued here that in order to achieve an intelligence community that is effective, yet ethical, the government needs to draft a code of conduct that has its base in the goals of these intelligence agencies.

INTELLIGENCE CODE OF ETHICS

Even though there is no specific code of ethics for intelligence agencies, there is a more general code of conduct that the Australian intelligence community adheres to—that of the Australian Public Service. At this stage, five of the six intelligence agencies use the Australian Public Service *Code of Conduct*, with the Australian Security Intelligence Organisation being the only agency with its own.¹ However, the ethical considerations of various professions are not identical. To quote Alexandra and Miller (2009: 99), "...the moral obligations of doctors are different to those of waiters." The implication for intelligence work is that the variety of roles within the Australian Public Service does not equate to the roles of intelligence personnel.

One example of this already being the case is with the medical profession. Despite being in the Australian Public Service, any medical practitioner, whether working for the Commonwealth Government or elsewhere, is required to be registered with one of the recognised boards of the Australian Health Practitioner Regulation Agency (AHPRA) (Australian Health Practitioner Regulation Agency, 2013). The AHPRA has a code of conduct that must be adhered to by practitioners, lest their certification be revoked. This is far from a directly transferable structure, but it provides a basic frame by which Australian intelligence agencies could form a professional set of ethics.

In the instance of intelligence operations, a similar code exists within the Australian Institute of Professional Intelligence Operators (AIPIO). Nevertheless, there is no requirement for intelligence personnel to join, negating the ability to ensure consequences for breaching the Code (AIPIO, 2012). Moreover, the Australian Public Service *Code of Conduct* is generic, tailored for no specific profession, so it is not entirely appropriate for intelligence personnel. While the *Code of Conduct* is likely to have been based on broad social norms and expectations, there are a recurring number of instances in intelligence work when these societal norms are out of step with an intelligence agency's mandate.

Another component of a professional code of conduct would be that it is effective. This might mean that it needs to be an aspirational code, rather than one that is prescriptive. If intelligence personnel are required to make judgments based on incomplete information, dubious sources and varying skillsets, then a prescriptive code, which cannot foresee all situations would not be realistic. It would likely restrict personnel in their options, and conceivably place them and their colleague's lives in danger (Gup, 2000). While complete freedom is not an option being advocated, prescriptive restrictions and permission are already in place in the form of the legislation, and ministerial and parliament oversight.

Rather than dictate further than what is required, an aspirational code could have the potential to complement existing legislation. Where a second layer of prescriptive doctrine may act only to add extra restrictions, having the potential to contradict if done poorly, an aspirational code could provide guiding principles that allow for judgment of personnel to be taken into account. An additional benefit to this approach would be to empower personnel. This becomes important when dealing with some of the morally grey areas in intelligence work.

One issue that presents itself is that of breaching human rights, specifically rights such as privacy, freedom of association, and freedom of beliefs (Gill, 2009). In a similar vein to intelligence legislation, the European Union Commission of Human Rights (EUHCR) provided a prescriptive statement that divides rights into three categories; 1) absolute; 2) limited; and 3) qualified. Of these, it specifies which rights fit into which categories, and when each category can be legitimately breached. In essence, it takes from the strength of both deontological and utilitarian ethics; it sets out universal rights that apply to all people, before stating under which conditions, based on consequence, these rights may be broken.

This approach by the EUHCR is helpful, but does not take into account the incomplete information some intelligence personnel may be working with (or, in some cases, outright deceptive information). Therefore, judgments as to when different rights can be breached would not be based solely on consequence, but also the risk of that consequence. Using a prescriptive code, it would be difficult to deal with a potential consequence that may or may not fit into a specific category.

Still, an aspirational code enables personnel to make judgments according to the information they have. For example, if a member of the public was known to be intending on engaging in an act of terrorism, the consequence of not conducting intelligence for the sake of maintaining rights to privacy would be disastrous, and there is a solid argument for breaching such rights. Yet, what of someone who is only suspected of planning such an act, with incomplete evidence to support it, and no history that would suggest such an act? In such a situation, trusting the intelligence operators dealing with the case according to the principles set out by the government, and based around their obligations to that government, would enable the operators to use their experience and skillsets to best effect. In this way, an aspirational code complements prescriptive legislation to create a situation that relies on the professional judgement of the operator, providing a tangible benefit to operations.

At the time of this writing, the Australian intelligence community was still (technically) bound by the Australian Public Service *Code of Conduct*, which contains adherence to the values of honesty, trustworthiness, and "...to uphold Australia's good reputation overseas" (Australian Government, n.d.). At times, this will not be possible for decision makers or intelligence personnel. These generic ethical guidelines are simply inappropriate for intelligence agencies to hold out to their personnel. Honesty, for instance, is a virtue for many professions,

but the use of false, misleading and deceptive information, common to counterintelligence operations, can also be a virtue. The misdirection of the enemy prior to the Allies D-Day invasion of Nazi-occupied Europe appropriately used misdirection (Prunckun, 2012: 50) despite the act's utter dishonesty. Take also the case where intelligence personnel collect data in relation to a foreign target, it is unlikely Australia's "good" reputation will be maintained, as demonstrated by the Indonesian telephone-tapping allegations of 2013. Finally, intelligence personnel may be required to hide their true names and occupation during a posting, or be required to keep information hidden in a manner that may be interpreted as dishonest. But to do otherwise would be contrary to the effective operating procedures and jeopardise their mission—and their lives.

In these situations, and many more intelligence related operations where context changes everything, and where the ethics put forward in the Australian Public Service *Code of Conduct* are glaringly inappropriate for intelligence operations. This does not make the intelligence work unethical, but rather due to their nature of the work, it makes adapting the Australian Public Service *Code of Conduct* inappropriate.

CONCLUSION

A code of conduct cannot simply be built around an agency's activities, as the resulting code would likely be more utilitarian-leaning and self-serving. Nonetheless, if intelligence work is to be considered as a profession, then a code of conduct needs to be established that specifically addresses the work intelligence personnel conduct for their agencies.

As intelligence operations are important to the function of liberal democratic governments, the decisions of intelligence agencies are reflective of the government's morality; and as such, should be ethical. The standard by which they are considered ethical is one that needs to be considered, empowering intelligence agencies rather than restricting them, while instilling confidence in the public that the government is acting ethically. In regard to the Australian intelligence community, this could be achieved by creating a professional code of conduct, perhaps overseen by an external professional body. This type of approach is consistent with the manner in which other licensed professions are overseen: doctors, lawyers, accountants, teachers, nurses, and so on.

Having such a professional body allows for the creation of a code of conduct specific to intelligence agency personnel, against which decisions can be tested

and ethical standards can be enforced. This provides legitimacy to the government should they be required to defend the intelligence community against unethical behaviour, without compromising or detailing specific decisions. Therefore, while not restricting the ability of the government to protect its citizens, it still allows for the concept of ethical intelligence to become less of an oxymoron through the advantages it gives to the nation state that employs them.

NOTE

1. The Defence Intelligence Organisation, Office National Assessment, Australian Signals Directorate, and Australian Geospatial Organisation belong to the Australian Public Service, while the Australian Secret Intelligence Service's claims to adhere to the APS *Code of Conduct* is stated on its website found at: <https://www.asis.gov.au/About-Us/Mission-and-Values.html>, which was access 10 February 2016. The Australian Security Intelligence Organisation stated it values through its website found at: <http://www.asio.gov.au/About-ASIO/Mission-and-Values.html> and accessed 10 February 2016.

DISCLAIMER

The views expressed in this paper are those of the author and are not intended to represent the views of the Commonwealth Government or any of its agencies.

ABOUT THE AUTHOR

Nathan J. Phillips hold the degrees of Bachelor of Arts (History), Graduate Certificate in International Relations, and Master of Policing, Intelligence and Counterterrorism. He is employed with an Australian defence organisation in Canberra. His areas of research include international maritime security and the practical application of intelligence methodologies.

REFERENCES

- Abbott, A. (1983). "Professional Ethics," in *American Journal of Sociology*, 88(5), 855-885
- Australian Institute of Professional Intelligence Officers. (2012, November 30). *The Constitution of the Australian Institute of Professional Intelligence Officers*. Retrieved from AIPIO: About Us: <http://www.aipio.asn.au/Index.asp?pagename=About+Us&site=1&siteid=7376>

- Alexandra, A., & Miller, S. (2009). Professional Role Morality. In A. Alexandra, & S. Miller, *Ethics in Practice: Moral Theory and the Professions* (pp.94-112). Sydney: University of NSW Press.
- Australian Government. (n.d.). *Code of Conduct*. Retrieved from Australian Public Service Commission: <http://www.apsc.gov.au/aps-employment-policy-and-advice/aps-values-and-code-of-conduct/code-of-conduct>
- Australian Health Practitioner Regulation Agency. (2013,). Retrieved from National Boards: <http://www.ahpra.gov.au/National-Boards.aspx>
- Australian Secret Intelligence Service. (2014). *About Us: History*. Retrieved from ASIS: Foreign Intelligence: <https://www.asis.gov.au/About-Us/History.html>
- Bar-Joseph, U. (2010). The Professional Ethics of Intelligence Analysts. *International Journal of Intelligence and Counterintelligence*, 23(1), 22-43.
- Barry, B. (1998). *Justice as Impartiality*. Oxford: Oxford University Press.
- Brennan, J. (2014, December 09). *CIA News and Information*. Retrieved from <https://www.cia.gov/news-information/press-releases-statements/2014-press-releases-statements/statement-from-director-brennan-on-ssci-study-on-detention-interrogation-program.html>
- Butler, J. (2004). *Precious Lives: The Powers of Mourning and Violence*. London: Verso.
- Chayes, A. (2013). Chapter VII 1/2: Is Jus Post Bellum Possible? *European Journal of International Law*, 24(1), 291-305.
- Clausewitz, C. v. (1976). *On War*. (M. Howard, P. Paret, Eds., M. Howard, & P. Paret, Trans.) Princeton, New Jersey: Princeton University Press.
- Elshtain, J. B. (1981). Kant, Politics, & Persons: The Implications of His Moral Philosophy. *Polity*, 14(2), 205-221.
- Gates, Robert, cited in Lathrop, Charles (2004). *The Literary Spy*. New Haven, CT: Yale University Press.
- Gill, P. (2009). Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'? *Intelligence and National Security*, 24(1), 78-102.
- Goldman, J. (2006). *The Ethics of Spying*. Lanham, MD: Scarecrow Press.

- Goldstone, Jack A. (2008). *Using Quantitative and Qualitative Models to Forecast Instability*. Washington, DC: US Institute for Peace.
- Gup, Ted (2000). *The Book of Honor: Covert Lives and Classified Deaths at the CIA*. New York: Doubleday.
- Herman, M. (2004). Ethics and Intelligence after September 2001. *Intelligence and National Security*, 19(2), 342-358.
- Hope, R. M. (1976). Royal Commission into Intelligence and Security. 3. Commonwealth of Australia.
- Lathrop, C. (2004). *The Literary Spy: The Ultimate Source for Quotations on Espionage and Intelligence*. New Haven, CT: Yale University Press.
- Orwell, George, pseud. Eric A. Blair, (1992). *Nineteen Eighty-Four*. New York: everyman's Library.
- Pelley, S. (2007, April 25). *George Tenet: At the Centre of the Storm*. Retrieved February 26, 2015, from CBS News: <http://www.cbsnews.com/news/george-tenet-at-the-center-of-the-storm/>
- Phythian, M. (2010). Ethics and Intelligence: The Implications of the Rise of the Armed Drone. *7th Gloabl Conference on War and Peace*. Prague.
- Poon, J & Hoxley, M. (2010). Use of moral theory to analyse the ethical codes of built environment professional organisations. *International Journal of Law in the Built Environment*, 2(3), 260-275. Retrieved September 03 from, <http://dx.doi.org/10.1108/17561451011087346>
- Prunckun, Hank (2012). *Counterintelligence Theory and Practice*. Lanham, Maryland: Rowman & Littlefield.
- Prunckun, Hank (2015). *Scientiffic Methods of Inquiry for Intelligence Analysis, Second Edition*. Lanham, Maryland: Rowman & Littlefield.
- Quinlan, M. (2007). Just Intelligence: Prolegomena to an ethical theory. *Intelligence and National Security*, 22(1), 1-13.
- Senate Select Comittee on Intelligence. (2012). *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*. Washington, DC: United States Senate.
- Suskind, R. (2006). *The One Percent Doctrine: Inside America's Pursuit of its Enemies since 9/11*. New York: Simon and Shuster.

Turner, S. (1985). *Secrecy and Democracy: The CIA in Transition*. Boston: Houghton Mifflin.

Walzer, M. (2006). *Just and Unjust Wars: A Moral Argument with Historical Illustrations*. New York: Basic Books.

- o O o -

THE PARADOX OF FICTION AND TERRORISM'S OVERSHADOWING OF ORGANISED CRIME AS A LAW ENFORCEMENT CONCERN

Henry Prunckun**

ABSTRACT

In light of criticism by political commentators and law enforcement experts about counterterrorism overshadowing the investigation of other forms of serious crime—in particular, organised crime—this study explored whether the use of intelligence-led policing would be better directed towards all serious crime, rather than prioritising terrorism. An expert jury comprising twelve subject/practitioner specialists were surveyed. The study used a purposive sampling technique to gauge the jury's views on the current policy priorities, with the options being counterterrorism to serious crime, and the value of intelligence in policing regarding these offences. The findings, though not conclusive, provide compelling support for the hypotheses. That is, the results of a decision-tree analysis showed that intelligence-led policing could provide approximately 2.1 times the utility over the current approach.

Keywords: Organised crime, counterterrorism, terrorism, paradox of fiction, corruption, intelligence-led policing, decision tree analysis, policy analysis

INTRODUCTION

If we were to use a nautical metaphor to represent where society is in relation to investigating and prosecuting serious crime, it might be stated something like this: “We are adrift in a sea of crime.” And, while wandering through these waters, it could be said that one crime in particular has drawn us close to some treacherous rocks—the crime of terrorism. The catalyst for the prioritisation of terrorism by law enforcement was the 9/11 attacks, and in Australia, this was accelerated by the attack on Australians in 2002 in Bali, Indonesia.

** Corresponding author: Australian Graduate School of Policing and Security, Charles Sturt University, P.O. Box 168, Manly, New South Wales, Australia, 1655

Like the mythical Greek Sirens, terrorism could be argued to have drawn society's attention to it. In doing so, it has been argued that counterterrorism has consumed a disproportionate amount of concern, energy, resources, and time (Colvin, 2005), metaphorically, placing society at peril of hitting these rocks. Continuing the metaphor, these rocks represent exposure to other forms of serious crime that, arguably, deserve more attention.

As far back as 2005, defence scholars questioned the resources being funneled into counterterrorism: "Aldo Borgu of the Australian Strategic Policy Institute and the Director of Terrorism Studies at the Australian National University, Clive Williams, want an audit of counter-terrorism spending in Australia since the September 11 attacks to find out whether taxpayers are getting their money's worth" (Colvin, 2005). Ten years later, these warnings are still being echoed by "...a number of defence scholars and former officials, caution[ing] against treating terrorism as a strategic force on a par with powerful nation states" (Australian Government, 2015: 20). But it seems the message is getting through to policy makers because during an address to the public in Washington DC in January 2016, Prime Minister Malcolm Turnbull stated, "[Islamic State of Iraq and Syria's] threat to sweep across continents like the armies of Mohammed, to stable their horses in the Vatican, are crazed delusions. We should not amplify them" (Turnbull, 2016: 8).

Until this point in time, anecdotal evidence ran contrary to this position. Take the case in Australia where the federal government allocated "...\$631.4 million in extra resources to track, disrupt and prosecute Australians involved in violent extremism, both at home and overseas" (Hockey and Cormann, 2014: 5). This expenditure was in addition to A\$306.4 million allocated for counterinsurgency operations Australia spent in Iraq. Yet, neither Australia nor any of the Five Eyes intelligence partner countries—comprising Australia, Canada, New Zealand, the United Kingdom and the United States—nor any country in Europe with an advanced economy was listed in the top fifteen countries that experienced either a terrorist attack or death, or had been involved in a kidnapping incident (NCTC, 2012: 9, 13).

In fact, only seventeen US private citizens were killed by terrorist attacks in 2011 and "these deaths occurred in Afghanistan (n=15), Jerusalem (n=1), and Iraq (n=1). Overall, US private citizen deaths constituted only 0.13 percent of the total number of deaths worldwide (N=12,533) caused by terrorism in 2011" (NCTC, 2012: 17). No Australian was killed.

As tragic as the events in Toronto, London, California, Sydney, Paris, and Brussels in 2015 and 2016 were, these events seem to have, again, justified the diversion of law enforcement resources towards counterterrorism. Nonetheless, organised crime's modus operandi involving money laundering, identity crime, trans-border travel, and arms trafficking were, arguably, the enablers for these terrorist events (William & Felbab-Brown, 2012). Therefore, it could be argued that political leaders, policy-makers, and law enforcement commanders have been, in general, lured from navigating a steady course through the waters of crime, and taking the ship of civil society dangerously close to a predominately single-issue focused enforcement strategy—that is, a focus subjugated by counterterrorism.

If this argument carries sway, then the question that presents itself is: Would it not be better to prosecute serious forms of crime using an all-crimes approach? Such an approach could be characterised by the now well-established strategy known as *intelligence-led policing*¹ (Ratcliffe, 2016).

CONTEXT

Policy development is rarely clear cut (Prunckun, 2015: 322). When formulating policy options, it often takes the form of a range of options, starting with the decision to do nothing² through to the “gold standard.” The span of options is designed to cater for what is available in terms of resources, fits with the political priority or economic imperative, the societal demand, available technology, as well as considerations. It is usually the case that finding an acceptable option is based on brokering a marriage between the desired level of outcome/output and the various inputs. In the case of terrorism during the early part of the 2000s, it appears that society needed a heavily weighted response, but now, some sixteen years later, this thinking is being questioned.

The risk of terrorist attacks on people or infrastructure in Australia [has been] mentioned repeatedly. Some, however, including a number of defence scholars and former [government] officials, cautioned against treating terrorism as a strategic force on a par with powerful states. (Australian Government, 2015: 20).

In fact, political observers are now questioning whether we are repeating our blindness to emerging threats by failing to recognise the consequences posed by organised crime. Take for instance Roach (2011: 448) who said that the complexities of 9/11 have raised “...questions of whether we have lost perspective and devoted too much of our limited resources to preventing terrorism when there

are many other threats to human security.” Observers are warning that organised crime is one threat that demands our attention (Dawson, 2015). According to the Australian Crime Commission—the Australia agency for criminal intelligence, organised crime has the capacity to:

...significantly affect the wellbeing of families and communities across Australia. Serious and organised crime diverts funds out of the legitimate economy and undermines the profitability of lawful business. It removes large amounts of money from the Australian economy that could be otherwise used to fund services, roads, hospitals and schools. This money is instead lining the pockets of criminals. (Dawson, 2015: 1)

For over a decade Australian law enforcers have acknowledged that organised crime activities are potential enablers for terrorists (Hesterman, 2013; Brown & Felbab-Brown, 2012). The link between serious organised crime and terrorism, though at times may be indirect or consequential, forms a persuasive argument for the use of intelligence-led policing in conjunction with the investigation of serious crime. Therefore, the findings of this exploratory study are likely to be of interest to decision-makers when considering the development of new policy approaches. The findings may also be of interest to intelligence agency chiefs and law enforcement commanders when it comes to prioritising the deployment of resources that are under their remit.

PARADOX OF FICTION

To deal with serious forms of crime, law enforcement agencies have employed different management strategies, borrowed mainly from the business sector, to allocate resources. But when it comes to the crime of terrorism, it appears that common-sense may have exited the equation. Why? Perhaps it is the nature of the crime itself. Citing an ancient Chinese stratagem, Prunckun wrote (2014), “the first pillar of terror” is to “kill one, frighten ten-thousand.” And, as he pointed out, with the electronic media, this message has the effect of reaching a larger audience than in decades, or centuries, past; and with the scale of killing possible (e.g. 9/11 attacks), it has the potential of frightening people everywhere on the globe. “The perpetrators of terrorism are ‘media hungry’ in their determination to shock the world. They are well aware that all of us spend a lot of time looking aghast at what has been called ‘terrorvision’ (Whittaker, 2002: 132).”

This strategy is borrowed from the literary theory known as the *paradox of fiction* (Radford, 1975: 67–80). Essentially, this theory states that in order for a

story (fiction) to achieve believability, it must convince the reader that it is real (Levinson, 1990: 79–80). Although the reader knows the story is fiction, the writer can, to a large degree, convince (i.e. deceive) the reader into believing the story through the use of various literary tropes, techniques and imagery. This is evident when a reader says, “the book was a page turner,” “I couldn’t put it down,” “the writing made my heart race,” and so on. It’s argued here that terrorists leverage the paradox of fiction in frightening the global population through, not writing, but a stage production (i.e. a form of theatrical fiction) when society intuitively knows the odds of harm coming to them or their societies are so slim, but nonetheless believe in the fiction being projected.

“The word ‘terror’ originated from the Latin verb *terrere* which means ‘to frighten’ (Sutalan, 2013: 70).” Zachara (2012: 283–284) points out that terrorism is simply theatre. It does not require any of the systems that the black market needs to flourish. Regardless of whichever definition one selects to describe terrorism, the common characteristic is that its end-state is political (and religion is just one manifestation of political positioning). Financing of an attack does feature in terrorism, but it is merely a means to achieve results. The chief characteristic of that result is the publicity of kidnappings, hijackings and indiscriminate killings through bomb, small arms and knife attacks; or by attacking critical infrastructure—thus drawing attention to the terrorist group’s political message by creating a fictional stage-show by killing one in order to frighten tens-of-thousands (Bhalla, 2010).

By way of example, a 2009 Australian National University study (McAllister, 2009) into the public’s fear of terrorism showed that 44 percent of people polled were either “somewhat concerned” or “very concerned” that they or a family member, could be the victim of terrorist attack (Australian Government, 2015: 132).³ From this study we can see that all it takes is a bit of “theatre” to spread “...significant and widespread concern about the threat of being the victim of a terrorist attack—however unlikely, statistically, that may be (McAllister, 2009: 9–10).”

The subject literature suggests there is nothing of substance beyond the terrorists’ fiction—their attacks are like the facade of a Hollywood movie set. Unlike failed states, such as Syria, in developed industrialised nations, there is no alternative “government” terrorists have ready to replace the existing systems of governance. They have no alternative political, social, or economic systems waiting in the wings. Although one might argue that ETA in the Basque region of

Spain and FARC in Colombia fit this description, the evidence to support these organisation's claims to *actually* be able to replace these governments may simply be hyperbole (William & Felbab-Brown, 2012: 7–8).

Yet, with organised crime, it is already a “shadow government.” Its shadow systems that are currently in place are under organised crime's firm control (Liddick, 2008: 1); take for example, some well-known regions in southern Italy (figure 1). Organised crime sits outside the control of civil society (Reid, 2014), and therefore, making these organisations low-profile targets for law enforcement. It is argued that organised crime is invisible; terrorism is highly visible.



Figure 1—Protesting organised crime in Naples, Italy (photograph by author)

Given the concerns generated by acts of terrorism, political leaders have responded in the strongest terms. On the face of this, this is not an unreasonable response. These are, after all, terrible crimes at the upper end of the scale of seriousness. But if one was to level-headedly consider the proportionality of the responses to date, perhaps a different set of actions should have been

recommended to these leaders. Especially in light of the paradox of fiction. If a risk-based approach were taken, would a different set of priorities emerge? Could organised crime emerge as the crime target society should focus its concerns? If so, could an intelligence-led methodology be more appropriate strategy for resource allocation across the spectrum of serious crimes?

INTELLIGENCE-LED POLICING

The term *intelligence-led policing* originated in England in the 1990s (Anderson, 1997: 5). The development of the scheme was the direct result of the Kent Constabulary having a finite amount of resources to control and investigate crime in its jurisdiction. The system was seen as a logical way to “...de-emphasized responses to service calls by prioritising calls and referring less serious calls for general non-police services to other agencies” (Peterson, 2005: 9).

Therefore, it is sometimes known as *intelligence-driven policing* (Ratcliffe, 2003: 1). The Kent Constabulary’s aim in the 1990s echoes the argument being made in this paper for allocating today’s equally limited law enforcement resources based on the same logic. Scholars such as Peterson (2005: 9) have endorsed this view calling for intelligence-led policing to be employed as the basis for investigating all forms of serious crime, citing “fusion centers” as a natural command structure for sharing intelligence. Currently, there is a growing number of law enforcement agencies that claim to be intelligence-led. This is evidenced by creation of fusion centres (sometimes termed, *joint/multi-agency taskforces*) in America, Canada, and Australia (Walsh, 2011).

Closely aligned to intelligence-led policing is the concept of *problem-oriented policing* (POP). Although similar, problem orientated policing varies in that it undertakes a study of the problems that give rise to crime and then crafts a tailored response for each issue. This model uses an approach comprising: 1) analyse; 2) study; and 3) evaluation (Goldstein, 2003: 14). Therefore, it is argued, that by using problem-orientated policing’s problem solving methodology with the approach used by intelligence-led policing, the latter’s effectiveness can be enhanced (Ratcliffe, 2016: 184–187). So, in the context of the proposition being put forward here, although the strategy is simply referred to as intelligence-led policing, it assumes the use of problem-oriented policing as its method.

METHODOLOGY

Statement of Guiding Purpose

Given the criticisms surrounding the current counterterrorism-centric approach to serious crime control, and the emerging concerns about the impact of organised crime, this exploratory study asked the question: Should decision-makers move to widen the use of an intelligence-led strategy? Such an approach would not only assess the risk of terrorism, but also the risk posed by other forms of serious crime in an objective framework. To facilitate an analysis of this problem, this investigative study used the following statement to guide its inquiry: Would prosecuting serious crime using an all-crimes approach using intelligence-led policing be a more desirable strategy?

Method

A hypothesis based on the statement of guiding purpose was tested using a survey of subject experts. The hypothesis was: adopting an all-crimes, intelligence-led policy is more desirable than maintaining the current counterterrorism focused policy. The null hypothesis was: Adopting an all-crimes, intelligence-led policy was *not* more desirable than maintaining the current terrorism focused policy.

Data Collection

The study empanelled a jury of twelve⁴ subject/practitioner experts using the principles of *purposive sampling* (Dane, 1990: 303; Vito et al., 2008: 126–127). Monette et al, (1990: 126) argue that this sampling method is suited to matters like the one under investigation because the study focuses on a cohort that is able to be defined in simple terms: that is, the participants were selected because they were authorities in the field of law enforcement (all held postgraduate degrees) with knowledge of serious crime investigation as well as criminal intelligence practice (all but one had been at some stage in their careers, been practitioners). In this regard, the group could be regarded as *opinion leaders* (Stringer, 2014: 79).

The purposive sample was drawn in near equal proportions from the Five Eyes intelligence countries. The country representation was as follows: Australia, n=3; Canada, n=2; New Zealand, n=2; United Kingdom, n=3; and the United States, n=2. The reason for selecting a heterogeneous selection of countries was to avoid the perception of bias that might occur if a single Five Eyes country was used (Richie et al., 2003: 79).

The task of this expert jury was to come to a view about the persuasiveness of the study's hypothesis. The twelve were asked to consider the hypothesis and based on their knowledge and experience, assign probability to the two policy options. That is, they were asked to allocate a percent to each policy that represented the likelihood each might have in achieving an outcome for investigating and prosecuting serious forms of crime.

Limits

As with all applied criminological research, there are limitations. In the main, the findings of this study cannot be used to generalise to any particular population outside the parameters of the group sampled. Nevertheless, although generalisation is an important goal of applied research, the desire in this case was to *control* for confounding variables that might be introduced by using a different sampling procedure (Monette, et al., 1990: 154).

In addition, the study did not allow for all possible permutations to be explored (for instance, the so-called *black swan*⁵ outcomes). But the study did not set-out to do this. The study simply sought to explore whether there was support, beyond mere postulation, by the sample cohort that the current thinking on the counterterrorism-centric approach to prosecuting serious crime would benefit by a substitution for one that uses intelligence-led policing.

Analysis

Using a decision-tree analysis (see figure 2), the jury was asked to rank five possible outcomes associated with these two policy choices. The ranking process ranged from the selecting the outcome with the most utility (5), to the lowest (1). The outcomes that the jury considered were:

- An intelligence-led policy might improve prosecution of more forms of serious crime;
- An intelligence-led policy might make no difference than to current terrorism-focused policy;
- An intelligence-led policy might result in an unpredicted negative impact in prosecution crime;
- The current terrorism-focused policy is likely to continue to yield no better—no worse results in terms of prosecution of serious crime; and

- Maintaining the current terrorism-focused policy could, in time, expose civil society to other forms of serious crime through its inability to target these crimes.

The resulting data were aggregated and the mean was calculated. The scores for the policy percentage split and the ranking of the policies outcomes were then used to compute the *expected utility* using decision-tree analysis. Expected utility is score assigned to one of a number of policy options. It is calculated by the sum of the utility for each possible outcome. The sum is derived by multiplying the probability of its likelihood by a utility factor. As such, if the null hypothesis is to be rejected, the results of the expert jury's decision would need to indicate a higher expected utility for the intelligence-led policy.

RESULTS

The verdict of the expert jury was conclusive regarding the desirability for an intelligence-led strategy. The percentage they assigned to this policy option ranged from 40% to 100%, with a mean of 66.7%. The standard deviation was $\sigma 18.5$. In comparison, the percentages assigned to the current counterterrorism policy ranged from 0% to 60%, with a mean of 33.3% ($\sigma 18.5$). These findings are shown in a scatter-plot in figure 2.

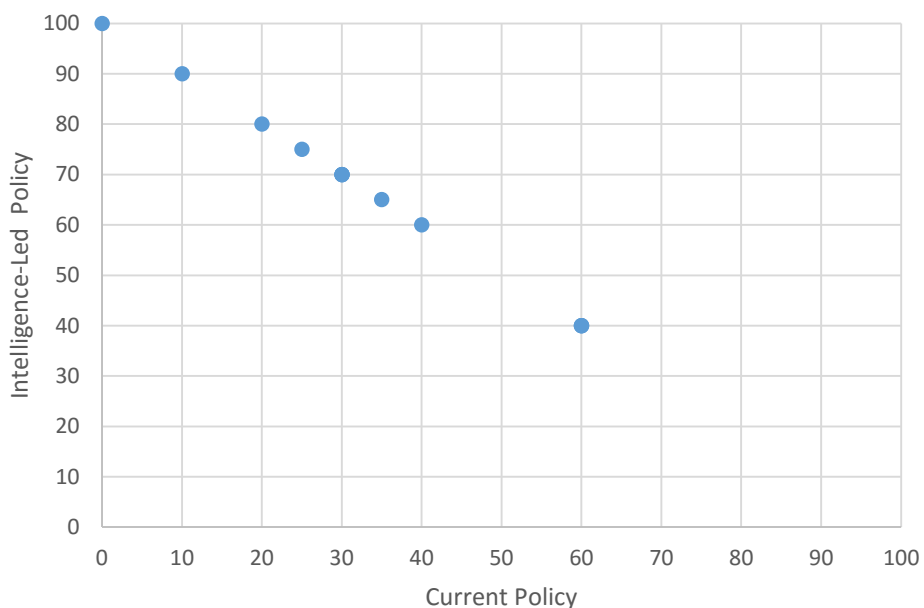


Figure 2—Percentages for the two policy options.

Note that there were four repeated values in the results, hence only eight data points are displayed. This suggests that “data saturation” was reached with a sample of twelve.⁴ The results show a clustering of data points in the upper half of the scatter-plot. This indicates a strong negative correlation regarding the current counterterrorist-centric policy, thus providing compelling support for the study’s hypothesis.

Table 1—Rankings for the five policy outcomes.

Potential Policy Outcomes	Average Likelihood Ranking from Highest to Lowest
An intelligence-led policy might improve prosecution of more forms of serious crime.	5.0
The current terrorism-focused policy is likely to continue to yield no better / no worse results in terms of prosecuting serious crime.	3.2
An intelligence-led policy might make no difference than the current terrorism-focused policy.	2.7
Maintaining the current terrorism-focused policy could, in time, expose civil society to other forms of serious crime through its inability to target these crimes.	2.7
An intelligence-led policy might result in unpredicted negative consequences in terms of being able to effectively prosecute serious crime.	-1.4

The Five Eyes experts’ deliberations regarding the ranking of the five possible outcomes of these two policy choices are shown in table 1. The rankings range from the most desirable (5) to the least desirable (1). The results show that an

intelligence-led policy was the most desired (i.e. 5). The jury's judgment in this regard also provides persuasive support for the study's hypothesis.

These two sets of data were then examined using decision tree analysis. The calculations and the results for the expected utility of each policy are displayed in figure 3. This figure shows the expected utility for staying with the current counterterrorism focused policy was 2.0 and the expected utility for the all-crimes, intelligence-led policy was 4.2. Another way to look at this result is to say that the expert jury considered, on average, that there would be 2.1 times the utility in implementing an intelligence-led approach. Like the previous result, this finding provides further support for the study's hypothesis.

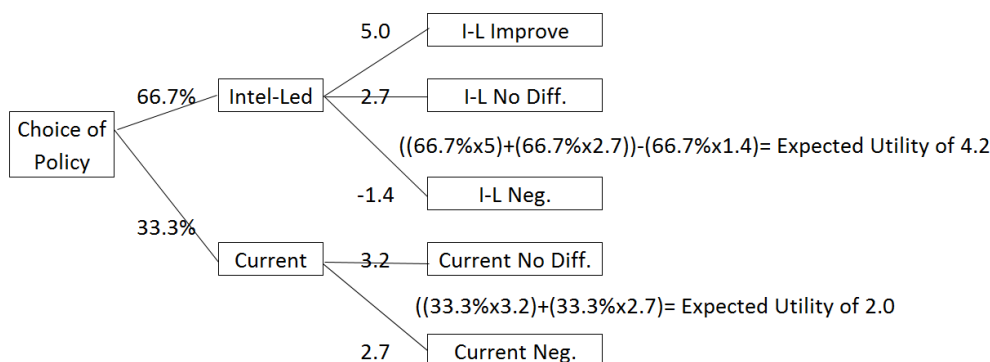


Figure 3—Decision-tree analysis for the expected utility of the two policy choices.

DISCUSSION AND CONCLUSION

The results of this study show that intelligence-led policy was the most desirable of the policies canvassed (i.e. 5 on a scale of 1 to 5). Although these results are exploratory, they are compelling indicators, suggesting that if an intelligence-led policy were adopted, it is likely to have approximately 2.1 times the utility than the current policy. This implies that if society is to be successful in its efforts to address the most pressing forms of crime, then law enforcement commanders need to intervene by adopting an intelligence-led approach to *all* serious crimes.

So, why has the concern for terrorism supplanted other forms of serious crime in society's collective conscious? The subject literature suggests a number of reasons, but the chief explanation is what has become known as *the first pillar of terror*; that is, kill one, frighten ten-thousand (Prunckun, 2014). This approach has its roots in the anarchist theory of *propaganda by deed* where "...acts of

violence are used more for visibility and drama than for military value” (Zachara, 2012: 283). “As a modern American analyst put it, terrorists want a lot of people watching rather than a lot of people dead (Pandey, 2006: 4).” And, history has shown that this theatrical tactic works. But as a Rand study has pointed out:

The nation’s zero tolerance for terrorism may soon come into direct conflict with the need to reduce budgets, including, perhaps for the first time, to consider real declines in counterterrorism funding. (Jenkins, et al., 2014: viii)

The Rand study (Jenkins, et al., 2014: viii) underscores the fact that nations with advanced economies have, and continue to, allocate disproportional amounts of resources to the investigation and prosecution of terrorism, rather than on what scholars are saying is a more serious form of crime—organised crime. This because the damage to civil society:

...is exacerbated by the fact that the most important criminals are typically political and societal elites: informal power brokers, powerful politicians, and businesspeople. The nexus between organised crime groups and state authorities is driven by the motives of profit and power and is exemplified by countless mutually beneficial exchange relationships. Acquiring access to state power allows crime groups to gain immunity for their illegal enterprises and exploit the social, economic, and political apparatus of the state, while for their part government officials pursue cooperative arrangements with organised criminals to fatten their wallets, secure votes, and control their political enemies. (Liddick, 2008: xiii–xiv)

Yet, some political leaders, across the political spectrum, still issue warnings that are out of step with those that acknowledge that there is no existential threat; that for instance the 2015 decree by the then-Australian Prime Minister: “Prime Minister Tony Abbott says the Islamic State group is ‘coming after us’ . . .” (APP, 2015). At the time of writing, US presidential candidate for the Republican nomination, Donald Trump, told a public gathering that, “torture works.” He stated, “We should go much stronger than water boarding ... They’re chopping off heads. Believe me, we should go much stronger because our country’s in trouble, we’re in danger” (*The Atlantic*, 2015).

Terrorist violence is aimed at generating fear and insecurity (i.e. a psychological impact) by suspending rational thought, thus prompting a violent response by authorities (and perhaps a legally draconian response through the law) (Wilkinson, 1977: 80–81). This is done so that terrorists can recruit people to its

cause (Lynn, 2012). Political comments, like those cited, as well as calls for stricter laws, only aid terrorists in reaching their objective (Lynn, 2012; Stohl, 2006). It is at the time of a terrorist attack that society needs to have a measured response; not a disproportional reaction (Stohl, 2006 :60).

Hitting at the mindset of the terrorist and discrediting the ideas that generate terrorism is the big prize. A law enforcement action that flows out of a "rule of law" paradigm, involving meticulous investigations and prosecution in courts, is likely to be far more damaging for the ideas that terrorists stand for (Abbas, 2013).

In this regard, intelligence-led policing presents itself as the foremost policy option. It takes an all-crimes and risk-based approach to responding. It offers political leaders sound evidence-based solutions to the range of criminal problems society faces—not emotionally charged description of problems that, on balance, are not as threatening as analysis would suggest. As Ratcliffe (2016: 185) argues, without a rationally-based approach, the current ways of thinking moves “...police away from being objective about crime threats to being driven by factors such as scaremongering. Instead of *intelligence-led policing*, we end up with *media-led policing*...”.

Terrorism is just one of the many forms of serious crime; but one that is unable to demonstrate that it poses an existential threat—this is a fiction: “[terrorists] do not threaten our national existence. That is the story ISIL wants to tell; that’s the kind of propaganda they use to recruit” (Obama, 2016). In this regard, it would pay dividends to recall the advice of then British Prime Minister, the late Baroness Thatcher who advised that all democracies “...must try to find ways to starve the terrorist and the hijacker of the oxygen of publicity on which they depend” (Thatcher, 1985).

Although, law enforcement agencies are using intelligence-led policing to address the issue of terrorism (Peterson, 2005), the results of this exploratory study suggest that political leaders would benefit from law enforcement commanders’ advice that we need to avoid a policy failure in addressing organised crime—we need a shift in our approach. We need a simple policy that states law enforcement agencies:

...will collect and analyse information on individuals and groups who are suspected of being involved in [*all forms of serious crimes*] and will provide this information to the chief executive officer for crime prevention and decision making purposes. (California Peace Officers’ Association. 1988: 8)

Moreover, society needs to acknowledge organised crime as a political problem, so that governments can respond. If organised crime is not acknowledged, then politicians are likely to deem that no problem exists and hence authorise no policy shift.

NOTES

- 1 Although originally termed *intelligence-led policing* (and abbreviated I-LP), the method is applicable to other agencies tasked with criminal investigations. So, although the term IL-P is used in this paper, it is implied that it could be substituted with the larger concept *intelligence-led law enforcement*.
- 2 Although it should be acknowledged that *doing nothing* could, in some situations, be deemed to be the best policy option (Prunckun, 2015: 322).
- 3 The survey conducted by the Social Research Centre of the Australian National University used a national random sample of the adult population aged over 18. The survey interviewed 1,200 people with a response rate of 32.5 percent. The results were then weighted to represent the national population, giving the survey's margin of error as ± 2.5 percent (McAllister, 2009: 18).
- 4 The subject literature on the topic of sample size for purposive sampling was silent as to the optimum number. So, following the time-honored legal method of having twelve jurors, this study employed an international jury of twelve subject/practitioner experts.
- 5 According to Nassim N. Taleb (2007) a black swan event, whether it is positive or negative, will have a massive consequence even though the likelihood of the event is improbable.

ACKNOWLEDGEMENTS

I would like to extend my thanks to several law enforcement practitioners who, during my research trips to Asia, were generous in providing background and contextual information on the operations of Asian organised crime groups: in Hong Kong—Superintendent Wui-nang Chan, Chief Inspector Ian Wilson, and Inspector Ping-Hung Wong (Hong Kong Police Force); and in Jakarta, Indonesia—Special Agent Ian Quirk (Australian Federal Police).

ABOUT THE AUTHOR

Dr Henry (Hank) Prunckun, BSc, MSocSc, PhD, is Associate Professor of Applied Research at the Australian Graduate School of Policing and Security, Charles Sturt University, Sydney. He is a research methodologist who 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. 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.

REFERENCES

- AAP (2015). “Tony Abbott says Daesh Death Cult is Coming After Us.” 27 June. Transcript at: <http://www.news.com.au/national/politics/tony-abbott-says-daesh-death-cult-is-coming-after-us/story-fns0jze1-1227417852623>. Accessed 20 October 2015.
- Abbas, Hassan (2013). “How Drones Create More Terrorist,” in *The Atlantic*. <http://www.theatlantic.com/international/archive/2013/08/how-drones-create-more-terrorists/278743/> (accessed 5 April 2016).
- Anderson, Richard (1997). “Intelligence-Led Policing: A British Perspective,” in *Intelligence-Led Policing: International Perspectives on Policing in the 21st Century*. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts.
- Atlantic, The (2015). “Donald Trump’s Specious Claims About Torture,” in *The Atlantic*. Washington, DC: Atlantic Media, 17 February. Transcript at: <http://www.theatlantic.com/politics/archive/2016/02/contra-donald-trump-torture-does-not-work/463293/>
- Australian Broadcasting Corporation (2015). “Half the Vanuatu Government Jailed for Corruption,” in *Law Report*. 27 October. Transcript at: <http://www.abc.net.au/radionational/programs/lawreport/half-the-vanuatu-government-jailed-for-corruption/6884278#transcript>

- Australian Government, Department of Defence (2015). *Guarding Against Uncertainty: Australian Attitudes to Defence*. Canberra: Commonwealth of Australia.
- Bhalla, Reva (2010). *Dispatch: Organized Crime vs Terrorism*. Stratfor Global Intelligence. 21 December. Transcript at: <https://www.stratfor.com/analysis/20101221-dispatch-organized-crime-vs-terrorism>. Accessed 22 October 2015.
- California Peace Officers' Association. 1988. *Criminal Intelligence Program for the Smaller Agency*. Sacramento, CA: California Peace Officers' Association.
- Colvin, Mark (2005). Experts Question Counter-Terrorism Spending" broadcast on "PM," *ABC Radio National*, 14 October 2005. Transcript at: <http://www.abc.net.au/pm/content/2005/s1482884.htm>. Accessed 20 January 2016.
- Dane, Francis C. (1990). *Research Methods*. Pacific Grove, CA: Brooks/Cole Publishing Company.
- Dawson, Chris (2015). *Organised Crime in Australia, 2015*. Canberra: Australian Crime Commission.
- Edwards, Michael (2015). "Calls for Reforms to Political Donations Laws After Mafia Links to Senior Politicians." *AM*. Canberra: Australian Broadcasting Corporation, 30 June. Transcript at: <http://www.abc.net.au/am/content/2015/s4264227.htm>. Accessed 20 October 2015.
- Goldstein, Herman. 2003. "On Further Developing Problem-Oriented Policing: The Most Critical Need, the Major Impediments, and a Proposal." *Crime Prevention Studies* 15: 13–57.
- Hesterman, Jennifer L. (2013). *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime and Terror Groups*. Boca Raton, FL: CRC Press.
- Hockey, Joseph and Cormann, Mathias (2014). *Mid-Year Economic and Fiscal Outlook 2014-15*. Canberra: Commonwealth of Australia.
- Hoffman, Jan (1995). "The Nation; Why a Jury Can Be 12, Even 6, but Not 5," in *New York Times*. 11 June 1995. Transcript at:

- <http://www.nytimes.com/1995/06/11/weekinreview/the-nation-why-a-jury-can-be-12-even-6-but-not-5.html> accessed 4 January 2016. Accessed 20 January 2016.
- Jenkins, Brian Michael; Liepman, Andrew; and Willis, Henry H. (2014). *Identifying Enemies Among Us: Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing*. Santa Monica, CA: Rand Corporation.
- Liddick, Don (2008a). "Organized Crime 2006: A Global Overview of Currents Events," in Frank G. Shanty (ed.), *Organized Crime: From Trafficking to Terrorism, Volume One*. Santa Barbara, ABC-Clio.
- Liddick, Don (2008b). "Organized Crime, Criminal Groups, and National and Regional Threats," in Frank G. Shanty (ed.), *Organized Crime: From Trafficking to Terrorism, Volume One*. Santa Barbara, ABC-Clio.
- Levinson, Jerrold (1990). "The Place of Real Emotion in Response to Fictions," in *The Journal of Aesthetics and Art Criticism*, Vol. 48, No. 1.
- Lynn, John A. (2012). "Fear and Outrage as Terrorists' Goals," in *Parameters: US Army War College*. Vol. 42, Issue 1, pp.51–62.
- McAllister, Ian (2009). *Public Opinion Towards Defence and Foreign Affairs*. Canberra: Australian National University.
- Monette, Duane R.; Sullivan, Thomas J.; and DeJong, Cornell R. (1990). *Applied Social Research*, Second Edition. Fort Worth, TX: Holt, Rinehart and Winston.
- National Counterterrorism Center, Office of the Director (2012). *Report on Terrorism, 2011*. Washington, DC: National Counterterrorism Center.
- Obama, Barack (2016). "Transcript of Obama's 2016 State of the Union Address," *The New York Times*, 12 January, transcript at: http://www.nytimes.com/2016/01/13/us/politics/obama-2016-sotu-transcript.html?_r=1
- Pandey, Satish Chandra (2006). *International Terrorism and the Contemporary World*. New Delhi: Sarup & Sons.
- Peterson, Merlyn (2005). *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, DC: US Department of Justice.

- Prunckun, Hank (2015). *Scientific Methods of Inquiry for Intelligence Analysis, Second Edition*. Lanham, MD: Rowman & Littlefield.
- Prunckun, Henry (2014). "The First Pillar of Terror—Kill One, Frighten Ten Thousand: A Critical Discussion of the Doctrinal Shift Associated with the 'New Terrorism'," in *Police Journal: Theory, Practice and Principles*. Vol. 87, No. 3, pp. 178–185.
- Radford, Colin (1975). "How Can We Be Moved by the Fate of Anna Karenina?" in *Proceedings of the Aristotelian Society*, Supplemental Vol. 49.
- Ratcliffe, Jerry H. (2003). "Intelligence-Led Policing," in *Trends and Issues*, No. 248. Canberra: Australian Institute of Criminology.
- Ratcliffe, Jerry H. (2016). *Intelligence-Led Policing*. New York: Routledge.
- Reid, Sue Titus (2014). *Crime and Criminology, Fourteenth Edition*. The Netherlands: Wolters Kluwer Law & Business.
- Richie, Jane; Lewis, Jane; and Elam, Gillian (2003). "Designing and Selecting Samples," in Richie, Jane, and Lewis, Jane (eds.), in *Qualitative Research Practice*. Thousand Oaks, CA: Sage.
- Roach, Kent (2011). *The 9/11 Effect: Comparative Counter-Terrorism*. Cambridge: Cambridge University Press.
- Schneider, Friedrich (2010). "Turnover of Organized Crime and Money Laundering: Some Preliminary Empirical Findings." *Public Choice*, September 2010, Volume 144, Issue 34, pp. 473–486.
- Stohl, Michael S. (2006). "Counterterrorism and Repression," in Richardson, Louise (ed.), *Roots of Terrorism*. New York: Routledge.
- Stringer, Ernest T. (2014). *Action Research, Fourth Edition*. Los Angeles: Sage.
- Sutalan, Zeynep (2013). "Terrorism, Media, and Public Information Management," in Gurbuz, Ugur (ed.), *Future Trends and New Approaches in Defeating the Terrorist Threat*. Amsterdam: IOS Press.
- Taleb, Nassim N. (2007). *The Black Swan: The Impact of the Highly Improbable*. New York: Random House.
- Thatcher, Margaret (1985). *Speech to the American Bar Association*. Albert Hall, South Kensington, London, 15 July.

- Turnull, Malcolm (2016) cited in Simon Benson, "Cheaper to Build at Home: Billions at Stake for Defence," in *Advertiser*, Adelaide, January 20.
- Vito, Gennaro F.; Kunselman, Julie; and Tewksbury, Richard (2008). *Introduction to Criminal Justice Research Methods*, Second Edition. Springfield, IL: Charles C. Thomas Publishers, Ltd.
- Walsh, Patrick F. (2011). *Intelligence and Intelligence Analysis*. Routledge: London.
- Whittaker, David J. (2002). *Terrorism: Understanding the Global Threat*. London: Longman.
- Wilkinson, Paul (1977). *Terrorism and the Liberal State*. London: Macmillan
- Williams, Phil, and Felbab-Brown, Vanda (2012). *Drug Trafficking, Violence and Instability*. Carlisle Barracks, PA: US Army War College.
- Zachara, Malgorzala (2012). "International Media: A Critical Tool in the Battle Against Terrorism," in Frank Shanty (ed.) *Counterterrorism: From Cold War to the War on Terror, Volume One*. Santa Barbara, CA: Praeger.

- o O o -

Branding Terror: The Logotypes and Iconography of Insurgent Groups and Terrorist Organizations

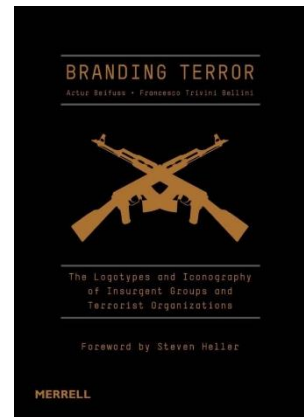
by Artur Beifuss and Francesco Trivini Bellini

Merrell Publishers, London

2013, 336 pages

ISBN-978-1858946016

Reviewed by Christian Luc Carnus



Visual branding as a means to improve the public image of terrorist organisations and insurgent groups is not a new concept. Nonetheless, relevant studies of terrorist iconography are under-represented in academic literature and the subject-matter is, arguably, poorly understood by intelligence practitioners. *Branding Terror*'s authors, former counterterrorism analyst Artur Beifuss, and graphic designer Francesco Trivini Bellini, systematically break down the images, colours and typographies represented in the logos and, when relevant, also the flags and other imagery, of sixty-five terrorist organisations. Their study suggests that terrorist groups perceive themselves as brands and that they use deliberate imagery to broadcast their aims.

The book itself is bound in leather and is aesthetically pleasing. Steven Heller, a former Art Director at the New York Times, sets the tone with an excellent foreword and his summation of the book's relevance to the contemporary international environment is one of the highlights.

Beifuss introduces the authors' aims early on; stating that in order to better understand the terrorist threat, they have analysed the "...visual language of terrorist organisations as conveyed through logos and other aspects of their visual communication." His writing is articulate and each group is portrayed in impartial and simple language. The book is well-researched and while it does not incorporate every known terrorist group, most of the major groups are included; as are all corners of the geographic, religious and political spectrums. These groups were selected from the official lists of designated foreign terrorist organisations of the United States, the European Union, Russia, India, and Australia.

Each organisation is given its own chapter; broken down into three sections. The first section provides an overview of the group and its capabilities are detailed; along with a timeline of its involvement in major terrorist attacks. The second section introduces the group's logo in black and white and specifies the logo's colour schemes and pantone coding. A full-colour version and an interpretation of its colours, imagery and slogans are presented in the final section.

While the details of each organisation are mainly descriptive, an overall analysis of the logos provides insight into their use of branding. For example, Beifuss notes the meaning of specific colours, such as green, blue and black—which represent Islam. Images are also analysed for their symbolism and it is apparent that specific objects are well-represented in the icons of certain ideologies, for example the map of Palestine, which often features within the logo of groups claiming to be dedicated to the liberation of Palestine. Certain animals are also regularly present in these logos, such as birds of prey which frequently appear in the logo of groups linked with violent struggle.

From a counterterrorism perspective, *Branding Terror* is highly relevant, particularly in this age of social media, which enables terrorist groups to effortlessly connect with potential recruits and sympathisers. These groups promote themselves as brands in the same sense that commercial advertisements market consumer products to strengthen their brand and global influence. Counterterrorism analysts can use the book's list of terrorist groups in order to identify which groups employ these branding mechanisms. Why is this important? Once a brand is identified, governments can work towards publicly undermining the group's particular narrative in order to discourage individuals from joining their cause or from lending financial and/or moral support.

The Islamic State of Iraq and al-Sham (ISIS) is an example of a successful and dynamically evolving terrorist brand. Its iconic black flag bearing the *Shahada* (the Muslim declaration of faith) in white, combined with their black uniforms and balaclavas and their theatrical use of the sword; a traditional symbol of Islam, has strengthened their visual brand as the legitimate emissaries of Islam and has made their iconography and members instantly recognisable to the general public.

While iconography is informative, it should be noted that the study of logos and icons alone is insufficient towards identifying a brand. Terrorist groups use other additional visual instruments, such as symbolic uniforms, to form their

trademarks. Clothing and action figures celebrating ISIS can even be purchased online. They also reinforce their brand through the use of dramatic and cinematic videos, military parades and religious rituals, such as beheadings. I would be interested in an updated edition of *Branding Terror*, which not only covers even more groups but also incorporates these types of additional branding devices.

The book provides an outstanding analysis of terrorist and insurgent iconography and is a superb introduction to terrorism. It is highly recommended to any intelligence practitioner. While the pantone coding and typography descriptions may not be greatly beneficial to an analyst, the study is also aimed at graphic designers. Being a counterterrorism analyst with the United Nations, I can attest that *Branding Terror* has been a valuable addition to my personal professional library.

ABOUT THE REVIEWER

Christian Luc Carnus, BA, MCrim, MA(Crim Intel), has been working as a Counterterrorism Analyst at the United Nations since 2009. Previously, he saw service in various operational and strategic law enforcement intelligence roles.

- o O o -

Call for Papers

Salus Journal is an international peer-reviewed open access journal for the publication of research papers on law enforcement, national security, and emergency management issues, as well as discussion papers and critical essays. *Salus Journal* seeks to contribute to practice by inspiring discussion through an interdisciplinary approach.

We invite international scholars to submit articles in the range of 3,000 to 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 use of exploratory approaches. The journal also accepts discussion papers and critical essays as long as a clear position is stated and the argument is grounded in sound practice, or the subject literature.

The Advisory Board advises that *Salus Journal* is an accredited Australian Research Council (ARC) *Excellence in Research for Australia* (ERA) journal. *Salus Journal* is indexed in EBSCOhost's research database, RMIT Publishing's *Informit* and the *Directory of Open Access Journals* (DOAJ).

- EBSCOhost is an online research database of academic libraries.
- RMIT Publishing is an aggregator of research information for students, lecturers, and researchers. Its *Informit* databases delivers content to scholars around the world through its online search facility.
- DOAJ is an online directory that indexes and provides international access to quality open access, peer-reviewed journals.
- The journal's ISSN is 2202-5677.

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: <http://www.salusjournal.com/submissions/>