Research Article

PUBLIC AND PRIVATE INTELLIGENCE: HISTORICAL AND CONTEMPORARY PERSPECTIVES

Ruth Delaforce[‡]

Intelligence is often regarded as information that is special or different, which must be safely kept. When sought, collected or used by the private sector, as opposed to public agencies, concerns are raised on the purpose and propriety of such an activity. However, in an historical context, intelligence collection or sharing between public and private interests for the purpose of national security was not unusual, particularly during the Cold War. Case studies from this era indicate that overlapping concerns were economic success combined with political strategy. Glimpses of these shared interests between the state and business can also be identified in the immediate post-Cold War era, and the aftermath of terrorist attacks in 2001. Perhaps the greatest contemporary change is not that "private" and "public "intelligence is shared between business and state, but the extent of such an enterprise. Further issues related to this change are: state dominance in the public-private relationship; potential fragmentation in the intelligence process; gaps in the historical record; and implications for future generations of intelligence professionals.

Keywords: Intelligence; public sector intelligence; private sector intelligence, national security intelligence

INTRODUCTION

Intelligence exchange between the public and private sectors for national security purposes—particularly in relation to strategic military, political and economic issues—is not new. Global security frameworks have long been dependent on intelligence exchange between a variety of actors, state and non-state. Glimpses of such praxis can be identified across the decades since 1945, during the Cold War and post-Cold War eras, through to the "durable disorder"

[‡] Corresponding author: r.delaforce@griffith.edu.au

that characterises today's global security climate (Cerny, 1998). Most notable, however, is the paradoxical nature of intelligence exchange now occurring, with overt collection in the public domain, while data analysis by state and private actors often appears to lack transparency and democratic oversight (Chesterman, 2008, 2006; Michaels, 2008).

During the Cold War, intelligence collection reflected an "institutionalised modern state" characterised by "covert action, high politics (and) intense secrecy" (Deibert, 2003: 175; Troy, 1991: 436). In the post-Cold War era, definitions of intelligence were widely debated, where scholars sought to reframe its meaning in terms of the "market state," introducing concepts of economic, business or competitive intelligence, and noting the benefits for both the state and for-profit companies by "sharing wares" (Treverton, 2003: 69–76). Since the events of 11 September, 2001, the concept of private intelligence has broadened to include data that is specifically collected and utilised by business for its own purposes, in addition to those companies contracted by governments to perform information gathering and processing activities.

Often the importance, priority and sensitivity attached to *intelligence* is not necessarily its content, but the source of such information—where and how it was obtained (that is, through human, signals or electronic means)—or contextual contribution, adding value to what is already known (Warner, 2007: 17–27). Intelligence collected by government agencies (the public sector) raises community and civil libertarian concerns on the purpose and propriety of such acts (Miller, 2007; Wong, 2006). However, these concerns are often voiced more strongly when the private sector is involved, as has been noted recently in the case of Edward Snowden (Ball, 22 August 2013).

In an historical and contemporary context, public-private intelligence exchange has underpinned both national and international security strategies, particularly for Great Britain and the United States. This paper proceeds with a summary of such strategies and case studies, during the Cold War, the post-Cold War era, and since 2001, where intelligence has gained precedence. The case studies illustrate British and American approaches towards public-private intelligence gathering and exchange. For the United States particularly, such public-private exchange has raised significant legal issues relating to privacy and lack of transparency. While the cases in this paper are demonstrative of these issues, there is limited scope to review in-depth the differing trans-Atlantic legal

regimes; the focus instead will be the changing concepts and state acquisition of intelligence that has occurred since 1945, and emerging issues.

Aside from the September 11 initiator of religious extremists prepared to use violence, intelligence is now aligned to other societal shifts, of globalisation, the growth of technology, and securitization across a range of government policies and programs. Tracing these changes in intelligence concepts since 1945, it is possible to identify the trajectory towards public-private partnerships, where "intelligence is now big business" (Herman 1996: xii).

In noting this intelligence sharing, four problematiques—emerging or potential problems—are reviewed. The first problematique considers the public-private relationship and state dominance of intelligence exchange. Secondly, the fragmentation of an intelligence process which, for those involved in national security analysis, can pose issues of information overload. Thirdly, the potential consequences from gaps in the historical record, related to archival limitations on privately collected intelligence. The last problematique posits the future loss of distinction between public-private sector employment for aspiring intelligence professionals.

THE COLD WAR

For intelligence professionals, the years between 1946 and 1989 have been described as a linear framework that was reasonably predictable (Liaropoulos, 2006: 6). In this era, public-private partnerships in both Great Britain and the United States (US) may be construed as a mutual patriotic opposition to communism. Intelligence during this era was derived from both human and electronic sources, was rigorously censored, and focused upon "strategic military arrangements" and countering the nuclear threat (Steele, 2002: v). Alternatively, private sector activities could also be considered illusory, with "front companies" that comprised personnel either recently retired or seconded from public security agencies.

One of the first glimpses of a public-private partnership in intelligence exchange is that of the International Diamond Security Organisation (IDSO), created in 1954 by Sir Percy Sillitoe (Sillitoe, 1955). Prior to retirement and founding of this company, Sillitoe was a former Chief Constable of Police, then head of MI5, the British internal security service. Soon after retirement, Sillitoe was approached by representatives of South African company, De Beers, a major diamond producer and exporter.

De Beers had concerns with diamond smuggling operations across the African continent that were undermining their control of the market, and Sillitoe was contracted to identify and disrupt these illegal activities (Fleming, 1957). Sillitoe did so by creating "an intelligence network which would penetrate" across Africa and the world, recruiting both former and serving British security agency personnel. Travelling between South Africa, Ghana, the Belgian Congo, Tanganyika and Sierra Leone, Sillitoe received a good deal of unofficial cooperation from intelligence officers located in these colonies, reportedly facilitated by Whitehall (Epstein, 1982; Fleming, 1957). This private intelligence network was deemed to have successfully eliminated the illicit trade, with the company being wound up two years later.

Established to support the market operations of a major diamond producer, IDSO was involved in the collection of private intelligence for private sector advantage. However, the involvement of public police and state security agencies is curious. One explanation is that, at the time, there were concerns by Western states on the Soviet expansion of its heavy industry manufacture, notably the production of military hardware (Epstein, 1982: 'Chapter 17'). Integral to these production processes were industrial diamonds (Dumett, 1985: 385–386). Therefore, reducing a flow of black market diamonds could impede Soviet industrial expansion. Intelligence exchange in the IDSO case occurred across the public-private sector, and collaboration would appear to be for two divergent purposes, politico-military strategy, and maintenance of a private monopoly. Also integral to this process were the use of sensitive sources and methods, represented by the cooperation of colonial intelligence officers, and employment of mercenaries to intercept diamond smugglers (Fleming, 1957; Kamil, 1979).

A further glimpse of public-private intelligence exchange may be ascertained from the North Yemen civil war of 1962 to 1970. The civil war commenced when the incumbent Imam al-Badr was deposed by a military junta, supported by the Soviet Union and Egypt (Curtis, 2004: 288–303; Fattah, 2010: 31–32). An insurgency by the ousted Royalists to regain power was supported by a British private security company led by Sir David Stirling (Connor, 1998: 192–195; Curtis, 2004: 295–303; Dorril, 2000: 684–686). Stirling, formerly founder of the British Special Air Services (SAS), recruited other SAS veterans through a private company, Television International Enterprises (TIE) based in London.

While the TIE self-identified as a private security company, many of its operations—surveillance, communications and targeted assassinations—were alleged to have assisted Western intelligence. In one instance, by identifying the use of Chinese-manufactured poison gas released from Egyptian aircraft; reports indicated that a British contractor was blinded and other Royalist tribesmen died from exposure (Kemp cited in Connor 1998: 194; Geraghty, 1981: 117). Although intelligence was purportedly derived from a private source, the preponderance of "former SAS men, and officers and troopers who were still serving with the Regiment" while working for Stirling, suggests at least some government facilitation (Connor 1998: 194).

Not all public-private intelligence exchange centred upon mercenary actors. Hulnick (1996: 18) notes instances of public intelligence supporting private US and British interests, particularly companies located in countries where incoming Marxist governments threatened to nationalise industry. In these cases, Western intelligence agencies supported covert activities and coups to remove such governments. During the 1950s, former government security personnel were employed by British Petroleum (BP) operations in Iran as security specialists. The company was included on distribution lists for British-derived intelligence, at a time when Mohammad Mossadegh, an Iranian leader, was threatening to nationalise foreign business operations (Prados 2006: 99; Smith 1982: 119–120).

This private intelligence net ceased in August 1951; Mossadegh was later ousted with the assistance of both US and British security services (Prados 2006: 99; Risen, 2000; Smith 1982: 119–120). Further examples include a 1954 US-sponsored coup instigated in Guatemala, following threatened nationalisation of the US-owned United Fruit Company; and Chile in 1970, with concerns raised by the American owned International Telephone and Telegraph Company, said to have influenced a US-sponsored removal of the Allende Government (Schlesinger & Kinzer, 1999; US Committee on Foreign Relations, 1973).

THE POST-COLD WAR ERA

Instances of public-private intelligence exchange can also be identified in the post-Cold War era. Between 1990 and 2001, the concept of intelligence changed, threats from nuclear-armed political adversaries were lessened, while potential benefits for the commercial sector and economic superiority were being promoted (Krizan, 1999; Herring, 1999 Shelley, 1995). Key factors at this time

were the reduction in military and security personnel employed by government agencies, increasing privatisation (particularly in the control and deployment of technological assets such as satellites) and realisation by industry that the state could not always guarantee protection (Berkowitz, 1996; Unsinger, 1999). The global security picture had changed, with a multiplicity of threats emanating from state and non-state actors, comprising criminal, religious, nationalist and ideological groups. Emphasis was also placed upon the market state, described as an economic battlefield (Wright, 1991: 209). Krizan (1999: 8) notes that, rather than intelligence being a government to government exchange, the environment was "receptive to government-private sector interaction."

The use of public intelligence to support private commerce was identified by CIA Director, Robert Gates, as necessary where "governments … try to steal our technology unfairly or illegally to disadvantage American business" (cited in Hulnick: 461). During the 1990s, Todd and Bloch (2003: 55) note that US government provision of intelligence to the private sector meant that American companies "won US$145 billion of business after government intelligence operations identified and defeated bribery or unfair conduct by foreign competitors." France also reportedly employed public intelligence resources to benefit French business (Hulnick, 1991: 459). Of particular concern was in-house intelligence collection by Japanese mega-corporations, such as Mitsubishi in New York, while other companies were beneficiaries of "overtly and covertly obtained economic and technical intelligence by the Japanese Ministry of International Trade and Industry" (Madsen, 1999: 436–437).

A notable feature of this era is the provision of training by former government security personnel to the private sector. Herring (1999) refers to the benefits for the private sector through adopting government approaches to intelligence, identifying priorities, processes and competitors.

Steele (1998) advocated an alternative option, that the private sector could support government agencies through more efficient provision of specific services such as commercial imagery, foreign language assistance, market research and media monitoring, all categorised as open source intelligence. Privately acquired data collections were also recognised for their potential assistance to business and academia. Examples include the creation of an intelligence network and investigation services for the maritime industry, the acquisition and maintenance of a private intelligence database on terrorism by an

academic institution, and the development of a global competitive intelligence organisation (Dugan, LaFree & Fogg, 2006; Unsinger, 1999).

Public-private intelligence exchange was also crucial in counterinsurgency operations, particularly for emerging private military and security contracting companies (Shearer, 1998; Silverstein, 1997). In one case, the private military company, Sandline—contracted by the Papua New Guinea government in 1997 to undertake a counterinsurgency operation and recapture the Panguna copper mine in Bougainville—was allegedly supported through the provision of signals intelligence by Great Britain and the US (Madsen 1999: 248–249; Todd & Bloch, 2003: 112). Sandline reportedly also had access to an in-house company—Quantum Strategic Consulting—that specialised in intelligence collection and analysis (Brooks, 1999).

Unprecedented growth of the internet during this timeframe was noted by one observer as potentially "the most fabulous surveillance program ever invented" (Young, cited in Todd & Bloch, 2003: 35). The internet also facilitated the collection of open source intelligence leading to private sector involvement in the process (Steele, 1995). Madsen (1999) charts the growth of the internet from its origins as a Cold War defence project, to its capacity for both public and private cyber-intelligence collection.

The transition of many defence-initiated projects from military control to the private sector occurred during this era, with 120 private companies being involved in the launch of more than 1,000 satellites, in turn, facilitating open access to technologies such as Global Positioning Systems (GPS), satellite telephones and detailed maps (Brooks, 1999; Todd & Bloch, 2003: 35–70). It is in the post-September 11 era, however, that intelligence exchange has undergone a transition; data, technology and personnel now increasingly operate across the public-private domain.

THE GLOBAL WAR ON TERROR

The declaration in 2001 of a global war on terror by US President, George W Bush (2001) signalled a change to the public-private intelligence relationship. While threats emanated from state adversaries and religious extremist groups, the assessments were also including individuals labelled as *lone wolves* and criminal networks. Further, the concept of security was applied to diverse programs related to food, water, natural resources and health (Buzan, Waever and De Wilde, 1998). The so-called "information revolution" that began in the 1990s

challenged the capacity of state intelligence agencies. Liriapoulos (2006: 8) notes these vulnerabilities as resulting from a lack of resources, loss of state monopoly and inability to restrain technological development—which can be utilised by anyone—in addition to significant reliance by the state upon commercial information infrastructure.

The reduction of state-employed intelligence personnel during the 1990s resulted in a critical manpower shortage for the counterterrorism campaigns after 2001 (Voelz, 2006: 12–13). The battlefield required personnel who could manage "the explosion in multilingual digital information," in addition to the more traditional ground-truthing expeditions (Steele, 2002: v–vi). Government responses have been to contract private sector personnel—foreign linguists and translators, military and security officers, interrogators and intelligence analysts—to augment state resources (Voelz, 2006: 12–21).

In the decade since 2001, private sector intelligence contracts are estimated to cost the US government between US$42 and 45 million annually (Chesterman, 2006: 1,058; Shorrock, 2008). The proliferation of private companies and personnel involved in intelligence activities is estimated to be 1,271 government organisations and 1,931 private companies, across 10,000 locations in the US, and comprising 854,000 personnel (military, civilian and contractors) with top secret security clearances (Priest & Arkin, 2010). A *Washington Post* investigation further estimated that this public-private endeavour produced 50,000 intelligence assessments annually (Priest & Arkin, 2010). Privatisation is also occurring in other countries, with the British General Communications Headquarters being subject to partial private sector contract management of its infrastructure, data streams and staffing (Aldrich, 2009: 899). While the state contracts private intelligence companies and their personnel, it also acquires data initially collected by the private sector.

Increasingly, citizens interface with the private sector, not government agencies; this interface and privately-derived intelligence occurs across the commercial, financial and telecommunication sectors (Michaels, 2008: 908). Either reluctantly or willingly, data held by the private sector is being provided to state agencies, where it is then often processed by private contractors (Chesterman, 2008). With an estimated 6 billion mobile telephone users and Internet access for 2.4 billion people, the capacity for governments alone to collect and process data is unaffordable and unachievable, particularly when this

data is held by the private sector (Internet World Stats, 2012; Steele, 2002: 21; World Bank, 2012).

Software and telecommunication companies, such as Google, Apple and Verizon, are of specific interest to government, with allegations that, in the US, intelligence analysts may sift through electronic data with no prior authorisation (Greenwald, 2013). In this regard, Chesterman (2008: 1,059–1,061) notes that, despite the existence of legislation requiring judicial oversight for state access to privately-sourced data, the secret cyber-collection programmes run by the National Security Agency may well preclude any requirement for a warrant. In this context, the hosting of social media sites (such as *Facebook*, *YouTube*, and *Instagram*) through telecommunication and software providers also can facilitate the (secret) gleaning of personal data (often self-disclosed by users) for state agencies (Gellman & Soltani, 31 October 2013; Kaplan & Haenlein, 2010). The collection of this personal data for targeted advertising by companies such as *Google* has resulted in multi-million dollar fines for privacy breaches (The Australian, 2012). As Michaels (2008: 902) notes, private organisations have the capacity to collect information "more easily, under fewer legal restrictions than governments."

Public-private intelligence exchange is also occurring on the territorial battlefield. In 2007, a private military company (Aegis) based in Iraq was collecting intelligence on infrastructure and convoy security threats, militia groups and criminal gangs, producing detailed maps, establishing an operations centre to collate and analyse data (Fainaru & Klein, 2007). In further examples, the private military contracting sector also offers services that include interpreters, linguists, and "human intelligence collectors" (Aldrich, 2009: 899; Voelz, 2006: 18).

Since 2001, public-private intelligence exchange appears to be mutually beneficial, with significant financial profits to companies directly contracted to undertake collection and analysis by the state. But, there is less benefit in such a partnership for companies whose core activity is not intelligence processing on behalf of the state, but where data acquired during normal business practice is then deemed to be valuable public intelligence. As Michaels (2008: 926–928) notes, the private sector is not an equal partner, being vulnerable to state pressure. Similarly, intelligence gathered through private security operations in conflict zones may be appropriated by the state. One critic of the Aegis operations centre in Iraq stated that any intelligence generated from private

contractors was "classified secret by the military and not distributed" thereby deterring wider contractor participation (Holly, cited in Fainaru & Klein, 2007).

It is unlikely that the current trajectory towards public-private intelligence exchange will cease. Instead, with the advances in digital technology, not only will the volume of data increase, but also the type of information that can be collected. This data proliferation is leading to a dispersed intelligence network, in contrast to the Cold War linear frameworks, and a need for burden-sharing through public-private partnerships (Berkowitz, 1996: 8; Steele, 2002: 21). There are a range of concerns highlighted in public-private intelligence exchange, of which four emerging or potential problems are considered in the following section.

PROBLEMATIQUES

The blurring of a public-private division on information collection, and the broadening concepts and appreciation for the utility of intelligence, are rapidly transforming the industry and its practice. This evolution is considered in the following section from four differing perspectives. These are nominated as: the unequal relationship between the public-private sectors and state dominance; fragmentation of the intelligence process and information overload; a potential for gaps in the historical record due to private sector ownership of data; and implications of public and private sector employment for future generations of intelligence professionals.

The electronic footprint of those with access to a mobile phone and the internet—estimated in 2012 to be 6 billion and 2.4 billion, respectively—occurs primarily through the private sector. A large proportion of these users are recording their lives online, with self-disclosure and dissemination that ultimately can be collected for commercial as well as security purposes. Michaels (2008) argues that the private sector has fewer legal restrictions than the government in collection and distribution of this digital data, but also notes that business is not an equal partner in the public-private relationship, being vulnerable to state pressure.

In turn, this creates an accountability gap, where business may be pressured into providing informal intelligence to the state, either due to patriotism, a misleading belief in government authority, or lack of knowledge on legal compliance (Michaels, 2008: 926–928). Similarly, government acquisition and restrictions upon privately derived intelligence also occur in military

operations, as noted in the Aegis case (Fainaru & Klein, 2007). Rather than a partnership, the inference is an ongoing "privatisation of state surveillance" across "multiple institutions" in the public-private sectors (Newkirk, 2010: 43–44).

The second problematique is a potential fragmentation in the intelligence process. The increased range of intelligence sources pose challenges for data collectors and analysts. Identifying gaps in the intelligence collection is challenging, but then knowing where such information may be sourced from is increasingly affected by the range of available sources, often referred to as information overload. Vulnerable points in the process are collection and collation of intelligence. While focus is placed upon the interchange of intelligence between and within government agencies, the number of private sector actors collecting data can also impede the process, in addition to issues of quality assurance (Liriapoulos, 2006: 15). After reviewing a US Defence Department program, a senior military officer noted that he was "Not aware of any agency with the authority, responsibility, or a process in place to coordinate all these interagency and commercial activities … The complexity of this system defies description" (Vines, cited in Priest & Arkin, 2010). A paradox of such information overload is that threats are more likely to be overlooked.

The third problematique to be considered is the (lack of) contribution to historical records. In most Western countries, government records are archived under legislation. While public access to these records may be limited, there is still a legal requirement to retain and store the data. Doing so enables historians, researchers and the public to (eventually) construct a picture of past events. Steele (2002: 20) argues that "the most fundamental, the most neglected (issues are) the lessons of history."

Nonetheless, in the contemporary era of public-private partnerships, private collectors are not bound to public rules, such that retention, storage, and later public access to records may occur. In this context, government records may identify the final outcome, but remain silent on processes of collection. For government agencies and analysts, this also introduces gaps in corporate knowledge, event chronology, and limited understanding of best (or worst) practice and available strategies. An alternative perspective is that a well-orchestrated intelligence operation should avoid identification and scrutiny (i.e. counterintelligence), and in an era of multiple threats, employing private agents may assist in this process (Prunckun, 2013).

The final problematique is a *potential* issue of concern: whether a public-private employment distinction can be maintained for future generations of intelligence professionals. During the Cold War and post-Cold War eras, it was not unusual for former state security agents to transition into private sector careers upon retirement. Miller (2007) contends there is a growing need for intelligence professionals in both the public and private sectors, while Steele (2002: 29) suggests that state employment should occur after training in the private sector. Shorrock (2008: 14) notes, however, a former CIA officer's observation, that "Everyone … is leaving and going into contracting, whether they are retiring or not," presumably enticed by the significant financial incentives. Notably, the career aspirations of younger generations such as Gen Y or Millenials do not centre on employer loyalty, but instead skills development and rapid promotion (Ng, Schweitzer & Lyons, 2010).

For future intelligence professionals, the blurring line between private-public partnerships may mean that, rather than a "revolving door," there is little distinction between work conducted for government or business, possibly leading to a blurring of patriotism and commercial ambition. Still, a third form of loyalty may be emerging, as indicated in the Edward Snowden case, and that is to the community or citizenry, rather than the state or company. Although the Snowden revelations had often been framed as whistleblowing, an underlying theme in such exposures is that of alerting citizens to the actions of their governments. A similar feature of Snowden (and other cases, such as Bradley Manning) is their age—30 and 25 years, respectively. Ng et al. (2010: 283) argue that a particular feature of this younger professional cohort is "their high expectations for social responsibility and ethical behaviour on the part of their employers."

For state intelligence agencies, however, the Snowden case may initiate a revocation of its previous policies and practices, with a reduction in private contracting and, instead, direct state employment of intelligence professionals. A further issue is that of the contractor company's role in managing its personnel, and state expectations in addressing potential leaks.

CONCLUSIONS

Public-private intelligence exchange is not a new phenomenon. As the above case studies illustrate, state and business have long had mutual interests in maintaining political and economic security. However, technological

development and open access have contributed to an exponential increase in the volume and types of raw data that may be considered of value, and therefore collected for both commercial and security purposes. It is unlikely that this trajectory will slow or cease.

A novel feature of this phenomenon, though, is that the distinction between a public-private interface is becoming less clear, with the migration of data and personnel across a permeable boundary. For intelligence personnel, the question is whether loyalty to the state is seen through the prism of both private and public sector employment. For the state, this public-private trajectory may be slowed due to concerns with security leaks from private contractors. For business, state capacity to appropriate privately-sourced data, and infiltrate and manage private operations, indicates an uneasy, if also unequal, relationship, and one which will be difficult to resist.

REFERENCES

Aldrich, Richard J. (2009). "Beyond The Vigilant State: Globalisation and Intelligence." *Review of International Studies* (35) 899–902.

Ball, James. (22 August 2013). "Edward Snowden NSA Files: Secret Surveillance and Our Revelations So Far." *The Guardian*. [http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations] last accessed 1 September 2013.

Berkowitz, Bruce D. (Summer 1996). "Information Age Intelligence." *Foreign Policy* (103).

Brooks, Douglas J. (July–September 1999). "The Business End of Military Intelligence: Private Military Companies." *Military Professional Intelligence Bulletin.* [http://huachuca-usaic.army.mil/mipb/HTML%20July-Sep99/brooks/brooks.htm] last accessed 1 September 2013.

Bush, George W. (20 September 2001). *Presidential Address to the Nation.* Washington DC. Transcript available at [http://edition.cnn.com/2001/US/09/20/gen.bush.transcript/] last accessed 1 September 2013.

Buzan, Barry, Ole Waever and Jaap De Wilde. (1998). *Security: A New Framework for Analysis*. Boulder, Co: Lynne Rienner.

Cerny, Philip G. (Spring 1998). "Neomedievalism, Civil War and the New Security Dilemma: Globalisation as Durable Disorder." *Civil Wars*. (1) 36–64.

Chesterman, S. (2008). "'We Can't Spy … If We Can't Buy!' The Privatization of Intelligence and The Limits of Outsourcing "Inherently Governmental Functions."' *The European Journal of International Law* (19:5) 1,055–1,074.

Chesterman, S. (2006). "The Spy Who Came In From The Cold War: Intelligence and International Law."*Michigan Journal of International Law* (27:4) 1,071–1,130.

Committee on Foreign Relations, United States Senate. (21 June 1971). *The International Telephone and Telegraph Company and Chile, 1970–71*. Washington DC: US Government Printing Office.

Connor, Ken. (1998). *Ghost Force: The History of the SAS.* London: Orion Books.

Curtis, Mark. (2004). *Unpeople: Britain's Secret Human Rights Abuses.* London: Vintage.

Deibert, Ronald J. (2003). "Deep Probe: The Evolution of Network Intelligence." *Intelligence and National Security.* (18:4) 175–193.

Dorril, Stephen. (2000). *MI6: Inside the Covert World of Her Majesty's Secret Service*. New York: The Free Press.

Dugan, Laura, Gary LaFree & Heather Fogg. (23–24 May 2006). "A First Look At Domestic and International Global Terrorist Events, 1970–1997." *Intelligence and Security Informatics. IEEE International Conference on Intelligence and Security Informatics.* San Diego, Ca.

Dumett, Raymond. (October 1985). "Africa's Strategic Minerals During the Second World War." *The Journal of African History* (26:4) 381–408.

Epstein, Edward Jay. (1982). *The Rise and Fall of Diamonds: The Shattering of a Brilliant Illusion.* Simon and Schuster. [http://www.edwardjayepstein.com/diamond/chap17.htm] last accessed 1 September 2013.

Fattah, Khaled. (November 2010). "A Political History of Civil-Military Relations in Yemen." *Alternative Politics* (1) 25–47.

Fleming, Ian. (1957). *The Diamond Smugglers.* London: Jonathan Cape.

Gellman, Barton and Ashkan Soltani. (31 October 2013). "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." *The Washington Post.*

Geraghty, Tony. (1981). *Who Dares Wins: The Story of the Special Air Service, 1950–1980.* Tiptree Essex: Anchor Press.

Greenwald, Glenn. (31 July 2013). "XKeyScore: NSA Tool Collects Everything A User Does On The Internet." *The Guardian.*

Herman, Michael. (1996). *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Herring, Jan P. (1999). "Key Intelligence Topics: A Process To Identify and Define Intelligence Needs." *Competitive Intelligence Review* (10:2) 4–14.

Hulnick, Arthur S. (1996). "The Uneasy Relationship Between Intelligence and Private Industry." *International Journal of Intelligence and Counter-Intelligence* (9:1) 17–31.

Hulnick, Arthur S. (1991). "Intelligence Co-operation in the Post-Cold War Era: A New Game Plan?" *International Journal of Intelligence and Counter-Intelligence* (5:4) 455–465.

Internet World Stats. (30 June 2012). *Internet Usage Statistics: World Internet Users and Population Stats.* [http://www.internetworldstats.com/stats.htm] last accessed 1 September 2013.

Kamil, Fred. (1979). *The Diamond Underworld.* London: Allen Lane.

Kaplan, Andreas M & Michael Haenlein. (January–February 2010). "Users of the World, Unite! The Challenges and Opportunities of Social Media." *Business Horizons* (53:1) 59–68.

Kemp, Anthony. (1994). *The SAS: Savage Wars of Peace*. London: John Murray.

Krizan, Lisa. (June 1999). *Intelligence Essentials For Everyone.* Occasional Paper Number 6. Washington DC: Joint Military Intelligence College.

Liaropoulos, Andrew, N. (June 2006). *A (R)evolution In Intelligence Affairs? In Search of a New Paradigm.* Research Institute for European and American Studies. Research Paper No 100.

Madsen, Wayne. (1999). *Genocide and Covert Operations in Africa, 1993–1999.* New York: Edwin Mellen Press.

Madsen, Wayne. (1993). "Intelligence Agency Threats to Computer Security." *International Journal of Intelligence and Counter-Intelligence* (6:4) 413–488.

Michaels, Jon D. (31 August 2008). "All The President's Spies: Private-Public Intelligence Partnerships in the War on Terror." *California Law Review.* ((96:4) 901–966.

Miller, Michael C. (2007–2008). "Standing in the Wake of the Terrorist Surveillance Program: A Modified Standard for Challenges to Secret Government Surveillance." *Rutgers Law Review* (60) 1039.

Newkirk, Anthony B. (2010). "The Rise of the Fusion-Intelligence Complex: A Critique of Political Surveillance After 9/11." *Surveillance and Society* (8:1) 43–60.

Ng, Eddy S W, Linda Schweitzer & Sean T Lyons. (2010). "New Generation, Great Expectations: A Field Study of the Millenial Generation." *Journal of Business Psychology* (25) 281–292.

Prados, John. (2006). *Safe For Democracy: The Secret Wars of the CIA.* Chicago: Ivan R Dee.

Priest, Dana & William Arkin. (19 July 2010). "The Growth of Top Secret America." *The Washington Post*. [http://projects.washingtonpost.com/top-secret-america/] last accessed 1 September 2013.

Prunckun, Hank (2013). Personal conversation on August 8, 2013, Canberra, Australia. I am very grateful to Dr Prunckun for pointing out this issue regarding intelligence tradecraft.

Risen, James. (16 April 2000). "Secrets of History: The CIA in Iran." *The New York Times.*

Schlesinger, Stephen & Stephen Kinzer. (1999). *Bitter Fruit: The Story of the American Coup in Guatemala*. Cambridge, Mass: Harvard University Press.

Shearer, David. (1998). *Private Armies and Military Intervention.* Adelphi Paper 316, International Institute of Strategic Studies.

Shelley, Louise. (Winter 1995). "Transnational Organised Crime: An Imminent Threat to the Nation-State?" *Journal of International Affairs* (48:2) pp 463–489.

Shorrock, Tim. (2008). *Spies For Hire: The Secret World of Intelligence Outsourcing.* New York: Simon & Schuster.

Sillitoe, Sir Percy. (1955). *Cloak Without Dagger*. London: Cassell and Company Ltd.

Silverstein, Kenneth. (28 July 1997). "Privatising War: How Affairs of State Are Outsourced to Corporations Beyond Public Control." *The Nation.*

Smith, Woodruff, D. (1982). *European Imperialism in the 19th and 20th Centuries.* Chicago: Nelson-Hall.

Steele, Robert David. (February 2002). *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Non-Traditional Threats.* Studies in Asymmetry. Carlisle, Pa: Strategic Studies Institute, US Army War College.

Steele, Robert David. (May 1998). "Open Source Intelligence: Private Sector Capabilities to Support DOD Policy, Acquisitions and Operations." *Defense Daily Network Special Report.* [http://www.fas.org/irp/eprint/oss980501.htm] last accessed 1 September 2013.

Steele, Robert David. (1995). "Private Enterprise Intelligence: Its Potential Contribution to National Security." *Intelligence and National Security* (10:4) 212–228.

Straw, Joseph. (2013). "Smashing Intelligence Stovepipes." *Security Management.* [http://www.securitymanagement.com/article/smashing-intelligence-stovepipes] last accessed 1 September 2013.

The Australian. (10 August 2012). "Google Fined $21.3m For Breaching Privacy of Apple Safari Users."

The World Bank. (2012). *Maximising Mobile: 2012 Information and Communications for Development.* Washington DC: The World Bank. [http://siteresources.worldbank.org/ExtInformationAndCommunicationAndTechnologies/Resources/IC4D-2012-Report.pdf] last accessed 1 September 2013.

Todd, Paul & Jonathan Bloch. (2003). *Global Intelligence: The World's Secret Services Today*. London: Zed Books.

Treverton, Gregory F. (2003). *Reshaping Intelligence for the Information Age.* Cambridge: Cambridge University Press.

Troy, Thomas F. (1991). "The "Correct" Definition of Intelligence." *The International Journal of Intelligence and Counter-Intelligence*. (5:4) 433–454.

Unsinger, Peter Charles. (1999). "Meeting A Commercial Need For Intelligence: The International Maritime Bureau." *The International Journal of Intelligence and Counter-Intelligence* (12:1) 58–72.

Voelz, Glenn J. (June 2006). *Managing the Private Spies: Use of Commercial Augmentation for Intelligence Operations*. Washington DC: Joint Military Intelligence College.

Warner, Michael. (2007). "Sources and Methods for the Study of Intelligence." In Johnson, Loch K. (Ed.) *Handbook of Intelligence Studies.* Abingdon, Oxon: Routledge.

Wong, Katherine. (2006). "The NSA Terrorist Surveillance Program." *Harvard Journal of Legislation.* (43:2) 517–534.

Wright, Jeffrey W. (1991). "Intelligence and Economic Security." *The International Journal of Intelligence and Counter-Intelligence* (5:2) 203–221.

ABOUT THE AUTHOR

Dr Ruth Delaforce is a lecturer with the School of Criminology and Criminal Justice, and adjunct investigator with the Australian Research Council, Centre of Excellence in Policing and Security, at Griffith University. She has previously been employed in the private and public sectors, and law enforcement. Her research interests include the military-crime nexus, private military and security companies, insurgency and counterinsurgency studies.

- o O o -