Research Article

**END OF THE HONEYMOON:
WHY THE RELATIONSHIP BETWEEN MEDIA AND
COUNTERTERRORISM AGENCIES TURNED SOUR**

Kate O'Donnell[†] and Hamish McLean

This paper sets out our exploratory research based on an analysis of four decades of Australian national security and counterterrorism policy from the dual perspectives of information sharing with industry and information sharing with the media. We comb a rich seam of complex and interrelated policy and through a series of in-depth elite interviews, analyse how and why information sharing (the *need-to-know*) with these two stakeholder groups developed and evolved in the way it did in practice. We find that a time when national security and counterterrorism policy was beginning to emerge in the 1970s, in practice the media was considered an essential part of counterterrorism efforts while industry was peripheral. This stands in sharp juxtaposition to contemporary policy and practice where the media is largely frozen out and industry is central to national security and counterterrorism efforts. We identify the shifts in policy and practice are explained through a maturing of policy driven by international and domestic incidents, the shift in ownership of critical infrastructure from the state to the private sector over time and a schism between policymakers and the media that opened in the 1980s and has never recovered. For the media, the honeymoon is over.

Keywords: Counterterrorism policy, media, counterterrorism exercises, D-Notices, counterterrorism policy

INTRODUCTION

In contemporary national security and counterterrorism policy development in Australia, there has been a developing narrative on information sharing couched in terms of the *need-to-know* and the *need-to-share* (Prunckun, 2015, pp. 332–333). Through policy analysis and elite interviews, we chart the policy trajectory geared towards information sharing with industry and the media in practice since the development of Australia's first plan for counterterrorism in

---

[†] Corresponding author: k.odonnell@griffith.edu.au

1973. We first combed a rich security policy history and find it evolved from advice to individual businesses in limited circumstances through to the present day where information sharing with industry is at the core of contemporary policy (Commonwealth of Australia, 2010, 2013; TISN for Critical Infrastructure Resilience, 2013). In a stark juxtaposition, we find the policy focus in the 1970s on information sharing sought to embrace the media, but largely left industry out in the cold. In the period between 1970s and early 1990s the media was considered a valuable contributor to an overall effective response capability. However, relationships with policymakers and the media have been tense and problematic since at least the early 1980s (SAC-PAV Review Team, 1993, pp. 27-28).

Our research compares the differences in policy approach to engaging with industry and the media over the past 40 years to explore three key questions:

1. How and why did the contemporary policy focus on information sharing with industry develop in the way it did?

2. How and why did the budding relationship between counterterrorism agencies and the media fostered in the 1970s turn sour?

3. In contemporary policy considerations, what might unlock the counterterrorism door to the media that have been effectively frozen out since the 1990s?

Drawing on key policy documents and in-depth semi-structured interviews with current and former elite policy officials, police, industry representatives and with the media, we make a fresh contribution to the emerging literature focused on the historiography of Australia's security and counterterrorism policy. As Australian historian Mark Finnane (2013) notes, this has been narrowly interpreted.

BUILDING AUSTRALIA'S FEDERAL COUNTERTERRORISM POLICY

In 2013, the Australian Government released its latest policy on national security: *Strong and Secure—A Strategy for Australia's National Security* (Commonwealth of Australia, 2013). Curiously, and in an extraordinary example of terminological pedanticism, it identifies it as "Australia's first National Security Strategy" (Commonwealth of Australia, 2013, p. ii). This deftly swept aside a rich and complex national security policy history from

which the current strategy draws and within which, distinctly different policy objectives on information sharing, are evident.

Australia's national security policies and plans for countering terrorism developed over time, involve Federal, State and Territory governments and their agencies and are set out in a number of complex and interrelated documents. Wright-Neville (2006, p. 1) contends Australia's approach to countering terrorism "evolved in several waves, each following high-profile terrorist attacks overseas," identifying the attacks in the US on 9/11, the bombings in Bali in 2002 and 2005, the bombing of Madrid commuter trains in 2004, and the London underground bombings in 2005. While this is the case, what this overlooks is that Australia's approach to national security policy and countering terrorism is rooted in much earlier domestic and international terrorist events: domestic Croatian terrorism during the 1960s and 1970s; the Munich Olympics massacre in 1972; and the bombing outside the Hilton Hotel in Sydney in 1978 (Finnane, 2013, 2014; Hocking, 1993).

Australia's first national plan for countering terrorism, the *Plan for Anti-Terrorism Action*, was developed in late 1973. It was influenced by the change agenda being driven by the Whitlam Labor government that had come to power in December 1972. Mr John Lines, a member of the Counterterrorism Branch, in the Protective Security Coordination Centre (PSCC) between 1978 and 1992 recalls:

> After Munich … we realised we had to lift our game. While the events of Munich were one factor that drove the development of the plan, in my personal opinion, a more significant driver was the incoming ALP government. The incoming ALP government had a significant reform agenda and things moved quickly (personal communication, May 21, 2013).

The 1973 *Plan for Anti-Terrorism Action* incorporated specific "arrangements for the public handling of a terrorist incident by Government in liaison with the media" (Commonwealth of Australia, 1980, p. 3). While Australia's first specific counterterrorism plan was a product of the Whitlam government, it was the former coalition government that was "first prompted to act on terrorism" (Finnane, 2013, p. 162). In the more than four decades since, the security and counterterrorism policy focus has developed and broadened to embed a principle of information sharing within and across governments and their agencies, with governments and industry, within and across industry, and to embrace as a key policy principle, resilience in the face of all hazards (which includes but is not

limited to terrorism) (Commonwealth of Australia, 2010). In contempory policy, the focus is the 'need to share'.

INSIDE THE COUNTERTERRORISM TENT

It was not until the 1990s that a formal and distinct shift towards greater and routine information sharing between governments and industry occurred. Prior to the 1990s, both in policy and in practice, information sharing with industry was issue-driven and not considered essential. A now de-classified Australian Security Intelligence Organisation (ASIO) minute from 1974 reveals that special prior approval was needed to clear the way for both ASIO and the then Commonwealth Police to discuss with ESSO-BHP specific and credible terrorist threats made against their interests in Australia (Australian Security Intelligence Organisation, 1974).

Mr Mick Palmer, AO, APM, former Commissioner of the Northern Territory Police, former Commissioner of the Australian Federal Police, and former Inspector of Transport Security, observed that between the 1970s and 1990s there was no clear policy or strategy for information sharing with industry. He elaborates:

> When the question did arise, the conversations simply went nowhere. My recollection is that when the question arose, discussion was ambushed by focusing on why it was too difficult and shouldn't be pursued. The premise was to look for these roadblocks not look beyond them to the benefits. The roadblocks that were put forward included: that industry representatives would need to obtain and maintain top secret security clearances to be provided with information (even if relevant to their business); and that industry representatives should be constant. These were then, and remain nonsense (personal communication, January 11, 2013).

Mr Roger Holdich AM, who in 1985 and 1986 when Deputy Secretary of the Department of the Special Minister for State conducted a review of Australia's counterterrorism capabilities, agrees that routine information sharing with industry was not on the policy agenda. He recalls:

> It isn't that it was considered and discounted. In my experience it did not arise. Looking back, there was a missing link in information sharing, and that was with industry (personal communication, December 18, 2012).

The lack of a formal policy focus on routinely sharing information with industry endured well into the 1990s. The shift in policy was influenced by the US

moving toward greater protection of critical information infrastructure and the looming threat of the Y2K bug. Mr Peter Ford, former First Assistant Secretary, Information and Security Law Division, Attorney-General's Department observed that key agencies, such as the Australian Federal Police, the then Defence Signals Directorate and ASIO, supported the concept of regular meetings with industry focused on critical infrastructure. It was industry, however, that treated the government's shift towards routine and structured information sharing with caution. Ford elaborates:

> Looking back, there was some initial skepticism from industry. The old *I'm from government and I'm here to help you* comes to mind. However, there was interest from industry in hearing from government on security related matters. However, there were genuine concerns from industry about sharing information with government (personal communication, February 28, 2013).

Mr Mike Rothery, current First Assistant Secretary, National Security Resilience Policy Division, Attorney-General's Department agrees information sharing with industry was "sparse" prior to 9/11. He notes:

> While there was no concerted effort to brief industry as a whole on threats or response and recovery, there are notable instances of information sharing with industry before 9/11. These include:
>
> • specific counterterrorism exercises that focused around individual companies and their operations;
>
> • advice to individual companies if specific threats were identified;
>
> • planning for specific events that required engagement with specific companies and their operations; and
>
> • the aviation sector was provided with some information through the Department of Transport (personal communication, December 19, 2012)

As part of the Australian Government's response to 9/11, and in recognition that the majority of Australia's key civil infrastructures were by then, privately owned or operated on a commercial basis, counterterrorism efforts were immediately and actively focused towards greater information sharing with government and industry and within and across industry (Business Government Taskforce on Critical Infrastructure, 2002; Commonwealth of Australia, 2002; Protective Security Coordination Centre, 2002).

Following 9/11, the Australian government established the Business Government Taskforce on Critical Infrastructure. Its focus was to give business input into the design of current arrangements to protect key civil infrastructures. One of the recommendations of the Taskforce was that formal consultative structures be established to facilitate policy and operational information sharing between government and industry, and between industries. This approach was endorsed by Government. In the wake of 9/11, both government and industry recognised information sharing relevant to industry sectors (such as transport, banking and finance, health and energy) was a "key priority" (Rothery 2012, December 19, personal communication). In 2003, the Trusted Information Sharing Network (TISN) was formed to provide a formal and structural mechanism to facilitate information sharing with industry (TISN for Critical Infrastructure Resilience, 2013).

Since its inception, the TISN's remit has been geared towards structurally supporting the policy goal of information sharing with industry (TISN for Critical Infrastructure Resilience, 2013). The creation of the Business Liaison Unit (BLU) within ASIO in 2005 and the subsequent sharing of *intelligence* with industry, was a subtle extension in precisely what information was sanctioned by ASIO to be routinely shared with industry. An Australian industry executive explains this difference and its significance:

> The creation of the Business Liaison Unit in 2005 within ASIO represented a clear shift in formalising information sharing with industry. This was the first formal engagement with the intelligence community and industry. Prior to that, information sharing occurred through more informal networks. BLU became and remains the interface (personal communication, March 1, 2013).

Whereas the BLU is the continuing interface between industry and ASIO, Rothery (personal communication, December 19, 2012) makes the point that "...the TISN remains the key structural mechanism for information sharing with industry and government, and between industries, in the face of all hazards, including terrorism."

In 2013 the TISN marked its tenth anniversary (TISN for Critical Infrastructure Resilience, 2013). It is an enduring artefact of more than a decade of sustained policy focus on information sharing with industry on matters of security and counterterrorism. In recognising "things have changed enormously over the past decades," there is some concern expressed by industry that "we are

far from seamless in information sharing between government and industry and there is still room for significant further development" (Australian Industry Executive, personal communication, March 1, 2013). There is a simultaneous and genuine confidence, however, that "ASIO, the AFP or other relevant agencies would immediately make contact if there was a security concern" (Australian Industry Executive, personal communication, March 1, 2013).

Successive counterterrorism plans have continued to reinforce the policy goals of cooperation within and between governments and with industry (Commonwealth of Australia, 2003, 2005, 2012b). These policy goals have been further reinforced by the policy objectives of the *Critical Infrastructure Resilience Strategy* (Commonwealth of Australia, 2010). At an individual and sector level, industry is firmly within the security and counterterrorism tent.

OUTSIDE THE COUNTERTERRORISM TENT

In contrast to information sharing with industry that developed and strengthened over time, this paper now turns to information sharing with the media. We identify how and why the media slipped from its honeymoon era of direct involvement in national counterterrorism exercises in the 1970s to being left out in the cold since the 1990s. The crucial role of the media in any counterterrorism activity—preparation, response and recovery—was recognised early in the development of Australia's counterterrorism capacity. After the PSCC was formed in July 1976, its reach and influence expanded quickly beyond its initial focus on dignitary protection to include a pivotal role in security and counterterrorism (Commonwealth of Australia, 1979; SAC-PAV Review Team, 1993). It is in its expanding remit that the PSCC recognised the need for interaction with the media. Lines (personal communication, May 21, 2013) recalls:

> The PSCC recognised very early on that the media would be a key figure in any counterterrorism response. Don Lawler, a respected journalist, was employed by the PSCC from its very early days. We all did media training courses and we all understood the importance of the media in any real event.

Engaging the media should be viewed in the broader context of the D-Notice system and what the Australian Government was specifically seeking to achieve through the PSCC's engagement with the media. The policy objective of the now defunct D-Notice system established in Australia in 1952, controversial since the 1970s and moribund by the mid-1990s, was restrained and responsible

reporting (Commission of Inquiry into the Australian Secret Intelligence Service, 1995). Australia's D-Notice system operated as a request to editors not to publish specific "sensitive defence, security and intelligence information" (Commission of Inquiry into the Australian Secret Intelligence Service, 1995, p. 113). Reinforcing how information had been shared with the media, the D-Notices themselves (reduced from seven to four in 1974) were developed with media input (Commission of Inquiry into the Australian Secret Intelligence Service, 1995).

In this broader policy context, distinctly different policy objectives of the PSCC are readily discernable. The first was ensuring the media liaison arrangements in any counterterrorism plan could be effectively implemented in the event of a terrorist incident. The second and more revealing in terms of how the role of the media was perceived, was to encourage and achieve "restrained and responsible reporting in counterterrorism" (Commonwealth of Australia, 1980, p. 7). The involvement of the media in real-time national security exercises represented the high point of the government's approach to engaging with the media in matters of security and counterterrorism. Somewhat paradoxically, in practice the media's failure to effectively engage in the exercise role-playing also represented a low point from which the relationship has never recovered. This occurred contemporaneously with the decline of the D-Notice system with its inherent involvement of the media.

Lines, reflecting on the vexed relationship government shared with the media, observes that during the 1970s departmental media officers were increasingly on the ascendency and wielding greater influence within the bureaucracy. He recalls that quite separately yet parallel to this, the PSCC worked hard to "engage the media in counterterrorism exercises" to the extent in some instances of "having journalists formally on the Directing Staff" (personal communication, February 2, 2014). Directing Staff (or Exercise Control Staff, EXCON) play a pivotal role in exercises as they manage components of the exercise play (Commonwealth of Australia, 2012a). In practice, from the PSCC's perspective, the involvement of journalists in EXCON roles was an unsatisfactory part of the exercise. On the one hand it gave rise to tensions within the ranks of the journalists involved who were not accustomed to playing subordinate roles (required as part of the command and control response structure). On the other hand, and more specifically for individual journalists, it gave rise to ethical issues that were difficult to overcome (J. Lines, personal

communication, February 21, 2014). Overall, there were underlying suspicions on the part of the media as to the "real" purpose of their involvement in exercises, as well an unwillingness to fully commit to the goals of the exercise. Lines elaborates:

> We always had great difficulty actually getting the media to understand the nature of exercises. The media viewed their involvement in the exercises as some form of hoax to shut them up, but this wasn't the case (personal communication, May 21, 2013).

It was when journalists and counterterrorism officials were at odds over the purpose of the exercises, the relationship chilled. Both sides were at cross-purposes, which as McLean and Power (2014) found, was a key reason why tension and mistrust was never far below the surface in the relationships between emergency managers and the media. However, any budding relationship between agencies and the media was effectively negated by the way the media engaged in exercises as Lines explains:

> As part of the exercises the media would door-stop the Minister, but rather than focus on the events being played out in the exercise [they] would try and embarrass the Minster on a different topic altogether. The reality is that in a real event, the media would not divert from topic. We were let down time and time again by the media that were involved. A serious and mutual distrust developed and could not be overcome (personal communication, February 21, 2013).

It is not unexpected that journalists would seize the opportunity to turn role-play exercises into real news-gathering opportunities. Borden and Tew (2007, p. 302) assert that journalists are "motivated by the self-conscious pursuit of excellence as a journalist" and "excellent journalists demonstrate correspondence between intention and performance—in other words they have integrity as journalists." The journalists' orientation to their role of news-gathering, rather than role-playing, is historically deeply rooted in their inherent "universal traits" (Dueze, 2005, p. 447) to provide a public service as watchdogs, be impartial, fair and objective, have a sense of immediacy and value ethics. A fundamental role of journalism is to serve democracy, otherwise "journalists are reduced to propagandists or entertainers" (Ahva, 2013, p. 793).

In a study on public service journalism, Ahva (2013, p. 802) found that journalists resented having to "perform" in marketing and publicity roles as part of a branding exercise. Thus, we argue, a similar resentment may be the

outcome of participation in role-playing exercises.   At the time of the relationship breakdown, Australian journalists were committed to their professional values of news-gathering, investigation and advocacy (Hanusch 2008). Given the period under discussion, it is useful to turn to Henningham's (1996) survey of 1,068 news people in Australia on their professional and ethical values. His pioneering study found that most journalists at the time had few ethical concerns about using leaked government documents or badgering unwilling sources, they valued confidentiality but rejected subterfuge and invasion of privacy.

The exercises of the time included the political levels of response and information. This fulfills the need for senior officials to face "the stress of decision-making" (Carafano 2011) demanded during a major incident. Despite the participation of Government Ministers in exercises being regarded as useful practice (Carafano 2011), it created further conflict over role orientation for the participating journalists conducting mock interviews. The motivation for those journalists to take the opportunity to then confront Ministers on the issues of the day may be explained by the adversarial role of the Australian journalist (Hanusch 2008) who "openly challenges the powers that be" Hanitzsch (2007, p. 373). In other words, journalists of the day would not stand aside from their "universal traits" (Dueze, 2005).

The report of the 1993 review of a key committee (the Standing Advisory Committee on Commonwealth State Cooperation for Protection Against Violence or SAC-PAV) suggests that "relations with the media were flagged as a fundamental problem in incident management" and had been since at least 1979 (SAC-PAV Review Team, 1993, p. viii). The report further suggests that it was "not until 1991 that a more suitable approach to media relations was devised" (SAC-PAV Review Team, 1993, p. viii).   This focus was one of "media management in exercises" and a focus on "a continued element in training that develops awareness of likely media behaviour during an incident" (SAC-PAV Review Team, 1993, p. viii).

By 2005, the policy goal of achieving restrained reporting was re-branded "media liaison" (Commonwealth of Australia, 2005, p. 4.4) and save for a minor editorial amendment has remained unchanged (Commonwealth of Australia 2012b). Cameron Stewart, Associate Editor of *The Australian* newspaper and one of a handful of journalists specialising in defence and terrorism, acknowledges the shift in trust and cooperation between the media and security

agencies in the 1990s due to an increasing bureaucracy with more complex media management strategies. He elaborates:

> It's much more difficult now to get a straightforward answer on the simplest of things compared to when I was doing my own job, say 20 years ago, for example, it was a very, very different situation. I could literally pick up a phone, there'd be one bloke at the end of the phone who ran the Defence Public Relations, Defence Media, he'd sort of say, 'Oh okay, righty-o, look I'll come back to you,' and he's there, come back, and he'd say, 'Okay, off the record the answer is blah, blah, blah. On the record we'll say blah, blah, blah.' It was over in half an hour (personal communication, July 24, 2013).

Stewart contends that media relations by counterterrorism agencies is micro-managed across a range of people, delaying the supply of information with little respect for deadlines. Much of the interaction with the agencies is at an interpersonal level. The greater the understanding between the parties, the more information, both on-and-off the record is exchanged. Stewart asserts that a major hurdle is people new to the media relations role. He explains:

> There'll be people who come through the job who I, you know, have known me, know of me, know of my work and I, you know, I can relate to them and we can have a good dual conversation of on the record and off the record, which is what you have to do with these agencies; you can't just rely on on-the -record stuff. You have to have sort of background briefings and background discussions. And so it can be really good, and then all of a sudden you get someone else coming through and you feel like you're back to square one. You feel like you've just set the clock back 10 years (personal communication, July 24, 2013).

Unlike the routine and structured relationship between counterterrorism agencies and industry, the relationship with the media continues to be brittle and ad-hoc. In reflecting on the shifts in information sharing within and between government and between governments and industry over the past four decades Holdich has reflected on media relations and suggests consideration could be given to re-opening the counterterrorism tent to the media. He continues, "I think perhaps it is time to open discussion on providing information to key media people on an ongoing basis … and there are a number of ways it could be achieved" (personal communication, December 18, 2013). Rothery notes that there are "structural mechanisms and therefore the potential for media briefings exists" that "could be used if the threat environment shifted from a chronic threat to an acute threat" (personal communication, December 19, 2012).   Rothery explains that

authorised "backgrounders" with components of on-and-off the record are provided to media about counterterrorism policy and aspects of national security. This stands in contrast to counterterrorism operational matters. He elaborates:

> In terms of specific security and counterterrorism operations, it would be more likely, if given at all, they would be given by State agencies. I can't recall any background briefings to journalists on security or counterterrorism operations. Terrorist investigations are sensitive and rare. For a policy shift to routine media briefings there would need to be a significant change in the threat level (personal communication, December 19, 2012).

Moving toward a meaningful engagement with the media may be stymied by the raft of the more than 54 legislative instruments between 2001 and 2011 tightening anti-terrorism laws which Ewart, Pearson and Lessing (2013, p. 104) note could "have implications for open justice and news reporting." They argue that "anti-terror laws tend to impact upon the truth-seeking and truth-telling functions of journalists in a democracy, partly through disruptions to, and imbalances in, the flow of information from government agencies to the citizen via the media" (2013, p. 105).

On 12 September 2014, based on advice from security and intelligence agencies, the Australian Government raised the National Terrorism Public Alert Level from medium to high (Prime Minister of Australia, 2014). This means a terrorist attack is likely. It remains to be seen whether or not this will be sufficient in and of itself to re-invigorate the stalled policy discussion mooted in 2009 by the then Attorney-General about a replacement to the D-Notice system in the form of a "national security protocol for reporting sensitive information" (Stewart, 2010) or more broadly a policy discussion about engagement with the media.

CONCLUSION

This paper has explored a complex web of counterterrorism policy spanning four decades to map the evolution of information sharing with industry and the media in Australia. In expanding how security and counterterrorism policy has been interpreted in the literature, we bring to light a trajectory that highlights a maturation of policy focused on genuine engagement with industry reflected in practice and a corresponding diminution of policy also reflected in practice, focused on genuine engagement with the media. The recollections of current and

former key policy-makers, police, industry representatives and the media have shed new light how and why the differential relationships so evident in contemporary policy developed the way they did.

In the context of a recognition that policymakers needed to "lift their game," the 1970s saw the emergence of new security and counterterrorism policy. This paper highlights distinct triggering events that have shaped why in contemporary policy and practice, information is now routinely shared with industry. The policy trajectory highlights a shift from an earlier focus on a need to know (in instances of credible specific threats) to a need to share. During the same period, the media has experienced a reversal of fortune with counterterrorism agencies.

During 1970s until the 1990s, the media enjoyed a budding relationship to the point of being at the command table during major exercises. However, this paper finds the relationship turned sour when the media of the day was unable to orientate their roles into exercise play and took advantage of mock interviews as opportunistic news-gathering exercises. Instead, driven by their basic instincts, journalists used exercises to ambush a Minister on issues of the day.

Distrust became difficult for counterterrorism agencies to overcome and the door to the media closed. In its broader context, this occurred contemporaneously with the effective demise of the D-Notice system. This paper argues that any thawing of the relationship is likely to be dependent on a heightened security threat, where the media may be seen again both in policy and practice as a valuable tool in building resilience to terrorism. With recent security developments, this is an area worthy of further research.

REFERENCES

Ahva, L. (2013). "Public Journalism and Professional Reflexivity," in *Journalism*, vol 14(6), pp. 790–806.

Australian Security Intelligence Organisation (1974). *Special Interdepartmental Committee on Counter Terrorism. Inspection of ESSO-BHP Oil Producing Installation—Victoria*. Canberra: ASIO.

Borden, S. and Tew, C. (2007). "The Role of Journalist and the Performance of Journalism: Ethical Lessons from 'Fake' News (Seriously), in *Journal of Mass Media Ethics: Exploring the Question of Media Morality*, 22(4), pp. 300–314.

Business Government Taskforce on Critical Infrastructure (2002). *Business-Government Taskforce on Critical Infrastructure Report*. Canberra: BGTCI.

Carafano, J. (2011). *The Great Japan Earthquake. Assessing Disaster Response and Lessons for the U.S*. Washington DC: The Heritage Foundation.

Commission of Inquiry into the Australian Secret Intelligence Service (1995). *Report on the Australian Secret Intelligence Service: Public Edition*. Canberra: Australian Government Publishing Service.

Commonwealth of Australia (1979). *Protective Security Review Report* Canberra: Australian Government Publishing Service.

Commonwealth of Australia (1980). Cabinet Minute Intelligence and Security Committee: Canberra, 18 March 1980: Decision No.10921 (IS): National Archives of Australia, Barcode Number 30484239.

Commonwealth of Australia (2002). *Business Government Taskforce on Critical Infrastructure Terms of Reference*. Canberra: Attorney-General's Department.

Commonwealth of Australia (2003). *National Counterterrorism Plan*. Canberra: National Counterterrorism Committee.

Commonwealth of Australia (2005). *National Counterterrorism Plan Second Edition September 2005 Plus amendments relating to National Counterterrorism Alert System introduced on 1 October 2008*. Canberra: Attorney-General's Department.

Commonwealth of Australia (2006). *Protecting Australia Against Terrorism*. Canberra: The Department of the Prime Minister and Cabinet.

Commonwealth of Australia (2010). *Critical Infrastructure Resilience Strategy*. Canberra: Attorney General's Department.

Commonwealth of Australia (2012a). *Australian Emergency Management Handbook Series: Handbook 3 Managing Exercises*. Canberra: Australian Emergency Management Institute.

Commonwealth of Australia (2012b). *National Counterterrorism Plan*. Canberra: National Counterterrorism Committee.

Commonwealth of Australia (2013). *Strong and Secure: A Strategy for Australia's National Security*. Canberra: Department of the Prime Minister and Cabinet.

Deuze, M. (2005) "What is Journalism?: Professional Identity and Ideology of Journalists Reconsidered," in *Journalism*, Vol 6(4), pp. 442–464.

Ewart, J, Pearson, M. & Lessing, J. (2013). "Anti-Terror Laws and the News Media in Australia since 2001: How Free Expression and National Security Compete in a Liberal Democracy, in *Journal of Media Law*, 5(1), pp.104–132.

Finnane, M. (2013). "Terrorism and Government: Between History and Criminology." Sir John Barry Memorial Lecture, University of Melbourne, 2012, in *Australian and New Zealand Journal of Criminolgy, 46*(2), 159–177. doi: 10.1177/0004865813483296

Finnane, M. (2014). *The Munich Olympics Massacre and the Development of Counterterrorism in Australia, Intelligence and National Security*. doi: 10.1080/02684527.2014.882680

Hanitzsch, T (2007). "Deconstructing Journalism Culture: Toward a Universal Theory," in *Communication Theory*, 17, pp.367–385.

Hanusch, F. (2008). "Mapping Australian Journalism Culture: Results from a Survey of Journalists' Role Perceptions, in *Australian Journalism Review*, vol 30(2), pp. 97–109.

Henningham, J. (1996). "Australian Journalists' Professional and Ethical Values, in *Journalism and Mass Communication Quarterly*, vol 73(10), pp. 206–218.

Hocking, J. (1993). *Beyond Terrorism The Development of the Australian Security State*. Canberra: Allan & Unwin.

McLean, H. and Power, M. (2014). "When Minutes Count: Tension and Trust in the Relationship between Emergency Managers and the Media, in *Journalism*, Vol 15(3), pp. 307–325.

Prime Minister of Australia (2014, 12 September). "National Terrorism Public Alert Level Raised to High," in *Media Release* Retrieved 7 October, 2014, from https://www.pm.gov.au/media/2014-09-12/national-terrorism-public-alert-level-raised-high

Protective Security Coordination Centre (2002). *Business-Government Taskforce on Critical Infrastructure —The Protection of Infrastructure from Physical Attack*. Canberra: Protective Security Coordination Centre.

Prunckun, H. (2015). *Scientific Methods of Inquiry for Intelligence Analysis*. Lanham, MD: Rowman and Littlefield.

SAC-PAV Review Team. (1993). *Report of the 1993 SAC-PAV Review*. Canberra: Attorney-General's Department.

Stewart, C. (2010, 26 November). Attorney-General Robert McClelland urges media to accept security curbs. *The Australian* Retrieved 19 January, 2015, from http://www.theaustralian.com.au/national-affairs/attorney-general-robert-mcclelland-urges-media-to-accept-security-curbs/story-fn59niix-1225961188070

TISN for Critical Infrastructure Resilience (2013). *Trusted Information Sharing Network for Critical Infrastructure Resilience: Tenth Anniversary*. Attorney-General's Department.

Wright-Neville, D. (2006). *The Politics of Fear: Counterterrorism and Australian Democracy. Working Paper (WP) 27/2007*. Real Instituto Elcano, 1–14.

ACKNOWLEDGMENT

ABOUT THE AUTHORS

Kate O'Donnell, BBus, MA, MCCJ(Hons), Australian Research Council, Centre of Excellence in Policing and Security, Griffith University, Brisbane. Ms O'Donnell is a doctoral candidate based at Griffith University. Her research focuses on the policing of disruptions to critical infrastructure by radical protest. Before commencing her doctoral research, Ms O'Donnell was a senior officer in the transport sector of the Queensland State Government, who in 2011 was seconded to the Australian Research Council Centre of Excellence in Policing and Security as a Practitioner-in-Residence. In a career spanning almost thirty years with the Queensland Public Service, Ms O'Donnell has held senior roles in human resource management and industrial relations, health administration, ministerial, and parliamentary liaison, as well as transport security.

Dr Hamish McLean, GradDipArts, MA(Hons), PhD, School of Humanities, Griffith University, Brisbane. Dr McLean lectures in risk and crisis communication. He has 30 years' experience in emergency management, journalism and police media, along with operating a crisis and media consultancy for more than a decade with international clients in the health, aviation, law and allied sectors. His PhD study is in media and disasters. Dr McLean's research interests are in political communication during disasters and risk communication involving community resilience and disaster planning, response and recovery. He is part of a European-based research collaboration on risk communication and predictive disaster modelling.

- o O o -