Outsourcing Intelligence: Private Intelligence Companies and the Issue of Legal Accountability

Timmermans, Sjoerd

Outsourcing Intelligence: Private Intelligence Companies and the Issue of Legal Accountability

Thesis by Sjoerd Timmermans

MSc Public Administration: Crisis and Security Management

Leiden University

Supervisor: Dr. S.D. Willmetts
Student: Sjoerd J.P. Timmermans
Student number: S1385860
Word count: 14266

Abstract

This thesis investigates the effectiveness of the legal accountability mechanisms that govern the marketization of intelligence agencies. The current scholarly debate focuses primarily on accountability issues related to privatization of military functions, failing to provide a similar discussion of the conduct of private intelligence actors. Within this research, four types of legal accountability mechanisms are identified: international law, extended jurisdiction of national law, public law values and contractual law, and soft law. Subsequently, three case studies, to which one or more of these mechanisms apply, are evaluated regarding the effectiveness of the legal accountability mechanism or mechanisms in place. The findings show that there are four reasons why legal accountability mechanisms fail to properly hold Private Intelligence Companies and their employees to account. First, there is no clear and legally binding definition of the ground rules of privatization. Second, there is legal asymmetry between the government and the private sector. Third, political interference in legal processes problematizes the establishment of accountability. And lastly, there is a clear reluctance to enforce laws in place that should contribute to good behavior.

Introduction

The privatization of government services is not a new phenomenon, nor is the privatization of security. The U.S. army relied heavily on Native American scouts in the nineteenth century in order to guide military movements (Storm 672). In the 1916 Punitive Expedition, the famous Pinkerton Agency provided critical support to U.S. forces (Storm 672). That same Pinkerton Agency was already very active during the U.S. Civil War. In 1955, the Lockheed Skunkwork company built the revolutionary U2 spy plane that allowed the U.S. to get a better picture of the Soviet weapon arsenal under a secret government contract (Gruskin 37). Nonetheless, up until the end of the Cold War, privatization was an exception rather than the rule. This changed in the post-Cold War period, in which the United States needed to reassess its military capabilities, since the imminent threat from the Soviet Union was no longer present. During the 2003 invasion of Iraq, private contractors were the second largest 'member' of the Coalition of the Willing - after the U.S. itself (Percy 57). The deployment of contractors in this theatre of conflict amounted to a 10-fold increase compared to the use of private actors in the first Gulf War in 1991. Where in the 1990s the ratio military to contractor was 50:1, this is now approximately 10:1 (Singer 2008). In 2019 $370 billion was spent on contracting, which amounts to more than half of the entire defense budget of $676 billion (Thompson).

In today's policy landscape in the United States, the privatization of security is an integral element of national security policy making. This does not mean that the use of private actors in the security realm is without controversy, on the contrary, private engagement in military and intelligence operations is highly criticized due to an ongoing list of scandals. The US-led War on Terror has produced numerous major scandals involving private intelligence and security contractors. One of the most striking scandals was Baghdad's "Bloody Sunday" on September 16, 2007, when Blackwater Worldwide (now Academi) contractors killed seventeen civilians while wounding twenty-seven others (Chapman 1048). Two years earlier, a video created by contractors in Iraq in which they were shooting at random civilians in 2005 likewise caused public outrage. Equally controversial, was the use of 'Enhanced Interrogation Techniques' (EIT's), or rather torture, on terrorism suspects during the most recent war in Iraq. In addition to these widely displayed cases of private security atrocities, there are numerous other, less lethal, scandals to be noted: an National Security Agency (NSA) project that cost $3 billion without ever being finished; Boeing's contract to develop new satellites, a multibillion dollar contract that resulted in the production of not one satellite; and the list goes on.

Although the scandals listed are different in one way or another, there is one factor that links them together: holding the perpetrators accountable proved highly difficult, and sometimes impossible. The majority of the perpetrators evaded consequences. Even though the four Blackwater employees that killed seventeen civilians were prosecuted at first, President Trump pardoned them. Hence, the question arises, why is it that private contractors in the security industry are rarely legally held accountable for their actions? Whilst the relative impunity of Private Military Companies (PMCs) has been a topic of study by, amongst others, Leander (2010), Maogoto et al. (2009), and Chapman (2010), a similar empirical investigation into the relative impunity of Private Intelligence Companies (PICs) is still missing in this academic field. To fill this gap in research and to provide lawmakers with an assessment of their oversight mechanisms, this thesis seeks to answer the following research question:

"**How effective are existing legal oversight mechanisms in the United States in holding PICs accountable for their actions?"**

The debate on PMC accountability provides a fruitful theoretical perspective that functions as the theoretical framework to research PIC legal accountability. Consequently, three different legal accountability mechanisms are assessed in regard to their effectiveness in holding private intelligence actors to account. In chapter 1, the field of the privatization of intelligence is outlined, discussing the marketization of intelligence and which functions are exactly outsourced. Additionally, it provides a theoretical framework for assessing legal accountability. Chapter 2 assesses the legal and contractual basis of the privatization of intelligence services as codified in OMB Circular A-76 and the Federal Acquisition Regulations System (FAR). In chapter 3, an evaluation of the judicial review of misconduct on foreign soil is conducted, through an assessment of the Uniform Code of Military Justice (UCMJ) and the Military Extraterritorial Jurisdiction Act (MEJA). The last legal accountability mechanism, to be discussed in chapter 4, discusses the effectiveness of the regulations that seek to prevent conflicts of interest, control financial disclosure laws and establish whistleblower protection.

Chapter 1

Privatizing intelligence and legal accountability

In order to be able to coherently and correctly assess the legal accountability mechanisms presiding over private intelligence actors, it is necessary to define what a Private Intelligence Company (PIC) is. Within this chapter, the definition of what constitutes a PIC is explored. Additionally, the historical background and the contemporary status of the privatization of intelligence are discussed. This discussion focuses on why intelligence functions are marketized. Additionally, the scope and size of the private intelligence industry is explored. In order to be able to assess the effectiveness of legal accountability mechanisms, it is necessary to clearly define the concept of legal accountability, and point out how this works in practice.

Defining PICs

Private Intelligence Companies are often seen as a phenomenon of the occurrence of Private Military Companies. The best way to define the former is to look closely at the definition of the latter, and clarify how both types of organisations differ. PMCs are sometimes seen as modern mercenaries. Traditionally, PMCs have been viewed as actors that operate in the continuum of either the provision of lethal force or training others to do so, or delivering logistical and administrative support (Prem 52). These companies provide services in the taxonomy of lethal/non-lethal, combat/non-combat and offensive/defensive (Prem 52). Singer (2008, p. 201) distinguishes PMCs along the “tip of the spear” metaphor, the place of the actor on the spear is determined by their location in the battlespace. PMCs can accordingly be classified as either 1) military provider firms, 2) military consulting firms or 3) military support firms (Singer, 2008, p. 200). Only the first type of PMCs engage in combat, the second and third category provide training and non-combat support.

However, in recent years it seems that the traditional PMC has undergone a transformation. The traditional form of the PMC, that of a modern mercenary army engaged in offensive military actions, is transitioning towards a more subtle, defensive oriented entity (Prem 52). Where notorious military provider firms such as Sandline and Executive Outcomes offered special forces services (Singer, 2008, p. 202), contemporary PMC focus more on logistic and non-combat contracts (Prem 52). Private Intelligence Companies and private intelligence

actors in general can be seen as an embodiment of this transition away from the provision of lethal violence, towards a less intrusive type of services provider.

The inherent difference between private military contractors and private intelligence contractors is the ability to exercise the monopoly on violence (Leander 469). Where PMCs have quasi-military functions, their intelligence counterparts deal mostly with the collection of information through non-violent means. Although these companies themselves do not engage in lethal combat, it is possible that the technology or hardware they provide (such as drones) can be used in combat. These private actors do not, however, handle the technology they create, and therefore don't participate directly in combat. In other cases, the distinction between private military and private intelligence actors can be blurry. The Abu Ghraib abuses of prisoners by interrogators, for example, are in a grey area between falling within the definition of a PIC and PMC. Although atypical for the intelligence industry, the tasks (collecting intelligence), mandate (only interrogation and not armed guarding) and employers (large intelligence corporations) of these interrogators lead to a classification as private intelligence functions. Hence, this thesis proposes a definition of PICs in relation to PMCs along three dimensions: tasks, mandate and the contracting party:

1. Tasks: the primary tasks of PICs is to engage in or support intelligence collection or analysis, either by delivering personnel or providing technical support;
2. mandate: no engagement in combat, it is however possible that the means used in combat are supplied;
3. contracting party: PICs are contracted by a government department that falls within the Intelligence Community.

Consequently, for private intelligence contractors, the abuses are often (but not always) more subtle. This does not mean that intelligence actors act without possibilities of legal violations. The issue of accountability, already complex given the secretive nature of the work intelligence agencies do, is exacerbated where private companies are involved. In the private sector, the capacity for secrecy is greater since corporations are not subject to public tools and independent oversight mechanisms (German). Due to this secrecy, the private-public relationship is more prone to fraud, waste and abuse of funds.

Why is intelligence privatized?

There are several reasons why governments choose to privatize state owned enterprises or public functions. One reason, as former NSA director Ken Minihan observed "Homeland security is too important to be left to the government" (Keefe 298). The overall goal of

privatization is an increase in both efficiency and effectiveness, and therewith a reduction in costs. These general arguments for privatization only partly capture the motivations to privatize intelligence. The overall notion that privatization is cost efficient in the intelligence sector is quickly debunked - an average contractor costs twice the price of a government employee (Chesterman 1056). However, contracting grants the government with great flexibility to scale up and down swiftly - government employees can't be fired or hired as easily - which makes outsourcing an attractive option.

The end of the Cold War marked the start of the marketization of intelligence. The focus and conceptualization of intelligence changed in the wake of the weakening of the nuclear Soviet threat - intelligence on the Soviet arsenal used to be the number one intelligence priority (Delaforce 25). This type of intelligence products were no longer required by the consumers of the U.S. intelligence agencies, as a result, the defense and intelligence budget was cut drastically after the end of the Cold War (Storm 13). Due to these budget cuts, the workforce of the intelligence agencies was reduced significantly. It is in this context that three main causes that resulted in increased privatization of intelligence occurred: critical shortages in skilled intelligence personnel, the vicious federal budgeting process and the shifted dominance in the national security technology landscape.

Critical shortages in skilled intelligence personnel

The personnel shortages that resulted from the budget cuts after the end of the Cold War would later, when the intelligence demand peaked during the Global War on Terror (GWoT), prove impossible to fill in with government personnel. This development forced the intelligence agencies to look at the private sector for skilled personnel (Storm 13). The CIA was for example tasked with providing the necessary linguists to guide the armed forces during the initial attack and occupation of Iraq, linguists they did not have (Gruskin 37). As a consequence, the agency appealed to the private sector to bridge this shortage.

Vicious federal budgeting process

The sudden demand for intelligence products proved not only impossible to address due to the lack of skilled workers, the federal budgeting process turned out to be too vicious to enable the IC to flexibly shift their capacities to address the new threat. The general intelligence budget is largely distributed over the National Foreign Intelligence Program (NFIP), the Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA), a budget that is allocated once a year. However, 85% of the combined intelligence budget is further allocated to the individual organizations in the IC by the Subcommittees on Defense of the House and Senate Committees (Nicola 3).

Accordingly, the allocation of budget occurs annually, and takes considerable time due to the required approval of funding levels (Nicola 3). In contrast, the hiring of contractors is subject to a different process within the federal budgeting process. Contracts are seen as a commodity, this means that the process for hiring contractors is similar to that of purchasing goods, a process that is not as lengthy and subject to funding levels as when an agency applies for a budget to increase their regular workforce (Krishnan 196). The hiring process for contractors is simply quicker than hiring civil/military servants, while the funds come from the very same federal budgets.

The shifted dominance in the national security technology landscape

The participation of the private sector is furthermore influenced by the shifted dominance of national security technology. First, the U.S. Department of Defense (DoD) is no longer the leading entity in the development of key technologies with application for national security. Due to the budget cuts in the wake of the Cold War, the DoD was no longer able to compete with the private sector in the development of defense technology. Throughout the 20th century, the DoD was the leading organisation for the research and development of defense technology. Amongst others, ARPANET, the predecessor of the internet as we know it today, was in-house developed. Due to the increased role of the market in the development of technology and budget cuts in the wake of the Cold War, companies took over this leading role in the development of these pivotal technologies for national security. Accordingly, the development of satellites and other spy equipment shifted to the private sector. Around the 2000s, 120 private companies were involved in the launch of more than 1000 satellites (Delaforce 27).

Which intelligence functions are outsourced?

The first validation of the vast amount of outsourcing, about which many have speculated, came in 2006. In a PowerPoint presentation, Terri Everett, a senior procurement officer, coined the sentence that would later become the slogan of scholars dealing with the topic of privatization within the intelligence community: ‘We can’t spy… If we can’t buy’ (Shorrock 16). In this PowerPoint presentation, the statistics were revealed: in 2006, over 70% of the $60 billion intelligence budget went to private contractors, amounting to a staggering $42 billion (Shorrock 13).

The CIA, in both its analysis branch and National Clandestine Service, outsources approximately 50 percent of its budget (Gruskin 38). The Defense Intelligence Agency (DIA) allocates between 35 and 52 percent of their budget to the market, whereas the National

Reconnaissance Office (NRO) outsources 95 percent of their budget (Krishnan 196, Shorrock 18). The numbers for the National Security Agency are not conclusive, it is, however, safe to argue that a large share of their budget goes to contractors since their core activities require private sector involvement. Moreover, between 2001 and 2006, the number of contracted companies rose from 140 to 5400 (Shorrock 18). The NSA for example, awarded a $6.7 billion contract to three companies in 2018 (Konkel).

So, the discussed agencies outsource between 35-95 percent of their budgets, with 70 percent of the total intelligence budget being outsourced. Which tasks in the Intelligence Community are then marketized? The majority of outsourcing happens in intelligence collection, about 27 percent of the contractors are hired to take part in one of the intelligence collection disciplines (Krishnan 196). In human intelligence (HUMINT) collection, the handling of sources, interrogation and rendition are in some instances privatized. For signals intelligence (SIGINT), first hand collection, electronic intercepts, electronic surveillance and technological solutions are outsourced (Chesterman 1070). Moreover, 4 percent of the contractors participate in some form of covert intelligence gathering operations (Krishnan 196).

Additionally, administrative tasks, linguistic services and software suppliance are often conducted by the private sector. Together with exploitation of facilities and research and development activities, this amounts to approximately 28 percent of the ‘green badge’ workforce (Krishnan 196). For analysis of information, contractors participate in the analysis of all three types of intelligence; tactical, strategic and tactical. About 19 percent of the contractor workforce are allocated to intelligence analysis (Krishnan 196). In the final stage in which intelligence is disseminated, an often overlooked area of privatization, private actors participate in the President’s Daily Brief and disseminate intelligence through their own channels (Krishnan 200). In addition to the contractors operating in the intelligence cycle area, 19 percent supports enterprise management, a vaguely defined term that is equivalent to handling the daily business of a company (Krishnan 196). The remaining 4 percent of the contracted workforce is scattered across the Intelligence Community.

These numbers show the deep involvement of the private sector in the Intelligence Community in the United States. Contractors take part in nearly all functions of the Intelligence Community, usurping approximately 70 percent of the entire intelligence budget. With such an amount of taxpayer money on the line, it is necessary that the contractors account for their conduct.

Legal accountability over PMCs

The range of interpretations of accountability legal scholars use is extremely broad, some see accountability as an umbrella concept that describes any mechanism that makes institutions responsive to their public (Bovens 8). Others identify multiple conceptual dimensions of accountability, amongst others relating to transparency, responsibility, responsiveness and liability (Bovens 8). In the most broadly supported definition, accountability is seen as “a retrospective process that obliges an actor (i) to explain and justify his or her conduct (ii) in a forum where questions can be put and (iii) an evaluation made or judgment is arrived” (Harlow 197). A negative outcome of this evaluation process indicates that there must be a consequence for the actor that is responsible for the unacceptable conduct (Harlow 197). Hence, effective accountability means that when misconduct is observed, consequences follow. The best way to discuss PIC accountability is to explore the scholarly discussion on PMC accountability, since the phenomena are closely related and a distinctive academic field on PIC accountability is absent.

In the context of legal accountability over PMCs, there are four main mechanisms to establish legal accountability. First, through the extension of national law to cover extra-territorial misbehavior and crimes perpetrated by contractors (Maogoto et al. 102). Second, by applying the international treaties on the conduct of warfare to contracted personnel (Maogoto et al. 102). The third mechanism focuses on the promotion of public law values through the procurement process and the content of the contractual agreements to hold PMCs accountable for their conduct (Dickinson, 2011, p. 72). The majority of scholars focus on hard law frameworks as the only legal accountability mechanisms to hold PMCs accountable. However, there are also ‘soft’ mechanisms that can contribute to the establishment of accountability. Hence, the fourth mechanism focuses on the effectiveness of soft law, such as codes of conduct, in establishing accountability (Leander 468). Below follows a more in-depth discussion of the identified legal accountability mechanisms.

International law

Although states are often considered the target subjects of international law, it is possible to establish legal accountability over the conduct of PMCs through the application of international law. There are several international treaties that can be useful, primarily the Geneva Convention 1977 and the UN Convention Against the Recruitment, Use, Financing and Training of Mercenaries 1989. The Geneva convention recognizes three types of actors: combatants, mercenaries and civilians. In order to establish liability in international law, the actor that engaged in a violation of the convention, must fall within the scope of one of those

categories. If not, the Convention is not applicable since it can not legally recognize the perpetrator of the crime (Doswald-Beck 2). Both Conventions define civilians along the line of exclusion, meaning that if one does not fall in any other category codified, he or she is considered a civilian (Schmitt 523).

Additional Protocol I of the 1977 Geneva Convention 1977, provides a definition of mercenaries along six conditions, that all have to be met in order to classify an individual as a mercenary (Doswald-Beck 8). The two distinctive elements that are useful in the classification of a contractor as mercenary are that the individual must have been recruited to fight in an armed conflict and must engage in direct combat (Kalidhass 6). The UN Convention provides a broader definition of mercenaries, and includes individuals that are recruited specifically to destabilize a government (Kalidhass 7). The UN Convention is, however, in accordance with the Geneva Convention in its assumption that a person can only be classified as a mercenary when he or she takes part in hostilities, which limits its applicability to contractors that perform logistic support or other non-combat roles.

The second option to establish accountability under international treaties stems from the classification of PMCs as combatants. Arnpriester (1209) argues that under the Geneva Convention “PMCs are only considered combatants if they either (1) (a) are incorporated into the state’s armed forces or (b) fight for a party to the conflict or (2) take a direct part in hostilities". PMCs and its personnel can also be considered combatants since they are quasi-state actors (Singer, 2003, p. 532). Additional Protocol I Article 43 includes, into its definition of armed forces, all groups or parties that fall under the responsibility of the state that takes part in the conflict (Schmitt 523). Since the companies that hire out the individuals are liable by contract to the state that hired them, they fall within this definition of a combatant (Singer, 2003, p. 532). For international law to be an effective mechanism to hold PMCs accountable, the actor under scrutiny must be classified as an actor that is included in the language of the Convention.

Extension of national law

In addition to the use of international law, another possibility to establish accountability over PMCs is to extend the jurisdiction of national law to contractors operating abroad. This would indicate that a PMC can be tried in U.S. courts when the violations committed abroad would be felonies if they had occurred on U.S. soil (Chapman 1064). For the United States, the Military Extraterritorial Jurisdiction Act (MEJA) gives investigators and civil courts the jurisdiction to investigate and try crimes committed by private citizens on foreign soil (Voelz 28). The MEJA gives federal investigators the needed legal framework to gather evidence on

crimes overseas. The act is limited to offenses that would constitute be punished with imprisonment for more than one year (Stein 593). Also, the MEJA includes provisions that military law precedes civil law when the military would have jurisdiction, therefore limiting the possibility that a jurisdiction gap between the MEJA and military law would occur (Stein 593). In theory, the Act gives prosecutors and investigators a far-reaching mandate to engage in such investigations (Kemp 503).

The application of military law to PMCs forms another legal source of accountability. When including PMCs into the legal boundaries in which the United States military operates, contractors can subject contractors to courts martial (Kemp 501). In the United States, the military is governed by the Uniform Code of Military Justice (UCMJ). When looking at the formulation of the UCMJ, individuals serving or accompanying the military in a non-official occupation are liable to its legal boundaries (Kemp 501). As a consequence, private contractors that accompany military units are subject to the same set of rules that govern the behavior of official military employees. Therefore, if they commit crimes while supporting military missions abroad, they should be brought before courts martial when they commit a crime.

Public law values and contractual accountability

During the procurement process of regular federal contracts, both the contractor and the procurement officers are bound by rigid rules that promote competition and transparency. In the defense and intelligence industry, however, many of the contracts are negotiated in secret behind closed doors (Dickinson, 2011, p. 71). The increased reliance on private companies by the military and intelligence agencies automatically results in an increase in contracts granted. This means that it is crucial to properly draft these contracts in line with the public and legal values governing the public domain - since a greater percentage of the workforce is contracted. As Dickinson (2011, p. 72) puts it: “Contractual terms can specify norms and can help structure the privatization relationship in ways that spur contractors to implement those norms”. But first, however, the contracting process must be transparent. Selection criteria must be specified before the contracting process, eliminating companies that are unlikely to deliver the service they are contracted for (Cottier 642). Therefore, within the contracting process, bidding companies can be obliged to submit information regarding qualifications, licenses and experience (Cottier 641).

The primary tool to establish accountability for PMCs are the contracts they have with government bodies (Hedahl 5). As Tkach (8) puts it: “Contracts are the governing authority between employers and PMCs”. The contracts determine the scope and activities to be

performed by the PMC, they are therefore accountable when they cannot fulfill their contractual obligations Cottier 640). Hence, contracts can function as the vehicle by which public values can be forced upon PMCs. For example, contracts can include clauses that provide for enhanced monitoring and oversight through the establishment of benchmarks (Dickinson, 2011, p. 73).

The very form of the contracts can contribute to accountability. As Tkach (4) argues, “when PMSCs have contractual performance incentives and face intra-sector competition, performance improves”. The structure of contracts can reduce the uncertainty of the government employers that services are not, or not properly, delivered (Tkach 12). By boarding up the contract, including the desired behavior and the desired service level of the contracting party, and attach performance incentives, PMC behavior can be effectively controlled (Tkach 13). After all, the reason for a PMC to enter into a contract with another party is to maximize profit.

Soft law: codes of conduct

Soft law, law that is not criminally litigable but rather provides guidelines of conduct, can be a tool to establish accountability. Codes of conduct often lay out ethical standards that govern the conduct of government officials. These codes of conduct can deal with the government side of contracting if they seek to incorporate specific values to the contracting process (Leander 468). Codes of conduct can also function to directly govern the behavior of contractors when ethical standards of conduct are directed at the activities contractors undertake. Codes of conduct need to be established, after which its application should be monitored and enforced by outside groups, such as independent oversight bodies (Dickinson, 2005, p. 175). It is unlikely that groups working for profit, such as PMCs, have a focus on ethical norms regarding human rights, since they are motivated primarily by money, not by standards of human dignity (Dickingson, 2005, p. 233). It is therefore necessary that codes of conduct are implemented and enforced top-down, that is from the employer of the PMC rather than from within the PMC.

Case studies

As the theoretical review of legal accountability over PMCs shows, there are several legal mechanisms that can contribute to the establishment of accountability. The case studies that follow seek to investigate whether these mechanisms also apply to PICs, and whether they are effective. Hence, chapters 2, 3 and 4 discuss existing legal accountability mechanisms that govern the conduct of private intelligence actors that are also present in the literature on PMC accountability. Chapter 2 investigates the effectiveness of the legal basis of intelligence

outsourcing, consisting of the definition of which functions can be marketized and how the procurement and contracting process is shaped. Chapter 3 evaluates the application of national law on foreign soil. Chapter 4 assesses ‘soft’ regulations in place that seek to counter conflicts of interests and provide whistleblower protection. The individual chapters conclude on the effectiveness of the respective legal accountability mechanisms they cover, the conclusion provides a discussion of the investigated legal accountability mechanism and an evaluation of their effectiveness. The analysis within these chapters focus on the applicability and effectivity of the discussed legal accountability structures.

Limitations

This research is conducted with several limitations. First, due to the secretive nature of the intelligence industry, it is very difficult to obtain first hand evidence. Those who did (amongst others Tim Shorrock) spent years creating and maintaining a network of people (formerly) working in or for the Intelligence Community. The scope of his research is therefore limited since it rests mainly on secondary sources, not taking into account congressional or judicial documents that are publicly available. However, when congressional or judicial documents are available, this means that there has been some sort of inquiry into the conduct of that specific case. This means that this type of primary source only exists when misconduct is identified. Also, due to the secretive nature of the IC, and the necessity to protect your modus operandi from becoming known to adversaries, only negative cases become aware to the public and consequently the subject of scholarly research. This results in an unavoidable researcher bias, there is simply only data available for investigated cases that are by nature negative. Due to these pitfalls, this thesis leans largely on secondary sources, i.e. scholarly articles and investigative journalism. However, due to the role of the PICs in the provision of national security, and the magnitude of the cases of misconduct identified, an assessment of the accountability structures that govern privatization in this sector is justified.

Chapter 2

The legal basis of outsourcing intelligence services and contractual accountability: OMB A-76 and the FAR.

Effective legal accountability starts with the delineation of the specific tasks that can be outsourced, and subsequently which private actors are eligible to perform these tasks. This distinction is essential, and serves as the very basis on which contracts are granted to the private sector. In the United States, the functions that can be outsourced are defined by OMB Circular A-76. The Federal Acquisition Regulation (FAR) seeks to establish contractual accountability through the structure of the contracts and the integrity of the procurement process. These pieces of legislation therefore function as the very basis of the privatization of intelligence, they determine which functions are opened up to the market, and which company can perform these functions. Hence, they function as ex ante legal accountability mechanisms. This chapter assesses the effectiveness of both articles of legislation in establishing legal accountability over PICs through their defining role in shaping outsourcing. First, the legal foundation of intelligence outsourcing is assessed. Second, an overview of the problematic conceptualization of functions that should be inherently performed by the government follows. Third, the procurement process and the shape of the intelligence contracts are discussed. The chapter concludes with the assessment of the effectiveness of this legal accountability framework.

OMB Circular A-76

The Constitution of the United States enumerates the functions and boundaries by which the activities of the government are delineated. The Constitution establishes the powers that the President of the United States enjoys and grants specific authority to civil and military servants (Storm 676). In broader terms, the Constitution determines what the exact function of the government is in performing their constitutional duty. Intelligence agencies are no exception. Like other government agencies they are limited in their behavior by the rule of law. Even the special powers the agencies enjoy due to the nature of their work are subject to the legislation that grants them these powers. As the Commission on the Roles and Capabilities of the United States Intelligence Community (Brown and Rudman), which was chartered by Congress to review the American intelligence apparatus, states: “U.S. intelligence agencies are bound, and consider themselves bound by the Constitution and

laws of the United States, including treaty obligations and other international agreements entered into by the United States" (Brown and Rudman). When government employees within the intelligence agencies violate these laws, they can be criminally prosecuted like any other employee of a government agency working in other fields of government (Brown and Rudman).

However, the Constitution does not provide any guidance in determining which functions of government can be outsourced to the private sector (Storm 676). The legal basis that allows for the marketization of intelligence activities is Executive Order 12333 United States Intelligence Activities (Voelz 23). This order grants intelligence agencies the possibility to contract private companies for the provision of services (Voelz 23). Title 10 of the U.S. code additionally provides military commanders the possibility to expand commercial security and intelligence related services to be delivered abroad (Voelz 23). Nevertheless, Executive Order 12333 does not provide any guidance as to which activities can be outsourced, and if so, which legal framework applies to these acts.

To fill this gap, the Office of Management and Budget (OMB) published Circular A-76, which lays out the requirements for tasks that should *not* be privatized. Circular A-76 puts forward that functions that relate either to the act of governing or that are intimately related to the public should be considered as inherently governmental (Voelz 24). Circular A-76 defines:

> "(...) An inherently governmental activity involves:
> *(1) Binding the United States to take or not to take some action by contract, policy, regulation, authorization, order, or otherwise;*
> *(2) Determining, protecting, and advancing economic, political, territorial, property, or other interests by military or diplomatic action, civil or criminal judicial proceedings, contract management, or otherwise;*
> *(3) Significantly affecting the life, liberty, or property of private persons; or*
> *(4) Exerting ultimate control over the acquisition, use, or disposition of United States property (real or personal, tangible or intangible), including establishing policies or procedures for the collection, control, or disbursement of appropriated and other federal funds."*

Thus, Circular A-76 provides some insight into which functions should be inherently governmental and which tasks can be outsourced to the market.

There are, however, two problem areas: 1) agencies have to develop procedures identifying inherently governmental functions themselves, this is not done by the OMB or any other governmental body and 2) Circular A-76 is subject to change. Firstly, the OMB provides a broad definition of which functions must be performed by government personnel in general terms. This means that the respective agencies have to apply the already ambiguously defined concepts to the tasks falling within the scope of their agency. The agencies therefore enjoy great discretion to interpret Circular A-76. The Government Accountability Office (GOA) underscored in a 2014 IC hearing that ODNI, CIA, DOJ and DOE did not apply the definitions put forward by the OMB into procedures (Singh 26). Secondly, the 2013 revision of circular A-76 opened the gates for activities to be outsourced in instances where contractors are not on the top of the chain of command, but if this condition is met, they can be tasked with the development of courses of action (Chesterman 1071). The changing nature of laws makes it problematic for agencies to develop standard codes of conduct to guide contracted behavior. Additionally, intelligence contracts are often long-term, and changes in laws will therefore not guarantee change within reasonable time.

Inherently governmental functions

Luckey et al. (2009) further specified this gap between the Constitution and the reality of privatization in government in their congressional study, by creating three categories of government functions. These categories comprise those functions that "must be performed by government employees, those that should be performed by government employees, and those suitable for private sector performance" (Luckey et al. 1). The first category comprises 'inherently governmental functions' that should only be carried out by government employees (Voelz 23). Whereas the second category is a grey area, functions that should be performed by government officials but where the market can play a role as well.

This ambiguous conceptualization turns out to be even more inconsistent in practice. The language of the ODNI definition of inherently governmental personnel, for example, is subject to change. At times, ODNI's conceptualization of core functions was interpretable as allowing contractors into these functions (Singh 25). Notwithstanding the ambiguity of what consists of inherently governmental and what not, the discussion seems almost futile when taking into consideration the position of the Office of Federal Procurement Policy (OFPP) on the matter. The OFPP is responsible for drawing up policy regarding federal procurements, intelligence outsourcing not being an exemption. In 2011, the OFPP failed to determine *who* must perform inherently governmental functions (Singh 26). Even if a clear cut definition of such functions would exist, they are not necessarily allocated to government officials.

An additional gap in the existing regulatory framework as proposed by the OMB and partly turned into policy by the OFPP is the use of Personal Service Contracts. Agencies are '(...) normally required to recruit its employees by direct hire under competitive appointment or other procedures required by the civil service laws', unless otherwise decided by Congress (Halchin 12). A Personal Service Contract establishes an employer-employee relation, which distinguishes it from a services contract in which a service is marketized rather than an employee (Cornell Law School). When a contractor is contracted through a Personal Services Contract, they should be classified as a government employee (due to the employer-employee relationship) which would make it impossible to prevent the contractor from participating in inherently governmental functions. The allocation of inherently governmental functions to the market would privatize functions that are only legal when government employees perform them, illegal activities under a government contract can't be legally overseen due to the contradicting status of such contracts.

The Federal Acquisition Regulations Systems (FAR)

When a specific task is allocated as suitable to be outsourced, the procurement process decides which company wins the contract. This process is shaped by the General Services Administration Acquisition Regulation (GSAR) and the Federal Acquisition Regulations (FAR) Systems (Office of the Director of National Intelligence). The vision of the FAR can best be summarized as 'to deliver on a timely basis the best value product or service to the customer, while maintaining the public's trust and fulfilling public policy objectives' (Federal Acquisition Regulations 1.102(a)). The contracts in the intelligence industry consist of cost-plus-fixed-fee contracts, in which contractors are reimbursed for their costs. The costs-plus element of this type of contract indicates that a contractor can exceed the initially agreed upon contract price when activities change due to the nature of the assignment. This type of contract is suitable for 'efforts that might otherwise present too great a risk to contractors, but it provides the contractor only a minimum incentive to control costs' (Federal Acquisition Regulations 16.306(a)).

The Government Accountability Office found that the DoD violated procurement rules which led to inadequate management and oversight on the performance of the private companies holding the contract (Halchin 1). The DoD started paying out to contractors 'before reaching a final agreement on the contract terms and conditions, including price' (Halchin 1). These arrangements, known as Undefinitized Contract Actions, are used 'to meet urgent need or when the scope of the work is not clearly defined', these undefined and illegitimate costs adding up to 221 million U.S. dollars in 2007 (Halchin 1).

Section 16.306(b)(2) of the FAR states that ‘a cost-plus-fixed-fee’ contract normally should not be used in development of major systems’. This clause refers to the minimal incentive that contractors have to control costs that they can charge to the client. The definition of what consists of a ‘major’ system is semantically difficult, there are however two failed billion dollar projects that can’t avoid the classification of ‘major’: NSA’s Trailblazer and the NRO’s Future Imagery Architecture project.

The NSA Trailblazer project

After being too late to translate the crucial message ‘Tomorrow is zero hour’, on the day before 9/11, the NSA wanted to design a system that can sift through large piles of telecommunication data (Barlett and Steele 3). One of the candidate systems was ThinThread, in-house developed by top NSA employees, ready to deploy, and relatively cheap with an estimated cost of 3 million USD (Shorrock, 2013, 4-15). The contract was nonetheless granted to SAIC in April 2001. The 26-month contract was initially worth 280 million USD, after four years and having spent over one billion USD, the project was declared as failed and stopped with no significant outcome (Barlett and Steele 3). For most companies, such a blatant failure would mean that they should forget about future contracts with this same client, but not for SAIC. In 2006, the NSA awarded the program ExecuteLocus to SAIC, to succeed the same Trailblazer project that never rendered any results (Harris).

Trailblazer is by some deemed as outright corruption and favoritism by former NSA director Michael V. Hayden and his associates (Shorrock 2013, 14). Tom Drake, one of the prominent NSA whistleblowers on Trailblazer, calls the project a scam invented by SAIC and the other corporations to milk as much money from the government as possible (Shorrock 2013, 14). Despite these accusations, the gross overspending and underperformance could have been prevented if the contracting process would have complied with the FAR. That SAIC was awarded the successor of Trailblazer shows the lack of functional regulations that prevent companies that fail, due to circumstances that fall within their power, from bidding on future projects of the same magnitude. The appearance of the current situation is that failure is awarded with more contracts, which directly opposes the vision of the FAR. These observations show that the FAR is effective in theory, it is rather a lack of enforcement that causes trouble. Whereas the OMB Circular A-76 offered discretion regarding the exact meaning of the regulation, in this case, the ground rules of the FAR are clearly stated and codified, it is here that a lack of applying the regulations lead to misconduct.

The NRO Future Imagery Architecture

Another case of overspending on a cost-plus contract was the Future Imagery Architecture (F.I.A.) project, outsourced by the NRO to Boeing in 1998. The NRO sought to replace their old fleet of large and expensive satellites with a constellation of smaller satellites that could provide a better cover of warzones in order to provide tactical intelligence to military commanders (Taubman). Despite the concerns of, amongst others, Porter Gross, the chairman of the House Permanent Select Committee on Intelligence warned for overspending and time issues in 1999 (Richelson 50). In 2002, Pete Teets, director of the NRO, however, claimed that the project was on schedule and well within budget (Richelson 51). The program, that started in 1998, was terminated in 2005 at a cost of over 4 billion USD without producing even a single satellite (Taubman).

The problems with the F.I.A. could have been avoided. Boeing is an excellent airplane manufacturer, but lacked the expertise to build satellites (Taubman). The sole competitor, Lockheed Martin, built the previous line of satellites and had a lot of in-house expertise in this specific area. Additionally, due to new policy, Boeing was responsible for the evaluation of their own project. Instances in which a supplier has to perform oversight on their own work seldomly work out well, after all, why would you oppose your own employer? As the head of the Boeing team, Ed Nowinsky, argued: “Look, we did report problems, but it was certainly in my best interest to be very optimistic about what we could do” (Taubman). Assessing these circumstances in the light of the FAR 16.306(a) warning that ‘major’ projects could lead to overspending show that the directive was directly opposed by 1) outsourcing a ‘major’ contract and 2) making the contracting company responsible for reporting. Therefore, all regulating guidelines that seek to diminish the abuse of government funds were effectively ignored.

Competition

The FAR provides straightforward guidance on the required competition when contracting out a service. The FAR section 6.102 (a) urges for either sealed bids, competitive proposals, a combination of competitive procedures or other competitive procedures. In practice, realizing competition in the intelligence industry is extremely difficult. The problems start at the bidding phase, the secretive nature of intelligence contracts and the required access to classified systems and documents require that personnel that executed the contracted service have high-level security clearances. The vetting process for new security clearances is an extremely lengthy process, at times the process is stopped completely due to mismanagement in the relevant office (Chesterman 1068). As a result, newcomers can

hardly get their personnel security clearances during a procurement process, which often takes less time than the vetting process. Therefore, only companies with enough high-level cleared personnel can bid on a contract (Shorrock 51). The need for security clearances therefore significantly reduces competition. The problems surrounding security clearances limit the possibilities of the procurement officers to effectively establish compliance to FAR section 6.102(a), thereby eliminating the effect of the legal ramification of the tender process that should prevent misuse.

Additionally, a 2008 audit by the SSCI concluded that '[The IC] has insufficient experienced professionals to properly oversee the execution and management of billions of dollars in annual acquisitions' (Halchin 18). Alternatively, contracting happens on the basis of people the agencies trust, not the competencies of the company those trustees work for or the quality of the bid. Former high-ranking intelligence officials (f.e. Tenet, Dempsey, Gannon, McConnell etc.) function as so-called 'rainmakers' to bring in new businesses from their former agencies from which they enjoy trust (Shorrock 33). The inspectors general for the Department of Defense and the Department of the Interior concluded that half of the contracts awarded in 2006 were granted without competition or checks on prices (O'Harrow and Higham). This results into violations of the FAR by not providing best value for service and ignoring the competitive process laid out in the regulatory framework.

Are OMB Circular A-76 and the FAR effective legal accountability mechanisms?

OMB Circular A-76, complemented with OFPP policy, fails to effectively shape the contours of the tasks that can be outsourced to the private sector. The result is a vaguely defined playing field for both the contractors and the procurement officials. The very definition of functions that can be outsourced are badly defined, creating a large grey area of contracting that falls outside the scope of the procurement process. Government officials negotiate these contracts in secret, the contracts themselves are consequently classified as top secret for security reasons and therefore not available to the public (Dickinson 71). Additionally, the rules for contracting put forward by the FAR are often not followed, which means that for those cases to which the procurement process applies, the process is handled improperly. The legal framework is in theory viable in preventing overspending and abuse, in practice the FAR is useless. In other words, the FAR is not being properly applied, nor enforced. The lack of competition makes the government extremely reliant on a small number of companies that will receive future contracts no matter how they perform. Additionally, the

very contracts in which a specific service is allocated to a specific company have a legal structure that does not allow for punishments for mismanagement or overspending. The cost-plus structure results in no incentives for companies to contain costs properly, and guarantees that the companies cannot be held accountable because overspending is justified by the contracts.

Therefore, the OMB Circular A-76 and the FAR are not effective legal accountability mechanisms. They fail to properly define the legal basis for the outsourcing of intelligence services, which results in many grey areas. Consequently, no oversight can be performed on these grey area cases since there is no legal basis. The result is the lack of a clear definition of the ground rules of privatization in the intelligence sector. This became visible in the case studies of Trailblazer and the Future Imagery Architecture, blatant failure was not met with any sort of legal repercussions. Additionally, the very basis of market efficiency - competition - is nearly completely absent, which results in grave inefficiencies in the allocation of government funds. This dynamic creates a vicious cycle in which 1) companies with a bad reputation can still win major contracts and 2) if they fail to deliver what they were contracted for, they are not punished but rather rewarded with new contracts.

Chapter 3

National and international law application to PIC misconduct on foreign soil: The MEJA and the UCMJ

This chapter focuses on the judicial review of misconduct by private intelligence actors on foreign soil. The Uniform Code of Military Justice (UCMJ) and the Military Extraterritorial Jurisdiction Act (MEJA) enable government and civil actors to hold private actors both ex ante and ex post to account for their actions. That is, the UCMJ and MEJA provide the legal boundaries to determine whether the actions of private actors on foreign soil are legal or not. Consequently, when misconduct occurs, they both function as legal tools to punish those responsible for misconduct. This chapter therefore evaluates the effectiveness of the UCMJ and MEJA as ex ante and ex post accountability mechanisms. First, an evaluation of MEJA will be explained. Second, the legal discrepancy between contractors and government employees follows. Third, the option to use international law to review conduct on foreign soil is explored. Fourth, the counterproductive influence of the executive branch on the functioning of the MEJA and UCMJ will be described. The chapter concludes with an assessment of the effectiveness of the judicial review of misconduct on foreign soil as a legal accountability mechanism.

The Military Extraterritorial Jurisdiction Act

For contracted personnel, working outside of U.S. territory but on a contract with the DoD, the MEJA outlines the legal jurisdictional basis. The act theoretically guarantees that contractors acting abroad on behalf of the DoD fall within the legal jurisdiction of U.S. legislation (Voelz 28). There is, however, a significant loophole in the MEJA, as it does not apply to non-U.S. personnel. The *Kiobel v. Royal Dutch Petroleum* ruling of 2013 solidified this loophole with case law, concluding that violations outside of the U.S. territory perpetrated by foreign nationals fall outside the jurisdiction of U.S. courts (CCR 2). In a traditional military theatre on foreign soil, governments can only use uniformed soldiers that have the nationality of the army they serve. However, companies can operate with international staff. Thus, in accordance with the *Kiobel v. Royal Dutch Petroleum* ruling, non-U.S. contractors are indeed exempt from U.S. legislation.

A second loophole in the MEJA is its incapability to hold contractors that are not hired by the DoD, but by another department of the U.S. government, liable (Lindemann 87). The case of the Abu Ghraib abuses in 2004 shows this inefficiency. In this case, both the CIA and the DoD used contractors to interrogate suspects in Abu Ghraib with ‘enhanced interrogation techniques’, an other word for torture. At the time of the abuses, 27 out of 33 interrogators were private contractors (Storm 674). None of the contractors were convicted for their role because they were either non-U.S. citizens or officially hired by the Ministry of Interior (Lindemann 87). Additionally, the Coalition Provisional Authority operating in Iraq signed an agreement with the Iraqi government exempting contractors from being prosecuted under Iraqi law (Voelz 28). The non-U.S. citizens that engaged in abuses could therefore not be held legally accountable by both the U.S. Military court under the MEJA nor the Iraqi courts.

When the application of MEJA proved insufficient, victims of the torture abuse in the Abu Ghraib prison sued both CACI int. and Titan Corp. for their involvement in the interrogations in Iraq in the *Saleh, et al. v. Titan Corp*. U.S. civil law case (Barouch 63). The claims brought to the companies were based on both U.S. and international law, when the case arrived at the DC Circuit Court of Appeals the claims left consisted of tort claims on a state level (Barouch 63). Another claim was supported by the Alien Tort Statute, giving federal courts jurisdiction in cases in which foreign nationals violate a U.S. treaty (Barouch 63). CACI Int. and Titan Corp. referred to federal legislation where action that was subject to the military chain of command could not be heard by civil courts but only by martial courts (Barouch 64). The judges ruled that federal law preempts state legislation meaning that contractors under direct military command could not be prosecuted in civil or federal courts (Barouch 63).

In 2019, however, the District Court for the Eastern District of Virginia ruled on the landmark case *Al Shimari et al. vs. CACI Premier Technology.* The Court ordered that the group of torture victims that started this specific case, could bring charges against CACI Premier Technology (Klasfeld). Although this decision created a precedent for other victims of contractor abuse, it shows that in the face of the government only the company can be held accountable, not individual employees. It is therefore not surprising that the only court ruling regarding the abuses at Abu Ghraib so far is a settlement concerning a pay-out of $5,3-million, imposed on L-3 Services Inc, a company that delivered translation services at Abu Ghraib (Bierman).

UCMJ and the discrepancy between contractors and government personnel

As opposed to the impunity of the contractors in Abu Ghraib, the judicial situation for DoD personnel is different. Military personnel working on behalf of the DoD outside the U.S. fall under the Uniform Code of Military Justice (UCMJ). Meaning that in this case, the DoD is responsible for crimes committed by DoD personnel during their overseas operations. Consequently, several military personnel faced sanctions after the Abu Ghraib abuses in the form of reprimands or convictions by military court (Storm 675). In March 2020, a total of 11 U.S. soldiers were convicted for crimes related to the abuses. Four of those were sentenced to time in prison, varying from 6 months to 10 years (CNN 'Iraq Prison Abuse Scandal Fast Facts'). Legal oversight on the actions of members of the U.S. Military is straightforward and happens quickly in line with the UCMJ.

This discrepancy shows the great difficulty the U.S. faces concerning the legal liability of personnel contracted by the U.S. government. There is a large difference between the enforcement of legal accountability for contractors in the intelligence realm engaging in atrocities and the legal accountability for U.S. military and intelligence personnel participating in the same abuses. The UCMJ and MEJA proved ineffective in holding the contractors legally accountable, whereas civil court cases were nearly all shelved after a decade of litigation. In contrast, the military personnel engaged in the same atrocities were effectively convicted. There has, however, been a shift in attention after the media coverage of the abuses at the Abu Ghraib prison. The MEJA was amended in 2004 to include contractors that were contracted by departments other than the DoD (Voelz 28). Under the MEJA, a contracted partner is now defined as contractors that work to further the broader DoD mission in the specific geographic area they are deployed, not only when they are factually hired by the DoD (Brown 443). This amendment was created to close the previously discussed jurisdictional gap through which intelligence contractors could evade prosecution (Brown 443).

In 2006, U.S. Congress attempted to close the legal gaps specifically related to PMCs that could possibly have to deal with gun-fights, by amending the UCMJ. The amendment concerns an addition of the following group of civilians being subject to UCMJ: "In time of declared war or a contingency operation, persons serving with or accompanying an armed force in the field." (Brown 445). The amendment guarantees that PMCs fall within the jurisdiction of the UCMJ when they accompany military units during operations even when there is no declaration of war at the location of the mission (Arnpriester 1217). However, this

literal reading of the code has been reversed by case law. In *Reid v. Covert*, the Supreme Court ruled that courts martial law is not the appropriate forum to hold individuals accountable that are not directly employed by the U.S. military (Kemp 502). Also, the UCMJ only applies when there is a declared war going on in the country in which the crime is committed (Kemp 503).

The amendment grants military commanders with extended powers to trial contracted personnel under the same set of rules that guide the behavior of military personnel. Another consequence of the amendment to the UCMJ is the change in chain of command required. When PMCs were not liable to the UCMJ, they maintained their own chain of command. With the change in liability, additional responsibilities are directed towards military leaders that can now incorporate PMC personnel into their chain of command. Placing contractors under the command of military commanders would therefore solve two problems: 1) the legal gap in instances of abuses is closed, and 2) contractors act in the sight of DoD personnel rather than outside the eye of government oversight.

Hence, there are five reasons why the UCMJ and MEJA, and its amendments do not work properly for atrocities committed by intelligence contractors. Firstly, if MEJA is even applicable to civilians acting on behalf of the United States on non-U.S. soil, the legal process is lengthy due to the several legal interpretations of the Act, as is clearly visible in *Saleh, et al. v. Titan Corp.* (Brown 443). Additionally, the application of the MEJA is problematic, as courts hesitate to try civilians in military courts in peacetime (Brown 443). Secondly, despite the legal possibilities to try civilians under the MEJA, the Act does not give the prosecutors the resources to investigate cases (Brown 444). The language barrier makes it incredibly difficult to hear witnesses abroad, it is even more challenging to get these witnesses to testify physically in a U.S. court (Chapman 1065). This means that prosecutors based in the U.S. can hardly investigate cases perpetrated on foreign soil, let alone in areas of conflict. Thirdly, the constitutionality of the UCMJ amendment is under discussion, since it would mean that civilians would be held legally responsible under Military law, which exempts the right to use the fifth and sixth amendment guaranteed to all civilians under the U.S. constitution (Arnpriester 1217). Fourthly, PMCs that do not accompany armed forces or act in a country where there is a declaration of war are excluded from jurisdiction under the UCMJ. Fifthly, the amendment to UCMJ that sought to include PMC into the code, is not seen as such by the Supreme Court.

International law

The establishment of legal accountability over the conduct of PMCs is problematic because of the ambiguous legal status of non-state participants in a conflict under international law (Maogoto et al. 102). As explained in Chapter 1, in order to be subject to international law, PMCs must fall within the scope of one of those categories. Although often argued, it is not easy to legally define PMCs as mercenaries. Protocol I of the 1977 Geneva conventions states that non-state actors in an armed conflict can only be classified as a mercenary when they directly participate in hostilities (Kalidhass 6). This categorically excludes all PICs that in no circumstance take part in hostile activities. Since intelligence gathering is generally non-violent, PICs are excluded from falling within this category. Also, if a non-hostile activity, such as guarding, training military personnel or food supply, turns into a hostile situation, the contractor is still excluded from being classified as a mercenary by the Additional Protocol 1 of the Geneva Convention (Kalidhass 6). Furthermore, the current international treaties such as Additional Protocol 1 of the Geneva Convention and the Convention Against Mercenaries do not explicitly criminalize a state when they use mercenaries (Mehra 6).

When PMCs are not seen as mercenaries, another way to establish accountability would be to incorporate them in the classification of combatants. But, PMCs are not combatants under international law either. As explained in chapter 1, the classification of an actor as a combatant also rests largely on the condition to take part in hostilities. Therefore, PICs are similarly excluded from falling within the definition of a combatant. Also, the incorporation of actors into the state's armed forces can provide grounds to classify such actors as combatants (Arnpriester 1209). However, the tentative conclusion that PMCs or PICs are part of the armed forces is not upheld by the International Court of Justice (ICJ).

The 1986 landmark case *Nicaragua v. United States,* in which the ICJ ruled on actions of various non-state actors, shows the difficulty of legally establishing this relation between the military and the non-state actors. The ICJ ruled that non-state actors fall under state responsibility when they are financed, coordinated, supervised and led by specific instructions to engage in the violation by a third state (Maogoto et al. 111). These conditions to hold private actors accountable focus on the use of violence. PICs, in general, do not have a mandate to engage in lethal action. It is therefore impossible to classify PICs as either combatants or mercenaries, which guarantees that crimes fall outside the scope of international law. However, the requirements laid out by the ICJ in the Nicaragua case would suggest otherwise. The U.S. government financed, in some instances coordinated and supervised and specifically instructed contractors to use torture. This would indicate that the

involved contractors are indirectly liable under international law, were it not that they fail to meet any of the classifications put forward in the Convention, and are therefore not recognized as legal participants to the conflict. Indirect liability in this sense means that the state is liable for the actions of the private actor, which then has to redirect this liability to individuals or corporations. This notion portrays the inherent problem with the application of international law for both PICs and PMCs, they fall outside the scope of the language of the international treaties in place.

Executive branch interference

In addition to the previously outlined jurisdictional gaps, the executive branch can interfere in a civil law-suit. After the court ruled, in one of the Abu Ghraib abuse cases, that several CACI employees could be prosecuted under U.S. law, the company asked for a dismissal of the case because it would raise a ‘political question’ (CCR 2). The ‘political question’ doctrine encompasses that judges should not rule in cases that discuss a political dispute (complies with trias politica). In practice, this means that instead of legal prosecution, the executive branch can decide before a court case starts whether the case concerns a political dispute. The inherent aspect of independence from the executive that guarantees the unbiased functioning of the judicial branch is of crucial importance to the legal process. When applying the ‘political question’ doctrine, the independence of the judicial branch is at stake when the executive branch can prevent sensitive cases from being taken to court. It is not the task of the executive branch to make judicial decisions, the executive branch has the tools to perform oversight within its own boundaries.

Also, the administration has the resources to provide legal guidance to specific activities. The Office of the Legal Council (OLC) produces opinions on policy on behalf of the President. The OLC seeks to predict the judgments of judges when a case relating to that policy is brought to court (Clark 457). For the abuses at Abu Ghraib, the OLC narrowed the definition of torture to such an extent that it was considered as a legal practice within the executive branch working with terrorism suspects (Weiner 426). According the OLC opinion, torture could only be defined as such when the interrogator intends to inflict damage on the suspect that is associated with organ failure or death (Clark 459). This legally binding executive memo shaped the precedent for the treatment of terrorism suspects. Therefore, the OLC memo indirectly allowed both contractors and government employees to use torture techniques that do not normally result in organ failure or death, techniques such as waterboarding and walling.

Additionally, agreements with a foreign administration can hamper the oversight process. The Coalition Provisional Authority in Iraq signed an agreement with the Iraqi government exempting contractors from being prosecuted under Iraqi law (Voelz 28). These political decisions eliminated a legal source that could potentially be used to establish accountability.

Are the UCMJ and MEJA effective in applying national law on foreign soil?

To what extent are the MEJA and UCMJ effective in applying national law to misconduct on foreign soil? In theory, after the implementation of the amendments, MEJA is an efficient legal accountability mechanism. Misconduct abroad is coherently incorporated in the amended version of the act. However, the practical implications of the jurisdictional ambiguities make the act hard to apply. Trial in court is extremely difficult due to the jurisdictional gaps and the lack of resources at the disposal of prosecutors to investigate the abuses that often happened overseas. Cooperation with local authorities, would normally be the case, is probably also not possible due to the secretive nature of the activities. This results in the inability to prosecute private intelligence actors for misconduct. Also, if charges are brought against an actor, it is often the company and not the individual. Additionally, the language in the UCMJ and MEJA, and the practical implications of the jurisdictional ambiguities, result in lengthy court cases that will cross several levels of courts (and therefore years) before a conviction can occur.

Furthermore, political interference, such as the arrangement between the Coalition Provisional Authority and the Iraqi government that guarantees that contractors cannot be tried under Iraqi law, eliminates specific legal channels which could successfully result in legal accountability of contractors guilty of abuses. Due to the problematic nature of practical use, the MEJA and UCMJ can in some cases identify and test PIC misconduct on foreign soil. It is however unlikely that those responsible will be punished. This is a strange discrepancy with military officials, who are directly liable under military law. This discrepancy shows that there is legal asymmetry between government actors and contractors.This legal accountability mechanism is therefore ineffective in holding PICs and their employees to account. The best explanation for the inability to properly oversee PICs on foreign soil is the relative newness of this type of service and the interest of political actors in avoiding scandals.

Chapter 4

Conflicts of interest regulations and whistleblower protection: 11 Code of Federal Regulations and administrative oversight.

This chapter provides an overview of the laws and regulations that together constitute the legal accountability mechanism that seeks to prevent conflicts of interests from influencing government behavior. Additionally, the whistleblower protection laws are evaluated. Democratic accountability rests on the assumption that the policy makers abide by the rule of law. They must act in the interest of the people, not for themselves. Therefore, the 11 Code of Federal Regulations (CFR) lays out rules in regard to donations from corporations to politically elected officials. First, the application of 11 CFR on donations from private intelligence companies to the members of both the House and Senate intelligence committees is evaluated. Second, several structural objections to parliamentary oversight on the Intelligence Community are laid out. Third, the effectiveness of the whistleblower protection framework is assessed. The chapter concludes with an evaluation of the overall effectiveness of this set of legal accountability mechanisms.

Conflicts of interest in administrative accountability mechanisms

In the United States, two parliamentary committees reside over intelligence related issues. The House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) (DCAF 4). Both committees have a strong mandate to check the legality of actions and effectiveness, they also hold authorisation and appropriation powers regarding the intelligence budget (DCAF 5). Within each committee, specialised subcommittees oversee specific functions of the intelligence apparatus (Barker et al. 2). Together, they have the mandate to inquire into all the intelligence related activities conducted by the U.S. Government (Barker et al. 2). The house committees shape the budgets for contracting. The budgets from which the contracts are funded, being most notably The National Foreign Intelligence Program (NFIP), the Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA), are all subject to scrutiny from the parliamentary committees.

In 2006, Representative Randy Cunningham was convicted to 8 years imprisonment for corruption charges. Cunningham seated in the House Intelligence Committee in which he had influence over the contracting process, he consequently took millions of dollars from intelligence contractors MZM to favour this company during procurement processes (Keefe 305). The money Cunningham received were outright bribes. Although this is a very rigorous case of a conflict of interest that compromised the administrative ability to establish accountability, more subtle forms of conflicts of interest are visible. PAC donations from private intelligence companies to parliamentary members sitting in the oversight committees are a common practice, despite the fact that it is prohibited by the 11 Code of Federal Regulations (CFR) 100.52(a) and 100.54.

Between 2005-2013, members of the HPSCI and SSCI received nearly 4 million USD from top intelligence contractors for their PACs (Maplight). Among the companies donating to the PACs of the members of the oversight committees are SAIC inc. CACI International, L-3, Booz Allen Hamilton and Lockheed Martin, all companies that have federal contracts and who were in some way involved in misconduct. Notable is the fact that Pat Robert, who was the SSCI's chairman in 2004, received nearly half of his total PAC donations from key contractors in the intelligence industry. Despite CFR articles prohibiting federal contractors from donating, none were punished. The Maplight data only contained donations to either SSCI or HPSCI members, to what extent are other members of the parliament on the receiving end of donations from large intelligence contractors? The total number of donations for the 2020 election cycle amounted to more than 45 million USD (Center for Responsive Politics). Amongst which, again, the same intelligence contracting moguls: Lockheed Martin (5,853,463 USD), L3 (2,488,611 USD), Booz Allen Hamilton (1,086,089 USD), CACI International (521,105 USD) and Boeing (463,388 USD).

Although it is difficult to quantify the influence of these donations on the capability to independently oversee contracting processes, the mere fact that corporations pay the members of the oversight mechanism is highly problematic. It at least creates the possibility to assume that the SSCI and HPSCI are influenced in their oversight activities by those companies. This space significantly reduces their credibility in the public's eye. Notable is that the SSCI and HPSCI are criticized for its structure, the public trust is low, the budgeting process is untransparent and unprofessionally set-up and both committees are understaffed (Cordera). Complemented with the influx of money from the very organizations that they seek to oversee, this gives the committees an incapable outlook.

Conflicts of interest due to non-financial linkages

The President's Daily Briefing (PDB) is a daily briefing performed by high-ranking officials from the IC that intends to up-date the President of the U.S. on the most pressing (national) security issues derived from the combined capacities of the entire IC. The PDB therefore has great influence on the intelligence that reaches the President, but also which intelligence remains within the IC. When taking into consideration that ODNI declared that 70% of the intelligence budget goes to contractors**,** it has significant influence on the perception of threats and therefore on the policy decision making process of the President of the U.S. (Gruskin 41). This policy decision making process subsequently determines where intelligence capabilities are allocated to in the future. The magnitude of this dynamic becomes apparent when looking at the contracts awarded during the wars in Iraq and Afghanistan. The Center for Public Integrity concluded that approximately 60 percent of the contracts awarded during these conflicts were given to companies with board members or prominent employees that served in official capacities (Dickinson 71).

This very mechanism is dangerous, as the war in Iraq shows. Intelligence contractor SAIC created their own centre for intelligence analysis called the 'Center for Counterterrorism Technology and Analysis' (CCTA). After the 9/11 attacks, this CCTA argued strongly that Iraq had Weapons of Mass Destruction (WMDs) that were ready to use (Krishnan 200). David Kay, in 1998 the director of the CCTA, testified before the Senate Armed Services Committee, strongly arguing that Iraq possesses WMDs and that the only course of action is to wage war (Barlett and Steele). This same David Kay was appointed chief U.S. weapons inspector in Iraq, and testified again in 2003 before several House of Representatives and Senate committees that Iraq did not possess WMDs (CNN 'Text of David Kay's unclassified statement'). It is necessary, however, to mention that the war in Iraq resulted in approximately $8 billion in contracts for CCTA's mother company: SAIC (Barlett and Steele). Showing a great monetary interest of SAIC to convince the U.S. government to engage in a war with Saddam Hussein.

SAIC had close ties with neoconservative elements in the George W. Bush administration (Krishnan 200). Barlett and Steele (n/a) argue that Kay and other private sector voices that urged for an invasion in Iraq echoed the voice of then Vice President Dick Cheney and Secretary of Defense Donald Rumsfeld. Although it is agreed that the closed nature of the Saddam Hussein administration resulted in fragmented and limited intelligence available to policy makers, the CIA reporting on Iraq was not perfect either, corporate analysis houses weighed the information that signaled the presence of WMDs too heavily.

The CIAs analysis of the situation in Iraq was more objective without taking into consideration political preferences. The agency refused to establish a relation between Osama Bin Laden and Iraq, an assumption that was broadly promoted by the private sector analysts (Krishnan 200). It is difficult, if not impossible, to assess whether the corporations influenced politics or the other way around. It is nonetheless clear that SAIC's executives and its analysis department had a great influence on the decision to wage war in Iraq, and that they profited greatly from this policy decision. The conclusion that government employees do not have a hidden agenda, but serve U.S. interests, is not true for corporations, who serve their stockholders. This example clearly signals a conflict of interest. Whereas the nature of the objective of the IC requires the specific agencies to provide information as objective as possible, corporate elements have another agenda, and fare well by information that steers at more contracts for the IC contracting sector.

Structural objections to parliamentary oversight

One of the issues with parliamentary oversight relates to the nature of democracies and their political system that is built on the concept of trias politica. It is undesirable that members of parliament become (more) engaged in the democratic oversight of intelligence agencies ex ante (Hijzen 236). The divide between the executive branch and parliament, along the lines of the trias politica, dictates that democratically elected governments execute policies, whereas parliaments function to oversee these policies (Hijzen 236). When members of the parliament would start to engage in ex ante oversight on future actions of intelligence agencies or contractors, this constitutional divide would become blurry. Moreover, parliament would become responsible for policies since they participated in the decision making process leading up to the execution (Hijzen 236). This would endanger parliamentary independence from the executive branch of government. It is therefore that parliamentary oversight is constitutionally limited to ex post facto oversight (Leigh 7).

An additional argument for the restriction of parliamentary oversight is the notion that the functioning of intelligence agencies should not be influenced by party politics (Leigh 7). If party politics would have a place in providing direction for day-to-day operations, the concern surfaces that these very agencies would be used for political purposes rather than their respective objectives in the security apparatus (Leigh 7). Additionally, if parliamentary commissions have before-action knowledge of specific actions to be undertaken by intelligence agencies, this will hamper the ability of such a commission to review the action independently afterwards (Leigh 7).

Whistleblower protection

Since 2001, 8700 retaliation claims have been filed by defense and intelligence employees against their employers (Taylor 2). Retaliation structures have been put in place to protect whistleblowers legally from acts of vengeance from their employer (i.e dismissal, suspension of clearances). However, retaliation not only happens on an individual level. Qwest refused to cooperate with the NSA in the Terrorist Surveillance Program, a refusal that led to a decrease in classified work contracted to them in the future and cancelation of contracts worth millions of U.S. dollars (Keefe 913). The bureaucratic process to blow the whistle is so lengthy that people rather let mismanagement or abuses go unnoticed than to engage themselves in this process (Taylor 2). In other instances, the whistleblowers are subject to an inquiry themselves, rather than the agency they blew the whistle on. After Thomas Drake cooperated with a Pentagon inspector general inquiry into Trailblazer, he was investigated and prosecuted by Federal investigators for leaking to a newspaper - which he did not do (Taylor 8). For contractors, the situation is even more difficult. There is no legislation to protect contractors from retaliation after they publicize misconduct (Taylor 2).

Are the conflicts of interest, financial disclosure and whistle protection mechanisms effective legal accountability mechanisms?

The existing framework that should prevent conflicts of interest and guarantee whistleblower protection would work in theory. The negligence of the 11 Code of Federal Regulations and the lack of a formal and enforced whistleblower protection framework make this legal accountability mechanism highly ineffective. Although the 11 Code of Federal Regulations lays out clear rules for PAC donations, these rules are rarely enforced. The members of the SSCI and HPSCI, who shape intelligence related policy and oversee intelligence conduct, frequently receive donations from PICs. Hence, the overseers are paid by those they oversee, which raises concerns of conflicts of interest. Although tangential, this indicates that the members of parliament cannot properly perform their duties as oversight committee members. Also, future policy can be influenced by the PICs that now have a (paid) voice within the political elite.

Additionally, the revolving door mechanism, due to which high-ranking officials switch jobs between the government and private sector, has a negative impact on oversight. The empirical evidence shows that these contacts can lead to the provision of false information on which national security policy is based. The PICs can therefore create their own market by signaling specific threats to the policy makers. Both the 11 Codes of Federal Regulations are not properly enforced, unacceptable conduct is not identified, tested nor punished.

Additionally, the revolving door diffuses the differences between the private sector and the government. This results in private company influences in decision making processes that are exclusively reserved for officials. These non-financial linkages form an important barrier to the establishment of legal accountability, that is, it is unlikely that you will heavily criticize your future colleague.

Another influential observation is the malfunctioning of the existing whistleblower protection framework. This framework should enable employees to identify misconduct within their agency or company, which is crucial to the establishment of accountability. When the eyes and ears that have to detect misconduct are treated badly, and will probably lose their career when they come forward, it becomes increasingly difficult to observe misconduct. For the private side of matters, this is even more problematic, and no official guidelines are available.

Conclusion

The previous chapters sketch the image of the marketization of a sector which is better described as lawless than subject to effective democratic accountability structures. All the discussed legal accountability mechanisms are subject to some sort of inadequacy, and in the more extreme cases, absolute failure. The research identified several causes that each explain the failure of the specific legal accountability mechanisms. However, there are several overlaps visible, there are several causes that apply to more than one case. This indicates that there is a more structural problem with the overall legal accountability system that governs private intelligence participation in the Intelligence Community. There are four main causes for the ineffectiveness of the legal accountability system visible: 1) a lack of a clear definition of the ground rules of privatization, 2) legal asymmetry between the government and the private sector, 3) political interference in legal processes, and 4) the reluctance to enforce laws.

Lack of a clear definition of the legal ground rules for the marketization of intelligence

OMB Circular A-76 and Executive Order 12333 fail to lay the legal basis for outsourcing intelligence functions. Both law and policy poorly define which functions can be marketized. Therefore, the existing mechanism fails to properly set the scene for the marketization of private intelligence activities. Consequently, the ground rules of the game are ambiguous, which leads to a broad margin of interpretation within both the government and the private sector. This results in the marketization of functions that would be better off being performed by the government. Also, regulations that should guide the procurement process can not be enforced properly since the very legal basis of the outsourced activity is ambiguous. Moreover, the very contracts are drafted poorly, and without stating clear benchmarks on good and bad conduct. The immaturity of the MEJA and UCMJ furthermore shows the inability of the legal system to place contractors properly in the legal playing field. Misconduct by actors taking part in non-lethal functions in conflict areas are legally undefined due to unaddressed jurisdictional difficulties. The possibility to hold PICs accountable through the extension of national law to crimes committed on foreign soil show the some pitfalls that were identified for its applicability to PMCs: it lacks the tools to effectively oversee and enforce national laws.

There is legal asymmetry between governmental actors and the private sector

It reoccurs that governmental actors and private sector actors are not susceptible to the same legal standards, or that the consequences of misconduct are asymmetrical. The application of national law to contractors operating on foreign soil could theoretically close this jurisdictional gap. However, both provisions lack practical usability due to a variety of imperfections. This discrepancy means that the same activity can be legally or without repercussions performed by the one, but not by the other. This makes sense when we look at the special powers intelligence agencies enjoy, these should not be granted to other actors. When punishing misconduct on foreign soil however, the private actors were not held accountable for misconduct in Abu Ghraib, whereas their governmental counterparts were punished through military law. This discrepancy is also visible in international treaties, in which contractors are not legally recognized as participants in the conflict - and therefore not liable to its rules. Where whistleblower protection is already problematic for government employees, such a legal framework is absent for their private counterparts. The legal basis of the marketization of intelligence is already troublesome, these observations of asymmetry show that the legal ambiguity of PICs conduct continues in the operational field.

Political interference problematizes accountability

Whereas the previous causes focus on legal aspects, political interference in these already flawed legal processes further problematize the establishment of legal accountability. The ‘political question doctrine’ is a powerful tool for the administration to shield companies from prosecution, as is visible in the Abu Ghraib case. The agreement with Coalition Provisional Authority in Iraq, to effectively grant immunity to contractors, shows that geopolitical considerations prevail over the establishment of accountability for misconduct. The conflicts of interest visible through the donations of PICs to members of parliamentary intelligence committees further problematizes the possibility of political interference. When the same parliament that receives donations from the companies can politically interfere with legal processes to hold those companies accountable, the accountability process lacks every element of democratic governance.

Repeated reluctance to enforce existing legal standards.

Although the 11 Code of Federal Regulations is straightforward in its wording, it is not properly enforced. The same can be said for the Federal Acquisition Regulations System (FAR), of which the rules regarding the procurement of ‘major systems’ are rarely followed.

The reluctance to accept the official definition of ‘inherently governmental functions’ by the Office of the Director of National Intelligence in their contracting process adds to the list. These observations show that those involved in the privatization process from the government side don’t always follow the rules in place. As the Government Accountability Office noted, this is partly the result of a lack of skilled, capable and senior procurement professionals within the IC. Another factor is the unwillingness of IC members to harm the interests of companies that can be their future employer. Also, the broken whistleblower protection framework makes it unattractive to ring the bell when colleagues don’t follow the rules. This effectively eliminates the ears and eyes of those that should establish accountability over PICs.

To conclude

The new field of outsourcing in the Intelligence Community needs to mature. Legal accountability mechanisms in place need to be rephrased to include the existence of private actors in the IC. The legal basis of these private actors must be clearly defined so that legally grey areas are minimized and inherently governmental functions are unambiguous. On this basis, the legal asymmetry between government actors and the private sector must be bridged in areas where PICs join in. These frameworks need to be updated throughout time so that the technological advancements on which the IC thrives are incorporated frequently. The large amounts of money at stake show strong signs of conflicts of interest, similar to the military industrial complex. If the United States wants to prevent the establishment of an intelligence industrial complex, if this does not already exist, it must sharpen and enforce its laws regulating the revolving door and political donations.

Bibliography

Arnpriester, Natasha. "Combating Impunity: The Private Military Industry, Human Rights, and the Legal Gap." U. Pa. J. Int'l L. 38 (2016): 1189.

Apuzzo, Matt. “Jurors’ Note Hints at Conviction in Blackwater Case.” The New York Times, 2 Oct. 2014, https://www.google.com/search?q=juror+note+hints+at+conviction+in+blackwater+case&rlz=1CAIPNW_enNL926NL926&oq=juror+note+hints+at+conviction+in+blackwater+case&aqs=chrome..69i57j69i60.8063j1j7&sourceid=chrome&ie=UTF-8

Avant, Deborah. "The privatization of security and change in the control of force." International Studies Perspectives 5.2 (2004): 153-157.

Barker, Cat, et al. Oversight of Intelligence Agencies: A Comparison of the'Five Eyes' Nations. Parliamentary Information and Research Service, 2017.

Barouch, Tim. "Performing imperious legal style: Saleh v. Titan Corp et al. and private military contractor accountability." African Yearbook of Rhetoric 9.1 (2019): 61-72.

Bartlett, Donald L., and James B. Steele. "Washington’s $8 billion shadow." Vanity Fair 1 (2007).

Bierman, Noah. “Few have faced consequences for abuses at Abu Ghraib prison in Iraq.” Los Angeles Times, 17 Mar. 2015, https://www.latimes.com/nation/la-na-abu-ghraib-lawsuit-20150317-story.html

Born, Hans. Who’s watching the spies: establishing intelligence service accountability. Potomac Books, Inc., 2005.

Brown, Aliya. "Prosecuting Private Armies: Could the Uniformed Services Employment and Reemployment Rights Act of 1994 Provide a Template for Prosecution of Private Military Contractors." Geo. J. Legal Ethics 32 (2019): 435.

Brown, Harold, and Warren B. Rudman. "Preparing for the 21st century: An appraisal of US intelligence." (1996).

Center for Constitutional Rights. “Kiobel v. Royal Dutch Petroleum Co. (Amicus).” 29 Mar. 2018, https://ccrjustice.org/home/what-we-do/our-cases/kiobel-v-royal-dutch-petroleum-co-amicus

Center for Responsive Politics. “Defense: Top Contributors to Federal Candidates, Parties, and Outside Groups.” 2020, https://www.opensecrets.org/industries/contrib.php?ind=D&Bkdn=DemRep&cycle=2018

Chesterman, Simon. "We Can't Spy… If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing ‘Inherently Governmental Functions." European Journal of International Law 19.5 (2008): 1055-1074.

Clark, Kathleen. "Ethical issues raised by the OLC torture memorandum." J. Nat'l Sec. L. & Pol'y 1 (2005): 455.

CNN. “Iraq Prison Abuse Scandal Fast Facts.” CNN, 30 Oct 2013, https://edition.cnn.com/2013/10/30/world/meast/iraq-prison-abuse-scandal-fast-facts/index.html

CNN. “Text of David Kay’s unclassified statement” CNN, 3 Oct 2003, https://edition.cnn.com/2003/ALLPOLITICS/10/02/kay.report/

Cordero, Carrie. “Enhancing Congressional Intelligence Committee Effectiveness.” *Center for a New American Security,* 5 Aug. 2019, https://www.cnas.org/publications/reports/enhancing-congressional-intelligence-committee-effectiveness

Cornell Law School. “Electronic Surveillance”, https://www.law.cornell.edu/wex/electronic_surveillance#:~:text=Because%20electronic%20surveillance%20is%20a,warrant%20requirements%20as%20other%20searches.&text=If%20a%20situation%20threatens%20a,may%20proceed%20without%20a%20warrant.

Cottier, Michael. "Elements for contracting and regulating private security and military companies." Int'l Rev. Red Cross 88 (2006): 637.

D.C.A.F. "Parliamentary oversight of intelligence services." Geneva: Centre for the Democratic Control of Armed Forces (2006).

Delaforce, Ruth. "Public and private intelligence: Historical and contemporary perspectives." Salus Journal 1.2 (2013): 21.

Dickinson, Laura A. "Government for hire: Privatizing foreign affairs and the problem of accountability under international law." Wm. & Mary L. Rev. 47 (2005): 135.

Dickinson, Laura Anne. Outsourcing war and peace: Preserving public values in a world of privatized foreign affairs. Yale University Press, 2011.

Doswald-Beck, Louise. "Private military companies under international humanitarian law." From Mercenaries to Market: The Rise and Regulation of Private Military Companies (2007): 115-138.

Federal Acquisition Regulations System, Title 48. https://www.law.cornell.edu/cfr/text/48/37.104

Federal Regulations, 11 code, Code of Federal Regulations. Government Publishing Office. 2020, https://www.fec.gov/regulations/

Gore Jr, Albert. National performance review. DIANE Publishing, 1994.

Gruskin, Peter. "The Public Sphere's Private Intelligence." Cornell Internation Affairs Review 4.1 (2010).

Halchin, L. Elaine. The intelligence community and its use of contractors: Congressional oversight issues. Congressional Research Service, 2015.

Harlow, Carol. "Accountability and constitutional law." *The Oxford Handbook of Public Accountability* (2014): 195-210.

Hedahl, Marcus. "Unaccountable: The current state of private military and security companies." Criminal justice ethics 31.3 (2012): 175-192.

Hijzen, Constant. "More than a ritual dance. The Dutch practice of parliamentary oversight and control of the intelligence community." Security and human rights 24.3-4 (2014): 227-238.

Kalidhass, P. R. "Determining the Status of Private Military Companies under International Law: A Quest to Solve Accountability Issues in Armed Conflicts." Amsterdam LF 6 (2014): 4.

Kaminski, Margot. “PRISM’s Legal Basis: How We Got Here, and What We Can Do to Get Back.” The Atlantic, 7 June 2012, https://www.theatlantic.com/national/archive/2013/06/prisms-legal-basis-how-we-got-here-and-what-we-can-do-to-get-back/276667/

Keefe, Patrick R. "Privatized spying: the emerging intelligence industry." The Oxford handbook of national security intelligence. 2010.

Kemp, John S. "Private military firms and responses to their accountability gap." Wash. UJL & Pol'y 32 (2010): 489.

Klasfeld, Adam. “Contractor Can Be Sued Over Abu Ghraib Torture.” Courthouse News Service, 27 Feb, 2019, https://www.courthousenews.com/judge-preps-abu-ghraib-torture-suit-for-trial/

Konkel, Frank. “After two years, the NSA finished rebidding its “Groundbreaker” program and is beginning work on a secretive new set of communications contracts.” Nextgov, 19 Oct. 2018, https://www.nextgov.com/it-modernization/2018/10/nsa-finalizes-67-billion-classified-tech-contracts/152165/

Krishnan, Armin. "The future of US intelligence outsourcing." Brown J. World Aff. 18 (2011): 195.

Leander, Anna. "The paradoxical impunity of private military companies: Authority and the limits to legal accountability." Security Dialogue 41.5 (2010): 467-490.

Lindemann, Marc. Civilian contractors under military law. ARMY WAR COLLEGE CARLISLE BARRACKS PA, 2007.

LoConte, Jessica. "FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications-Is It Reasonable." Pace Int'l L. Rev. Online Companion (2010): i.

Luckey, John R., Valerie B. Grasso, and Kate M. Manuel. "Inherently governmental functions and Department of Defense operations: background, issues, and options for Congress." LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2009.

MapLight News Archive. “Intelligence Contractors Give Millions to Lawmakers Overseeing Government Surveillance.” 7 Dec. 2013, https://maplight.org/story/intelligence-contractors-give-millions-to-lawmakers-overseeing-government-surveillance/

Michaels, Jon D. "All the President's spies: Private-public intelligence partnerships in the War on Terror." Calif. L. Rev. 96 (2008): 901.

Monahan, Torin. "Surveillance and terrorism." Routledge handbook of surveillance studies (2012): 285.

Nicola, Thomas J. "9/11 Commission Recommendations: Intelligence Budget." (2004).

O’Harrow, Robert and Higham, Scott. “Interior, Pentagon Faulted In Audits Effort to Speed Defense Contracts Wasted Millions.” The Washington Post, 25 Dec. 2006, https://www.washingtonpost.com/archive/politics/2006/12/25/interior-pentagon-faulted-in-audits-span-classbankheadeffort-to-speed-defense-contracts-wasted-millions-span/8958dd08-a20f-416b-a52a-53d47848bd67/

Office of Management and Budget. “Circular No. A-76”, Executive Office of the President, 29 May 2003, https://www.whitehouse.gov/wp-content/uploads/2021/01/a76_incl_tech_correction.pdf

Office of the Director of National Intelligence. “Plan an Acquisition.”, https://www.dni.gov/index.php/who-we-are/organizations/ise/archive/additional-resources/2141-acquisition

Percy, Sarah. "Private security companies and civil wars." Civil Wars 11.1 (2009): 57-74.

Richelson, Jeffrey T. "The satellite gap." Bulletin of the Atomic Scientists 59.1 (2003): 48-54.

Schmidt, Sarah. "Companies Fail the Test; Junk Food Marketing Aimed at Kids Faulted." The Gazette [Montreal], 10 Mar. 2010, p. A.11. Canadian Newsstand.

Schmitt, Michael N. "Humanitarian law and direct participation in hostilities by private contractors or civilian employees." Chi. J. Int'l L. 5 (2004): 511.

Shorrock, Tim. "Obama's crackdown on whistleblowers." The Nation (2013).

Shorrock, Tim. Spies for hire: The secret world of intelligence outsourcing. Simon and Schuster, 2008.

Singer, Peter W. Corporate warriors: The rise of the privatized military industry. Cornell University Press, 2008.

Singer, Peter W. "War, profits, and the vacuum of law: Privatized military firms and international law." Colum. J. Transnat'l L. 42 (2003): 521.

Singh, Sunny Jiten. "The U.S. Intelligence Enterprise and the Role of Privatizing Intelligence." Recanati-Kaplan Fellowship Series Belfer Center for Science and International Affairs. (2019).

Stein, Fredrick A. "Have We Closed the Barn Door Yet-A Look at the Current Loopholes in the Military Extraterritorial Jurisdiction Act." Hous. J. Int'l L. 27 (2004): 579.

Storm, Joshua R. "Outsourcing intelligence analysis: legal and policy risks." J. Nat'l Sec. L. & Pol'y 9 (2017): 669.

Taubman, Philip. "In Death of Spy Satellite Program, Lofty Plans and Unrealistic Bids." New York Times, 11 Nov. 2007, https://www.nytimes.com/2007/11/11/washington/11satellite.html

Taylor, Marisa. "Intelligence, defense whistleblowers remain mired in broken system." Intelligence (2014).

Thompson, Mark. "The Bunker: The Contractors' Pie Keeps Growing." Project On Government Oversight. (2020).

Tkach, Benjamin. "Private military and security companies, contract structure, market competition, and violence in Iraq." Conflict Management and Peace Science 36.3 (2019): 291-311.

U.S. Constitution. Art./Amend. XII, Sec. 4.

Uniform Code of Military Justice. 10 United States Code Chapter 47, https://www.law.cornell.edu/uscode/text/10/subtitle-A/part-II/chapter-47

United States, Congress. Public Law 106-523. Military Extraterritorial Jurisdiction Act of 2000, 106th Congress, U.S. Government Printing Office, https://www.govinfo.gov/content/pkg/PLAW-106publ523/html/PLAW-106publ523.htm

Van Buuren, Jelle. "From oversight to undersight: The internationalization of intelligence." Security and Human Rights 24.3-4 (2014): 239-252.

Vickers, John, and George Yarrow. "Economic perspectives on privatization." Journal of economic perspectives 5.2 (1991): 111-132.

Voelz, Glenn J. "Contractors and intelligence: The private sector in the intelligence community." International Journal of Intelligence and Counterintelligence 22.4 (2009): 586-613.

Weiner, Ross L. "The Office of Legal Counsel and Torture: The Law as Both a Sword and Shield." Geo. Wash. L. Rev. 77 (2008): 524.

Wills, Aidan. "Understanding intelligence oversight." Geneva: DCAF (2010): 25-27.

Wood, Christopher. "Private Military Companies and International Security." E-International Relations Students. Available at: www. e-ir. info/2013/03/21/private-military-companies-and-international-security/(accessed 1 February 2020) (2013).