Paper presentated at the International Studies Association
San Diego, April 2012

This paper deals with subjects examined at greater length in
Simon Chesterman, *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford University Press, 2011)

The Turn to Outsourcing in U.S. Intelligence

Simon Chesterman
National University of Singapore Faculty of Law

Though it lagged behind the privatization of military services, the privatization of intelligence expanded dramatically with the growth in intelligence activities following the September 11 attacks on the United States. Privatization of intelligence services raises many concerns familiar to the debates over private military and security companies (PMSCs). One of the key problems posed by PMSCs is their use of potentially lethal force in an environment where accountability may be legally uncertain and practically unlikely; in some circumstances, PMSCs may also affect the strategic balance of a conflict. The engagement of private actors in the collection of intelligence exacerbates the first set of problems: it frequently encompasses a far wider range of conduct that would normally be unlawful, with express or implied immunity from legal process, in an environment designed to avoid scrutiny. Engagement of such actors in analysis raises the second set of issues: top-level analysis is precisely intended to shape strategic policy—the more such tasks are delegated to private actors, the further they are removed from traditional accountability structures such as judicial and parliamentary oversight, and the more influence those actors may have on the executive.

The Turn to Outsourcing in U.S. Intelligence

Simon Chesterman
National University of Singapore Faculty of Law

> We also have to work, though, sort of the dark side, if you will. We've got to spend time in the shadows in the intelligence world. A lot of what needs to be done here will have to be done quietly, without any discussion, using sources and methods that are available to our intelligence agencies, if we're going to be successful. That's the world these folks operate in, and so it's going to be vital for us to use any means at our disposal, basically, to achieve our objective.
>
> *Vice President Dick Cheney*[1]

Six days after the September 11 attacks, at a press conference held in the Pentagon, President George W Bush said that the United States was ready to defend freedom at any cost: 'We will win the war, and there will be costs.' Calling Osama bin Laden the prime suspect in the attacks he was asked whether he wanted bin Laden dead. 'I want justice,' he responded. 'There's an old poster out West that said, "Wanted, dead or alive."'[2]

Within the CIA, a small unit was already examining the possibility of taking this injunction literally. The model appears to have been the Israeli response to the Munich Olympics attack in 1972. 'It was straight out of the movies,' one former intelligence official later told the *Wall Street Journal*. 'It was like: Let's kill them all.' The programme was kept secret from Congress for almost eight years until Leon Panetta took over as Director of the CIA under a new White House in 2009. In June of that year, four months into his tenure, Panetta was briefed on the programme and immediately terminated it and informed Congress. It appears that no actual operations

[1] Richard (Dick) Cheney, 'The Vice President appears on Meet the Press with Tim Russert' (Meet the Press, Camp David, 16 September 2001).

[2] Charles Babington, '"Dead or Alive": Bush Unveils Wild West Rhetoric', *Washington Post*, 17 September 2001.

to assassinate alleged terrorists were launched.[3] But one of the more interesting aspects of the programme was the decision that any such operations should be undertaken by a private military and security company. A 2004 contract awarded Blackwater USA several million dollars for training and weapons. Reliance on a contractor was said to provide additional cover to the Agency in case 'something went wrong', but the move from the CIA's Counterterrorist Center also appears to have coincided with the retirement of key officials who went to work for Blackwater.[4]

The attacks of September 11 radically changed the way in which national security is perceived generally, while eroding some traditional protections long taken for granted in the United States in particular. This paper first considers the changes that were made to laws relating to intelligence activities following the September 11 attacks, before situating these in the context of more longstanding debates over reforming the US intelligence 'community' — a somewhat misleading term that suggests collegiality among 16 organizations that employ around 200,000 people with a budget in the order of $75 billion. Though the abuse of detainees and the erosion of civil liberties have been the subject of much debate, the paper then focuses on a striking trend over the past decade that may have more long-term consequences: the reliance on private contractors for an increasing portion of US intelligence.

1 The Dark Side

The US Constitution — one of the oldest constitutions still in force — was crafted with an eye to limiting the powers of centralized authority through checks and balances. The liberties that it embraces reflect the time in which it was written, however. In the late eighteenth century, physical surveillance consisted of following people, eavesdropping on them, or examining their property. To limit such surveillance the Fourth Amendment required that searches and seizures by government be 'reasonable'. Psychological surveillance was possible through forced testimony or torture: the Fifth and Eighth Amendments forbade compelled self-incrimination and cruel and unusual punishment. A third mode of surveillance used at the time was the record and dossier system of the European monarchies that

[3] Siobhan Gorman, 'CIA Had Secret Al Qaeda Plan', *Wall Street Journal*, 13 July 2009.

[4] Mark Mazzetti, 'CIA Sought Blackwater's Help to Kill Jihadists', *New York Times*, 19 August 2009; Joby Warrick and R Jeffrey Smith, 'CIA Hired Firm for Assassin Program', *Washington Post*, 20 August 2009.

controlled the movement of the population and the activities of 'disloyal' groups. In the United States the decision not to employ a passport or dossier system — for practical as well as political reasons — ensured a degree of freedom unusual in the industrializing world.[5]

Until the end of the following century, such provisions were seen as adequate. The development of the telephone in the 1880s and the microphone in the 1890s challenged the paradigms that had emerged and the ability of law to adapt to new technological realities. Notably, the Fourth Amendment only applies to searches and seizures, not other types of investigation. An investigative method is only considered a 'search' if it invades a 'reasonable expectation of privacy'.[6] Tapping into a telephone or using a hidden microphone is a search, for example, but observation by an undercover agent who is in the room during a conversation is not — even if that agent is transmitting the conversation.[7] Government inspection of bank records is not a search, as the customer has made such information available to the bank and its employees.[8] Similarly, installing a 'pen register' that records all numbers dialled from a telephone line is not a search — though listening to the calls would be — as customers voluntarily convey these numbers to the telephone company when using the device.[9] The more recent explosion of electronic communications in which far more data are shared with relevant companies, such as the metadata that travel with an e-mail, means that ever greater information is revealed even without opening the actual missive.

Some of these gaps have been filled by legislation, but the focus has typically been law enforcement; the application of constitutional and legislative protections to the growing intelligence community has not always been clear. The Right to Financial Privacy Act 1978, for example, gave customers a measure of privacy in their bank records that was more than the Supreme Court had offered under the Fourth Amendment, but included a section on 'special procedures' that exempted

---

5 Alan F Westin, 'Civil Liberties Issues in Public Databanks', in Alan F Westin (ed), *Information Technology in a Democracy* (Cambridge, MA: Harvard University Press, 1971), 301 at 301-2.

6 *Katz v United States*, 389 US 347, 360 (1967).

7 *United States v White*, 401 US 745 (1971).

8 *United States v Miller*, 425 US 435 (1976).

9 *Smith v Maryland*, 442 US 735 (1979). See further Stephen J Schulhofer, *The Enemy Within: Intelligence Gathering, Law Enforcement, and Civil Liberties in the Wake of September 11* (New York: Century Foundation Press, 2002), 34-6.

government agencies engaged in intelligence or counter-intelligence activities.[10] The Pen Register Act was part of the Electronic Communications Privacy Act 1986, but only requires that a law enforcement agency show that the information is relevant to an ongoing criminal investigation. The original definition of what could be collected was clearly limited to telephone numbers, but this has been broadened to include virtually all data transmitted in electronic communications except the content.[11] Intelligence agencies are exempted from the Pen Register Act if they obtain an order under the Foreign Intelligence Surveillance Act.

These legislative moves attempted to keep pace with technological change, but also coincided with the aftermath of intelligence scandals. The excesses and abuse revealed in the 1970s led to significantly greater scrutiny of US spies and these protections were intended to prevent wrongdoing and safeguard privacy. When the nation suffered the most lethal attack in its history, the view quickly formed that US vulnerability could at least in part be blamed on excessive constraints on the ability of intelligence services to collect information.

1.1 September 11 and the Patriot Act

The main legislative response was sweeping legislation adopted five weeks after the September 11 attacks under an unwieldy title that formed the acronym 'USA Patriot'.[12] Many provisions in the Patriot Act of 2001 merely corrected oversights in prior law, reduced administrative obstacles, or adjusted language to reflect new technologies. Prior law, for example, had allowed courts to authorize 'roving' wiretaps (that is, surveillance of a person rather than a particular telephone line) for domestic law enforcement, but there was no equivalent for foreign intelligence investigations. Where prosecutors had previously been required to file separate warrants in each federal district, the Patriot Act empowered federal judges to issue nationwide search warrants. Subpoenas and search warrants could be used to obtain records from telephone companies and Internet service providers; the Act extended this to cable television companies, which by then were providing similar services.[13]

---

[10] Right to Financial Privacy Act 1978 (US), § 1114(a)(1)(A); 12 USC §§ 3401-22.

[11] 18 USC §§ 3121-7.

[12] The full title is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

[13] Patriot Act 2001 (US), § 206 (roving surveillance), §§ 216, 219, 220 (nationwide warrants), and § 211 (cable companies); Schulhofer, *The Enemy Within*, 30.

But the Patriot Act also extended the search powers of law enforcement agencies and reduced restrictions on foreign intelligence gathering within the United States. Among other things, it increased the ability of the FBI and certain other government agencies to search telephone, e-mail, and financial records without a court order through the use of National Security Letters (NSLs), a form of administrative subpoena issued without judicial oversight. NSLs were first created as exceptions to legislative privacy protections in the Right to Financial Privacy Act and the Electronic Communications Privacy Act, with some expansion in the 1990s. The Patriot Act greatly broadened the circumstances in which these could be used, replacing the requirement that the information relate to an agent of a foreign power with the far looser requirement that it be relevant to an investigation to protect against international terrorism or foreign espionage.[14] These powers were supplemented by gag orders that prohibited anyone asked to give information from disclosing that the FBI had asked for it. Lawsuits led to this last provision being removed.[15]

The Patriot Act was criticized for, among other things, allowing the indefinite detention of immigrants. Where the Attorney General has reasonable grounds to believe that an alien may cause a terrorist act, that person can be detained for an unlimited series of six month periods.[16] Other restrictions on civil liberties included new 'sneak and peek' powers, also referred to as delayed-notice searches, in which law enforcement agents may surreptitiously search and photograph items without advising the owner and without leaving a copy of a warrant.[17] The Act further expanded the crime of providing material support to terrorists by including monetary instruments and expert advice or assistance within the definition of 'material support'.[18] Another provision that produced much discussion empowered the FBI to apply for an order to obtain, among other things, library records. Though these records are held by a third party and therefore not protected by the Fourth

---

[14] Patriot Act, § 505. See also Eric Lichtblau and Mark Mazzetti, 'Military Expands Intelligence Role in US', *New York Times*, 14 January 2007; Charles Doyle, National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments (Washington, DC: Congressional Research Service, 28 March 2008). The Patriot Act also broadened the general exemption from the Right to Financial Privacy Act to include agencies engaged in investigation or 'analysis' of international terrorism. Patriot Act, § 358(f)(2).

[15] Laura K Donohue, 'Anglo-American Privacy and Surveillance', *Journal of Criminal Law & Criminology* 96 (2006) 1059 at 1112.

[16] 8 USC § 1226a. Indefinite extensions of six months are allowed 'if the release of the alien will threaten the national security of the United States or the safety of the community or any person'.

[17] Patriot Act, § 213; Brett A Shumate, 'From "Sneak and Peek" to "Sneak and Steal": Section 213 of the USA PATRIOT Act', *Regent University Law Review* 19 (2006) 203.

[18] Patriot Act, § 805(a)(2); Jonathan D Stewart, 'Balancing the Scales of Due Process: Material Support of Terrorism and the Fifth Amendment', *Georgetown Journal of Law & Public Policy* 3 (2005) 311.

Amendment, the news prompted extraordinary protests from librarians, some of whom began shredding library records to avoid being compelled to produce them.[19]

Some of the more controversial provisions of the Patriot Act had sunset clauses that expired at the end of 2005. As discussed [elsewhere], however, these new powers were accompanied by other, undisclosed expansions of the powers of US intelligence services, as well as activities by specific agencies that went well beyond their authorized powers — though sometimes with tacit approval of the executive.

The consequences of these new assertions of power were both human and systemic. Some were attributable to changes in the letter of the law; others, perhaps, to the implied spirit the new laws reflected. Nearly 100 detainees died while in US custody in Iraq and Afghanistan, 34 of whom were identified by the US military as victims of homicide. Of these, only 12 resulted in any form of punishment.[20] While the CIA was implicated in many deaths, only one person — a contractor — has been charged or convicted of a crime.[21] An unknown number of detainees were subjected to 'enhanced' interrogation, including the waterboarding of at least two dozen detainees; one, Khalid Sheikh Mohammed, was waterboarded 183 times.[22] A confidential report by the International Committee of the Red Cross (ICRC) concluded that the ill-treatment inflicted on detainees constituted torture.[23]

More than a thousand aliens were detained in the weeks and months after September 11 within the United States, many of them later deported. Hundreds were detained abroad in facilities at Guantánamo Bay, Bagram Air Field in Afghanistan, and various black sites. In addition to the human suffering caused by these actions, the damage to the moral standing of the United States abroad, and the possible chilling effect on political life at home, these excesses also caused operational problems in combating terrorism. When the FBI became aware of the enhanced interrogation methods being used by the CIA, for example, it ceased to participate in the

---

[19] Daniel J Solove, *The Digital Person: Privacy and Technology in the Information Age* (New York: New York University Press, 2004), 200-9; Dean E Murphy, 'Some Librarians Use Shredder to Show Opposition to New FBI Powers', *New York Times*, 7 April 2003; Kathryn Martin, 'The USA PATRIOT Act's Application to Library Patron Records', *Journal of Legislation* 29 (2003) 283. See generally Timothy Casey, *The USA PATRIOT Act: The Decline of Legitimacy in the Age of Terrorism* (Oxford: Oxford University Press, 2009).

[20] Hina Shamsi, Command's Responsibility: Detainee Deaths in US Custody in Iraq and Afghanistan (New York: Human Rights First, February 2006).

[21] See section 3.1.3.

[22] Scott Shane, '2 US Architects of Harsh Tactics in 9/11's Wake', *New York Times*, 12 August 2009.

[23] ICRC Report on the Treatment of Fourteen 'High Value Detainees' in CIA Custody (Washington, DC: International Committee of the Red Cross, February 2007), 26.

interrogations, exacerbating tensions between the agencies.[24] The use of such methods as the practice of extraordinary rendition also caused rifts with traditional allies of the United States, raising legal barriers to the extradition of suspects and inhibiting the sharing of intelligence.

1.2 Understanding the US Response

The reaction of the United States to the September 11 attacks has been described even by thoughtful commentators as 'panicked', with major legislation hastily passed in response to an undefined threat from a poorly understood source.[25] Friends and allies underestimated the extent to which the attacks radically changed the worldview of many Americans, but also how they exacerbated pre-existing tendencies towards unilateralism in international affairs and a unitary executive domestically. The US response was also subject to the idiosyncrasies of its political system. In deference to Second Amendment fetishists, for example, an individual listed on a terrorist watch-list could be barred from boarding an airplane but not from purchasing a firearm.[26]

Much has now been written about the Bush White House, showing how these predilections turned into policies.[27] For present purposes, two areas are of particular interest: how the challenge posed by September 11 was understood and the limited role that law played in developing the response.

The threats facing the nation were presented as requiring a 'global war on terror' — GWOT in military argot. This conceptualization framed the planet as a battlefield in which traditional rule of law restrictions might not apply, consistent with the President's Wild West rhetoric. Yet each of the words posed political and strategic problems. As was often noted, a war 'on terror' makes no sense as it essentially declares war on a tactic and is by definition unwinnable. The language of 'war' introduced two concerns: first, it suggested a military dimension to domestic

---

[24] Ali Soufan, 'My Tortured Decision', *New York Times*, 22 April 2009; A Review of the FBI's Involvement in and Observations of Detainee Interrogations in Guantanamo Bay, Afghanistan, and Iraq (Washington, DC: US Department of Justice, Office of the Inspector General, October 2009).

[25] Bruce Ackerman, *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism* (New Haven, CT: Yale University Press, 2006), 2; Philip B Heymann and Juliette N Kayyem, *Protecting Liberty in an Age of Terror* (Cambridge, MA: MIT Press, 2005), 5.

[26] Firearm and Explosives Background Checks Involving Terrorist Watch List Records (Washington, DC: Government Accountability Office, GAO-09-125R, 21 May 2009).

[27] See in particular James Mann, *Rise of the Vulcans: The History of Bush's War Cabinet* (New York: Viking, 2004); Jack Goldsmith, *The Terror Presidency* (New York: Norton, 2007); Jane Mayer, *The Dark Side: The Inside Story of How the War on Terror Turned Into a War on American Ideals* (New York: Doubleday, 2008).

counterterrorism efforts; secondly, it implicitly defined the perpetrators of attacks on civilians as 'soldiers'. Referring to a major terrorist attack on London, Britain's chief prosecutor later rejected both implications:

> London is not a battlefield. Those innocents who were murdered on July 7, 2005 were not victims of war. And the men who killed them were not, as in their vanity they claimed on their ludicrous videos, 'soldiers'. They were deluded, narcissistic inadequates. They were criminals. They were fantasists.
>
> We need to be very clear about this. On the streets of London, there is no such thing as a war on terror. The fight against terrorism on the streets of Britain is not a war. It is the prevention of crime, the enforcement of our laws and the winning of justice for those damaged by their infringement.[28]

The use of military rhetoric against an abstract noun also led to the belief on the part of some that traditional restrictions in battle might not apply. The reciprocity that characterized the emergence of laws of armed conflict is lacking in a war on terror — it is noteworthy that some of those most vocal in their opposition to the abuse of detainees were the uniformed military lawyers who understood the consequences that this might have for future claims of prisoner-of-war status by US soldiers.

In addition, however, the appellation 'global' may have constituted a strategic error in casting what is really more like 60 different groups scattered across the globe as part of a single unified fight. Seeing the worldwide enemy as al Qaeda or Islamist extremism in fact encouraged self-identification by disparate groups with, potentially, disaggregated interests: Lashkar-e-Taiba in Pakistan, Jemaah Islamiah in Indonesia, Abu Sayyaf in the Philippines, and so on.[29] In March 2009, the Department of Defense quietly issued a memorandum stating that the term 'global war on terror' would in future be replaced by the more anodyne phrase 'overseas contingency operations'.[30]

Lawyers often pay most attention to language and its consequences, and it is striking that the Bush White House included remarkably few of them. Neither the President, Vice President, Secretary of Defense, Secretary of State, nor the National Security Adviser was a lawyer. All of these positions during the Clinton

---

[28] Sir Ken Macdonald, quoted in Lucy Bannerman, 'There Is No War on Terror in the UK, Says DPP', *The Times* (London), 24 January 2007.

[29] George Packer, 'Knowing the Enemy: Can Social Scientists Redefine the "War on Terror"?', *New Yorker*, 18 December 2006, 60.

[30] Scott Wilson and Al Kamen, '"Global War on Terror" Is Given New Name', *Washington Post*, 25 March 2009.

administration were held by lawyers, with the exception of the Vice President (who had attended law school briefly). President Bill Clinton was known for reminding the lawyers who worked for him that he had previously taught constitutional law.[31]

The quantity of lawyers may not, of course, lead to good decisions. The quality of what legal advice the Bush administration did receive has also been criticized, with ethical and legal investigations of Jay Bybee and John Yoo, who wrote the so-called 'torture memos'. Jack Goldsmith, former head of the Justice Department's Office of Legal Counsel, later told the Senate Judiciary Committee that the legal justifications for the National Security Agency's (NSA) programme of warrantless electronic surveillance were deeply flawed. At one White House meeting in 2004, Goldsmith's deputy, James Comey, said that 'no lawyer' would endorse Yoo's justification for the NSA programme. David Addington, legal counsel to Vice President Cheney, disagreed, saying that he was a lawyer and found it convincing. 'No *good* lawyer,' Comey is said to have replied.[32] An internal Justice Department report ultimately concluded that Bybee and Yoo had used flawed legal reasoning but were not guilty of professional misconduct.[33]

These strategic issues of how the US response to terrorism was conceived and the role that law should play in calibrating a response tended to be ignored in the post-September 11 debates over reform of the intelligence services. Those debates were made more urgent when a second scandal rocked the US intelligence community.

2 Reform

Within the space of 18 months, from September 2001 to March 2003, the US intelligence community experienced two of its worst ever intelligence failures. The inability to prevent the September 11 attacks on New York and Washington, DC, has been compared to the strategic surprise of Pearl Harbor; flawed and manipulated intelligence in relation to Iraq has been blamed for the worst foreign policy decision in a generation, if not in the history of the United States.

---

[31] Mayer, *Dark Side*, 54.

[32] Dan Eggen, 'White House Secrecy on Wiretaps Described', *Washington Post*, 3 October 2007; Scott Shane, David Johnston, and James Risen, 'Secret US Endorsement of Severe Interrogations', *New York Times*, 4 October 2007. See now Goldsmith, *The Terror Presidency*.

[33] Eric Lichtblau and Scott Shane, 'Report Faults 2 Authors of Bush Terror Memos', *New York Times*, 19 February 2010.

Dozens of classified and unclassified reports, scores of books, and thousands of articles have since been written about these failures. Perhaps the most prominent, the 9/11 Commission Report, was a bestseller and one of very few government reports to be selected as a finalist for a National Book Award.[34] On top of a slew of works that describe the history and aftermath of each incident, various authors have set about showing how over-protection of civil liberties contributed to the vulnerability of the United States, while others argue that that vulnerability has been exploited in a sustained attack on civil liberties. There is also an expanding corpus of writing on improving the effectiveness of intelligence services, though this, too, polarizes around two ultimately contradictory positions: either agents and analysts must be liberated from bureaucracy with individual excellence encouraged, or else that bureaucracy must be strengthened to ensure that coordinated and coherent advice reaches policymakers.[35]

What is frequently lost in this burgeoning literature is the question: how important *is* intelligence, anyway? One lesson of September 11 may be that intelligence cannot always offer up clear and actionable warnings of attacks by asymmetric forces that will push a large government into action. One lesson of Iraq is that when such a government does move into action, improved intelligence may not be able to stop it. The Silberman-Robb Commission established by President Bush to investigate intelligence failures with respect to Iraq, for example, concluded that the US intelligence community was 'dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction'. It also noted, however, that that same community boasts an almost perfect record of resisting external recommendations for change.[36]

The United States has undergone three major efforts at intelligence reform since it emerged as a superpower, each case marked with the passage of legislation and institutional reform.[37] The first, in the wake of the Pearl Harbor attack, established the basic structure of its modern intelligence community after the Second World War. The second, following the Watergate scandal and during the tail end of

---

[34] 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States (Washington, DC: US Government Printing Office, 2004).

[35] See the Introduction to this volume, section 1.

[36] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Silberman-Robb Commission Report) (Washington, DC: Laurence H Silberman and Charles S Robb, co-chairs, 31 March 2005), preface, 6.

[37] Richard K Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007), 3-4.

the Vietnam War, sought to rein that community in through constraints on domestic intelligence collection and formalized oversight by Congress and a new Foreign Intelligence Surveillance Court. The third came after the September 11 attacks and saw the expansion of powers under the Patriot Act and new efforts at centralization under a Director of National Intelligence.

The barriers to reform are considerable. They include the usual obstacles posed by large bureaucracies, but also certain problems specific to the intelligence world. First, how is the mission of an intelligence service to be understood? The aims of intelligence services typically include avoiding strategic surprise, providing long-term expertise, supporting the policy process, and maintaining the secrecy of information, needs, and methods.[38] The common theme is that intelligence exists to improve the decisions of policy makers. Very different prescriptions for reform will be reached if one understands that the policy goal should be a rational weighing of costs and benefits posed by certain courses of action (or inaction), or that the goal should be preventing attacks on the homeland at any cost. A second set of questions concern how the mission of intelligence can best be achieved, in particular what legal and bureaucratic structures will improve the efficiency and effectiveness of the various agencies.

2.1 Prevention and the Dog that Didn't Bark

Establishing prevention of attacks as the test of an intelligence community's effectiveness is a dubious metric. Tactical surprise, such as an individual attack by an otherwise unknown terrorist group, cannot wholly be avoided. If it is not of sufficient magnitude to threaten the existence of the state or its way of life, occasional surprises can be managed.[39] It is also hard to prove when success has been achieved in avoiding surprise. As Sherlock Holmes once observed, it is difficult to establish why a dog *didn't* bark on a given night.[40] Assertions by government officials that terrorist plots have been discovered and averted are now frequently greeted with suspicion. Such plots — in some cases years old and not beyond the planning stages — may be

[38] Mark M Lowenthal, *Intelligence: From Secrets to Policy*, 3rd edn (Washington, DC: CQ Press, 2006), 2-5.

[39] Richard K Betts, 'Analysis, War, and Decision: Why Intelligence Failures Are Inevitable', *World Politics* 31(1) (1978) 61.

[40] Arthur Conan Doyle, 'Silver Blaze', *Strand Magazine* 4 (1892) 645.

invoked opportunistically in order to justify the troubling things that governments must do in a 'war on terror'.

Prevention can also distort discussions of reform. It is tempting to focus on cases where attacks did take place and then consider whether they might have been prevented. Thomas Copeland, for example, describes five devastating attacks on the United States and looks for explanations in failures of leadership, organizational obstacles, the volume of information available, and analytical pathologies. Yet the premise that attacks on the homeland can and should be prevented at times blinds him to the dangers of unfettered national security agencies. Copeland argues, among other things, that the prospects for averting tragedy were reduced in every case as a result of legal restrictions on intelligence collection — the sort of argument that held sway in the Justice Department after September 11, where enthusiastic lawyers sought to remove *any* constraints on the power of the executive, but from which the Bush and Obama administrations gradually retreated. Elsewhere he suggests that terrorism prevention should always be the dominant focus of any US president. Though US policy might well have been improved had President Clinton not been distracted by the Monica Lewinsky scandal in 1998, it is a stretch to blame the 1993 World Trade Center attack on Clinton's focus on 'economic and social issues', the Oklahoma City bombing on 'gun control and the Oslo Peace Accords', and so on.[41] It is also telling that a book on the failure of the United States to act on what the author asserts was adequate evidence of threats to the homeland does not mention the intelligence failures that led to the 2003 invasion of Iraq.

A more plausible critique of the poor performance of US intelligence services focuses on the under-resourcing of human intelligence. This is not helped by promotion structures that favour quantity over quality of recruits. Richard Russell worked as a political-military analyst for the CIA for 17 years and offers anecdotal evidence of junior case officers who develop second- or third-rate assets whose information is of little value but whose recruitment advances the officer's career. He describes reading a classified report on Iran and then hearing nearly identical comments from his Iranian taxi-driver on the way to the airport. Improving the quality of human intelligence requires understanding how ineffective it has been in the past, even in the days when one could meet potential contacts at a diplomatic cocktail party rather than in the tribal areas of Pakistan. His main recommendations are longer tours

---

[41] Thomas E Copeland, *Fool Me Twice: Intelligence Failure and Mass Casualty Terrorism* (Leiden: Koninklijke Brill NV, 2007), 241.

by CIA case officers, better use of walk-ins, more engagement with foreign intelligence services, and streamlining security vetting processes.[42]

Improving analytical capacity requires hiring real experts, with the model being a strong university faculty or perhaps a think tank with government connections such as the RAND Corporation. Russell's solution here is to hire fewer analysts on better terms, in particular bringing in more PhDs with real expertise in relevant areas. (Russell earned his PhD from the University of Virginia in 1997.) More effective use should be made of red teams or devil's advocates, encouraging individuals to express an unpopular dissenting opinion in order to allow decision-makers to consider alternative views. More generally, the CIA needs to foster a culture of education and learning.[43]

This is all well and good, but it is far from clear how any of it would solve the problems that Russell seeks to address. In his discussion of the failure of intelligence on Iraq's weapons of mass destruction (WMD) programme, he attributes the flawed assessment that Iraq had an active WMD capacity not to politicization of intelligence but rather to the insistence of senior CIA officers on definitive 'answers' that required the removal of caveats and equivocation. He denounces this as 'intellectual arrogance that permeates the CIA's managerial culture'.[44] Such *fausse naïveté* concerning the well-documented efforts to shape intelligence around policy is unpersuasive, but for his own argument the rejection of calls for 'answers' appears especially problematic. Strategic intelligence, to be useful, requires clarity and clarity entails risk of error. What Russell advocates is in fact greater freedom for case officers and analysts, a form of academic freedom more like the university world into which he has moved, but perhaps less likely to shape policy. As Paul Pillar — another PhD who left the CIA for academia — has written, the most remarkable thing about pre-war US intelligence on Iraq is not that it got things so wrong and misled policymakers; rather it is that intelligence played such a small role in one of the most important foreign policy decisions in decades.[45]

---

[42] Richard L Russell, *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right* (Cambridge: Cambridge University Press, 2007), 99-102, 7-13.

[43] Ibid, 119-48.

[44] Ibid, 85.

[45] Paul R Pillar, 'Intelligence, Policy, and the War in Iraq', *Foreign Affairs* 85(2) (2006) 15 at 16.

2.2 *Structures and Systems*

Where Russell repeatedly decries the organizational chart approach to intelligence reform and seeks to free case officers and analysts from bureaucracy, others like Amy Zegart argue that good organizational structures matter and can have an impact on policy successes and failures that is greater than key individuals. Zegart's aim is to bring a scholarly eye not to what went wrong but *why*. A professor at UCLA's School of Public Affairs, she worked on the Clinton administration's National Security Council Staff in 1993 and spent three years at the management consultancy McKinsey & Co. Her analysis focuses on what she claims is the single most important reason for the United States' vulnerability on September 11: 'the stunning inability of US intelligence agencies to adapt to the end of the Cold War'.[46] This suggests a somewhat rosier interpretation of Cold War intelligence than Russell, but in fact many of the deficiencies Zegart identifies have their origins in the establishment of the US intelligence architecture at the end of the Second World War, something she had described in a doctoral thesis at Stanford University supervised by Condoleezza Rice, who later became National Security Adviser before being appointed Secretary of State in the Bush White House.[47]

The missed opportunities to prevent the attacks on New York and Washington, DC, are now familiar. The CIA observed an al Qaeda planning meeting in Kuala Lumpur in January 2000, among other things gathering information on Khalid al-Mihdhar, whom it discovered had a multiple-entry visa to the United States. Yet he was put on a State Department watch-list only on 23 August 2001 — months after he had entered the country, obtained a California photo identification card, and started taking flying lessons. The FBI, for its part, failed to act on a memo from a field agent in Phoenix who warned in July 2001 that Osama bin Laden might be using US flight schools to train terrorists, and refused to seek a search warrant to investigate the computer files of Zacarias Moussaoui after he was detained. There is also the President's 6 August 2001 briefing from the CIA entitled 'Bin Laden Determined to Strike in US'.[48]

---

[46] Amy B Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2007), 3.

[47] See Amy B Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999).

[48] Zegart, *Spying Blind*, 101-19; 9/11 Commission Report, 254-77..

Echoing the approach of the 9/11 Commission — and the reason for the most vehement criticism of its findings — Zegart attributes blame for these failures not to individuals but to systemic and organizational problems. The three broad deficiencies she identifies are a culture that is resistant to change, perverse incentives that reward the wrong behaviour, and structural deficiencies that prevent the CIA, FBI, and other members of the US intelligence community cooperating effectively.

As she concedes, none of this is new. In the ten years before 2001, for example, at least six classified reports and a dozen major unclassified studies sought to improve the counterterrorism work of the intelligence services. Hundreds of recommendations were made, the vast majority of which resulted in no action whatsoever. The various recommendations made in the 1990s broadly concurred on four major problems confronting the intelligence community: personnel problems that fail to recruit and keep those with the most needed skills, insufficient resources for and unnecessary barriers to human intelligence activities, lack of coordination within and across agencies, and inadequate leadership by policymakers in setting intelligence priorities. Oddly, Zegart's own catalogue broadly corresponds to the first three problems but does not adequately address the last — leadership by policymakers — except where she notes that presidents have had little incentive to spend the political capital necessary to make major reforms.[49]

Organization theory is invoked to explore intelligence services' apparent failure to adapt. There are, however, significant limitations to applying theories designed for the private sector to the public sector, and in particular to the work of intelligence services where the imperative of secrecy adds a further complication. One of the insights of organization theory is that individual organizations do not adapt: *groups* of organizations do. This form of Darwinian selection is possible only when there is significant turnover — 'creative destruction' far more applicable to the private sector than the public. Failure to adapt will only rarely lead to the abolition of a government entity, and there may be few other incentives to change: the US Army, for example, maintained a horse cavalry until the Second World War; until the mid-1990s, customs forms required ships entering US ports to list the number of cannons on board.[50]

---

[49] Zegart, *Spying Blind*, 57.

[50] Ibid, 43-7, 50-1. See generally Joseph A Schumpeter, *Capitalism, Socialism and Democracy* [1942] (New York: Harper, 1975).

Certainly, both the CIA and FBI suffer from fundamental structural problems. The CIA is at once tasked with being the lead agency for human intelligence activities outside the United States through its National Clandestine Service (previously the Directorate of Operations), and the body that undertakes all-source national security and foreign policy analysis in its Directorate of Intelligence. In many other countries these functions are performed by different agencies in a vertical relationship that passes collected information up through analysts to policymakers — rather than setting them up in a horizontal relationship that causes predictable tension between 'cowboys' and 'Ivy Leaguers'.[51] The head of the CIA was, until April 2005, also the Director of Central Intelligence (DCI): notoriously, he had responsibility for all 16 intelligence services but little power over any but his own — in particular, the DCI had no budgetary controls over those agencies located in the Defense Department that consume the lion's share of the budget. In 1998, George Tenet produced the first strategic plan for the US intelligence community since the end of the Cold War. Only a handful of agency heads ever received it; all of them ignored it.[52]

The FBI, for its part, has a far deeper identity crisis between its domestic law enforcement and intelligence responsibilities, combining functions that in many countries are located in separate organs of government. Law enforcement long ago won this battle and J Edgar Hoover's 'G-men' and today's 'Feds' have long placed far greater emphasis on solving crimes than preventing terrorist attacks. The Phoenix memo, referred to earlier, was forwarded to a Portland FBI field office as it appeared pertinent to an ongoing criminal investigation — but it was never shared with the CIA despite an explicit request to do so within the document itself. Around the same time, during a period of intensifying warnings about possible terror attacks, the FBI's acting director held a conference call with all field office special-agents-in-charge in which he mentioned the heightened threat levels but recommended only that each field office have its evidence response teams ready to investigate an attack at short notice *after* it occurred.[53]

Even more mundane reforms have been difficult. FBI efforts at information technology modernization are, rightly, the subject of ridicule. Its main information system, the Automated Case Support (ACS) system, cost $67 million and was launched in 1995 with 1980s technology; it proved so unreliable that many agents

---

[51] Zegart, *Spying Blind*, 66-7.

[52] 9/11 Commission Report, 357.

[53] Zegart, *Spying Blind*, 156-68.

simply didn't use it, preferring to keep case files in shoeboxes under their desks. Even in 2001, the ACS system was incapable of performing a data search using more than one word. One could search for the word 'flight', for example, or 'schools' — but not 'flight schools'. FBI Director Louis Freeh had his own computer removed from his office entirely because he never used it. The September 11 attacks provided new energy to the technology reform process, but in February 2005 Robert Mueller, who had taken over as Director of the FBI just a week before September 11, abandoned the new electronic case filing system Trilogy as a $170 million failure.[54]

As for relations between the CIA and the FBI, the turf battles between the two organizations are the stuff of legend. Even the limited provision for temporary secondments came to be known as the 'hostage exchange program'.[55] Information sharing was also complicated by a legal regime that appeared to create a 'wall' between the government's intelligence and law enforcement capacities, arguably to the detriment of both.

2.3 Politics

Eight months before the March 2003 invasion of Iraq, British Prime Minister Tony Blair met with senior foreign policy and security officials to discuss the building crisis. The classified minutes, later published by London's *Sunday Times*, show that their discussion focused more on Britain's relationship with the United States than on Iraq itself. John Scarlett, head of the Joint Intelligence Committee, began the meeting with a briefing on the state of Saddam Hussein's regime. Then came an account of meetings with Bush administration officials by Sir Richard Dearlove, head of Britain's Secret Intelligence Service (MI6), known as 'C':

> C reported on his recent talks in Washington. There was a perceptible shift in attitude. Military action was now seen as inevitable. Bush wanted to remove Saddam, through military action, justified by the conjunction of terrorism and [weapons of mass destruction]. But the intelligence and facts were being fixed around the policy. The [US National Security Council] had no patience with the UN route, and no

[54] Ibid, 44, 136-9.

[55] Ibid, 79.

> enthusiasm for publishing material on the Iraqi regime's record. There was little discussion in Washington of the aftermath after military action.[56]

The disconnect between what intelligence offers a leader and the choices he or she makes is hardly new: during the Second World War, Joseph Stalin is said to have ignored 84 separate warnings from his intelligence services of the German invasion of the Soviet Union that took place in June 1941.[57] Good intelligence will not guarantee success, but bad intelligence frequently contributes to failure.[58] The various efforts at reform seek to improve the quality of intelligence available to policymakers — or to minimize the harm that it can do. The danger, however, lies frequently in how that intelligence will be used.

Quite apart from the ability to inform government policy, an emerging problem is the separation of much of intelligence from public institutions entirely, as a growing proportion of collection and, to some extent, analysis is conducted by private actors.

3 The Turn to Outsourcing

On 14 May 2007, a senior procurement executive from the Office of the Director of National Intelligence gave a presentation to an intelligence industry conference in Colorado convened by the Defense Intelligence Agency (DIA), part of the US Department of Defense. Her unclassified PowerPoint presentation, 'Procuring the Future', was posted on the DIA website, but later modified and subsequently removed. In it, she revealed that the proportion of the US intelligence budget spent on private contractors is 70 percent. By removing the scale from a table on intelligence expenditures but not the underlying figures, she also inadvertently revealed that the amount the United States spends on such contractors is $42 billion, out of an implied

---

[56] Iraq: Prime Minister's Meeting (Memorandum by David Manning; Secret and Strictly Personal — UK Eyes Only) (London: S 195 /02, 23 July 2003), available in 'The Secret Downing Street Memo', *The Sunday Times* (London), 1 May 2005.

[57] Barton Whaley, *Codeword Barbarossa* (Cambridge, MA: MIT Press, 1973).

[58] Murice R Greenberg and Richard Haass, 'Introduction', in Murice R Greenberg and Richard Haass (eds), *Making Intelligence Smarter: The Future of US Intelligence* (New York: Council on Foreign Relations, 1996), 13.

total intelligence budget of $60 billion for the 2005 financial year. At its midpoint the presentation cheerily exhorted: 'We can't spy … if we can't buy!'[59]

Though it lagged behind the privatization of military services, the privatization of intelligence expanded dramatically with the growth in intelligence activities following the September 11 attacks on the United States. In a report published three days after those attacks, the Senate Select Committee on Intelligence encouraged a 'symbiotic relationship between the Intelligence Community and the private sector'.[60] In addition to dollars spent — dominated by large items such as spy satellites — this has seen an important increase in the proportion of personnel working on contract. More than 70 percent of the Pentagon's Counterintelligence Field Activity (CIFA) unit is staffed by contractors, known as 'green badgers', who also represent the majority of personnel in the DIA, the CIA's National Clandestine Service, and the National Counterterrorism Center. At the CIA's station in Islamabad, contractors reportedly outnumber government employees three-to-one.[61]

Controversy over government reliance on outsourcing in this area frequently coalesces around issues of cost (a contractor costs on average $250,000 per year, about double that of a government employee), 'brain-drain', and periodic allegations of self-dealing and other forms of corruption. More recently, however, the confirmation by the Director of the CIA that contractors participated in waterboarding of detainees at CIA interrogation facilities has sparked a renewed debate over what activities it is appropriate to delegate to contractors, and what activities should remain 'inherently governmental'.[62] This debate is, of course, separate from whether such activities should be carried out in the first place.

Privatization of intelligence services raises many concerns familiar to the debates over private military and security companies (PMSCs). One of the key problems posed by PMSCs is their use of potentially lethal force in an environment

---

[59] Terri Everett, 'Procuring the Future: 21st Century IC Acquisition (PowerPoint Presentation)' (Defense Intelligence Agency, Keystone, Colorado, 14 May 2007); Tim Shorrock, The Corporate Takeover of US Intelligence (Salon.com, 1 June 2007); RJ Hillhouse, Update: DNI Inadvertently Reveals Key to Classified National Intel Budget, (The Spy Who Billed Me, posted 4 June 2007), available at <http://www.thespywhobilledme.com/the_spy_who_billed_me/2007/06/update_dni_inad.html>. A copy of the original PowerPoint presentation remains available from the Web site of the Federation of American Scientists.

[60] Senate Report on Intelligence Authorization Act for Fiscal Year 2002 (Washington, DC: Senate Select Committee on Intelligence, Report 107-63, 14 September 2001).

[61] Walter Pincus, 'Lawmakers Want More Data on Contracting Out Intelligence', *Washington Post*, 7 May 2006; Patrick Radden Keefe, 'Don't Privatize Our Spies', *New York Times*, 25 June 2007.

[62] Cf Sarah Percy, 'Morality and Regulation', in Simon Chesterman and Chia Lehnardt (eds), *From Mercenaries to Market: The Rise and Regulation of Private Military Companies* (Oxford: Oxford University Press, 2007), 11.

where accountability may be legally uncertain and practically unlikely; in some circumstances, PMSCs may also affect the strategic balance of a conflict.[63] The engagement of private actors in the *collection* of intelligence exacerbates the first set of problems: it frequently encompasses a far wider range of conduct that would normally be unlawful, with express or implied immunity from legal process, in an environment designed to avoid scrutiny. Engagement of such actors in *analysis* raises the second set of issues: top-level analysis is precisely intended to shape strategic policy — the more such tasks are delegated to private actors, the further they are removed from traditional accountability structures such as judicial and parliamentary oversight, and the more influence those actors may have on the executive.

3.1 Collection

Contracting out hard- and software requirements is probably the biggest single item of outsourcing, but is not significantly different from other forms of government contracting. There are occasional scandals, such as the NSA's contract with Science Applications International Corporation (SAIC) to modernize its ability to sift vast amounts of electronic information with a proposed system known as 'Trailblazer'. Between 2002 and 2005, the project's $280 million budget ballooned to over $1 billion and was later described as a 'complete and abject failure'. Perhaps the most spectacular such failure was Boeing's Future Imagery Architecture, a 1999 contract with the National Reconnaissance Office (NRO) to design a new generation of spy satellites. It was finally cancelled in 2005 after approximately ten billion dollars had been spent. Nevertheless the pool of potential contractors — in particular given the requirement for security clearances — remains small. Thus when the NSA sought a replacement to the failed Trailblazer, the contractor it retained to develop the new programme ExecuteLocus was SAIC.[64]

Somewhat more sensitive than contracts for equipment and software is direct involvement in covert operations. Abraxas, for example, a company founded by CIA veterans in McLean, Virginia, devises 'covers' for overseas case officers. In Iraq, US reliance on contractors appears to have extended also to recruiting and managing

[63] See generally Chesterman and Lehnardt (eds), *From Mercenaries to Market*; Simon Chesterman and Angelina Fisher (eds), *Private Security, Public Order: The Outsourcing of Public Services and Its Limits* (Oxford: Oxford University Press, 2009).

[64] Keefe, 'Don't Privatize Our Spies'; Philip Taubman, 'In Death of Spy Satellite Program, Lofty Plans and Unrealistic Bids', *New York Times*, 11 November 2007.

human intelligence sources.[65] In 2004, Aegis Defence Services, a British company, was awarded a $300 million contract that explicitly required hiring a team of analysts with 'NATO equivalent SECRET clearance'; responsibilities included 'analysis of foreign intelligence services, terrorist organizations, and their surrogates targeting [Department of Defense] personnel, resources and facilities.'[66]

The reasons given for reliance on private contractors in intelligence are similar for those given by the military: the need for swift increases in skilled personnel that had been scaled back during the 1990s, and the flexibility of such increases being temporary rather than adding permanent government employees.[67] Such hires have also been used to avoid personnel ceilings imposed by Congress; outsourcing may also enable the intelligence services to avoid congressional and other oversight of specific activities. Some of these justifications have been accepted but oversight bodies have emphasized that 'in the long term' the intelligence community must reduce its dependence on contractors, if only for reasons of cost.[68]

Privatization raises particular concerns in areas that may be construed as 'inherently governmental'. One test of this is where activities significantly affect the 'life, liberty, or property of private persons',[69] a test that would at least raise questions with respect to electronic surveillance, rendition, and interrogation.

3.1.1 Telecommunications Companies and Electronic Surveillance

The controversy over warrantless electronic surveillance as part of the Bush administration's 'Terrorist Surveillance Program' was discussed [elsewhere]. Legislation was passed in August 2007 to provide a legal framework for surveillance,[70] but as its sunset date of 1 February 2008 approached there was a debate over whether to extend it. The two major points of contention were the appropriate levels of oversight for such powers (the 2007 Act essentially substituted

---

[65] Greg Miller, 'Spy Agencies Outsourcing to Fill Key Jobs', *Los Angeles Times*, 17 September 2006; James Bamford, 'This Spy for Rent', *New York Times*, 13 June 2004.

[66] Steve Fainaru and Alec Klein, 'In Iraq, a Private Realm of Intelligence-Gathering', *Washington Post*, 1 July 2007.

[67] Ronald P Sanders (Associate Director of National Intelligence), 'Letter to the Editor: The Value of Private Spies', *Washington Post*, 18 July 2007.

[68] Senate Report on Intelligence Authorization Act for Fiscal Year 2008 (Washington, DC: Senate Select Committee on Intelligence, Report 110-75, 31 May 2007), 11.

[69] Policy Letter 92-1: Inherently Governmental Functions (Washington, DC: Office of Federal Procurement Policy, 23 September 1992), para 5(c).

[70] Protect America Act 2007 (US).

internal NSA processes for the requirement of FISA warrants) and, crucially, whether to grant immunity to telecommunications companies that had helped the government conduct surveillance without warrants and thus potentially exposed themselves to civil liability.[71] President Bush authorized a 15 day extension and urged Congress to grant 'liability protection' to those companies:

> In order to be able to discover enemy — the enemy's plans, we need the cooperation of telecommunication companies. If these companies are subjected to lawsuits that could cost them billions of dollars, they won't participate; they won't help us; they won't help protect America. Liability protection is critical to securing the private sector's cooperation with our intelligence efforts.[72]

John Ashcroft, Attorney General from 2001 to 2005, had weighed in earlier, arguing that, whatever one's view of warrantless surveillance and its legal basis, allowing litigation against cooperative telecommunications companies would be 'extraordinarily unfair'. As the by-line on his *New York Times* opinion piece noted, Ashcroft now heads a consulting firm with telecommunications companies as clients.[73]

The legislation ultimately lapsed. The following week, the Bush administration asserted that the government had 'lost intelligence information' because of the failure by Democrats in Congress to pass appropriate legislation, causing some telecommunications companies to refuse to cooperate. Hours later, the statement was retracted — apparently after the last holdout among the companies agreed to cooperate fully, even without new authorizing legislation.[74] Five months later, legislation was passed essentially granting the companies immunity as part of an overhaul of FISA.[75]

Examples of potential problems in outsourcing collection in this manner are not hard to find. As a result of an 'apparent miscommunication', an Internet provider complying with a warrant to forward e-mails from one account instead gave the FBI

---

[71] The number of 'contractor facilities' cleared by the National Security Agency grew from 41 in 2002 to 1,265 in 2006. Keefe, 'Don't Privatize Our Spies'.

[72] George W Bush, 'President Bush Discusses Protect America Act' (Washington, DC, 13 February 2008).

[73] John Ashcroft, 'Uncle Sam on the Line', *New York Times*, 5 November 2007.

[74] Dan Eggen and Ellen Nakashima, 'Spy Law Lapse Blamed for Lost Information; Some Telecom Firms not Cooperating for Fear of Liability, US Says', *Washington Post*, 23 February 2008; Josh Meyer, 'White House Backtracks on Lost Intelligence; Officials Acknowledge that Telecom Firms Are Furnishing All Requested Information', *Los Angeles Times*, 24 February 2008.

[75] Foreign Intelligence Surveillance Act of 1978 Amendments Act 2008 (US), § 802.

e-mails from every account on the domain for which it served as host. Intelligence officials refer to this as 'overproduction', when third parties provide them with more information than actually required.[76] In the case of the NSA's programme, the absence of the requirement for a warrant, the secrecy of the programme, and the self-interest of companies engaging in legally questionable activity suggest little reason for confidence in oversight. Legislators only became involved after the story had become public.

Such issues are not, of course, limited to the United States. In March 2008, for example, India's government threatened to ban Research In Motion's BlackBerry service unless the company facilitated decryption of communication across its network. The admission that India was incapable of breaking the BlackBerry code was unusual, but an agreement was eventually concluded allowing RIM to sell its smart-phones, presumably with some provision allowing for government interception of data.[77]

3.1.2 Private Aircraft and Rendition

In the case of telecommunications companies, involvement of private actors was necessary as a technical matter in order to access information. With respect to private involvement in rendition, recourse to the private sector appears to have been part of a clear effort to avoid oversight.

The CIA's use of private aircraft for moving detainees between black site detention centres is now well documented. Enterprising journalists, blogger activists, and hobbyist plane spotters combined to share information about planes that are believed to have been at the heart of the 'extraordinary rendition' programme,[78] which was originally authorized under the Clinton administration.[79] The use of proprietary or 'front' companies by the CIA is not unusual, though reliance upon private companies for active support rather than cover is atypical. Officials who were involved in the practice suggested this was in order to protect government officials from involvement

---

[76] Eric Lichtblau, 'Error Gave FBI Unauthorized Access to E-Mail', *New York Times*, 17 February 2008.

[77] Matt Hartley, 'RIM's Double-edged Encryption Sword', *Globe and Mail* (Toronto), 28 May 2008; Ashwini Shrivastava, 'Govt, Blackberry Makers to Jointly Resolve Security Issues', *The Press Trust of India*, 2 October 2008; Rick Westhead, 'Indian Investment', *Toronto Star*, 17 October 2009.

[78] Stephen Grey, *Ghost Plane: The True Story of the CIA Torture Program* (New York: St. Martin's Press, 2006); Jane Mayer, 'Outsourcing: The CIA's Travel Agent', *New Yorker*, 30 October 2006.

[79] Presidential Decision Directive 95: US Policy on Counterterrorism (PDD-95) (Washington, DC: White House, 21 June 1995)..

in a legally questionable process.[80] The rendition programme became a scandal in Europe, with a report from the European Parliament leading to a resolution recommending, among other things, that 'all European countries that have not done so should initiate independent investigations into all stopovers made by civilian aircraft carried out by the CIA'.[81]

3.1.3 Green Badgers and Interrogation

A third area in which outsourcing has taken place is interrogations. In February 2008, CIA Director Michael Hayden testified before the Senate and House — appearances most memorable for his confirmation that the United States had waterboarded at least three detainees.[82] He was also asked about the use of contractors. Before the Senate Select Intelligence Committee he confirmed that the CIA continued to use 'green badgers' at its secret detention facilities.[83] In testimony before the House two days later he was asked whether contractors were involved in waterboarding al Qaeda detainees. He responded by saying 'I'm not sure of the specifics. I'll give you a tentative answer: I believe so.'[84]

The involvement of private contractors in interrogations raises the most serious questions about accountability of persons outside government wielding extraordinary authority and discretion in an environment clearly weighted against either investigation or prosecution. As in the case of private military contractors using potentially lethal force in a conflict zone, these concerns include the dubious prospect of after the fact accountability, but also the absence of standardized levels of training or a defined command structure.

Both sets of concerns were proven justified after revelations that detainees had been abused at the Abu Ghraib prison in Iraq. No charges have been laid against contractors, despite repeated allegations that they participated in abuse. The companies Titan and CACI provided interpreters and interrogators to the US military

---

[80] Dana Priest, 'Jet Is an Open Secret in Terror War', *Washington Post*, 27 December 2004.

[81] Transportation and Illegal Detention of Prisoners: European Parliament Resolution on the Alleged Use of European Countries by the CIA for the Transportation and Illegal Detention of Prisoners (P6_TA-PROV(2007)0032-(2006/2200(INI)), 2007), para 190.

[82] Scott Shane, 'CIA Chief Doubts Tactic to Interrogate Is Still Legal', *New York Times*, 8 February 2008.

[83] Annual Worldwide Threat Assessment Hearings (Washington, DC: Senate Select Committee on Intelligence, 5 February 2008), 26 (referring to 'greenbaggers', presumably a transcription error).

[84] Annual Worldwide Threat Assessment Hearings (Washington, DC: House Permanent Select Committee on Intelligence, 7 February 2008), 26.

respectively; the commanding officer at the prison, Brigadier General Janis Karpinski (later demoted to colonel), claimed in an interview with a Spanish newspaper that she had seen a letter signed by Secretary of Defense Donald Rumsfeld allowing civilian contractors to use techniques such as sleep deprivation during interrogation.[85] A class action against Titan and CACI under the Alien Tort Claims Act was lodged in 2004 and is ongoing in the US District Court for the Southern District of California. The case against Titan was dismissed as its linguists were found to have been 'fully integrated into the military units to which they were assigned and that they performed their duties under the direct command and exclusive operational control of military personnel.' As CACI interrogators were subject to a 'dual chain of command', with significant independent authority retained by CACI supervisors, the case against it was allowed to continue.[86]

There appears to be only one case of a contractor being convicted of a crime in the United States connected with interrogations during the 'war on terror'. David Passaro, a contractor working for the CIA, was convicted of misdemeanour assault and felony assault with a dangerous weapon charges for his connection with the torture and beating to death of Abdul Wali in Afghanistan in June 2003. In February 2007, Passaro was sentenced to eight years and four months prison. His background is testimony to the danger of contracting out such interrogations: both his previous wives have alleged that he was abusive at home, and he had been fired from the police force after being arrested for beating a man in a parking lot brawl.[87] Soon after the Passaro story broke a 'Detainee Abuse Task Force' was established, but does not appear to have brought any charges against contractors.[88]

3.2 Analysis

The involvement of contractors in analysis raises somewhat different questions from their involvement in collection of intelligence. A company's analytical work is less likely to be linked to abusive behaviour or the type of activities typically discussed in

---

85 'Rumsfeld Okayed Abuses Says Former US Army General', *Reuters*, 25 November 2006.

86 *Ibrahim v Titan*, 556 F Supp 2d 1, 28-30 (DC, 2007).

87 James Dao, 'A Man of Violence, or Just "110 Percent" Gung-Ho?', *New York Times*, 19 June 2004. See also EL Gaston, 'Mercenarism 2.0? The Rise of the Modern Private Security Industry and Its Implications for International Humanitarian Law Enforcement', *Harvard International Law Journal* 49 (2008) 221 at 229.

88 Susan Burke, 'Accountability for Corporate Complicity in Torture', *Gonzaga Journal of International Law* 10 (2006) 81 at 85; Corporate Accountability in the "War on Terror" (New York: Amnesty International USA, 2007).

the context of private military contractor accountability. Nevertheless, through its participation in and influencing of high-level decisions about national security, the consequences are troubling if they indicate a removal of such decisions from democratically accountable structures.[89]

For the most part, problems in this area have tended to be at the level of personnel, notably the drain encouraged by significantly higher salaries in the private sector. A practice known as 'bidding back' sees officials leaving for industry and then being brought back in the capacity of consultant at a higher salary. Some estimate that as many as two-thirds of the Department of Homeland Security's senior personnel and experts have left for industry in recent years.[90] A 2006 report by the Office of the Director of National Intelligence noted that the intelligence community increasingly finds itself in competition with its contractors:

> Confronted by arbitrary staffing ceilings and uncertain funding, components are left with no choice but to use contractors for work that may be borderline 'inherently governmental' – only to find that to do that work, those same contractors recruit our own employees, already cleared and trained at government expense, and then 'lease' them back to us at considerably greater expense.[91]

From 1 June 2007, the CIA began to bar contractors from hiring former agency employees and then offering their services back to the CIA within the first year and a half of retirement.[92]

As indicated earlier, a second general concern is the cost of retaining contractors. In May 2007, the Senate Select Committee on Intelligence criticized the intelligence services' 'increasing reliance on contractors'.[93] The CIA subsequently announced that it would reduce the number of contractors by ten percent.[94]

---

89 A separate concern would be the potential for misuse of personal data..

90 Keefe, 'Don't Privatize Our Spies'; Bamford, 'This Spy for Rent'.

91 The US Intelligence Community's Five Year Strategic Human Capital Plan (An Annex to the US National Intelligence Strategy) (Washington, DC: Office of the Director of National Intelligence (ODNI), 22 June 2006), 6.

92 Walter Pincus and Stephen Barr, 'CIA Plans Cutbacks, Limits on Contractor Staffing', *Washington Post*, 11 June 2007.

93 Senate Report on Intelligence Authorization Act for Fiscal Year 2008, 11.

94 Keefe, 'Don't Privatize Our Spies'; Mark Tarallo, 'Hayden Wants Fewer CIA Contractors', *Federal Computer Week*, 25 June 2007.

In addition to individual contractors, firms such as Booz Allen Hamilton have established themselves as consultants to the intelligence community. Booz Allen currently employs a former CIA director (R James Woolsey), a former executive director of the President's Foreign Intelligence Advisory Board (Joan Dempsey), and a former director of the National Reconnaissance Office (Keith Hall). Mike McConnell headed the NSA and then went to Booz Allen in 1996 as a Senior Vice President working on intelligence and national security issues; in 2007, President Bush appointed him as Director of National Intelligence.[95] Dedicated human resources personnel handle job applicants with security clearances.

Though there are occasional breathless accounts of contractor involvement in high-level analytical documents such as the President's Daily Brief,[96] it is enough to note that even the perception of a conflict of interest should raise questions about the involvement of the corporate sector in the analytical functions of the intelligence services. It might be argued that this is little different from the influence of wealth on US politics more generally, though the secrecy, incentive structures, and potentially abusive powers of the intelligence community warrant special care in regularizing the participation of private actors.

3.3 Accountability

Oversight and review of intelligence services is always difficult given the secrecy necessary for many of their activities to be carried out effectively. In the case of privatization of these services within the US intelligence community, however, secrecy appears to have compounded ignorance.

In May 2007 — the same month as the 'We can't spy … if we can't buy!' presentation — the House Permanent Select Committee on Intelligence reported that the leaders of the US intelligence community

> do not have an adequate understanding of the size and composition of the contractor work force, a consistent and well-articulated method for assessing contractor performance, or strategies for managing a combined staff-contractor workforce. In addition, the Committee is concerned that the Intelligence Community does not have

[95] Tim Shorrock, The Spy Who Came In from the Boardroom (Salon.com, 8 January 2007).

[96] See, eg, RJ Hillhouse, Corporate Content and the President's Daily Brief, (The Spy Who Billed Me, posted 23 July 2007), available at <http://www.thespywhobilledme.com/the_spy_who_billed_me/2007/07/corporate-conte.html>.

> a clear definition of what functions are 'inherently governmental' and, as a result, whether there are contractors performing inherently governmental functions.[97]

Legislators subsequently called for the Department of Defense to compile a database of all intelligence-related contracts, and for a Government Accountability Office investigation of contractors in Iraq.[98]

Reports have been commissioned before. In fact, only one month before the House report a year-long examination of outsourcing by US intelligence services was held up by the Director of National Intelligence, and then reclassified as a national secret.[99] The secrecy was justified on the basis that the United States does not reveal the cost and size of its intelligence operations, though recent disclosures on that topic by senior officials belie this explanation.

Such information as does exist about the involvement of contractors often remains classified. Much is available to the contractors themselves, however, who are able to lobby members of Congress using that information. SAIC, for example, spent well over a million dollars in each of the past ten years on lobbying; in that period it was awarded between one and three billion dollars in government contracts annually. Earmarks, in which members of Congress add provisions to legislation directing funds to specific projects, have long been tacitly accepted in the intelligence sector but rarely made public. In some cases a list of the amounts of projects might be made available, but redacting the names of companies.[100] In November 2007, Congress broke with tradition by releasing information about $80 million worth of earmarks included in a defence appropriations bill.[101]

As is frequently the case, this new found transparency was driven by scandal. The previous year Randy 'Duke' Cunningham, a Republican Congressman from California, had been sentenced to eight years in prison for accepting $2 million in

---

97 House of Representatives Report on Intelligence Authorization Act for Fiscal Year 2008 (Washington, DC: Permanent Select Committee on Intelligence, Report 110-131, 7 May 2007), 42. Cf Conference Report on Intelligence Authorization Act for Fiscal Year 2008 (Washington, DC: House of Representatives, Report 110-478, 6 December 2007), 68.

98 Walter Pincus, 'Defense Agency Proposes Outsourcing More Spying', *Washington Post*, 19 August 2007; Fainaru and Klein, 'In Iraq, a Private Realm of Intelligence-Gathering'.

99 Scott Shane, 'Government Keeps a Secret After Studying Spy Agencies', *New York Times*, 26 April 2007; RJ Hillhouse, 'Who Runs the CIA? Outsiders for Hire', *Washington Post*, 8 July 2007.

100 Shorrock, Corporate Takeover.

101 Roxana Tiron, 'Congress Discloses Intel Earmarks for First Time', *The Hill*, 24 November 2007. See Conference Report on Making Appropriations for the Department of Defense for the Fiscal Year Ending September 30, 2008, and for Other Purposes (Washington, DC: House of Representatives, Report 110–434, 6 November 2007), 378-9.

bribes from MZM, a defence contractor. Cunningham had used his position on the House appropriations and intelligence committees to win MZM tens of millions of dollars' worth of contracts with the CIA and the Pentagon's CIFA office. In a related case, Kyle 'Dusty' Foggo, a former executive director of the CIA (its third-ranking official), was indicted for conspiring with former MZM CEO Brent Wilkes (who inexplicably lacked a folksy nickname) to direct contracts to the company.[102]

In addition to undermining effective oversight either by formal or informal means, such as media scrutiny, access to secrets creates the possibility of abuse of those secrets. In 2006, the Boeing Corporation, a major defence contractor, agreed to a $565 million civil settlement arising from its use of sensitive bid information to win rocket launch contracts. The information had been provided by an engineer formerly employed by a competitor for the contracts, who had moved to the Department of Defense.[103]

The abuse of sensitive information is suggestive of the potential conflict of interest on the part of private actors engaged in intelligence activities. Discussions of this issue frequently paint a somewhat idealized picture of the patriotism and competence of full-time government employees, but there are reasonable grounds to be wary of inserting a profit motive into intelligence activities. The former head of the CIA's clandestine service has been quoted as saying that 'There's a commercial side to it that I frankly don't like … I would much prefer to see staff case officers who are in the chain of command and making a day-in and day-out conscious decision as civil servants in the intelligence business.'[104]

It is also arguable that the freedom to outsource alters the incentives of the intelligence services themselves. John Gannon, a former CIA Deputy Director for Intelligence and now head of BAE Systems' Global Analysis Group, has noted that this freedom offers flexibility but also avoids the need to justify a fulltime employee and allocate responsibility, thereby breeding duplication and inhibiting collaboration. In the 1980s, 'what we discovered was that having smaller numbers forced collaboration, and collaboration was a good thing. As soon as you start throwing money at the intelligence community, not only does it lead to more contractors, it also

---

[102] Shorrock, Corporate Takeover.

[103] Semiannual Report to the Congress, April 1, 2006-September 30, 2006 (Washington, DC: Inspector General, United States Department of Defense, 2006), 55.

[104] Miller, 'Spy Agencies Outsourcing' (quoting James Pavitt).

leads to individual units thinking "We want to get one of our own."'[105] This in turn makes it harder to contain costs.

It is possible, of course, that a profit motive may encourage *better* behaviour through the operation of a kind of market. There is evidence that this may be happening gradually in the context of PMSCs, particularly through professionalization of the industry and the creation of industry associations such as the British Association of Private Security Companies and the International Peace Operations Association. The move is largely being driven by self-interest as some actors seek to establish themselves as 'legitimate' and thereby raise the costs of entry for competitors while enabling the charging of higher fees for similar services.[106]

Markets can indeed be an effective form of regulation, but they operate best where there is competition, an expectation of repeat encounters, and a free flow of information. It is far from clear that these qualities apply to the commercial military sector; there is even more reason to be wary of embracing such a philosophy in the realm of intelligence.

Competition is severely restricted by the requirement that intelligence contractors meet security clearances. The process of granting new clearances is famously inefficient while the government frequently needs to hire people quickly.[107] The 'market' thus tends to be dominated by former military and civilian officials who already have such clearances, exacerbating the 'brain drain' cited earlier and creating predictable monopoly-type problems.

Though this arrangement has led to some established relationships with a select group of firms, in respect of individuals being retained to collect human intelligence — especially interrogators and interpreters — the need to get personnel on the ground and results back home has negated considerations of repeat encounters. As in the case of PMSCs, the assumption that such activities are atypical reduces the incentive to use any leverage that does exist to require adequate training or oversight.[108]

---

[105] Sebastian Abbot, 'The Outsourcing of US Intelligence Analysis', *News21*, 28 July 2006 (quoting John Gannon).

[106] Simon Chesterman and Chia Lehnardt, 'Conclusion: From Mercenaries to Market', in Chesterman and Lehnardt (eds), *From Mercenaries to Market*, 251 at 254-5.

[107] Lawrence Wright, 'The Spymaster', *New Yorker*, 21 January 2008, 42.

[108] See, eg, Martha Minow, 'Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy', *Boston College Law Review* 46 (2005) 989 at 1005-16.

Finally, and most obviously, the secrecy necessary for certain intelligence operations undermines the possibility of information flowing freely. In some circumstances there may be collusion in avoiding oversight, as when activities — such as rendition — are outsourced precisely for this reason. More generally, the movement of a limited number of individuals between the government and private intelligence worlds may encourage a form of regulatory capture if government employees are nominally tasked with overseeing former colleagues and future employers.

3.4 'Inherently Governmental' Functions

The simplest way of containing many of these problems would be to forbid certain activities from being delegated or outsourced to private actors at all. Intelligence services have a chequered history of abuse, but their legitimate activities tend to be justified in established democracies by reference to their grounding in the rule of law — a relatively recent requirement in some countries — and the existence of an accountability chain to democratic institutions.[109]

In the United States, this question is framed in the language of 'inherently governmental' functions, which are presumed to be carried out by government employees only. Debates concerning public functions in the United States frequently emphasize not the need to maintain certain functions in public hands but rather to justify passing them to the government in the first place; the definition of 'inherently governmental' has thus emerged not as a sphere to be protected, but as an exception to the more general push to privatization. Legislation adopted by Congress in 1998 as part of a larger privatization effort required government agencies to identify inherently governmental functions in order to enable cost comparisons between private bids and public budgets for everything else. An inherently governmental function was defined as a 'function that is so intimately related to the public interest as to require performance by Federal Government employees.'[110]

The Government Accountability Office (GAO) noted in a 2002 report that there had been some uncertainty about how to apply this broad definition, but argued that it was 'clear that government workers need to perform certain warfighting,

[109] See generally Hans Born and Marina Caparini (eds), *Democratic Control of Intelligence Services: Containing Rogue Elephants* (Aldershot: Ashgate, 2007).

[110] 31 USC § 501 note.

judicial, enforcement, regulatory, and policy-making functions … Certain other capabilities, … such as those directly linked to national security, also must be retained in-house to help ensure effective mission execution.'[111] Uncertainties about the limits continue, however, and the Department of Defense in particular has failed to adopt or apply a clear interpretation.[112]

The executive has adopted various guidelines seeking to define what is meant by the term. The 1983 version of an Office of Management and Budget (OMB) circular stated that 'Certain functions are inherently Governmental in nature, being so intimately related to the public interest as to mandate performance only by Federal employees.' The definition was said to include 'those activities which require either the exercise of discretion in applying Government authority or the use of value judgment in making decisions for the Government' and embraced 'direction of intelligence and counter-intelligence operations'.[113] A 1992 'Policy Letter' from the Office of Federal Procurement Policy essentially repeated the same text, but also included 'the interpretation and execution of the laws of the United States so as to … significantly affect the life, liberty, or property of private persons'.[114] The illustrative list of examples provided in an appendix included the 'direction *and control* of intelligence and counter-intelligence operations'.[115]

A 2003 revision kept the general definition in place, but opened up significant loopholes by allowing for activities to be performed by contractors 'where the contractor does not have the authority to decide on the course of action, but is tasked to develop options or implement a course of action, with agency oversight'. The revision also dropped any reference to intelligence or counter-intelligence operations. Another aspect of the Circular worthy of note is the ability of the Defense Department to 'determine if this circular applies to the Department of Defense during times of a

---

[111] Commercial Activities Panel: Improving the Sourcing Decisions of the Federal Government (Washington, DC: US General Accounting Office (GAO), GAO-02-847T, 27 September 2002), 21.

[112] Steven L Schooner, 'Contractor Atrocities at Abu Ghraib: Compromised Accountability in a Streamlined, Outsourced Government', *Stanford Law and Policy Review* 16 (2005) 549 at 554-7.

[113] OMB Circular No A-76: Performance of Commercial Activities (superseded) (Washington, DC: White House Office of Management and Budget, 1983), paras (b), (e).

[114] Policy Letter 92-1, para 5(c).

[115] Ibid, Appendix A, para 8 (emphasis added). Cf OMB Circular No A-76: Performance of Commercial Activities (Revised 1999) (superseded) (Washington, DC: White House Office of Management and Budget, 1999).

declared war or military mobilization'.[116] It is not clear whether this provision has been implemented.

In the absence of strong political direction, there is little prospect of intelligence services adopting a robust definition of 'inherently governmental' functions. In any case, the significance of this limitation is diminished by the ability to outsource even inherently governmental functions in so far as they may be construed merely as implementing policy with some form of oversight.

With respect to the activities considered in this paper, electronic surveillance by telecommunications companies may be an acceptable or necessary delegation of the implementation of government policy, though in some circumstances it might have fallen foul of the broader 'control' of intelligence operations test included in the 1992 Policy Letter. Rendition might also be construed as mere implementation of government policy, though it may violate other laws — notably including those of the territories through which CIA transport planes have passed.[117] There would, however, seem to be some prospect for agreement at the political level that interrogation of detainees falls 'squarely within the definition of an inherently governmental activity'. [118] Analysis by private contractors is somewhat trickier: clearly if it amounted to direction or the exercise of government discretion this would cross the line, but in most circumstances it would be easy to construe the work as merely 'developing options'.

Uncertainty in this area appears to be intentional and thus exacerbates the accountability challenges posed by secrecy and problematic incentives. At the very least, the responsibility to determine what is and is not 'inherently governmental' should itself be an inherently governmental task.

---

[116] OMB Circular No A-76 (Revised): Performance of Commercial Activities (Washington, DC: White House Office of Management and Budget, 29 May 2003), Attachment A: Inventory Process, para B(1)(a)-(c), 5(h).

[117] See Monica Hakimi, 'The Council of Europe Addresses CIA Rendition and Detention Program', *American Journal of International Law* 101 (2007) 442.

[118] Dianne Feinstein, Letter to the Honorable Michael B Mukasey, Attorney General of the United States (6 February 2008); Gorman, 'CIA Likely Let Contractors Perform Waterboarding'.

4 Back to the Light?

'Americans will always do the right thing,' Winston Churchill once observed, 'after they've exhausted all the alternatives.' In the wake of the repudiation of torture, renewed vigilance on the part of the judiciary, and the falling of scales from the eyes of the American public, there is some reason to hope that the cliché will be borne out.

Difficulties remain. On the second full day of his presidency in January 2009, Barack Obama issued executive orders to close the detention facility at Guantánamo Bay, end the CIA's secret prison programme, and renounce torture.[119] Yet the closure of Guantánamo presented the question of where detainees could be held or how they could be tried: some were released, others transferred to detention in third countries, while many remain in a legal limbo. The closure of secret prisons has not halted the growth of the detention facility at Bagram Air Field outside Kabul, which is less visible and attracts less criticism than its counterpart in Cuba. The renunciation of torture was accompanied by agonized debate over the extent to which past actions should be the subject of investigation.

The surveillance powers of the state have, to some extent, been regularized, though anecdotal evidence continues to emerge that rules are routinely disregarded. One trend that shows little sign of abating is the reliance upon private actors. Indeed, under the Obama administration there was a significant increase in the use of unmanned drones for targeting alleged terrorists in the Afghanistan-Pakistan border region. These drones, technically under the control of the CIA, are maintained by Xe Services — the corporate reincarnation of Blackwater.[120]

Reliance on the private sector is, to some extent, inevitable. Procuring hardware and software from the private sector and engaging in electronic surveillance through the cooperation of telecommunications companies may be the only way to carry out such functions effectively. More troubling are those circumstances in which outsourcing has been undertaken to avoid oversight, as in the case of rendition, where it places the life or liberty of persons in the hands of private actors, as in the case of interrogation, or where it renders the formulation of national security policy susceptible to actual or apparent influence.

---

[119] Scott Shane, Mark Mazzetti, and Helene Cooper, 'Obama Reverses Key Bush Security Policies', *New York Times*, 22 January 2009.

[120] Simon Chesterman, 'Blackwater and the Limits to Outsourcing Security', *International Herald Tribune*, 13 November 2009.

Consideration of these issues has tended to focus on overblown costs, drains on government personnel, and episodic outrage at scandals in the form of corruption or, more recently, abuse. Addressing the problems raised by privatization of intelligence services requires engagement with the structural bars to accountability; accepting the necessary secrecy of much — but not all — of these activities requires a corresponding limitation on their further removal from public scrutiny. Understanding the incentives also suggests the need for wariness in embracing a market regulatory approach to the problem. Clarity could most effectively be achieved by a transparent definition of what functions should be 'inherently governmental', though this requires political capital that is unlikely to be spent in the absence of scandal.

Such a scandal in the form of Blackwater's activities in Iraq — in particular the killing of 17 civilians in Baghdad in September 2007 — pushed the United States and Iraq to revisit the accountability of private military companies. Despite revelations that contractors employed by the US government appear to have engaged in torture, in the form of waterboarding, this was insufficient to start a major debate on the topic. Instead, reforms — if any — seem most likely to come because each of those torturers cost the US taxpayer double the salary of a Federal employee.