Chapter 5 - ‘Partnerships’ in trouble: The emergence of accountability problems and triggers

This chapter examines how the intelligence community’s reliance on the private sector has impacted on the intelligence accountability process between 2001 and 2009. Two parts of this process are examined in detail: the occurrence of accountability problems and the accountability holders’ awareness of, and reactions to, these problems. Accountability problems typically emerge when the conditions for accountability to occur such as favourable political and legal standards, accountability holders’ access to information and the availability and the use of sanctions are not fulfilled. During the presidency of George W. Bush, the accountability standards guiding public-private intelligence ‘partnerships’ were notably affected by the government’s priorities and after 9/11 the executive and legislative branches of government favoured effective security sometimes at the cost of efficiency and liberal democratic values. In this context, deficiencies in the domain of contract management became particularly apparent and the evolution of public-private intelligence ‘partnerships’ generated a need for more adequate legal standards. The growth of public-private interactions also raised legitimate concerns about the influence of the private sector on the standards followed by public accountability holders. In addition, accountability holders’ access to information from private companies was complicated by a series of legal and organisational factors, and sanctions (when they existed) were not applied consistently. This enforcement problem can be related to a lack of legal clarity, organisational difficulties and, above all, a lack of political willingness within government to apply sanctions. Overall, from 2001 to 2009, the accountability regime applying to public-private intelligence ‘partnerships’ was imperfect and hampered by hasty privatisation.

In the course of the presidency of George W. Bush, the existence of problems regarding public-private intelligence ‘partnerships’ became increasingly apparent to accountability holders. A series of incidents triggered reactions from key intelligence accountability holders and this chapter distinguishes between light triggers, or incidents generating reactions that are essentially limited to some accountability holders, and heavy triggers, or incidents generating sustained reactions from most accountability holders including society. The existence of light triggers demonstrates a continuous awareness of some problems among policy-makers and some executive agencies such as the CIA Office of the Inspector General. However, in the absence of sustained media coverage, the
accountability holders’ activity reached a limited audience. Between 2002 and 2006 a succession of high-profile incidents involving the private sector fostered public scrutiny of public-private intelligence ‘partnerships’. Executive, legislative and judicial reactions to these heavy triggers, and media exposure, were significant. These scandals crystallised accountability around four issues: conflicts of interests, efficiency, human rights, and civil liberties. Together they forced the US government to consider the imperative for change.

Accountability problems

Accountability standards

Government priorities and management deficiencies
Following the 9/11 attacks, policy-makers and senior intelligence officials prioritised effective national security to the detriment of liberal democratic values and efficiency. This political decision was clearly expressed by President Bush when, to justify ‘the largest increase in defense spending in two decades’, he considered that ‘the price of freedom and security is never too high’.¹ This resolute defence of ‘freedom and security’ impacted on the way public-private intelligence ‘partnerships’ were carried out. Senior intelligence managers have admitted that, in the context of crisis that followed 9/11, contract management was not considered as a priority by the intelligence community’s leadership. Michael Hayden, the former director of the NSA and the CIA, recognised that the intelligence community was ‘effective’ but not ‘efficient’ in the years following the 9/11 attacks and explained ‘there’s no way we could have done it that quickly, that rapidly, that expansively, and had done it well, had done it efficiently’.² In other words, he has suggested that during his tenure, the administration prioritised results, or effective national security, over cost-effectiveness.

Under the authority of George W. Bush, executive control of intelligence contractors was wanting. At the strategic level, the intelligence community did not plan its reliance on the private sector and senior intelligence officials did not keep track of the number of contractors.³ With hindsight, officials have emphasised that the government procurement

model makes counting contractors more complicated than counting government employees. For example, individual contractors may work for a series of companies at the same time, and do not always work for a full year. Yet, the difficulty of the task does not explain the absence of overall effort to collect data on the aggregate number of intelligence community contractors before 2006. Up to then, the 16 agencies forming the intelligence community had ‘no single standard to count or distinguish contractors’. In this context, congressional committees - which often rely on the executive branch to access information about intelligence activities - could not be expected to seriously oversee the evolution of public-private intelligence ‘partnerships’. The Senate Select Committee on Intelligence (SSCI) complained in 2006 that it had ‘seen no metrics that would link the additional proposed personnel to improvements in the Intelligence Community’s ability to detect, predict, analyse, and counter current and future threats to the United States’. Put simply, the intelligence community expanded its reliance on the private sector without knowing whether it would improve its capabilities at the margins. Similarly, the House Permanent Select Committee on Intelligence (HPSCI) concluded in 2007 that US officials ‘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’. Under such conditions, it is legitimate to speculate whether or not functions vital to national security were being contracted beyond the government’s capability for control.

In order to spot abuses and apply adequate sanctions, the government needed a contract management workforce able to maintain ‘adequate civilian oversight over intelligence operations’. After 9/11, this specialised workforce faced multiple challenges.

\[\text{4 Congressional Budget Office, Contractors’ Support of U.S. Operations in Iraq, August 2008, p10.}\]
\[\text{6 Sanders, Results of the Fiscal Year 2007 U.S. Intelligence Community Inventory of Core Contractor Personnel, p.13.}\]
\[\text{7 Paula J. Roberts, Statement before the US Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, 112th Congress, 1st sess., 20 September 2011, p.31.}\]
\[\text{10 Patrick T. Henry, Department of the Army, Office of the Assistant Secretary, Manpower and Reserve Affairs, Intelligence Exemption, 26 December 2000, p.2. For a similar expectation, see: Office of Federal Procurement Policy, Policy Letter 92-1 to the Heads of Executive Agencies and Departments, 23 September 1992.}\]
because it had been significantly downsized in the 1990s. In addition, rapid technological development, especially in the realm of information technology, further complicated intelligence acquisitions programmes and contract arrangements, which required further workforce adaptation. However, while outsourcing boomed from 2001 onwards, the contract management workforce did not significantly expand. This was particularly problematic since, as the former Director of the Defense Contract Audit Agency remarks ‘when contractors grow that fast, the procedures, processes, and systems have trouble keeping up’. In this light, it should not come as a surprise that the workforce embraced ‘whatever means necessary to meet its customers’ needs.

Numerous reviews and experts identified significant shortfalls plaguing contractor management in the realm of defence and national security during the GWOT. Criticisms concerned many components of the IC and focussed on the paucity of a contract management workforce, its lack of experience and the inadequacy of the procedures followed by this workforce. The Gansler Commission pointed out in 2007 that contracting officer representatives (COR), who play a central role in controlling contractors during overseas operations, were poorly trained and valued within the armed forces. An external report from the Intelligence and National Security Alliance (INSA) in 2008, an interest group supporting the intelligence industry, emphasised a lack of ‘acquisition and procurement officials available to review and process contracts, many of whom are over-extended and under-experienced’. A degradation of resources affected the DOD Inspector General (IG) who

11 Former Senior Intelligence Official A, interview with author, 8 August 2011, Washington DC.
17 Commission on Army Acquisition and Program Management in Expeditionary Operations (Gansler Commission), Urgent Reform Required : Army Expeditionary Contracting, 31 October 2007, p.3.
considered that, as a result of cuts, it was ‘not able to provide sufficient audit coverage of DoD acquisition programs given the dollars expended by the Department.’ Former senior officials have argued that the government had lost part of its ability to understand how to acquire and manage the capabilities it needed during this time. A report by the ODNI noted that ‘some IC elements lack strong program and procurement offices; clearly defined program requirements, performance measures, and acceptance terms; and program management systems to support the acquisition decision-making process.’ In the mid-2000s, the Baltimore Sun reported that the NSA lacked ‘mechanism to systematically assess whether it is spending its money effectively and getting what it has paid for’. A recent report from the ODNI IG recognised that, as a result of the agency’s lack of strategic and human capital planning, ‘there is not a road map upon which to plan for the effective application and management of core contractor workforce’. In addition, the report found that within the agency itself, the ODNI ‘has not implemented internal controls necessary to ensure the acquisition process is meeting its needs’. On the whole, it is reasonable to argue that the IC struggled to manage public-private ‘partnerships’.

### Inadequate standards

Between 2001 and 2009, the existence and application of political and legal standards to public-private intelligence ‘partnerships’ were inadequate. Yet, within the intelligence community, government employees were in charge of controlling the contractor workforce. Since 2002, ‘each component of the IC has a designated Chief Human Capital Officer or similar official who is responsible for developing workforce strategy, attracting and retaining

---

19 Department of Defense, Office of the Inspector General, Department of Defense Inspector General Growth Plan for Increasing Audit and Investigative Capabilities Fiscal Years 2008 – 2015, 31 March 2008, p.11. This situation is well represented in a chart provided in the same report. A copy of this chart is provided in appendix 10.


21 Office of the Director of National Intelligence, Critical Intelligence Community Management Challenges, p.11.


24 Ibid.

25 Standards reflect accountability holder’s political preferences regarding the trade-off between national security and liberal democratic values. They become legal standards when this preference is expressed in law.
talent, and assessing workforce needs’. At the CIA, a contract law division within the Office of General Counsel has ensured that procurement respects such legal standards. Former intelligence officials have considered that existing standards were sufficient to ensure the ascendancy of public authority. Mark Lowenthal, who was Assistant Director of Central Intelligence for Analysis and Production from 2002 to 2005, remarked that it was very clear that the contractors working with his staff ‘could not monitor other contracts. They could not be involved in solicitations. They could not be involved in acquisitions’. Similarly, General Miller, who was commander of the Joint Task Force at Guantanamo, pointed out in a hearing in 2004 that ‘the civilian contractors who work in our intelligence organizations are accountable to the chain of command of the intelligence organization’. He added that ‘in our organization, currently, no civilian contractor is in a supervisory position. It’s the military who has the priority - who sets the priorities and ensures that we meet our standards’.

However, in some areas, the absence of standards was more apparent. An Army investigation into detainee mistreatment noted in 2004 that ‘no doctrine exists to guide interrogators and their intelligence leaders in the contract management or command and control of contractors in a wartime environment’. During his nomination hearing to be Director of National Intelligence, General James Clapper recognised the persisting need to set standards to determine ‘limits on the amount of revenue that would accrue to contractors’.

---

and ‘limits on the number of full-time equivalent contractors who are embedded in the intelligence community’. In other cases, existing standards have been insufficient. For instance, a report by the ODNI IG noted that ‘many procurements receive limited oversight because they fall below the threshold for mandatory oversight’. This threshold is usually related to the definition of ‘major systems’, for which ‘total expenditures for research, development, test and evaluation are estimated to be more than $640 million if developed by DOD agencies or $160 million if developed by non-DOD agencies (based on FY 2006 dollars)’. Following the intensification of public-private intelligence ‘partnerships’ and the shift towards the outsourcing of services, more acquisition procedures may have become obsolete.

A focus on particular intelligence activities such as interrogation reveals that ‘policies and laws governing the involvement of contract personnel vary literally by agency’. Accountability problems in the field of interrogation were clear at the Department of Defense, where existing standards have not been respected thoroughly. In 2004, the Army’s investigation of the Abu Ghraib Joint Interrogation and Detention Center emphasised contractor personnel’s lack of ‘qualifications, experience, and training’. Even military supervisors were confused over their legal responsibilities for contractor personnel. Confusion was reinforced by the absence of contracting officer’s technical representative (COTR) on-site. In these conditions, Major General George Fay (US Army) noted, ‘it is very difficult, if not impossible, to effectively administer a contract’. The independent panel to review the Department of Defense’s detention operations emphasised that ‘oversight of contractor personnel and activities was not sufficient [during Operation Iraqi Freedom] to

---

32 James Clapper, US Senate, Select Committee on Intelligence, Nomination of Lieutenant General James Clapper, Jr., USAF, Ret., To Be Director of National Intelligence, 111th Congress, 2nd sess., 20 July 2010, p.12.
33 Office of the Director of National Intelligence, Critical Intelligence Community Management Challenges, p.11.
34 Ibid.
38 Department of Defense, AR 15-6 Investigation of the Abu Ghraib Detention Facility, p.50.
39 Department of Defense, AR 15-6 Investigation of the Abu Ghraib Detention Facility, p.50.
40 Ibid.
ensure intelligence operations fell within the law and the authorized chain of command’.\footnote{James R. Schlesinger et. al., Independent panel to review DoD Detention Operations, Final Report, August 2004, p.69 [explanation added].}


This arrangement allowed the Army to bypass a directive which banned the private provision of interrogators.\footnote{Henry, Intelligence Exemption, p.1.} Existing procedures were misused when contracts for activities such as human intelligence support, interrogation and screening followed a procedure designed for contracting engineering and information technology services.\footnote{Government Accountability Office, Interagency Contracting, p.8; See also: Department of the Interior, Office of the Inspector General, Review of 12 Procurements placed under General Services Administration Federal Supply Schedules 70 and 871 by the National business Center, 16 July 2004. For a more detailed review of this type of irregularities, see: Voelz, ‘Commercial Augmentation for Intelligence Operations’, pp. 419-33.}

For the GAO, the way in which ‘DoD used Interior to acquire interrogators and screeners [at Abu Ghraib] on an information technology contract’ raised questions ‘about the integrity of the federal procurement process’.\footnote{Government Accountability Office, Interagency Contracting, p.2.} According to a government report, this situation resulted from the ‘lack of an effective system of policies, procedures, and process controls’, and the ‘lack of monitoring and oversight, and the ‘eagerness’ of procurement personnel who ‘have found shortcuts to federal procurement procedures’.\footnote{Department of the Interior, Office of Inspector General, Memorandum from Earl E. Devaney to Assistant Secretary for Policy, Management and Budget, in Review of 12 Procurements Place Under General Services Administration Federal Supply Schedules 70 and 871 by the National Business Center (Assignment No. W-EV-OSS-0075-2004), 16 July 2004, p.3.}

However, external commentators have been more suspicious. Solomon Hughes suggests the US government used ‘some creative accounting to keep the contract relatively obscure’.\footnote{Solomon Hughes, War on Terror Inc. Corporate Profiteering from the Politics of Fear (London: Verso 2007) p.193.} Danielle Brian, the executive director of the Project on Government Oversight questions ‘how can a person at Interior know what
qualities you’re looking for in a contractor doing something as sensitive as interrogating prisoners of war?”

In this particular case, although legal standards and procedures existed, they were not properly used.

**Public-private confusion and accountability standards**

The close ties between some US government officials and the private intelligence industry after 2001 occasionally threatened the ascendancy between accountability holders’ public authority and private accountability holdees’ interests. In theory, the Federal Acquisition Regulation limited the possibility that contractors could skew the public interest in their favour because it requires ‘enhanced management controls’ to ensure the contractors carrying out functions that are close to be inherently governmental aren’t ‘influencing the government in making policy decisions’.

This is based on the notion that the public and private actors do not always uphold the same standards to the same degree and in the words of the former Comptroller General of the United States:

> the closer contractor services come to supporting inherently governmental functions, the greater the risk of their influencing the government’s control over and accountability for decisions that may be based, in part, on contractor work. This situation may result in decisions that are not in the best interest of the government and American taxpayer, while also increasing overall vulnerability to waste, fraud, or abuse.

Morten Hansen has questioned this logic and argued that public and private employees ‘appear to be intrinsically motivated and loyal primarily to the mission at hand, national security’.

This argument revolves around the idea that most contractors have had a career in the government and were therefore recruited on the same basis than their government counterparts. As a consequence security clearance requirements make it difficult ‘to conceal interests and loyalties that ran counter to the national security objective’. A synthesis of both approaches is possible by considering that contractors, as well as government

---


50 US Senate, Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, 112th Congress, 1st sess., 20 September 2011, p.34.


53 Ibid, p.16.
employees, are motivated both by a monetary interest and the possibility to contribute to national security.

From a legal point of view, the standards applying to government officials and private contractors have been different and government employees have been asked to respect stricter ethical standards than their private ‘partners’. Dan Guttman, a Washington DC attorney and specialist on privatisation has pointed out that ‘the work of officials is subject to a body of conflict-of-interest provisions, pay caps, and labor rules that do not apply to contractors’. Similarly, a former legal counsel for the US government noted that government employees, unlike private contractors, go through financial conflict review. Jon Michaels, a legal scholar, also emphasised ‘regulatory asymmetries’ and noted that ‘private organizations can at times obtain and share information more easily and under fewer legal restrictions than the government when it collects similar information on its own’. Such asymmetries are particularly problematic when contractors carry out important tasks, for example in the domain of contract management. In addition, contractors have sometimes been placed in positions where their profit interest could conflict with their activity in support of the government. They have been put ‘in charge of “reading on” competitor contractors (where they have an incentive to exclude or delay employees of competing firms)’, or ‘assisting the government in writing new contracts, new Request for Proposals, and new Statements of Work’. This was the case at Abu Ghraib where a CACI employee helped the contracting officer’s representative (COR) ‘in writing the statement of work prior to the award of the contract’. A report from the Department of Defense IG also found that ‘government contractors are writing statements of the work for which they are the beneficiaries. And, contractors routinely direct/authorize each other’s work’. Although it is normal to involve contractors in the procurement process so that they can refine their offer, the increasingly important role they have played in this context is a concern.

55 Former Senior Intelligence Official B, interview with author, 26 July 2011, Washington DC.
57 Foust, Statement before the U.S. Senate Committee on Homeland Security and Governmental Affairs, p.4. For further evidence, see: Government Accountability Office, Contracting Problems with DOD’s and Interior’s Orders to Support Military Operations, p.7.
58 Department of Defense, AR 15-6 Investigation of the Abu Ghraib Detention Facility, p.49.
The influence of commercial companies on public accountability holders is also an issue at the political level. The money that some companies devote to lobbying members of Congress lies at the heart of the problem. Science Applications International Corporation (SAIC) spent $1,460,000 in 2007 to lobby in the area of intelligence, and Verizon Communications Inc. spent $5,300,000. The same year, SAIC voluntary political action committee provided contributions to four senators in the SSCI and eight representatives in the HPSCI. Representatives are particularly important targets for private companies since they hold the governmental purse and can decide of special funding requests or earmarks. According to a study of the totality of the earmarks that went to companies in Fiscal Year (FY) 2005, ‘on average, companies generated $28 in earmark revenue for every dollar they spent lobbying’. Although lobbying is a legal activity, concerns that this system creates political dependencies on commercial companies’ money and skews national security politics are genuine.

Similar issues enveloped congressional committees especially with regard to the revolving door. The career path of staffers in the Senate Select Committee on Intelligence often involves work experience in a company involved with the intelligence community. For instance, Amy Hopkins was a SAIC intelligence contractor working for the Pacific Command from 2003 to 2007, before she joined the SSCI as professional staff member in 2011. Bob Filippone worked at Raytheon, a major defence contractor, just after leaving his post as deputy staff director of the SSCI. Melvin Dubee worked at Lockheed Martin, after serving as a deputy staff director of the SSCI between 2000 and 2009. Many more SSCI staffers found a job in the lobbying industry in Washington DC after their time serving the


committee. These career paths do not constitute conflicts of interest *per se* and public-private mobility and interactions are desirable to the extent that public and private partners need to understand how to work together. Nevertheless, the existence of a revolving door at this level poses important questions about these staffers’ ability to impartially oversee the same private companies when they interact with the intelligence community. Questions of impartiality can also be raised when the SSCI relies on the expertise of individuals working for the private security industry to carry out its oversight duty. This has been the case of some individuals in the Technical Advisory Group (TAG) which informs and advises committee’s members on scientific and technological issues. Such a rapprochement between public and private interests and organisations creates an environment that fosters conflicts of interest and can lead to unethical practices and abuses of power. However the mere existence of public-private interactions does not prove the private sector is systematically exerting undue influence on congressional oversight and, ultimately, public accountability holders are responsible for the decisions they make.

**Accountability holders’ access to private sector information**

Privatising intelligence complicates public accountability holders’ access to the private sector information that provides a factual basis for their assessments. Some experts have argued that privatisation generates an institutional shift that simply deteriorates accountability

---

66 For more details on former SSCI staffers crossing the revolving door, see: Center for Responsive Politics, ‘Revolving Door: Search Results; Congressional Committee search: Select Intelligence Committee’, <http://www.opensecrets.org/revolving/search_result.php?cmte=Select+Intelligence&id=SITL> (accessed 10 September 2012).


69 Conflicts of interests can be defined as situations ‘where employment or financial relationships impair an individual employee’s or a corporation’s ability to act impartially, objectively, and in the best interest of the government’. See: US Senate, Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Background: Intelligence Community Contractors: Are We Striking the Right Balance?, 112th Congress, 1st sess., 20 September 2011, p.79.

holder’s access to the information necessary to carry out their mission.\textsuperscript{71} However, the situation is far more complex because accountability holders have unequal access to private sector information. In the case of citizens, Tim Shorrock emphasised a disparity of access to information between companies who can access budgetary information on individual agencies and the taxpayers who are left out of the loop.\textsuperscript{72} Jon Michaels has rightly argued that the US law protects corporate secrecy more than public secrecy.\textsuperscript{73} In the US, the Freedom of Information Act (FOIA) does not apply to companies or individual contractors, but only to executive agencies’ records.\textsuperscript{74} In the realm of national security intelligence, private companies’ billings are considered confidential by both the companies and the government, so they are not disclosed to the taxpayers.\textsuperscript{75} In the intelligence committees’ budget reports, the names of the contractors granted earmarks are not usually disclosed.\textsuperscript{76} The ODNI in 2005 gave publicly traded contractors the right to exclude certain material events from their public findings with the Securities Exchange Commission, including the signing of contract with the CIA and the NSA.\textsuperscript{77} Jacob Gale has remarked that, for outsiders, ‘information concerning how service contracts are performed on a daily basis is in exceedingly short supply’.\textsuperscript{78} On the whole, however, these problems of transparency can be related to the secret nature of intelligence activities rather than their supply by private organisations. Citizens are not usually allowed to access budgetary information about intelligence activities or information


\textsuperscript{73} Michaels, ‘All the President’s Spies’, pp. 929-30.


\textsuperscript{77} Shorrock, \textit{Spies for Hire}, p.22.

\textsuperscript{78} Jacob B. Gale, ‘Intelligence Outsourcing in the U.S. Department of Defense: Theory, Practice, And Implications’, Thesis submitted to the Faculty of the Graduate School of Arts and Sciences of Georgetown University in partial fulfilment of the requirements for the degree of Master of Arts in Security Studies, 15 April 2011, Washington DC, p.32.
relating to intelligence sources and methods, regardless of the public or private status of the entities involved in the intelligence process.

Accountability holders within the executive and legislative branches have had relatively good access to information on private intelligence ‘partners’. Since the executive branch has been directly involved with its private ‘partners’ and originated most of their relations, in theory, it has a good access to the information necessary to control their activities when they worked for the government.\(^{79}\) According to the ODNI, in 2007, 73 percent of core contractor personnel involved in the National Intelligence Program were working on government agencies’ premises.\(^{80}\) This layout theoretically allowed for direct control by the government managers working on-site. In other cases, such as overseas contract, it has been more complicated because although contracting officers have legal responsibility for contracts, they ‘may have limited knowledge of the subject matter of a particular contract and may work at substantial remove from the contract’s locale’.\(^{81}\) That is why officers usually rely on a representative to monitor contractors’ performance and ensure compliance with the government instructions on the ground. In the case of Reconstruction Operations Centers in Iraq a system of regulation and control was in place and David Strachan-Morris noted that ‘the personnel working within the intelligence interface were well aware that they were subject to US legislation and regulations concerning access and use of classified information’\(^{82}\). At the more senior level, Michael Hayden, the former Director of the CIA, recognised that despite his responsibility ‘for everything done in the agency’s name’, his ‘ability to control’ got ‘weaker with each layer or class of actor’ ranging from agency employees, government contractors, to liaison services and sources acting on behalf of the US government.\(^{83}\) At a more specialised level, some IGs have struggled to access information about contractors for legal reasons. A report accompanying the Intelligence Authorization Act for Fiscal Year (FY) 2007 noted that administrative IGs at the NRO, DIA, NSA, and NGA:

lack the explicit statutory authorization to access information relevant to their audits or investigations, or to compel the production of such information via subpoena. This lack of authority has impeded access to information – in

\(^{79}\) Former Intelligence Official A, interview with author, 14 June 2011, Arlington, VA; Former senior DOD official, interview with author, 27 July 2011, College Park, MD.
\(^{80}\) Sanders, Results of the Fiscal Year 2007 U.S. Intelligence Community, p.4.
\(^{83}\) Hayden, interview with Frontline.
particular, information from contractors – that is necessary for these Inspector General to perform their important function. 84

Congressional staffers with experience in the national security domain emphasised that, in theory, the intelligence committees have full access to information when the intelligence community relies on private companies. 85 In practice, this access can be more complicated than when activities are carried out by government employees alone. Guttman notes that contractors are not required to publish personnel directories or organisation charts which complicates congressional oversight. 86 The reliance on the private sector adds organisational layers and as a result it can take more time and effort to access key pieces of information. A former congressional staffer has pointed out that the intelligence committees took ‘two or three years to know how many contractors there were’ in the IC 87 and in this case the committees waited for information that had not been put together by the executive branch. Marion Bowman, a former Deputy Director at the National Counterintelligence Executive, has remarked that the privatisation of security increases the ‘distance between both Executive and Congressional oversight of both public money and the means to accomplish public goals’. 88 In this context, information has more chances to get distorted or lost. Another expert with experience in the government has noted that Congress cannot get a full picture of a company since it can only oversee that for which the company was contracted by the government. In this sense, contracts limit the amount of information that congressional investigators are able to obtain. 89 This becomes particularly problematic when public accountability holders try to access information about sub-contractors. 90 By definition, sub-contractors are not directly accountable to the government but to the company contracting with the government, which therefore becomes the ‘de facto government contracting office’. 91 In the most extreme cases, subcontracting runs ‘several tiers deep,

85 Congressional staffer working on national security affairs A, interview with author, 10 June 2011, Washington DC; Congressional staffer working on national security affairs B, interview with author, 17 June 2011, Washington DC.
87 Congressional staffer working on national security affairs B, interview with author.
89 Former Senior Intelligence Official B, interview with author, 26 July 2011, Washington DC.
90 Ibid.
further decentralizing administration of the workforce’ and complicating overall assessment and control of the contracting workforce.  

**Availability and use of sanctions**

Intelligence accountability holders have made a parsimonious use of sanctions against the intelligence community’s private ‘partners’. At the most basic level, sanctions are based on legal provisions and these can take the form of regulations or laws promulgated by the executive branch under a delegation of authority from the legislature (statutes), which are promulgated by Congress. At the regulatory level, two systems stand out. The US government has set up a licensing and registering system to regulate the delivery of defence supplies and services. This system, the International Traffic in Arms Regulation (ITAR) which is part of the Arms Export Control Act, is managed by the State Department’s Office of Defense Trade Control. The ITAR applies to a long list of military products and services, most of which are in the US Munitions List (USML) which includes electronic systems configured to collect, analyse and produce information or counteract electronic surveillance. Thomas McVey, an expert on the ITAR, noted that services related to items listed on the USML are also subject to the ITAR. The NSA export control policy, for instance, mentioned the ‘furnishing of assistance, including training, to foreign persons, in the U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation or use of defense articles’. In accordance with the ITAR, these products and services are submitted to an upstream control based on a market approach. Once registered, a company needs a licence for every contract it undertakes. Contracts are then subjected to governmental scrutiny through various consultations in the Department of State and the Department of Defense. Eventually, if a company violates the ITAR requirements, the company, its directors and employees risk criminal or civil

---

penalties. In practice, however, the ITAR system has been criticised for allowing weak monitoring to take place once a company is licensed.

The Federal Acquisition Regulation is another notoriously complex and consequent body of law that normally applies to intelligence contractors. At the agency level, the FAR is usually accompanied by further guidance, such as the Defense Federal Acquisition Regulation Supplement (DFARS) at the DOD. In the military, contractors are ‘responsible for ensuring that employees comply with laws, regulations, and military orders issued in the theatre of operations’. As a result, the military commander ‘has limited authority for taking disciplinary action’, except when a criminal behaviour occurs. Following the FAR, the executive branch can rely on contract debarment to sanction private contractor wrongdoings. However, this type of sanction is largely insufficient given the impact wrongdoings can have on public spending, human rights, and civil liberties. Moreover, debarring or fining contractors for their failure to perform remains a ‘post-event remedy’ that is, according to one expert, ill-suited to the needs of commanders operating in a conflict environment. Furthermore, sanctions have not always been applied convincingly since suspended and debarred contractors have continued to be contracted for other similar tasks. Overall, Bowman has pointed out that the regulatory process applying to contractors was ‘designed in a different era and for different deliverables’.

---

98 McVey, ‘ITAR – what government contractors need to know’.
104 For examples of debarment and the inconsistent application of sanction to defence contractors, see: Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Report to Congress on Contracting Fraud, January 2011, pp. 4-5. These cases do not directly concern intelligence activities, but the report mentions the debarment of contracts of some defence contractors, such as L-3 Communications or ManTech, that also provide intelligence services to the US government.
become more frequent.\textsuperscript{106} In addition, regulations do not apply equally to all agencies and the CIA benefit from exemptions, or ‘extraordinary’ authorities.\textsuperscript{107} According to a CIA lawyer, ‘many of the requirements and restrictions of the generally-applicable procurement authorities would frustrate the collection of intelligence and the protection of intelligence sources and methods’.\textsuperscript{108}

Available evidence suggests that congressional efforts to enforce sanctions against private intelligence providers have been virtually non-existent. This can be related to the position of Congress as an outsider because it does not control but oversees the activities of the intelligence community. Congressional power of the purse through oversight is limited since companies supporting the intelligence community do not figure in the intelligence budget.\textsuperscript{109} Deborah Avant and Lee Sigelman further remarked that Congress has been unable to use its powers ‘to structure the internal working of PMSCS [Private Military and Security Companies] - who gets promoted, blanket requirements for particular jobs, punishments for wrongdoing and so on as it has the workings of the military branches’.\textsuperscript{110} Although Congress could have legislated to sanction the outsourcing of a particular type of activity or bar outsourcing to a particular company, it did not directly do so from 2001 to 2009.\textsuperscript{111}

With respect to the judicial branch, the prosecution and conviction of intelligence contractors has been the exception rather than the rule. In the specific case of intelligence contractors, national law is the most relevant since most intelligence activities are typically illegal under international law.\textsuperscript{112} However, there is very little, if any, literature on the topic. Considering the literature on PMSCs, a series of statutes could apply to intelligence contractors. The Military Extraterritorial Jurisdiction Act (MEJA) applies to contractors if


\textsuperscript{108} Ibid, p.1198.

\textsuperscript{109} Congressional staffer working on national security affairs B, interview with author.


\textsuperscript{111} Congressional responses, not sanctions, to the increasingly apparent problems plaguing public-private intelligence ‘partnerships’ in the early twenty-first century are explored in further details in the next chapter.

they ‘commit acts abroad that would qualify as federal crimes’. Until 2004, the MEJA only applied to contractors working directly for the Department of Defense. Since 2004, this statute applies to entities ‘supporting a Department of Defense mission’ and, according to a legal scholar, this could include government entities such as the CIA. However, the role of the MEJA has been criticised for relying on ‘US Attorneys to “accept” cases referred to them from an overseas-military command’. This procedure perhaps explains why very few civilians have been prosecuted for violating the MEJA. Other federal statutes which are frequently mentioned in the literature include the War Crimes Act, the Torture statute, and the Uniform Code of Military Justice (UCMJ). The UCMJ became particularly relevant following the passage of the National Defense Authorization Act for FY 2007, which amended the code to make it applicable not only in times of declared war but also in ‘contingency operations’. However, trying civilians under military law poses serious constitutional and operational questions. As a result, Rep. David Price (D-NC) argued that the ‘UCMJ should not be considered a reliable basis for providing accountability to PSCs overseas’.

The mere existence of statutes does not ensure relevant sanctions are applied. Many commentators have emphasised the insufficiency of the legal basis to control PMSCs and their employees. For Eric Rosenbach and Aki Peritz the laws applying to contractors in conflict zone ‘remain vague’. For example, jurisdictional limitations have made it difficult to prove that an accused contractor is acting as an agent of the US government. The lack of

113 Dickinson, Outsourcing War and Peace, p.50.  
116 Dickinson, Outsourcing War and Peace, p.50.  
122 See for example: Bruneau, ‘Contracting Out Security’, p.16.  
jurisdiction was particularly prominent in the case of the Abu Ghraib abuses where no existing statute ‘covered the actions of private military contractors’. Similarly, a legislative attorney for the Congressional Research Service argued that ‘some contractor personnel who commit crimes might not fall within the statutory definitions’. Overall, although laws have regulated the use and behaviour of intelligence contractors from 2001 to 2009, the legal basis for sanctioning their wrongdoings remained uncertain. The legal framework applying to PMSCs and intelligence contractors has also suffered from an enforcement gap and various factors explain this ‘failure of law in action’. A congressional expert emphasised an ‘uncertainty with respect to the courts’ interpretation of the statutes and willingness to apply them to particular facts, which may effectively discourage prosecution’. Uncertainties have further been reinforced by the traditionally deferential stance of the courts towards the executive branch in matters of national security. In some cases, determining contractors’ responsibilities can prove challenging because the lines of authority are more confused in a blended workforce. Frederick Kaiser, a former expert at the Congressional Research Service, noted that ‘a lot of contracts are bundled…that means there are a number of separate private firms that are operating within, under a certain contract. That means further decentralization and difficulty in actually identifying or pinpointing who is responsible for what part of the contract’. In some cases, contractors do not only supervise other contractors but also government employees. This fragmentation of the government’s authority has weakened the enforcement of existing statutes. Moreover, when contractors operate abroad, gathering a satisfying degree of evidence often becomes practically impossible because in most cases,

132 Laura Dickinson, Outsourcing War and Peace, p.54; Corn, ‘Contractors and the Law’, p.171 (note 43).
substantive judicial review supposes very high costs since it would require transporting evidence or relocate the court on the field, secure witnesses and so on. Thomas Bruneau has also pointed out the ‘complications arising from the strict rules regarding evidence in US courts and the ability of the contractors to hire the best lawyers that money can buy’.

From 2001 to 2009, the number of indictments targeting intelligence contractors has been extremely limited. Since the beginning of the GWOT, only one intelligence contractor was prosecuted and convicted for a case of human rights abuse. David A. Passaro, a former CIA independent contractor, was indicted for ‘knowingly and intentionally’ assaulting an Afghan prisoner, which ‘resulted in serious bodily injury’. The Afghan prisoner ultimately died from these injuries, and Passaro was convicted of assault in a US Federal Court under the Special Maritime and Territorial Jurisdiction. According to the Attorney General, the case ‘would have been more difficult to investigate and prosecute were it not for the USA PATRIOT Act’ which ‘extended U.S. law enforcement jurisdiction over crimes committed by or against U.S. nationals on land or facilities designated for use by the United States government’, regardless of the agency in charge. In another case, Iraqi detainee Manadel al-Jamadi died during an interrogation and the Justice Department decided to open a torture and war crimes grand jury investigation into the role of the CIA employee leading the interrogation, Mark Swanner. A military autopsy concluded that al-Jamadi’s death was caused by homicide. However according to a CIA investigation, ‘Swanner never abused al-Jamadi’. Recently, the Department of Justice declined to prosecute Swanner because it judged that the admissible evidence was insufficient ‘to obtain and sustain a conviction beyond reasonable doubt’ and in other cases, CIA officers involved in human rights abuses

---

139 Department of Justice, Office of Public Affairs, ‘Statement of Attorney General Eric Holder on Closure of Investigation into the Interrogation of Certain Detainees’, 30 August 2012,
have only been reprimanded.\textsuperscript{140} In contrast, lawsuits against the company CACI for detainee abuses at Abu Ghraib are pending (2013).\textsuperscript{141} Recently, in a $5.28 million settlement, the firm L-3 Services Inc. has paid victims for the abuses committed on 71 former inmates at Abu Ghraib and other detention facilities.\textsuperscript{142} The trial involving CACI is expected to take place in summer 2013 as Iraqis who were allegedly tortured are still seeking compensation from the company. Regardless of the outcome of these cases, court decisions have been long overdue and intelligence accountability demands an urgency that is often anathema to due legal process.

The scarcity of prosecution targeting private intelligence providers is surprising given the IC’s extensive reliance on the private sector.\textsuperscript{143} This situation can be explained by regulatory gaps and vague statutes.\textsuperscript{144} However, the absence of prosecutions can also be related to political preferences and the relatively weak democratic accountability standards set by the policies followed by the administration of George W. Bush. In the broader context of PMSCs, Rep. Price (D-NC) pointed out a ‘lack of political willingness of the administration’ and a lack of resources ‘to investigate and prosecute alleged crimes overseas’.\textsuperscript{145} Laura Dickinson also argued that the problem is ‘the mobilization of sufficient political will to actually enforce the laws that exist’.\textsuperscript{146} Ultimately, the government remains

\begin{flushleft}


\textsuperscript{143} For a similar argument about the lack of legal clarity surrounding the use of private security contractors: Corn, ‘Contractors and the Law’, p.175.

\textsuperscript{144} Price, ‘Private Contractors, Public Consequences’, pp. 222-3.

\textsuperscript{145} Laura Dickinson, Outsourcing War and Peace, p.42.

\textsuperscript{146} Dickinson, Outsourcing War and Peace, p.42.
\end{flushleft}
responsible when wrongdoings occur, whether the intelligence community’s reliance on the private sector is under-regulated or not. In the first case, the government is responsible for being unable to pass new or amend existing laws. The government has a duty to control and regulate intelligence activities to make sure they remain effective, efficient, and respect liberal democratic values as much as possible. This duty does not disappear when government activities are privatised. In the second case, if relevant sanctions are available, the government is responsible for its inability or unwillingness to bring justice to contractors’ victims.147

From 2001 onwards, key accountability holders’ have not put enough effort into the control, the oversight and the review of public-private intelligence ‘partnerships’. This situation is worrying considering the imperfection, the ineffectiveness and the inability of the market for intelligence to self-regulate. Research has long established that for privatisation to be successful, ‘it must be carefully designed and executed’.148 This was not the case of intelligence following the 9/11 attacks. The privatisation of intelligence during the GWOT occurred without the adequate government acquisition workforce and regulations. Joshua Foust argued that ‘the government has designed a system that encourages abuse’.149 In this view, the government is responsible for fostering the US intelligence community’s reliance on the private sector while overlooking issues of contract management. Michael Hayden himself has recognised that ‘the problem is not with contractors’ but ‘with our management of contractors’.150 These issues, it should be noted, were not new and the ‘sins of outsourcing’ have been very well examined by the literature on privatisation.151 Furthermore, key accountability holders such as the SSCI were already aware of the existence of some flaws in the intelligence acquisition process in the 1990s.152

---

147 For a similar argument, see: Michaels, ‘All the President’s Spies’, p.905.
149 Foust, Statement before the U.S. Senate Committee on Homeland Security and Governmental Affairs, p.2.
150 Hayden, interview with Frontline.
Triggering awareness

From 2001 to 2009, a series of incidents triggered intelligence accountability holders’ awareness of the problems relating to public-private intelligence ‘partnerships’ and can be best described in terms of ‘light’ and ‘heavy’ triggers. Light triggers are minor incidents that generate a limited degree of accountability activity or a few reactions involving some accountability holders. In this case, a continuous stream of executive reports and some congressional reactions focused on efficiency in the case of the NSA acquisition system, and the propriety of public-private intelligence interactions in the case of CIA IG investigations. Heavy triggers are major incidents that generate sustained public reactions (public debate, official statements, media coverage, congressional hearings) and extensive accountability activity involving many accountability holders. From 2002 onwards a succession of heavy triggers involving the private sector raised public awareness of the accountability problems concerning public-private intelligence interactions. The role of media, and investigative journalism in particular, in this transition from light to heavy trigger was particularly central. In turn, these triggers crystallised intelligence accountability holders’s focus around four broad issues: conflict of interest, efficiency, civil liberties, and human rights. Each of these issues came to the fore following a relatively similar pattern involving revelations and sustained coverage in media outlets, then there was public pressure from interest groups and reactions by at least two of the three branches of government. In each case, accountability holders devoted varying degrees of attention to the issue at hand and to the involvement of the private sector.

Light triggers

*The Inspector General at the CIA*

Under George W. Bush, the Office of the Inspector General (OIG) at the CIA demonstrated a continuous awareness and made evident efforts to tackle accountability problems relating to public-private interactions within the agency. During his nomination hearing, John L. Helgerson, the Inspector General (IG) between 2002 and 2009, mentioned that he intended ‘to concentrate on the CIA procurement acquisition process for information technology and information systems’ because ‘this is an area that frankly in any government agency is ripe

---

153 These issues are organised according to the approximate degree of public attention they generated, starting from little national coverage to extensive national and international coverage.
for waste, fraud and abuse’. Declassified reports from the OIG at the CIA reveal continuous scrutiny over public-private intelligence interactions between 2001 and 2009. By statutory requirement, the IG provides semi-annual reports summarising its activities for the immediately preceding six-month period to the Director of the CIA. These documents are particularly relevant since the IG has ‘full and direct access to all Agency information relevant to the performance of its duties’. From January 2001 to December 2008, the IG submitted 16 semi-annual reports to the Director of the CIA. In addition to these reports, a special review on Counterterrorism Detention and Interrogation Activities is also publicly available. These documents show persisting concern with the propriety and efficiency of public-private intelligence ‘partnerships’. Among various tasks, the IG conducted recurrent investigations into allegations of contract fraud (see table 1).

![Table 1 - Current Investigations concerning Procurement Fraud, 2001 - 2008 (OIG, CIA)](chart)

**Table 1 - Current Investigations concerning Procurement Fraud, 2001 - 2008 (OIG, CIA)**

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of investigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>20</td>
</tr>
<tr>
<td>2002</td>
<td>15</td>
</tr>
<tr>
<td>2003</td>
<td>10</td>
</tr>
<tr>
<td>2004</td>
<td>15</td>
</tr>
<tr>
<td>2005</td>
<td>20</td>
</tr>
<tr>
<td>2006</td>
<td>25</td>
</tr>
<tr>
<td>2007</td>
<td>20</td>
</tr>
<tr>
<td>2008</td>
<td>15</td>
</tr>
</tbody>
</table>

**KEY**

- **OIG reports**
- **Linear (OIG reports)**

---

156 Within the CIA, the OIG is sometimes regarded as a cumbersome outsider because it was created by and is directly answerable to Congress. For more on this see: L. Britt Snider, *The Agency and the Hill: CIA’s Relationship with Congress, 1946-2004* (Washington DC: Center for the Study of Intelligence 2008) pp. 68-9, 147-9, 373.
157 These 17 documents were made available by the Electronic Frontier Foundation (EFF) as a result of a FOIA lawsuit it filed in July 2009 against the CIA and half a dozen other intelligence agencies. See: EFF, ‘Intelligence Agencies’ Misconduct Reports’ <https://www.eff.org/foia/intelligence-agencies-misconduct-reports> (accessed 6 February 2012). Most of the pages in these documents remain excised.
158 The graph and its trend line show that the sheer number of investigations concerning procurement problems did not grow exponentially during the GWOT.
Beside procurement fraud, investigations, audits or reviews dwelled on many other aspects such as: the mischarging and overpayment of contract,\textsuperscript{159} wasteful or improper contract practices,\textsuperscript{160} ethics improprieties such as the acceptance of gratuities from Agency contractors, or an improper relationship between a contracting officer’s technical representative and an agency contractor.\textsuperscript{161} In at least two cases, reports mentioned potential counter-intelligence concerns in terms of information security and background investigation involving contractors.\textsuperscript{162}

The IG also played a more active role in furthering employees’ awareness of these problems and when necessary referred cases to other accountability holders. Accountability at this level takes the form of ordinary, not to say banal, bureaucratic tasks that are nonetheless essential to the executive control of intelligence. In early 2001, in order to minimise problems regarding contract and procurement fraud, investigation staff representatives provided ‘awareness briefings to contracting officers concerning common types of fraud indicators’ and ‘organized a fraud focus group to gather and share information’.\textsuperscript{163} The staff also issued employees bulletin on labour mischarging and other types of fraud.\textsuperscript{164} In the cases where there was a reasonable belief that violations of federal criminal law had been committed, the OIG formally referred matters to the Department of Justice.\textsuperscript{165} For example, a series of staff

\textsuperscript{159} Central Intelligence Agency, Inspector General, Semiannual report to the Director of Central Intelligence, July-December 2001; idem, Semiannual report to the Director of Central Intelligence, January-June 2002. The second report refers to a review of Contract Invoicing allegations. See also: idem, Semiannual report to the Director of Central Intelligence, January-June 2003; idem, Semiannual report to the Director, Central Intelligence Agency, January-June 2005; idem, Semiannual report to the Director, Central Intelligence Agency, July-December 2005.


\textsuperscript{162} Idem, Semiannual report to the Director of Central Intelligence, January-June 2004. This report refers to an audit into the Security of National security Systems Operated by Agency contractors. Idem, Semiannual report to the Director of Central Intelligence, January-June 2007, p.36. This report refers to a contractor who pleaded guilty for ‘falsifying background investigation reports on potential employees’.


\textsuperscript{164} See for example: idem, Semiannual report, January-June 2008, p.31; idem, Semiannual report to the Director, Central Intelligence Agency, July-December 2008, p.43.

\textsuperscript{165} Idem, Semiannual report, January-June 2005.
investigations resulted in contractors’ guilty pleas and monetary restitutions to the Agency.\footnote{Central Intelligence Agency, Inspector General, Semiannual report, January-June 2005, p.60; Idem, Semiannual report, July-December 2005, p.2.} In another case, ‘an employee was convicted of conspiracy to accept gratuities in exchange for giving preferential treatment to an Agency contractor’.\footnote{Idem, Semiannual report to the Director of Central Intelligence, July-December 2002, p.3.} Overall, these issues drew some attention from accountability holders but mostly remained at the level of the executive and judicial branches. Most of the details behind the OIG investigations and audits have remained unknown to the public and this limited reach explains why, on the whole, these activities are considered as light triggers.

Congressional oversight

Congress demonstrated an awareness of the need and the risks of intelligence outsourcing in the early twenty-first century. The legislative branch as a whole adopted a relatively supporting approach to intelligence contracting. In the Intelligence Authorization Acts for FY 2002 and 2003 Congress explicitly supported intelligence community contracting, considering that:

The Director of Central Intelligence should continue to direct that elements of the intelligence community, whenever compatible with the national security interests of the United States and consistent with operational and security concerns related to the conduct of intelligence activities, and where fiscally sound, should competitively award contracts in a manner that maximizes the procurement of products properly designated as having been made in the United States.\footnote{US Congress, Pub. Law 107-108, Intelligence Authorization Act for Fiscal Year 2002, 107\textsuperscript{th} Congress, 1\textsuperscript{st} sess., 28 December 2001, section 303; US Congress, Pub. Law 107-306, Intelligence Authorization Act for Fiscal Year 2003, 107\textsuperscript{th} Congress, 2\textsuperscript{nd} sess., 27 November 2002, section 303.} Recognising a need for intelligence contractors’ augmentation, a SSCI report accompanying the Intelligence Authorization for FY 2004 suggested providing authority for the Intelligence Community elements of the Department of Defense to award contracts.\footnote{US Senate, Select Committee on Intelligence, Intelligence Authorization for Fiscal Year 2004, Report 108-44, 108\textsuperscript{th} Congress, 1\textsuperscript{st} sess., 8 May 2003, p.19. See also: US Senate, Select Committee on Intelligence, Intelligence Authorization for Fiscal Year 2007, Report 110-2, 110\textsuperscript{th} Congress, 1\textsuperscript{st} sess., 24 January 2007, pp. 36-37. The latter report recommends providing authority for the Bureau of Intelligence and Research of the Department of State to award personnel services contracts.} The authorisation act itself granted a similar authority to the Federal Bureau of Investigation.\footnote{US Congress, Pub. Law 108-177, Intelligence Authorization Act for Fiscal Year 2004, 108\textsuperscript{th} Congress, 1\textsuperscript{st} sess., 28 November 2003, section 311. Interestingly, section 302 (b) of the Act also requires an annual report from the Director of the FBI including: the number of contracts entered into during the period, the cost, length and type of service provided under each such contract, and the availability of the US government personnel to perform similar services.} These
authorisations show that congressional oversight does not only take place when a scandal or major incidents occur and confirm that Congress endorsed the privatisation of intelligence.

Nevertheless, Congress also voiced concern about the efficiency of public-private intelligence ‘partnerships’. The NSA’s efforts to modernise itself underwent increased scrutiny from congressional committees in the first decade of the twenty-first century.\(^{171}\) From early 2001 to 2004 the Intelligence Committees arranged a series of briefings and produced reports that expressed particular frustration with ‘the state of the NSA acquisition process’.\(^{172}\) The Senate Armed Service Committee (SASC) in 2003 set a deadline for the NSA to ‘put its books in order’.\(^{173}\) Ultimately, the Defense Authorization Act for FY 2004 took away NSA’s authority to sign major acquisition contracts and gave it to the Undersecretary of Defense for acquisitions, technology and logistics,\(^{174}\) in order to ‘stimulate better executive branch oversight of NSA systems acquisition’.\(^{175}\) This kind of problem was not limited to the NSA. The HPSCI found that ‘the magnitude and consistency of the growth of recent acquisitions indicates a systemic bias on the part of Intelligence Community components to underestimate the funding required for major acquisitions’.\(^{176}\) Congressional interest in the IC acquisition process clearly raised the issue at a level of public awareness superior to most of the procurement fraud investigated by the CIA IG. However, up to 2005, these concerns did not generate widespread media coverage. According to a search on Nexis,

\(^{171}\) The case of the NSA is particularly relevant since the agency absorbs a significant part of the budget of the US intelligence community every year. In 2004, Bob Woodward estimated the NSA budget at around $6 billion. See: Bob Woodward, Plan of Attack (New York and London: Simon & Schuster 2004) p.213.


between 1 January 2001 and 31 December 2005 the *New York Times* published only two articles mentioning acquisition problems at the NSA, and the *Washington Post* three. Overall the congressional attitude at the time can be characterised as cautious because key committees supported the privatisation of intelligence but condemned the way in which it was carried out by some agencies.

**Heavy triggers**

**Conflicts of interest**

Conflicts of interest involving public accountability holders and private contractors have drawn particularly widespread attention. A congressman sitting on the HPSCI and the Executive Director of the CIA interacted so closely with private intelligence providers that they endangered the public interest. Marcus Stern revealed in 2005 that ‘a defense contractor [the firm MZM Inc.] with ties to Rep. Randy Cunningham took a $700,000 loss on the purchase of the congressman’s San Diego house’ and four days after the scandal broke, the FBI opened an investigation. According to an FBI affidavit, ‘Cunningham demanded, and Wade and Wilkes [respectively, the founder of MZM Inc. and ADCS Inc.] provided over $2 million in bribes in exchange for Cunningham using his office to influence the awarding of public funds to the defense contractors’ companies’. In exchange, Cunningham sought to use his position on the House intelligence committee ‘through requests for congressional

---

funding that benefited Wilkes, Wade and their companies182 and lobbied to obtain HPSCI support ‘for a new counterintelligence project at the Counterintelligence Field Activity’.183 This case was first brought to the attention of the Department of Defense in 2004 when the IG received a hotline complaint.184 Once public, the story sparked near immediate reactions by the Democratic Party and public interest groups that called for a full-scale investigation.185 On the whole, the scandal demonstrates how elected public accountability holders can shirk their responsibility to further private interests. From the perspective of the accountability process, it shows well how higher levels of accountability activity are correlated with public knowledge of an incident.

The Cunningham affair led investigators to a second case involving defence contractor Brent Wilkes and former CIA Executive Director Kyle Foggo.186 Foggo had already been under investigation from the CIA IG for his potential involvement in the Cunningham case through Wilkes.187 Although the Cunningham connection did not reveal any wrongdoing, on 13 February 2007 Foggo and Wilkes were indicted and Foggo subsequently pleaded guilty to a single count of fraud concerning bribery and misconduct over a contract while prosecutors agreed to dismiss 27 other charges.188 This case inevitably surfaced in the CIA Inspector General semi-annual reports although the names of the defendants remain excised from the publicly available documents.189 Considering Congress, the case of the former CIA EXDIR was barely mentioned during a congressional hearing of

183 Ibid. See also: Department of Justice, Defense contractor Mitchell Wade pleads guilty to bribing former Congressman “Duke” Cunningham, corrupting Department of Defense officials, and election fraud, 24 February 2006, p.3.
184 Hattier, Affidavit, p.52.
186 Wilkes was a co-conspirator in the Cunningham case and was later sentenced to 12 years of imprisonment. See: Dean Calbreath and Jerry Kammer, ‘Poway contractor provided a loaner’, Copley News Service, 10 September 2005 <http://www.lexisnexis.com/uk/nexis/search/newssubmitForm.do> (12 January 2012).
189 CIA Inspector General, Semiannual report, January – June 2007, p.2. The report mentions an investigation involving ‘a former high-ranking official who, during the reporting period, was indicted on 30 counts related to his handling of Agency contracts’.
the committee on the Judiciary concerning the resignation of a US Attorney. It is only when Congress was directly concerned, in the Cunningham affair, that its members notably reacted. Overall, both of these cases drew sustained public attention to the conflicts of interest that can arise when public-private ‘partnerships’ go so far that the distinction between public authority and private interest collapses. In such cases, the privatisation of intelligence offers an opportunity for unscrupulous accountability holders to disregard ethical and legal standards and use their position to make money instead of holding intelligence providers to account. Considering the accountability process, it should be noted that these problems were a consequence of public accountability holders’ decisions and not a result of privatisation per se.

**Efficiency**

The problems of efficiency plaguing public-private ‘partnerships’ have also triggered sustained reactions from multiple accountability holders. Public attention focused particularly on the failure of the Trailblazer programme, which came to embody acquisition flaws at the NSA. Although the programme had triggered executive and legislative scrutiny as early as 2002, it really became a heavy trigger when the media depicted it as an extravagant failure. The programme relied on a series of contractors and aimed to modernise NSA’s information system. Following 9/11, the Director of the NSA gathered the impetus to push Trailblazer

---

190 See: US Senate, Committee on the Judiciary, Committee on the Judiciary, Report 110-522, Resolutions of Contempt - Report to Accompany Resolutions finding Karl Rove and Joshua Bollen in Contempt of Congress, 110th Congress, 2nd sess., 19 November 2008, pp. 32, 47, 55. Fogg and Wilkes are mentioned here as the committee investigates whether the case was related to the resignation of a former US Attorney for the Southern District of California.

191 Another flawed programme was codenamed GROUNDBREAKER. For more on this programme, see: National Security Agency/Central Security Service, Transition 2001, December 2000, p.33. Allegations of mismanagement and waste relating to the handling of contracts also concerned the Counter-Intelligence Field Activity within the Department of Defense. See: Department of Defense, Allegations of Mismanagement and waste within the Counterintelligence Field Activity.


forward instead of another programme called ThinThread which some considered more effective and less intrusive.\(^ {194}\) According to the *Washington Post*, a group of serving and retired NSA officials, among which Thomas Drake, then senior executive at the NSA, became increasingly concerned about Trailblazer and alerted Diane Roark, a Republican staffer on the House intelligence committee. Roark contacted senior officials in the executive branch but did not manage to trigger any significant investigation or audit. In September 2002, the same group of NSA colleagues filed a complaint with the Department of Defense IG alleging that ‘NSA actions in the development of THINTHREAD and TRAILBLAZER resulted in fraud, waste, and abuse.’\(^ {195}\) The NSA IG discovered inadequate management and oversight as well as overpayment of contractors as early as 2003.\(^ {196}\) Its final report considered that:

The National Security Agency is inefficiently using resources to develop a digital network exploitation system that is not capable of fully exploiting the digital network intelligence available to analysts from the Global Information Network... The NSA transformation effort may be developing a less capable long-term digital network exploitation solution that will take longer and cost significantly more to develop. The NSA continued to support the “less capable” program and its successor.\(^ {197}\)

These findings were strongly contested by the management of the NSA.\(^ {198}\) However, mistakes were not denied and during his nomination hearing to become Principal Deputy Director of National Intelligence, Michael Hayden, then Director of the NSA, publicly recognised that the agency ‘underestimated the costs by a couple to several hundred


\(^ {195}\) Department of Defense, Requirements for the Trailblazer and Thinthread Systems, p.i; Ellen Nakashima, ‘Former NSA executive Thomas A. Drake may pay high price for media leak’, *Washington Post*, 14 July 2010, C01.


\(^ {198}\) Department of Defense, Requirements for the Trailblazer and Thinthread Systems, pp. 95, 107-10. The details of these disagreements remain classified. However the report shows signs of strong disagreement between the NSA management team and the office of the IG at the Department of Defense.
million’. Reflecting on this underestimation, a former senior intelligence official noted that ‘it was just far more difficult than anyone anticipated’. Subsequently, the Baltimore Sun published a series of articles about NSA mismanagement, fraud and waste. These articles raised the issue at a new level and eventually, Trailblazer was terminated in 2007 without fulfilling its objectives and ‘after an expenditure of $1.2 billion’. Overall, the relatively constant spotlight that intelligence managers and Congress have kept on intelligence acquisition programmes did not prevent the persistence of problems.

**Human Rights, detention and interrogation**

The involvement of intelligence contractors in human rights abuses at Abu Ghraib has been the most widely publicised incident involving intelligence contractors in the twenty-first century. On 28 April 2004, the CBS network programme *60 Minutes II* exposed the torture scandal of the Abu Ghraib prison. Although public interest groups such as Amnesty International and Human Rights Watch and the news media had already highlighted the mistreatment of detainees, it is the *60 Minutes II* story and its shocking photographs that raised the affair to an international level, triggering a worldwide outcry. In the US, the story generated a sustained series of reactions from the entire population of intelligence accountability holders. Among all these reactions, a lesser, yet significant, part focused on the

199 US Senate, Select Committee on Intelligence, Nomination of Lieutenant General Michael V. Hayden, pp. 21, 69-71.
200 Former Senior Intelligence Official A, interview with author.
involvement of contractors in the abuses. The troubling involvement of contractors in detainee abuses was picked up by American broadsheet media such as the Washington Post and the New York Times and also figured prominently in foreign media. On the domestic front, public interest groups such as the Project on Government Oversight used the media to voice their concern, sometimes over very specific issues such as the type of contract used for translation services at Abu Ghraib.

The issue of possible prisoner abuse was not new to the US Army when it became public. In January 2004, Major General Antonio Taguba (US Army) was directed to investigate the 800th Military Police Brigade’s detention and internment operations with a specific focus on allegations of maltreatment at the Abu Ghraib prison and according to his report at least two CACI contractors were involved in the abuses. A former legal counsel for the intelligence community during the presidency of George W. Bush noted that the involvement of contractors in the Abu Ghraib scandal was probably a turning point in terms of public awareness. A former staffer at the Senate Armed Service Committee (SASC) remembered that the involvement of contractors in the scandal generated discussions about inherently governmental responsibilities and following the public outbreak of the scandal, representatives sent clear calls for action. The SASC convened a series of hearings on allegations of mistreatment of Iraqi prisoners where senior officials of the Department of Defense testified. Senators used this occasion to pick up on the use of contractors. For example, Senator Warner (R-VA) used a hearing to ask senior DOD officials:

How is it in our nation's interest to have civilian contractors, rather than military personnel, performing vital national security functions, such as prisoner interrogations, in a war zone? When soldiers break the law, or fail to follow orders, commanders can hold them accountable for their misconduct. Military commanders don't have the same authority over civilian contractors.

209 Taguba, Article 15-6 Investigation of the 800th Military Police Brigade, p.48.
210 Former Senior Intelligence Official B, interview with author.
211 Former Intelligence Official A, interview with author.
Furthermore, Senator Akaka (D-HI) wondered ‘what are the roles of the private contractors at this and other detention facilities in Iraq and Afghanistan? And who monitors and supervises these contracted employees?’ In his answer, Secretary of Defense Rumsfeld was keen to point out that civilian contractors are ‘responsible to military intelligence who hire them, and have the responsibility for supervising them’. According to an article from the Washington Post, Representative Janice Schakowsky (D-IL) ‘asked President Bush to suspend the prison contracts until investigations are complete’. The congresswoman further wondered whether contractors were ‘taking orders from their CEOs and shareholders and then telling our soldiers what to do’. In the following months, executive and legislative branch investigations into detentions in Afghanistan and Iraq multiplied. Some of them clearly pointed at issues with the government’s procurement process. The Fay report found that civilian contractors had ‘some degree of responsibility or complicity in the abuses that occurred at Abu Ghraib’, and pointed out at ‘there was no credible exercise of appropriate oversight of contract performance at Abu Ghraib’. Nevertheless, while soldiers were convicted for detainee abuses at Abu Ghraib, so far none of the contractors


216 Department of the Interior, Memorandum from Earl E. Devaney to Assistant Secretary for Policy, Management and Budget, pp. 1-2. Devaney found that the Department of the Interior contract personnel had misused GSA’s schedules. See also: Department of the Army, Detainee Operations Inspection, p.87. This report found that contract interrogators’ lack of training contributed to detainee abuse. For more on the involvement of the Department of the Interior contract office in the Department of Defense’s outsourcing of interrogation, see: Government Accountability Office, Interagency Contracting, pp. 1-2.

217 Department of Defense, AR 15-6 Investigation of the Abu Ghraib Detention Facility, pp. 18, 33, 49-50, 52. For similar conclusion, see: Department of Defense, Independent Panel to review DoD Detention Operations, Final Report (also called the Schlesinger panel), 24 August 2004, p.69.
who were involved have been criminally prosecuted\textsuperscript{218} and the reasons for this situation remain unclear. A DOD report found that, since ‘some employees at Abu Ghraib were not DoD contractor employees’, criminal prosecution under the MEJA ‘may not’ be possible.\textsuperscript{219} Laura Dickinson has convincingly pointed out the lack of political willingness and noted that ‘the Bush administration was reluctant even to characterize abuses committed at Abu Ghraib as torture or war crimes’ and was ‘therefore, not surprisingly, reluctant to initiate prosecutions of contractors implicated in the abuse.’\textsuperscript{220} In sum, these abuses significantly intensified the executive, judicial, legislative and societal scrutiny of intelligence contractors even though the participation of private contractors in the abuses was not a necessary condition for them to occur.

\textit{Civil Liberties}

The debate on the expansion of domestic surveillance in the aftermath of the 9/11 attacks was vivid and focused more on the role of the government than the private sector. The \textit{New York Times} published in 2002 an article on the Information Awareness Office, a part of the Department of Defense and described this office’s contact with Silicon Valley researchers and the development of ‘advanced surveillance and data-mining techniques’ that ‘raised new concerns among civil liberties groups in the United States’.\textsuperscript{221} Despite DOD’s effort to establish oversight boards for this specific programme, media continued to voice their concern.\textsuperscript{222} The Electronic Privacy Information Center (EPIC), a public interest group, warned that the Total Information Awareness System had hired ‘at least eight private companies’ to help gathering and analysing vast arrays of information on American


\textsuperscript{219} Department of Defense, AR 15-6 Investigation of the Abu Ghraib Detention Facility, p.50.


citizens. The programme has triggered congressional interest and Senator Charles E. Grassley (R-IA) sent a letter to the Department of Defense IG, asking a review of the programme. Senator Feingold (D-WI) even introduced a bill ‘to impose a moratorium on the implementation of data-mining under the Total Information Awareness program’ and ask a report on these data-mining activities. The DOD provided this report and restated its commitment to civil liberties. However, Congress prohibited further funding of the programme in the Defense Appropriations Act for FY 2004. Subsequently, public interest groups remained wary of the damage public-private intelligence ‘partnerships’ can cause to civil liberties and the American Civil Liberties Union (ACLU) released a report decrying the growth of a new ‘surveillance-industrial complex’.

These apprehensions were reinforced by one of the biggest public scandals the US intelligence community faced during the presidency of George W. Bush. On 16 December 2005, the New York Times revealed that President Bush had authorised the NSA to monitor telephone conversations and e-mails travelling to or from the USA, which could have involved US persons, without court-approved warrants. A few months later, USA Today reported that the NSA had been ‘secretly collecting the phone call records of tens of millions of Americans’. According to the same article, three telecommunication companies were ‘working under contract with the NSA’. Government releases have confirmed that, following the 9/11 attacks, the administration of George W. Bush expanded the intelligence community’s surveillance activities, intercepting ‘the content of communications into and out of the United States where there was a reasonable basis to conclude that one party to the

---

231 Ibid.
communication was a member of al-Qa'ida or related terrorist organizations. Inevitably, this expansion involved the participation of telecommunication companies such as AT&T, Bell South and Verizon, which provided access to their clients’ information. With hindsight, Jon Michaels, a legal scholar, made a distinction between two programmes. On the one hand, the call-data programme was ‘an arrangement whereby telecommunications companies agreed to transfer vast amounts of telephone and Internet information, even of purely domestic telephone calls and emails, to the NSA’. Michaels remarked that ‘the program purportedly has provided only what is known as metadata or envelope information, meaning names, lists of calls and emails placed and received, and call duration’. On the other hand, the terrorist surveillance programme ‘gave the NSA access to the content of international communications’.

Most public reactions to this controversy focused on threats to civil liberties rather than the involvement of the private sector. The expansion of government surveillance was particularly controversial because the eavesdropping programme seemed to compromise the Fourth Amendment right of US persons, which guards against ‘unreasonable searches and seizures’. In particular, the administration did not acquire warrants from the Foreign Intelligence Surveillance Court (FISC) judges. This seemed to contradict the Foreign Intelligence Surveillance Act (FISA) of 1978 which requires intelligence agencies to acquire a warrant from the FISC judge before conducting electronic surveillance targeting communications in which US persons are involved. Moreover, some commentators considered that, in the case of the call-data programme, private companies could have circumvented the Communications Act of 1934, which sets privacy requirements for telecommunications carriers. From the perspective of accountability channels, the executive branch briefed a limited number of representatives on the programme and as

233 See: Cauley, ‘NSA Has Massive Database of Americans’ Phone Calls’.
237 For more on the constraints the administration has put on these briefings, see: Alfred Cumming, ‘Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions’, Congressional Research Service Report for Congress, 18 January 2006, pp. 7-9.
early as 11 October 2001, Rep. Nancy Pelosi (D-CA), then a member of the HPSCI, sent a letter to the Director of the NSA to express her concern with his ‘expansive view of [his] authorities with respect to the conduct of electronic surveillance under the Foreign Intelligence Surveillance Act’. In her letter, Pelosi further remarked ‘for several reasons it has not been possible to get answers to [her] questions’.238 Similarly, although he was briefed on the programme, Senator Rockefeller (D-WV) later complained that his ability to question it was limited by security regulations and the use of secret briefing by the administration. In order to express his concerns, he thus wrote a letter to Vice President Cheney explaining that ‘without more information and the ability to draw on any independent legal or technical expertise, I simply cannot satisfy lingering concerns raised by the briefing we received’.239

Media revelations on the programme raised the stakes and changed the attitudes of various stakeholders.240 According to a Newsweek poll, ‘the revelation was another blow to Bush, whose approval rating … dipped to 35 percent, his record low in the survey’.241 The administration reacted by providing legal explanations to make the case for the warrantless electronic surveillance programme.242 A series of public interest groups challenged these explanations, and sued the government and the telecommunication companies involved in the

241 Hosenball and Thomas, ‘Hold the Phone; Big Brother knows whom you call’, p.23.
warrantless surveillance programme and a bipartisan group of senators requested that the SSCI and the Committee on the Judiciary ‘jointly undertake an inquiry into the fact and law surrounding these allegations’. Senators Patrick Leahy (D-VT) and Ted Kennedy (D-MA) further introduced a resolution stating that ‘the Authorization for Use of Military Force does not authorize warrantless domestic surveillance of United States citizens’. However, the resolution was never passed. The Democratic Party’s gains at the 2006 mid-term elections allowed it to strengthen its opposition to the programme. According to Tara Sugiyama and Marisa Perry, following the Democrats’ efforts, ‘the administration began cooperating on a limited basis’. For example, they point out that the Office of Personnel Responsibility (OPR) at the Department of Justice ‘started a formal inquiry into the internal dissension over the legal foundation of the program within the department’. However, the OPR was not able to carry out its investigation since it was ‘denied security clearances for access to information about the N.S.A. program’. In 2007, the administration eventually decided to let the courts review the surveillance programme and according to Kathleen Clark, this decision may have been caused by a ‘less friendly’ Democratic-controlled Congress and the pressure from


244 Senators Dianne Feinstein (D-CA), Carl Levin (D-MI), Chuck Hagel (R-NE), Olympia Snowe(R-ME), Ron Wyden (D-OR), Letter to Senators Arlen Specter (R-PA) and Patrick Leahy (D-VT), chairman and ranking member of the Judiciary Committee, and Pat Roberts (R-KS) and John D. Rockefeller IV (D-WV), chairman and vice chairman of the Select Committee on Intelligence, 19 December 2005 <http://blog.thedemocratdaily.com/?p=1469> (accessed 22 February 2012).


telecommunication companies which did not want to take legal risks.\textsuperscript{249} Ultimately, with the support of the President,\textsuperscript{250} Congress passed the FISA Amendments Act of 2008 and gave immunity from liability to the telecommunication companies which had been collaborating with the NSA.\textsuperscript{251} The act also required the NSA programme to be investigated by a series of IGs\textsuperscript{252} and, remarkably, the declassified version of the final IG report does not mention the reliance on the telecommunication companies despite the central role they played in implementing the programme.\textsuperscript{253}

Conclusion

This chapter found that the conditions for the accountability of public-private intelligence ‘partnerships’ were not entirely fulfilled from 2001 to 2009. First, the political and legal standards at the basis of any accountability activity were insufficient. Decision-makers neglected questions of contract management in the aftermath of the 9/11 attacks. This partly explains why existing legal standards governing the interactions between the IC and the private sector were loosely applied. Furthermore, the intensification of public-private interactions raised legitimate concerns about conflicts of interest and the ascendency between public authority and private interests. Even though these concerns were verified, wrongdoings in this area were not systematic. Second, key intelligence accountability holders theoretically have access to all the information they need about public-private intelligence ‘partnerships’. In practice, however, the intelligence community’s reliance on the private sector has complicated their task. At the societal level, given the amount of media coverage generated by a series of controversies, the interested public had some awareness of the troubles concerning public-private intelligence ‘partnerships’. However, key intelligence accountability holders’ access to relevant private sector information was complicated by senior executive officials’ relative disinterest in contract management. Third, a number of


\textsuperscript{251} US Congress, Pub. Law 110-261, Foreign Intelligence Surveillance Act of 1978 Amendments Act, 110\textsuperscript{th} Congress, 2\textsuperscript{nd} sess., 10 July 2008, title II.


\textsuperscript{253} The unclassified version of the final report retraces this controversial story, see: Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, Unclassified Report on the President’s Surveillance Program.
laws were available to the executive and judicial branches to punish private intelligence providers when deemed necessary. Nevertheless, the application of available sanctions was limited by a lack of legal clarity and accountability holders’ lack of political willingness to apply them. In sum, from 2001 to 2009, the privatisation of intelligence challenged the intelligence accountability process but key intelligence accountability holders maintained their ability to access information, refer to some standards to form judgments and sanction wrongdoings. That is why it is possible to argue that the US government was responsible for intensifying its reliance on the private sector without taking necessary precautions.

From 2001 onwards, key intelligence accountability holders have reacted to a series of problems plaguing public-private intelligence ‘partnerships’. Throughout the presidency of George W. Bush, the IC and Congress were very well aware of some of the problems relating to public-private intelligence interactions. Procurement fraud, for example, was a recurring issue on the agenda of the CIA IG, and Congress expressed concern about some serious deficiencies in the NSA acquisition system. Yet the move towards privatisation was neither effectively opposed nor carefully controlled and overseen. It corresponded to American values and perceptions, and more importantly to its material interest in the GWOT. From 2002 onwards a series of public scandals drew increasing attention on some of the most disturbing problems raised by the intensification of public-private intelligence interactions. In particular, problems concerned conflicts of interests, efficiency, human rights and civil liberties. Historically, similar issues have been raised by the activities of governmental intelligence agencies. In this view, the involvement of the private sector was another expression of some of the sins that have traditionally been committed by public intelligence agencies. Considering the intelligence accountability process, it is only after a series of scandals occurred that accountability holders seriously considered the imperative for change.