Once Silence is Broken

The Transparency Discourse of the NSA and CIA

Leiden University

Mariam Mirfattahi

s2300613

m.mirfattahi@umail.leidenuniv.nl

Master Thesis

MA International Relations: Global Conflict in the Modern Era

Supervisor: Dr. Eugenio Cusumano

Word count: 14 360

22 July 2019

Table of Contents

Abbreviations

CDA	-	Critical Discourse Analysis
CIA	-	Central Intelligence Agency
DNI	-	Director of National Intelligence
HUMINT	-	Human Intelligence
NSA	-	National Security Agency
OPCL	-	Office of Privacy and Civil Liberties
SIGINT	-	Signals Intelligence

Abstract

When in 2013 the American public learned about the mass surveillance conducted by the National Security Agency, the US Intelligence Community's public image was severely damaged. The disclosures of Edward Snowden represented the high-water mark of the problematic relationship between secrecy and privacy in the age of the Internet. With the creation of social media accounts, Privacy and Civil Liberties Offices and 'Q&A's about transparency, US intelligence agencies have attempted to regain the public's trust. The paradox of secret agencies' increasing online visibility and rhetoric on transparency has been left widely unconceptualised by scholars. This study examines how the US Intelligence Community attempts to re-establish its legitimacy by regaining power over the transparency discourse online. It further contributes to the literature by broadening the securitisation framework with the inclusion of silence in discussing when the secret state starts speaking.

Keywords: US; Intelligence Community; Transparency; Silence

1. Introduction

In 2013, Edwards Snowden's disclosure of an estimated 1.7 million documents sparked a worldwide debate about the NSA's violation of civil liberties (Aldrich & Moran, 2018). Revelations about the bulk collection of communications records made critical damage to the Intelligence Community's public image in an unprecedented manner (PEN American Center, 2015; Lucas, 2014). However, the events of June 2013 were not surprising considering the nature of the US Intelligence Community, as it has developed over the 20th and 21st century (Aldrich and Moran, 2018). Moreover, the events were symptomatic of the long-standing debate over the trade-offs between national security and civil liberties, attenuated by the rise of the Internet (Byman & Wittes, 2014, 127). The consequences of Snowden's disclosures were that the majority of the American public learned about the government's online surveillance programs, with 57% of the population affirming that 'monitoring of the general population is unacceptable' (Rainie & Madden, 2015; Stoycheff 2016, 297). In a recent interview Snowden pointed out the Intelligence Community's online efforts to re-establish trust, noting: 'They want to be friendly. They want to be on your side' (Snowden, 2019).

Critical voices argue that transparency has become 'the new buzzword in intelligence circles as officials attempt to preserve as much of their post-9/11 surveillance powers as they can from congressional restrictions' (Ackerman, 2014). The introduction of blog reels, the declassification of documents, Twitter accounts and the establishment of civil liberties offices describe only some of the recent efforts by the Intelligence Community to increase transparency. Whereas, however, the Intelligence Community has promoted its online efforts to revise its public approachability, this 'image campaign' has not yet been adequately analysed and put into a theoretical debate.

At the core of this debate about national security and public consensus lies the much-discussed relationship between secrecy and the democratic and transparent state. The scholarly focus on the post-9/11 online rhetoric of the Intelligence Community has highlighted crucial tools of national security language. Scholars argue that the US Intelligence Community's expansion in the 21st century builds on the concept of the 'state of exception', which enables expanded political power predicated on the maintenance of constant emergency of the state (MacDonald & Hunter, 2019; Agamben, 1998; 2005; Schmitt, 1922). Secrecy in the agencies' conduct operates in the name of national security and further acts as tool to uphold their 'legitimacy of power' (Weber, 1958).

This study stresses the importance of taking a closer look at how securitising actors conceptualise the notion of transparency. It is therefore pertinent to examine the linguistic tools used by intelligence agencies in their attempt to reshape a discourse that has been heretofore dominated by the public. The analysis of this study focuses especially on the NSA and Central intelligence Agency (CIA), due to the following reason: whereas the Snowden disclosures of 2013 have been most closely associated with the NSA and its foreign Signals Intelligence gathering (SIGINT), the CIA's gathering of foreign Human Intelligence (HUMINT) has received comparatively lesser attention in public discourse. The blurring lines between domestic and foreign intelligence make both the NSA and CIA interesting subjects of analysis, considering that the agencies can conversely represent a 'threat' to the democratic public when intruding on privacy for foreign intelligence purposes.

The assumption of this study is the following: Controversy, such as the NSA's surveillance programme and the CIA's foreign operations, exists within the public

sphere *inter alia* after Snowden. As such, the online rhetoric of the intelligence agencies changes because they require public legitimacy. The premise is therefore that, within a liberal democracy, public commotion concerning security policies impacts the government's security discourse, which has to uphold its legitimacy according to its establishment as democratic government.

It is crucial to ask how the state's legitimacy of power is upheld through (re)shaping the discourse on transparency. The research question is therefore as follows:

How do the CIA and NSA reshape the notion of transparency through their online discourse?

The analysis of the NSA and CIA rhetoric on their official websites, public speeches, blog posts and press releases shall demonstrate how the politics of silence have to be conceptualised by looking at when and how the secret state starts speaking. Examining the online discourse is crucial considering that today websites and social media are as important as traditional media for creating and maintaining a public image. The cross-time analysis of the agencies' websites illustrates how their narrative of transparency allows them to propagate their national security agenda within a light of visibility. The agencies thereby re-establish power through 'breaking the silence' in their own terms.

Aldrich and Moran (2018, 12) ask whether it is 'too adventurous' to talk about the agencies' efforts in 'intelligence–branding'. This study argues that, in fact, it is pertinent considering the changing nature of intelligence due to new technologies of communication and increasing privatisation of the state security body. This study further suggests that within a liberal democracy, public controversy can impact the government's security language, which ought to be catering the maintenance of its legitimacy. The 'language game' deployed by the Intelligence Community and its efforts to shape the transparency discourse are therefore highlighted. Further, the analysis of the online rhetoric of the NSA and CIA shall demonstrate how the politics of silence can be discussed through looking at the agencies' changing transparency narrative. The analysis will outline the agencies' image campaigns through their narrative on transparency.

This thesis is organised as follows. The first chapter elaborates on the Intelligence Community's organisational structure and the CIA and NSA in particular. Second, a brief section informs about the consequences of Edward Snowden's disclosures. Third, the

literature the literature review outlines relevant scholars for this study and puts them into a discussion. Fourth, the methodology chapter informs about how the agencies' websites were analysed and elucidates the theoretical framework. Fifth, the analysis chapter presents empirical findings and then proceeds to demonstrate the most significant rhetorical patterns. Finally, the concluding remarks offer a reflection of this study.

2. The US Intelligence Community

The following chapter discusses the US Intelligence Community's landscape and budget, the differentiation between types of intelligence and the emergence of the CIA and NSA. This shall inform about the significance and purpose of the NSA and CIA within the Intelligence Community.

The US Intelligence Community consists of the Office of the Director of National Intelligence (DNI) and sixteen more organisations. Even though popular and academic discourse refers to the agencies being part of a 'community', difficulties with rivalries and a lack of effective communication between agencies speak against such a description (Ellis, 2010, 2). The general aim of the agencies is to reduce uncertainty in the 'development and implementation of national security and law enforcement policy' (ibid., 2). Intelligence activities involve collecting and analysing information and 'its transformation into intelligence' (Richelson, 2012). Counterintelligence and covert operations are further 'intertwined with intelligence activity' (Richelson, 2012, 3). The collection of Human Intelligence and Signals Intelligence count as the most prominent sources of intelligence. Human Intelligence (HUMINT) refers to information collected by a human source (USNI, 2013, 45). A further separation is made between overt and clandestine HUMINT, which differ in the manner in which they are collected (ibid.). Signals Intelligence (SIGINT) refers to 'intelligence gathered from data transmissions, including Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT)' (USNI, 2013, 47).

The expansion and increasing budget of US intelligence agencies has been the subject of extensive public debates in the 21st century. In 2004 the 9/11 Commission recommended the declassification of the budgets of US intelligence agencies, however fearing 'that disclosure of numbers below the topline' might harm national security (DeVine, 2018, 5). The publication of the expenditures shows that the Intelligence

Community's costs reached an all-time high of $81,5 billion in 2018 (DNI, 2019). Nevertheless, Aldrich (2010) suggests that it is impossible to capture the exact size and the costs of the intelligence agencies.

The NSA and CIA in particular belong to the four national intelligence organisations. This entails that they are responsible for gathering and performing intelligence for the entire government through informing national-level policymakers (Richelson, 2012, 17).

2.1. The Central Intelligence Agency

During the Second World War, the Office of Strategic Services was created as 'America's first central intelligence organization' responsible for espionage operations (Richelson, 2012, 17). When in 1945 President Harry S. Truman ordered its dissolution, the National Intelligence Authority and Central Intelligence Group were created. The National Security Act 1947 replaced the latter with the newly created Central Intelligence Agency (ibid.). The CIA's responsibility was and still is Human Intelligence collection as well as, controversially, covert operations. The CIA's paramilitary operations, pursuant to the US's anti-communist foreign policy during the Cold War, count among its most contentious operations in the 20th century (Gleijeses, 2016, 291). These operations were consistent with the foreign policy of President Truman and his predecessor, President Woodrow Wilson, which was predicated on the idea of a US-dominated liberal world order (Thompson, 2010, 42). It is pertinent to consider US's foreign intelligence operations within the history of the US's extensive involvement abroad. The interference in foreign politics is closely related to the US's agenda to protect foreign military and intelligence bases (Chomsky, 2017). The Executive Order 12333 signed by President Ronald Reagan allowed the CIA to 'collect "significant" foreign intelligence' also *within* the US (Richelson, 2012, 19). This development was illustrative of the increasingly blurred lines between foreign and domestic intelligence operations. Today the CIA's primary tasks are 'coordination, de-confliction and evaluation of clandestine (HUMINT) operations across the IC' (USNI, 2013, 12).

2.2. The National Security Agency

In 1952 President Truman dissolved the Armed Forces Security Agency and created the National Security Agency (NSA), one of the historically least visible security agencies in the US (Richelson 2012, 30). Since then the NSA has been responsible for Signals Intelligence collection but has not, however, been responsible for creating finished

intelligence reports as widely believed (Aid, 2001, 27). During the Cold War, Signals Intelligence formed a crucial part of US intelligence-gathering activities when other types of intelligence gathering failed (ibid). The majority of the US's intelligence was targeted at the Soviet Union. After the end of the Cold War, the NSA closed key European ground stations, which reflected a shift in US intelligence and foreign policy priorities (Richelson, 2012, 538). Just like the CIA, the NSA follows the Executive Order 12333 enacted by Ronald Reagan, which shall be further discussed later on.

3. Edward Snowden's Disclosures

For this study's it is important to discuss the impact of Snowden's disclosures since the analysis focuses on the NSA's and CIA's discourse after the incident.

Edward Snowden's disclosure of an estimated 1.7 million top-secret documents in June 2013 shed light on the issue of the large-scale surveillance of American citizens, as well as the further global surveillance by the Five Eyes agencies (Lashmar, 2019, 416). Snowden, an NSA contractor, had earlier voiced his concerns about the NSA surveillance of domestic communications to officials but later decided to leak policies, which had been hidden and enforced by the US government (Fidler, 2015, 2). President Barack Obama denied that Snowden was eligible for 'whistleblower protection' according to the Intelligence Community Whistleblower Protection Act of 1998 after the disclosures (PEN American Centre, 2015). Before his inauguration Obama had stressed his support for whistleblowers, and in the beginning of his presidency, his administration had put a strong emphasis on transparency (PEN American Centre, 2015, 5; Fenster, 2012). The highest number of whistleblowers ever was, however, persecuted under the Obama-administration (Aldrich & Moran, 2018, 2). The definition of whistleblower protection used by the Office of the Inspector General of the NSA follows the idea that 'whistleblowing and leaking are not the same' (OIG, 2019). The definition suggests that whistleblowing is a term more positively connoted than 'leaking' in the US. The prosecution of Snowden under the Espionage Act of 1917 was hindered by Snowden's escape to Hong Kong before the disclosures were released (Fidler, 2015, 2).

Snowden's disclosures had a variety of consequences. First, international relations with presidents such as Angela Merkel and Dilma Rousseff were negatively impacted after they learned that they had been the subject of the surveillance operated by the NSA (Byman & Wittes, 2014). Second, wireless telephone companies, e-mail and cloud

storage providers were angered after learning about the role they had played in the NSA's mass surveillance activities (Fenster, 2017, 111). Third, the US's image of a 'moral' power in debates around cybersecurity was shaken, especially after having accused China of cyber-attacks (Byman & Wittes, 2014). Fourth, the leaks sparked a broader debate about mass surveillance of citizens in democratic countries (Fidler, 2015, 2). Fifth, the disclosures precipitated a number of legislative changes in the US, including the reform of the NSA's bulk data collection programme pursuant to the USA Freedom Act (USA Freedom Act, 2015). Further, the UN General Assembly adopted resolution 68/167, which declared online privacy to be a fundamental human right (OHCR, 2013).

The fifth consequence, most important for this study, was the significant loss of the public's trust in the Intelligence Community. In this context, however, 'the public' does not necessarily refer to the American population at large. The loudest critics within the US were the liberal media and public intellectuals, which 'translate' what the population was not able to grasp from Snowden's disclosure of the documents alone (Aldrich, 2010; Fenster, 2017). Nevertheless, ten months after the incident, twenty million Twitter messages had mentioned the NSA or Snowden, demonstrating the wide public attention the disclosures received (Boynton & Richardson, 2016, 1917).

In contrast, when WikiLeaks disclosed sensitive material on US misconduct in Iraq in 2010, the public discontent turned out to be lower than expected (Fenster, 2017, 109). The result of WikiLeaks' disclosures for the government was the 'tightening [of] controls on classified information' (ibid). The difference between WikiLeaks' and Snowden's disclosures was that Snowden's documents addressed a specific policy whilst WikiLeaks highlighted a broader 'hypocrisy of U.S. foreign policy' (Fenster, 2017, 111). Whereas the WikiLeaks disclosures seemed to concern the 'distant and diffuse' conflict in Iraq (ibid.), Snowden's leaks highlighted how the American public itself was targeted through surveillance, arguably invoking broader criticism.

4. Literature review

The following literature review outlines the scholarly discussions important for the purposes of this study. The paradox of intelligence agencies becoming increasingly visible to the public requires the following procedure of discussion (Aldrich, 2010, 236). First, scholars' stances on secrecy within liberal democracies are elucidated. Second, this study sets out an overview of the literature discussing the concepts of transparency and

privacy within the US. Third, prior studies on the Intelligence Community's publicity are presented. Fourth, the securitisation framework in connection to theories of silence is explained. Finally, the changing nature of the US Intelligence Community is elaborated in historical context.

4.1. State Secrecy and Democracy

The Intelligence Community's conduct has been mostly debated in assessing secrecy and democracy. Whilst scholars within the field of political science have been focusing on the 'trade-off between secrecy and openness in government policy', other disciplines such as anthropology have been approaching secrecy within democratic states 'as an effective mode of communication and a technology of power' (Walters, 2015, 288).

Further reflections can be derived from the field of cultural sociology and its focus on cultural context. Consideration of cultural context is important for this study because it focuses specifically on intelligence in the US. Ku (1998, 176) locates the origins of the 'democratic struggle against state secrecy' in early modern Europe, where monarchies kept specific political actions secret and produced an image of authority to the public. Whereas the development of a free media body function has been a crucial element of a liberal democracy (ibid.), the 'increasing visibility of secrecy' in democracies has not entailed a decrease in secrecy. As Thompson (1995, 124, 125) notes, it has rather led to the establishment of 'new forms of invisible power'.

Scholars have typically focused on the negative versus positive nature of secrecy within a modern democracy (Warren & Laslett, 1977; Alexander & Smith, 1993). Bellaby (2018, 61) argues that intelligence plays a vital and 'ethical role in protecting the political community'. Lowenthal (2017) even emphasises that secrecy and democracy 'harmoniously co-exist'. He suggests that in a democracy, the public elects representatives who consent to the conduct of the Intelligence Community. According to Lowenthal's argument, the public indirectly impacts intelligence oversight since intelligence agencies act according to the government's policies (2017, 987). Further, the separation of domestic and foreign intelligence enables this coexistence in assuring a degree of independence between the two (ibid.). However, in the specific context of the US, Masco (2010) highlights the secrecy of foreign counterterrorism operations. Operations conducted against the will of the American public are kept secret. Citizens

are therefore continuously 'kept in the dark' about foreign operations causing 'long-term political effects' abroad within 'a discourse of imminent threat' (Masco, 2010, 450, 433).

The majority of scholars highlights the problem of civilian oversight over intelligence operations within the domain of civil-military relations. Bruneau and Dombroski (2014, 1) argue that transparency can only be assured to a certain degree, so that agencies can operate secretly. Bruneau and Dombroski therefore suggest that a balance between 'security needs and social welfare expectations' is kept only via public oversight (ibid., 6).

The wider debate about secrecy and democracy builds on the premise of 'national security *against* the insistence of the democratic right to know' (Hughes & Jackson, 2008, 17). Nevertheless, scholarly debates about the pros and cons of secret intelligence have to be considered through a critical lens. Especially the case of the US, which is a 'stratified' and multi-layered society, entails a polyvalent discussion of privacy and publicity (Ku, 1998, 179). The stance taken in this thesis adopts Bellman's argument that intelligence can be 'either negative or positive, consensual or non-consensual, legitimate or illegitimate' (1981, 6). This is due to the difficulty of measuring successful intelligence since intelligence operates in secrecy (Duyvesteyn, 2011). Additionally, intelligence today is an interconnected effort of several entities, which makes success and failure difficult to accredit to specific institutions (Byman & Wittes, 2014). Operations are most likely to become visible when they fail (Aldrich, 2010). As such, the research conduct of this thesis does not intend to highlight the positive/negative dichotomy of intelligence *per se,* but rather, how intelligence reacts to the increasing public debate about state secrecy and transparency.

Leaks and whistleblowing are phenomena with significant implications for secrecy and democracy. They can reveal illegitimate intelligence practices, including practices that have been conducted over a longer period of time (Ku, 1998, 177). Social disapproval in the form of whistleblowing has the ability to pull the secret politics of security back 'into the public realm' (Williams, 2003, 524). Bellaby (2018, 63) emphasises how whistleblowing can result from intelligence agencies lacking a 'external moral compass'. Without any 'external reference point', criticism by Intelligence Community staff members can be easily perceived 'as an act of betrayal', as exemplified by the case of Snowden (ibid.). In relation to Snowden's disclosures, scholars have also discussed whether or not these disclosures have had an impact on the American population's

opinion or American government's policies (Fenster, 2017; Aldrich & Moran, 2018; Byman & Wittes, 2014; Lucas 2014). Whereas authors such as Byman and Wittes (2014) ask whether the 'NSA can win back the public's trust', they only consider the historical build-up to a problematic relationship between 'level of security, on the one hand, and strict privacy protections, accountability, and transparency, on the other'. The impact of the disclosures on the IC's rhetoric has received little scholarly attention.

4.2. State Secrecy and Transparency

For the purposes of this study the meaning of the term 'transparency' must be contextualised within the US, since ideas of transparency are highly connected to cultural contexts (Altmanm 1977). The notion of transparency is further examined in close connection to debates about privacy.

Altman (1977) argues that the term privacy is culturally specific and its meaning changes across time. Fenster (2010, 449) notes that through the 'enormous democratization of information access enabled by the Internet', the twenty first century 'witnessed a fundamental shift in the idea and mechanisms of openness and transparency in the United States'. The public scandals in the 1970s (see 3.1.) were crucial in the formation of what Fenster (2017) conceptualises as the 'transparency movement'. The idea of an ideal, 'transparent' government derives from figures like Daniel Ellsberg and US press advocates, who demanded open government laws and access to government information. Fenster (2018) describes this concept of transparency 'the transparency fix'. Under this logic, the government is obligated to inform the public about intelligence operations and ensure visibility of government institutions and officials. This can only be achieved through administrative laws and 'constitutional protections against secrecy', which obligate the government to keep its conduct visible to the public (ibid., 9-10). 'Freedom of information' and the 'right to know' have been particularly important concepts for the transparency movement. These terms originate from a 'classically liberal conception of a limited state checked by the press' (Fenster, 2018, 22). The terms build upon the idea of a 'natural public right to information and free information flows' (ibid.). Members of the transparency movement saw the Obama administration as disappointment, especially in light of its treatment of Chelsea Manning and Edward Snowden and the administration's promise to be the most transparent in US history (Aldrich & Moran, 2018). The movement saw the triumph of

secrecy as 'a failure of leadership and institutional will' (Fenster, 2017, 10). The transparency movement has viewed the return of US leadership to a 'lesser evil narrative', a narrative which claims that it's 'not always possible to preserve full democratic disclosures and transparency' in counterintelligence, as a failure of transparency (Ignatieff, 2004, 21).

Dean (2002, 16), however, notes that free information flow in cyber space causes an endless journey of 'uncovering the secret'. Citizens turn into constant 'suspicious subjects', which are sceptical of the Intelligence Community's conduct and have to find information to uncover secrets through the Internet (ibid.). Dean's argument highlights how the narrow focus on transparency of the Intelligence Community's conduct can hinder public criticism on more than declassification of information. The danger here is that citizens become fixated on the idea of transparency rather than taking political action to fight for structural changes of the intelligence sector (ibid., 174).

This stands in contrast to Lucas' (2014, 36) stance, which suggests that transparency is provided once surveillance is admitted and intelligence agencies clearly state 'who is exercising accountability and oversight'. Lucas, however, does not adequately address the structural reproduction of the idea of state secrecy. He rather suggests an idea that implies that the secret state itself remains unquestioned if transparency is given. Thus, when discussing transparency, attention has to be given to the idea of the secret itself. As Masco (2010, 456) argues, 'the "idea" of secret knowledge itself becomes deployable, corrupting public understandings of what is possible and what is not'.

4.2.1. Privacy

Altman (1977) and Macnish (2018) argue that there is a variety of definitions of the term 'privacy' that have to be considered. The philosophical debate around privacy can be split into two different stances on information access. The 'access account' argues that loss of privacy only occurs once one's information is accessed (Macnish, 2018, 417). This stance is widely held by intelligence agencies. The 'control account' on the other hand is concerned that 'the loss of control over one's information constitutes a loss of privacy' (Macnish, 2018, 417). Those opposing mass intelligence collection typically favour the control account. Even though intelligence agencies persist with denying the loss of a person's privacy unless their data is accessed, this account has become problematic in times of electronic systems. Macnish (2018, 431) therefore suggests that

since all data is searched by automated intelligence systems, private information is continuously accessed and privacy has consequently been lost. Lucas (2014, 35) identifies a paradox between two perceptions of privacy, 'one that functions with special vigor in the cyber domain' and one that stresses the injustice of citizens being 'unduly subject to grave but avoidable harm'.

4.3. Public Discourse of the Intelligence Community

Scholars have been focusing on the US government's security discourses justifying the 'war on terror' and constant reproduction of threats. Especially pertinent for this study is MacDonald and Hunter's (2019) research, which focuses on the critical discourse analysis of US intelligence webpages post 9/11. The study conceptualises the Intelligence Community's discourse through Foucault's conceptualisation of discourse and power, similar to this thesis. MacDonald and Hunter analyse the Intelligence Community's discourse considering the impact of the events of 9/11 'upon the political and popular consciousness of the US' (ibid, 29). The construction of the 'Other' is particularly significant in the analysis of government documents, which portray an image of the 'American people' in opposition to the 'Other' or 'terrorists' (MacDonald and Hunter, 2019, 66; Caldas-Coulthard, 2003). The concept of 'the state of exception' (Agamben, 2005; Schmitt 1922) highlights how US politics continuously use the events of 9/11 for contemporary 'draconian security policies' (MacDonald and Hunter, 2017, 494). MacDonald and Hunter's CDA of US intelligence webpages post-9/11 demonstrate how the events of 9/11 are being used to justify 'the imposition of new 'juridical powers and the curtailing of civil liberties' (MacDonald & Hunter, 2017, 494).

Similar to MacDonald and Hunter (2019), Lashmar (2019) draws on Agamben's (2005) conceptualisation of the post-9/11 'state of exception'. Lashmar (2019, 411) suggests that in the case of UK intelligence services have evolved as an 'intelligence lobby', which engages with the public 'to promote a narrative and vision of what UK intelligence should do'. The scope conditions of Lashmar's study focused on a content analysis of the public narrative of former intelligence officials three years after the Snowden revelations. Lashmar (2019, 415) argues that the 'UK intelligence lobby' is the reaction to controversy of US intelligence operations. The study suggests that over the last 25 years, 'the once invisible and silent Intelligence Community has gradually entered into the public sphere' (ibid, 426). The study concludes that there are a number of 'political

and democratic issues' regarding the expansion and growing power of intelligence services, which entails a growing 'intelligence lobby' to promote the agencies publically (Lashmar, 2019, 427).

It is further crucial, however, to view the public relations of the Intelligence Community within its strive to uphold its legitimacy. Given the IC's increasing privatisation, the debate can also be seen to involve the question of how private security legitimises its conduct in the public eye. Schneiker and Joachim (2012, 365) discuss the 'image problem' of private security companies due to their controversial public image. The private security companies attempt to present themselves as 'legitimate and acceptable' can be analysed through their public discourse. Through seeking to portray themselves as 'average', private security companies attempt to establish a discourse in which they are seen as accountable and trustworthy (Schneiker, 2007, 85).

Whilst the state-of-exception-model is popular in theorising security discourse and its 'constant reproduction of danger' (Bodei, 2011; Alvarez, 2006, 75), this study proposes to look beyond such a conceptualisation. Although any discourse of security can be argued to be simultaneously a discourse of danger (Dillon, 1996), scholars have refrained from explaining how the 'state of exception' model can explain the Intelligence Community's efforts to reshape its image of a 'draconian' security body, particularly through its emphasis on its own transparency measures. Even though this study acknowledges the continuous discourse of an 'imminent threat' produced by US national security discourses (Masco, 2010, 433), past scholarly discussions have overlooked the Intelligence Community's recent narrative on transparency. It is crucial to analyse the discourse through the included theoretical lens of silence and power, which allows for an important discussion of the discourse of transparency and the legitimacy of state secrecy.

4.4. The Changing Nature of US Intelligence

For the discussion of this study, it is important to provide an overview of the post-WWII history of US intelligence and how it developed over time. It is therefore outlined how the debate about transparency and state secrecy developed through changes in the Intelligence Community. It is illustrated how the IC's 'post-World War II system of secrecy' evolved from its Cold War 'countercommunist' orientation to a post 9/11 'counterterrorist' intelligence focus (Masco, 2010, 545).

4.4.1. Countercommunist Secrecy

Prior to the late 19th century, US intelligence was mostly active during war and more or less 'disappeared' in times of peace (Tidd, 2008, 5). The expanding size of the US Intelligence Community has to be considered within the context of the US's extensive involvement in foreign states. The US's increasing interest in foreign politics suggests to be part of the reason why permanently operating intelligence organisations were established.

WWII resulted in the expansion of the Intelligence Community, which started to be focused on domestic activities (Tidd, 2008, 11). Masco (2010, 433) argues that it was after WWII that the US transformed into 'a new kind of secret society'. Essential to this secret society was the realisation of state power through the constant 'mobilisation of threats' in order to 'manage the public/secret divide' (ibid.). Within this concept, classified information has the ability to damage the nation once it is made public (ibid., 443). What Masco terms the 'security/threat matrix' describes the emergence of an ideology entrenched in the Cold War, which continues to justify contemporary security policies with the reproduction of external threats. The beginning of the Cold War 'created and shaped' US intelligence as it exists today (Tidd, 2008, 5).

Aldrich (2002, 5) argues that secret services are essential for understanding the Cold War since they legitimated policies 'launched in the conflict's name'. The arms race against the Soviet Union was underpinned by the idea of an 'atomic secret' that had to be protected for the sake of the 'countercommunist state' (Masco, 2010, 433). This acted further as an incentive to introduce organisations with advanced technology to gather intelligence (Tidd, 2008, 5). The image of the US intelligence agencies, however, suffered under a number of scandals in the 1970s. The leaks of the Pentagon Papers by State Department official Daniel Ellsberg in 1971 revealed sensitive information about aggressive US involvement in the Vietnam War between 1945 and 1967, which had been kept secret from the American public (Hughes & Jackson, 2008). One year later President Richard Nixon's authorisation of illegal wiretapping of 'alleged political enemies' became public in what became known as the Watergate scandal (Schudson, 2014, 1232). This led to further media investigation of US intelligence and finally to the establishment of committees of inquiry into the scandals (Lashmar, 2019, 415). More and more, the US media informed the public how the US government had been

spying on journalists, member of congress, civil rights leaders, such as Martin Luther King Jr., and opponents of the Vietnam War (Byman & Wittes, 2014). This led to distrust of the government's secret conducts and surveillance (ibid.). However, following the end of the Cold War, the Intelligence Community's resources were reduced, a policy further pursued after 1993 by Vice President Al Gore under the Clinton administration (Ellis, 2010, 5). The federal civil service was downsized and much of its work privatised (ibid.; Richelson, 2008, 19). The effects of this were an overall increase of the Intelligence Community through the privatisation of intelligence activities and the relative decentralisation of intelligence. The increasing number and complexity of intelligence missions connected to a multitude of independent intelligence agencies led to a decrease in centralised control (Tidd, 2008, 5). Later in the 1990s, the main task of the intelligence services shifted to tackling organised crime (Aldrich, 2010, 236).

4.4.2. Counterterrorist Secrecy

The most significant development in the evolution of the Intelligence Community as it exists today were the events of 9/11. The ability of a non-state actor like Al-Qaeda to operate a large-scale attack against the highly militarised United States impacted the course of national security policy in the US (MacDonald and Hunter, 2019, 35). From then on, the main goal of the US Intelligence Community became preventing the occurrence of similar terrorist attacks (Zeghart & Morell, 2019), marking the shift to a 'counterterrorist state' (Masco, 2010). A significant extension of state security power was implemented, much 'at the expense of civil liberties' (Lidberg & Muller, 2018, 2). Congress allocated significant funds to restructure and significantly expand US Intelligence Community, which aimed for a significant expansion (Masco, 2010; Richelson, 2012, 19).

The consequence was a package of controversial legislation under the Bush administration, which inaugurated the 'war on terror' (Masco, 2010, 433). The Department of Justice recommended that all intelligence agencies 'limit the scope of Freedom of Information Act requests wherever possible' (ibid., 446). The Homeland Security Act 2002 officially installed the Department of Homeland Security, as a federal agency with primary focus on counterterrorist intelligence (HSA, 2002; USIN, 2013). Furthermore, the USA PATRIOT Act of 2001 enabled 'enhanced surveillance procedures', authorising 'the interception of wire, oral, and electronic communications' (USA

PATRIOT Act, 2001). Whilst the Foreign Intelligence Surveillance Act (FISA) had already been enacted in 1978, Section 702 was subsequently inserted into the Act in 2008, allowing the NSA to gather intelligence on 'foreign persons located outside the United States' without prior judicial approval (DNI, 2017; Daugirdas & Davis Mortenson, 2018, 303).

Kaufmann (2004) highlights the risk of the US government abusing intelligence for its own purposes, which can be exemplified by the 2003 Iraq invasion. The White House was able to selectively choose intelligence information and to make it public, which gave it the 'unique ability to shape public perceptions' (Kaufmann, 2004, 37). In that way the threat of 'weapons of mass destruction' in Iraq was supported by information released to the public, whereas contradictory intelligence remained classified (ibid.). The elimination of the position of the Director of Central Intelligence and establishment of the position of Director of National Intelligence was undertaken to improve communication between intelligence departments, which had failed to adequately communicate with each other prior to 9/11 (Richelson, 2012, 538). Rovner (2011, 186) argues that the failure to prevent 9/11 was largely due to the Intelligence Community's inability to 'connect the dots'. The 'wall between domestic and foreign intelligence' caused crucial intelligence to fall into a grey area (ibid.). The 9/11 commission concluded that much of the failure to prevent 9/11 was due to 'vertical stove-piping and compartmentalized hoarding of information', meaning that crucial information wasn't passed on to the right entities (Aldrich & Moran, 2018, 7).

4.4.3. US Intelligence and the Rise of the Internet

With the rise of the Internet and fast-paced technological advancement the Intelligence Community had to face new problems in the beginning of the 21st century (Zeghart & Morell, 2019). Even though traditional Human Intelligence collection still plays an important part in the digital age, Aldrich and Moran (2018, 6) argue that 'big data is transforming the national security realm and opening the door to what we might call knowledge-intensive security'. The actual collection of intelligence today is more concerned with non-state actors than military forces (ibid.). Technological advancement is both beneficial as well as threatening to the IC (Richelson, 2008, 542). The diffusion of threats through the cyber sphere and transnational crime contribute to blurring lines between domestic and foreign intelligence (Mccarthy, 2002, 442). It is now more

complicated for the IC to identify possible threats due to the close entanglement of domestic and foreign communication via technological devices (Byman & Wittes, 2014). This further leads to 'everything and everyone' becoming a potential threat, which acts as justification of intrusive surveillance conduct (Ellis, 2010, 4).

In order to expand the Intelligence Community body, the process of privatisation, starting under the Clinton administration, was 'accelerated' under President George W. Bush in his second administration (Aldrich & Moran, 2018, 9). The US's pivot towards private sector intelligence activities was incentivised by *inter alia*, the increasing popularity of the Internet since the 1990s, the growing amount of data and the reduction of federal staff (ibid.). Both the technological deficit of the federal government in comparison to the private sector and the need to analyse the vast amounts of collected data acted as incentive for increasing privatisation (Ellis, 2010, 3). Ellis (2010, 7), however, highlights a number of issues associated with the outsourcing process of the IC. First, communication between government managers and contractors is not as strong as communications between governmental staff. This bears the risk of a contractor acting against the government's will. Second, if the government asks a contractor to operate in breach of its contractual obligations, the consequence is that it becomes more difficult to hold the government accountable. Third, the interest of the contractor might be very different to the government's interest. Contractors can possess or access considerable amounts of data on US citizens, which runs the risk of the contractor abusing this access for its own purposes.

Aldrich and Moran (2018, 3) therefore argue that Snowden's disclosures were simply symptomatic of 'systemic changes in the nature of intelligence'. According to that argument, Snowden is not the mere cause of the current image crisis of the Intelligence Community but rather symbolic of the structural changes that have taken place since the emergence of advanced technology (ibid.). His leaks highlighted a conflict present in intelligence within the digital age, namely the tension between assuring security and protecting data privacy (Byman & Wittes, 2014).

6. Methodology

This chapter sets out the research methodology of this study. The research methodology was chosen according to the question:

How do the NSA and CIA reshape the notion of transparency through their online discourse?

This study follows qualitative research and uses the tools of Fairclough's concept of Critical Discourse Analysis, which uses three interconnected levels of analysis (see 4.1.4.). The theoretical assumption grounds on the suggestion that Snowden's disclosures in 2013 had an impact on the IC's discourse on transparency. The NSA and CIA were selected as subjects of interest, especially their web publications, speeches, blog posts and press releases between 2011 and 2019. Findings were acquired through both a within-case and between-case comparison of the agencies. The Critical Discourse Analysis of the agencies' narratives on transparency highlighted crucial patterns across time, which confirmed the theoretical assumption of an 'Snowden-impact'. The agencies' conceptualisations of the term transparency illustrate the assumption of this impact.

6.1. Case Selection

The case selection resulted in focussing on the NSA and the CIA. The selection followed the following premises. Firstly, the case of the Intelligence Community of the United States appears as interesting due to the extensiveness of this security organ (Lowenthal, 2017, 987). Secondly, blurring lines between domestic and foreign intelligence are part of the changing nature of intelligence. Thirdly, while the NSA received significant public attention through Snowden's disclosures, the CIA was mentioned comparatively less frequently within public debate, even though Snowden was a former CIA employee and the disclosures also revealed information regarding activities of the CIA. Snowden and the NSA were mentioned 20 million times on Twitter in the ten months following Snowden's disclosures whereas the CIA remained less mentioned (Boynton & Richardson, 2016, 1917). It is crucial to look at the agencies' online discourse, as, in the information age, members of the public are most likely to acquire information online. In this regard, the agencies' 'image campaigns' are strongly concentrated on their online presence, which is further underlined by the discussion of findings below.

6.2. Research Design

Initially, abductive reasoning was deployed for an unstructured examination of the NSA website's rhetoric and establishing the theoretical assumption of a 'Snowden-impact' on the transparency narrative. The formulation of a research question therefore followed the premise of 'abduction', which is a kind of scientific reasoning in-between 'deduction'

and 'induction' (Peirce, 1998). The concept is grounded on the theoretical premise that a hypothesis is formed after initial observations, which require further analysis to prove the hypothesis (Lipscomb, 2012). This means that the initial hypothesis remains at risk of being 'in error' after the analysis is conducted (ibid., 247). Abductive reasoning led to the suggested hypothesis of a changing intelligence discourse post-Snowden, which then invited a more in-depth analysis of the NSA's online discourse.

The CIA was chosen as second case for comparison. Findings were therefore made through both a within-case and between-case comparison of the agencies. The scope conditions for the analysis were the agencies' rhetoric between 2011 and 2019. The year of 2011 was chosen in order to analyse what the rhetoric looked like before Snowden's disclosures in 2013.

6.3. Research Method

To conduct this study, the 18 website sections, 314 press releases, 72 blog posts and 49 speeches were roughly coded first. The coding process allowed a first analysis of significant patterns in the agencies' narratives. Coding was further necessary owing to the large amount of online material published by the agencies. As an initial step, the text was coded for cross-cutting categories in order to discern overarching narratives. The headlines of press releases were defined with codes such as 'remembering', which was further developed into subcategories like 'heroisation and cold-war-history'. These subcategories were established through taking a closer look at the language used in press statements within the 'remembering'-category. Categories, which appeared more frequently throughout time, pointed towards a changing online discourse of the agencies. After coding the material available on the NSA and CIA websites, the linguistic tool of Critical Discourse Analysis enabled a closer look at the underlying narratives on transparency. The keywords used to develop a closer focus were: transparency, privacy, accountability, public, citizens, whistleblowing and leaks. As a result, the CDA was narrowed down to 12 speeches, 30 press releases, 12 CIA blog posts and 18 webpages.

Table 1

NSA and CIA material coded/material more specifically analysed via CDA.

Timeframe 2011-2019.

	NSA	CIA
Webpages (same across time)	10/10	8/8
Press Releases	198/16	116/14
Speeches	18/7	31/5
Blog Posts	0/0	72/12

6.4. Limitations of Study

A key obstacle to this study's discourse analysis was that patterns are challenging to trace back to specific events such as whistleblowing incidents. This is for several reasons.

First, websites are rarely subject to immediate change as updates to websites require time and labour. Additionally, other factors such as policies, changes of government and political events have the ability to influence the agencies' rhetoric and 'social media trends'. As Fenster (2017, 104) notes, 'it is difficult to trace the disclosures' causal effects as a natural experiment, given both the improbability of identifying a control group against which to compare and the complex set of conditions at play in the world before, during, and after the disclosure'. As such, this study is less concerned with the question of whether or not Snowden's disclosures were the only impact in changing in the agencies' discourse and rather *how* the agencies react to their increasing publicity and controversy.

Furthermore, this study refrains from suggesting a complete representation of the intelligence discourse since 'discourse is not, and can never be a transparent medium that 'mirrors' the world' (Miller, 1989, 116). Looking at the agencies' websites, press releases, blog posts and speeches can only demonstrate a part of discourse. The Critical Discourse Analysis shall build on the theoretical premise that discourse is 'all that we can discuss or know' (ibid.).

6.5. Theoretical Framework

The following sections inform about the theoretical debates this thesis used to conceptualise the results of the Critical Discourse Analysis. First, the selection of the theoretical framework is explained. Second, the concepts of silence and power in discourse are discussed in connection to this study. Third, the broadening of the securitisation framework through the concept of silence is elucidated. Fourth, the techniques of the Critical Discourse Analysis after Fairclough are discussed and illustrated through examples of this study.

6.5.1. Selection of Framework

Although this study acknowledges the importance of the securitisation framework when looking at security discourses, this framework bears shortcomings, particularly for the purposes of this study. The centrality of the speech acts for securitisation theory risks dismissing the 'social contexts and complex communicative and institutional process of securitisation' in politics (Williams, 2003, 528). The discourse analysis of this study strives to embed securitising speech-acts into the social context (Williams, 2003) of a public 'transparency-demand' and elaborates on the development of US. Whereas securitisation theory is criticised for its strong focus on securitising actors, which has led to comparatively less discussion of the 'securitised' actors, securitisation theory compliments this study in its focus on the Intelligence Community's language, which has been dismissed in previous studies (Roe, 2012).

The CDA shows the important inclusion of theories of silence and power in discourse in order to embed the findings into a theoretical debate. However, conceptualisations of silence have to be critically assessed. Dingli (2015) and Guillaume (2018) describe the shortcomings of past approaches to silence in international relations as excessively focusing on what specific silences mean and the approach of silence as not more than the absence of speech. However, according to Foucault's understanding of silence in discourse, silence exists *within* discourse. Foucault has conceptualised security discourses within their 'milieus' and not merely as speech acts, rather in 'dispersed processes, mechanisms and technologies that have a contingent relationship to the state' (Walters, 2015, 28; Barnett, 2015). In this realm MacDonald and Hunter (2019, 93) argue that the discourse of security exists within a variety of texts, which circulate through institution's different sites and the media into the public sphere.

By looking at the online discourse of the intelligence agencies, this study highlights mechanisms how they attempt to re-establish their power over the notion of transparency. The agencies' websites acts as in Foucault's (1979) words 'sites where knowledge is formed'. Therefore silence shall not be approached in an interpretation of what it means *per se* but rather, through a cross-time CDA of how exists within the Intelligence Community's public discourse. Through the focus on how the Intelligence Community breaks silence after whistleblowing has occurred, it is be illustrated how the agencies justify silence within the public demand of transparency. Thus, the study is less focused on 'what silence does' but rather, how securitising actors create a narrative on 'how to do silence' and transparency.

6.5.2. Silence and Power in Discourse

It is a theoretical assumption of this study that the act of whistleblowing has an impact on the Intelligence Community discourse. Consequently it is suggested that the intelligence agencies attempt to 'break the silence' in their own terms to uphold their image and legitimacy. It is suggested that the IC's narrative aims to reshape the notion of transparency, a discourse that has traditionally been dominated by public discussions.

Secrecy as a strategy for political purposes can be described as form of institutionalised silence. Silence is part of securitising discourses, which are 'powerful' political strategies that 'internalise and individualise threats' (Ku, 1998, 818; Hansen, 2000, 306).

Discussions of the concept of silence have been popular among scholars of international relations theory but as Dingli (2015) argues, their conceptualisation of silence is often too narrow. It is important to note that silence cannot be merely defined as an 'absence' but rather as being 'constitutive of political discourse and practice' (Dingli, 2015, 724; Bhambra & Shilliam, 2009). This aligns with Foucault's conceptualisation of silence not as an absence of speech but as 'an element that functions alongside the things said' and which exists already prior the initiation of discourse (Foucault, 1979, 27; Bindeman 2017, 143). Connecting this to the discourse of the Intelligence Community, Foucault's concept highlights silence as part of political strategy (Hansen, 2000).

Essential in the examination of silence in discourse is a close inspection of the 'language game' that is being played and the question of by which actors (Guillaume, 2018, 489). While scholars have typically focused on the *silenced* in discourse (ibid., 723), this study is interested in the language of *silencing* actor. In the context of this study, the silencing

actor is the Intelligence Community, which decides when and where 'to speak', and breaks the silence in its own terms. The analysis of the intelligence rhetoric therefore tried to outline the 'language game' of the Intelligence Community, how it can be disturbed by the act of whistleblowing and as a consequence, how it strives to re-establish dominance over the discourse through its own transparency narrative. Through defining transparency, the agencies are able to stretch its conceptualisation according to their own benefit. Their discourse about transparency acts as education on how much silence is needed in order to 'defend the nation'. As such, the discourse analysis of this study shall 'determine the different ways of not saying' what might be controversial in the public eye and examine 'which type of discourse is authorised' by the U.S. government (Foucault, 1979, 27).

The concept of power in discourse is crucial in connection to silence, since discourse arises out of power relations and silencing of what benefits the uphold of the former (Miller, 1989, 121). The online discourse by the intelligence agencies can be described, in Foucault's words (1979, 62), as a 'point in the exercise of power' or a 'site where knowledge is formed'. The conceptualisation of power in the intelligence discourse can be linked to the benefit it serves to the US' national security agenda (Miller, 1989, 123). This is examined through speech acts, which further highlight an underlying agenda when analysed critically through 'historical conditions, their effects, what interests they serve and what relations of power they uphold' (Macdonell, 1986, 67). This argument by Macdonell (1986) is considered by highlighting the historical development of US intelligence and discussing its mission to uphold its public legitimacy.

6.5.3. Broadening the Securitisation Framework with Silence

Central to this study is the notion that the US government decided when and where silence in politics is legitimate, which shows silence as something 'productive' in discourse. Silence in this sense is productive because it is part of a 'language game', which also justifies silence in political conduct (Guillaume, 2018, 488). As such, this study draws a link between silence and the concept of securitisation, in which the state speaks 'security', claiming a 'right to use whatever means are necessary to block' threats (Buzan et al., 1998, 24).

While scholars have discussed whether or not language has become crucial to security studies (Fierke, 2002), the question of 'how and why' this is the case must also be

examined, as argued by Guillaume (2018, 477). Guillaume (2018, 478) suggests that security is the consequence of the 'ability of certain actors to speak (in)security so that the public agrees with [...] proposed measures', which follows the concept of the securitisation framework (Weldes et al., 1999; Buzan et al., 1998).

The framework of securitisation is essential in its premise that the reaction 'threats' is justified by extraordinary means, such as in the form of state secrecy as 'institutionalised security' (Buzan et al., 1998, 27). It further highlights how security concerns are discussed offside public debates and rather 'operate in the realm of secrecy' (Williams, 2003, 524). The discourse deployment of the intelligence agencies builds on Buzan et al.'s (1998, 28) premise that within a liberal democracy the question of why a specific situation would require extraordinary means of security must be argued publicly. This describes a continuous legitimisation process in which the state has to justify 'black security boxes in the political process', which is the 'natural environment' of the IC (ibid., 28). Roe (2012, 245) argues that silence describes the lack of external oversight over the securitising actor. In this study it appears especially crucial to examine what happens when the securitising actor, the NSA and CIA, itself becomes a 'dangerous object' of violating the public's privacy.

6.5.4. Critical Discourse Analysis after Fairclough

According to the research question, the method of Critical Discourse Analysis (CDA) was chosen to analyse the material. CDA originates from critical linguistics and therefore highlights 'how authors use language and grammatical features to create meaning' as well as to 'persuade people to think about events in particular ways' (Machin & Mayr, 2012, pp. 1). A critical analysis means 'denaturalising' the text and its concepts, a process which shall be later discussed in connection to the CIA's and NSA's definitions of what transparency implies (Machin & Mayr, 2012, 5). The ability to highlight 'manipulation' and the 'concealing of communicative intension' is especially fitting for analysing the websites of the CIA and NSA (ibid., 1).

In the context of this study's discourse analysis, an emphasis on the 'absence of text' is important for the comparison of the websites across time and for examining the emergence of transparency narratives. The question as to what a discourse implies can only be analysed by looking at 'sets of relations', since it cannot be discussed as an independent entity (Fairclough 1995, 16). Fairclough's three interconnected processes

of CDA support the analysis of the online material in offering a structured yet flexible examination of text for detecting 'linguistic selections, their juxta positioning and their sequencing' (Janks, 1997, 329). The analysis can start at different levels, either with the text, or discursive or sociocultural practice (Fairclough, 1995; 1998). The process of CDA and these steps is repeated multiple times since the analysis can show that a specific level has to be reassessed (Janks, 1997, 341). Fairclough's formulation of ten questions for use when analysing text are divided into vocabulary, grammar and textual structures (1989, 111). These tools shall be exemplified in the next section through the use of an excerpt of an official CIA statement.

"Ben relayed a whole-of-Agency commitment to protecting Americans' privacy and civil liberties. (...) 'The moment you become a CIA officer is when you go to our memorial wall and you stand up in front of those 133 stars and swear a constitutional oath to protect and defend the constitution" (CIA, 2019a)

Here the analyst might ask according to some key questions (Fairclough, 1989, 110, 111): Are there ideologically contested words ('*133 stars*')? What relational values do the words have (referring to CIA Privacy and Civil Liberties Officer Benjamin Huebner as 'Ben')? What metaphors are being used ('*you stand up in front of those 133 stars*')? Are sentences active/passive ('*Ben relayed commitment to protecting ...*')?

The next step in interpreting text and answering some of the former questions is the use of 'discursive practice' after Fairclough (1995). This dimension of the analysis highlights the 'context of production and reception' (Janks, 1997, 329). In the discursive analysis, the situational and the intertextual context are especially crucial to understand the embedment of the text into its context (Fairclough, 1992). Regarding the situational context of the text, the analyst might ask about the *time* and *place* of the emergence of the text (Janks, 1997, 338). In this study's case *time* refers to the timeframe after Snowden's disclosures in 2013 whilst *place* refers to the text's emergence within US culture. The intertextual context refers to the examination of other sources of text, which assists with interpretation. The intertextual context in this study motivated to look, after examining the NSA's website for a change in rhetoric, for similar changes on the website of the CIA. It is further crucial to look at *text hybridity*, which acts as indicator for the intention to favour specific strands of discourse (Chouliaraki &

Fairclough, 2001). There is a multitude of discourses that can be chosen to discuss a specific topic, each of which 'serves a particular interest' (Janks, 1997, 340). As a last step, the analysis moves into the third stage of the social analysis. This step concentrates on the socio-historical conditions 'that govern these processes' of discourse deployment (Janks, 1997, 329) and are pertinent to be considered through an examination of US national security practices regarding secrecy, which have undergone public debates.

The CDA offers an insight into the 'language game' that has been deployed by the Intelligence Community. The suggested aim of the elite is to reshape the discourse and to re-install its public legitimacy. In Foucault's (1979, 62) words, it is useful to look at the 'site where knowledge is formed', therefore this study analyses the IC's website discourse on the notion of transparency. Snowden's disclosures in 2013 were significant because of the critical public debate about intelligence they provoked. This shall be highlighted through Fairclough's (1989) consideration of power in discourse and what happens to discourse when power relations change over time. Fairclough notes that 'even if power relations remain relatively stable, they need to renew themselves in a constantly changing world, and transformations of orders of discourse may thus be necessary even for a dominant social grouping to keep its position' (1989, 40). Accordingly, the changing rhetoric of the CIA and NSA demonstrates how political power has to uphold and re-uphold its legitimacy in the face of external changes, such as the development of fast-paced information flows over the Internet and the increasing possibility of leaks but also, most importantly, increasing public criticism. The analysis therefore considers Fairclough's concept of 'power behind discourse', which describes the elite's struggle for 'control over orders of discourse' as a 'powerful mechanism for sustaining power' (ibid., 74). The struggle of the political elite's 'control over discourse' is highlighted through the IC's silence prior to the deployment of its narrative about transparency. It is the very silence deployed on transparency prior to Snowden that illustrates the state's struggle of upholding the legitimacy of state secrecy.

7. Analysis

The following section sets out this study's findings from the coding process and CDA of the CIA and NSA websites, press releases, blog posts and speeches. First, the most significant empirical findings are demonstrated. Second, analytical comparisons of the

respective 'transparency debates' of the NSA and CIA are presented. This is done by comparing the agencies' most significant rhetorical patterns regarding transparency. The patterns examined are crucial parts of the agencies' image campaigns and their strategies for addressing transparency in order to regain public trust.

The results of the coding process show that the respective strategies of the NSA and the CIA for addressing transparency and their image problems developed at different paces. This may be explained by the fact that the Snowden revelations concerning NSA surveillance resulted in a bigger public controversy than revelations about the activities of the CIA. The CIA's strategies concerning transparency showed greater changes beginning from 2017 than after the Snowden disclosures in 2013. This is demonstrated by changes in its advancement of social media accounts and the instalment of the Office of Privacy and Civil Liberties (OPCL) in 2017. Whereas whistleblowing is not suggested as the only factor in impacting a change of the Intelligence Community's online rhetoric, the public demand for more transparency following the Snowden disclosure's can be a significant factor consideration that, within a liberal democracy, security establishments have to continuously justify their legitimacy of power (Weber, 1958). Williams' (2003, 524) argument that 'security policies and relationships are susceptible to being pulled back into the public realm' when the 'social consensus' on the policies is challenged is worth repeating in this context.

The agencies' creation of social media accounts and their continuous communications drawing attention to these accounts through their websites and press releases demonstrates their effort to engage into more direct contact with the public. This suggests that governments use 'social and online media as tools of contemporary governance' in order to improve their political image (Krzyżanowski & Tucker, 2018, 146).

The CIA addressed transparency and privacy protection less frequently than the NSA, even after the independent CIA Office of Privacy and Civil Liberties was introduced in 2017. The majority of CIA statements on transparency were made by the Privacy and Civil Liberties Officer Benjamin Huebner. On the other hand, the NSA's Privacy and Civil Liberties Office was created almost immediately after the Snowden leaks in 2013. This suggests a 'faster reaction' than that of the CIA due to the proportionally greater public

discussion on the NSA's mass-scale electronic surveillance in Snowden's disclosures (Fidler, 2015, 2).

The NSA's press releases highlighted the creation of IC On The Record in August 2013, a Tumblr page on which it publishes declassified documents regarding foreign surveillance by the US Intelligence Community (IC On The Record, 2019). Additionally, the NSA joined Twitter in December 2013, which further shows a growing interest in creating their image through social media. The comparison of the NSA's website between 2011 and 2015 showed a variety of changes of language on transparency, as shall be discussed later in this study's findings.

Whereas the NSA showed a more immediate reaction to the public discussions post-Snowden in 2013, this was not the case for the CIA. The transparency debate concerning the CIA required taking a closer look at what is being said about transparency indirectly. Rather, as is shown in the subsequent discussion of the analysis, the CIA indirectly portrays its values of transparency through its emphasis on its 'mission to protect the country'. It can be noted, however, that the CIA has always been more 'visible' to the public in comparison to the NSA, which further entails different kinds of narratives.

The following table demonstrates crucial patterns in narrative, which were examined between 2013 and 2019.

Table 2

Patterns identified in NSA and CIA narrative on transparency between 2013-2019.

Narrative	NSA	CIA
7.1. Let's Talk about Transparency	on privacy in cyber space shaping the term together	on transparency of missions definition according to CIA
7.2. Ethos of Privacy Protection	committed to public	committed to mission
7.3. Privacy and Civil Liberties Officers	officials deeming whistleblowing and leaks, PCLOs on the side of the public	
7.4. Diverse Workforce	diversity to create trust	diversity to benefit mission
7.5. Public Figures as Fans	to praise workforce	to dismantle 'movie-image'
	trust through stories on past heroes and spies	
7.6. References to Online Culture	puzzles and mathematicians trust in workforce	dogs and #AskMollyHale trust in mission
7.7. Cyber Space Paradox	itself under attack privacy safety recommendations	

7.1. Let's Talk about Transparency

The discourse analysis showed that from 2013 on the NSA mentioned privacy rights and increasing transparency more often than the CIA. In 2014 NSA Director Michael Allen even stated:

    'Time has passed that maybe we're coming out of the Snowden hangover effect' (NSA, 2014a).

The NSA's narrative of advocating the protection of privacy reveals underlying power relations when examined more closely. This is exemplified by the NSA General Counsel Glenn S. Gerstell stating:

'If we want to play a role in shaping those (privacy) policies to suit our own notions of privacy, we need an overarching effort to address privacy and digital technology here in the US' (NSA, 2018a).

Here it becomes visible how the NSA aims to have a dominant role in the definition of what the term privacy implies. By suggesting that the term 'privacy' is vague and inadequately conceptualised, the NSA is put into the `powerful' position of shaping the term. This stands in disregard to public debates about transparency. Underlying this statement is an ongoing struggle for power over the privacy debate, which the NSA considers essential to be regained in order to maintain the legitimacy of the Intelligence Community's institutional power. This is further important considering the frequent depiction of Europe as 'better suited to manage the privacy challenges posed by the digital age' (NSA, 2018a). This observation suggests that dominating the discourse over privacy is both crucial for shaping privacy polices internationally as well as regain power over the public discourse on privacy in order to come out of the 'Snowden-hangover' (NSA, 2014a).

In comparison, there was little conversation about privacy in the analysed publications of the CIA until the introduction of the independent Privacy and Civil Liberties Office in 2017. Notwithstanding the introduction of this office, CIA press releases and speeches have largely continued to refrain from engaging in a public conversation about privacy. The most significant public event in regards to privacy was an interview with the Privacy and Civil Liberties Director Benjamin Huebner in June 2019, which discussed the CIA's 'balance between transparency and secrecy' (CIA, 2019a). A Q&A section with Huebner was added prior in May 2019, which highlighted the CIA's conception of the term 'transparency':

'For me, when we talk about transparency, release is part of it, but it's not the whole ball of wax. Accessibility is part of transparency. Providing information to people in a way that's easier to find, understandable, and relevant. Those are all parts of transparency too' (CIA, 2019d).

This statement illustrates how the CIA emphasises its own definition of transparency. Stressing that transparency entails the declassification and accessibility of information evokes the notion conceptualised by Dean (2002) of citizens as ever-searching 'suspicious subject', who have the ability to find all information regarding intelligence operations online.

Whilst the NSA attempts to insert itself into the public discourse of transparency through positioning itself as 'one with the public' when defining privacy, the CIA follows a less public-oriented stance. This is demonstrated by presenting its own definition of what transparency implies with little mention of 'the public'.

7.2. The Ethos of Privacy Protection

A further rhetoric analysed through the website sections was the connection of the protection of privacy and the protection of civil liberties under an 'ethos'. The analysis of the CIA website from between 2011 and 2015 showed that references to its 'core values' were changed into references to an 'ethos' (CIA, 2015a). The frequent reference to an intelligence workforce committed to privacy and the 'protection of the nation' can be seen in the context of a rhetorical 'tactic of persuasion'. Aristotle's conceptualisation of *ethos* as a linguistic choice next to *pathos* and *logos* describes the 'ethical appeal', which ought to convey 'believability, reliability and competence' through speech (Halmari & Virtanen, 2015, 5). As has already been highlighted in the methodology chapter, the following quote by CIA Privacy and Civil Liberties Officer Benjamin Huebner illustrates this mode of persuasion through the *ethos*.

'The moment you become a CIA officer is when you go to our memorial wall and you stand up in front of those 133 stars and swear a constitutional oath to protect and defend the constitution' (CIA, 2019).

The image of swearing an oath to protect, not only the nation but also its citizens' privacy rights emphasises patriotism to convince the public of the CIA's sincerity to commit to improve privacy protections. As Fairclough (1989, 3) argues, 'ideology is the prime means of manufacturing consent'. The linguistic element of the *ethos* thus constitutes a strong underlying element in the Intelligence Community's narrative on transparency and privacy.

The depiction of classified information as 'sacred secrets' was a narrative further analysed through looking at what is being said about state secrecy. The CIA refers to its 'sacred work' and a 'sacred mission' within the 'clandestine nature' of its conduct (CIA, 2018a). Under the section on 'ethos' on its website, the CIA further states:

'We preserve our ability to obtain secrets by protecting sources and methods from the moment we enter on duty until our last breath' (CIA, 2015a).

The theme of secrecy within the CIA narrative concentrates on this exact preservation of the 'ability to obtain secrets', which serves the 'higher duty' of their 'ethos'. Rhetorical efforts highlighting that the CIA requires a 'profound degree of trust from the American people' therefore show that the narrative on state secrecy mostly revolves around 'educating' the public on the necessity of having 'faith' in secrecy to defend the US (CIA, 2018c).

The NSA likewise associates 'fighting' for the privacy of American individuals with the ideology of protecting the nation. This is further illustrated through amendments to the NSA's website directly addressing its 'fellow citizens' and its 'commitments' to its website (NSA, 2015c). This special emphasis on the NSA 's 'continuous strive for increasing transparency' appears under the *ethos* of addressing the public directly as well as stressing the dedication of fighting simultaneously both for but also the nation.

Thus, whereas in the case of the CIA the *ethos* of protecting the public's privacy and ensuring transparency is more closely associated with the 'sacred mission', the NSA shows a greater emphasis on connecting the commitment of privacy protection to its 'fellow citizens' (NSA, 2015c).

7.3. Trustworthy Privacy and Civil Liberties Officers

In the narratives on whistleblowing and leaks, contrasting and inconsistent stances were found between the agencies' officials and the Privacy and Civil Liberties Officers of those same agencies.

Whereas NSA Privacy and Civil Liberties Director Rebecca Richards refrained from taking a clear position when asked if she would call Snowden 'a traitor', officials like then-NSA Director Keith Alexander showed less reluctance, calling Snowden's actions 'flat wrong' (NSA, 2014b; NSA, 2013a).

Similarly, CIA Director Mike Pompeo states:

'While we do our best to quietly collect information on those who pose very real threats to our country, individuals such as Julian Assange and Edward Snowden seek to use that information to make a name for themselves' (CIA, 2017b).

In contrast, CIA Privacy and Civil Liberties officer Benjamin Huebner deployed a rhetoric of remorsefulness in admitting that the CIA could have done 'a better job' in educating the public on its conduct (CIA, 2019a).

This suggests that statements by intelligence officials follow a 'harsher' stance in deeming whistleblowing as 'traitorous', revealing the 'general assumption' that 'secrecy is aimed not at domestic, bureaucratic, or political rivals or the American public but at foreign enemies' (Ellsberg, 2010, 773). According to this assumption, 'breaching secrecy exposes the country, its people, and its troops to danger' (ibid.).

This suggests that the position of the Privacy and Civil Liberties officer, both in the case of the CIA and NSA, functions as a 'figure of public trust' that informs the public about illegitimate hidden politics and is depicted as employed by and for the American public. This is in keeping with the NSA's frequent depiction of itself as an agency 'serving the public'. The agency's attempts to directly address the public as 'our fellow citizens' further demonstrates the NSA's attempt to create a dialogue with the public.

The greater reluctance to take a clear stance *against* Snowden's disclosures by the NSA and CIA Civil Liberties and Privacy officers show their effort to establish an image of being responsible for protecting the public's privacy. This is highlighted by the CIA's statement when launching its social media accounts in 2014:

'The agency is more accessible to the American public that we serve, consistent with our national security mission' (CIA, 2014a).

7.4. A Trustworthy, Diverse Workforce

The recruitment efforts by both the NSA and CIA are also a vital part of their transparency narrative. An emphasis on diversity was mostly visible regarding publications of the two agencies concerning recruitment. This was examined by this study not only in relation to press releases and website information but also in the narrative of intelligence officials. NSA research director Deborah Frincke states:

'The more eyes you can get on a problem, the more you can take advantage of the passion and the knowledge others bring with their diverse perspectives. And then we can get out of the 'same-old' mindset' (NSA, 2015d).

The NSA Director of Public Affairs Chad Jones further states:

'Hopefully when they are confronted by some of the negative stereotypes regarding Islam, [they]… can say, I know a Muslim, he was a pretty nice guy, kind of funny, likes baseball, and believes in defending our country just like I do' (NSA, 2015e).

This notion particularly emphasises the idea that a diverse representation of minorities in the work sphere creates a 'trustworthy' image. The quote reveals the NSA's underlying narrative of 'defending our country' as well as its emphasis on connecting to the public through commonly popular American sports like basketball. This narrative highlights what scholars have been discussing as 'Othering' of Muslims in US security discourses. The NSA attempts to create a narrative of trust by highlighting diversity and indirectly reacts to criticism of specifically targeting Muslims in the US (Sorkin, 2014). In this realm, the narrative of Muslim staff members reveals the notion of 'making the unfamiliar familiar'.

The CIA, on the other hand, emphasises its diversity efforts mostly in relation to its 'core mission', highlighting:

'A diverse and inclusive workforce allows us to fulfill our global intelligence mission to preempt threats' (CIA 2018b).

The CIA therefore shows a stronger focus on its responsibility to fulfil 'the mission', which is depicted as 'sacred' and requiring 'diverse knowledge'. This suggests that recruitment efforts by the CIA are rather focused on promoting their conduct than, like the NSA, connecting diversity to transparency.

7.5. Public Figures as Fans

The increasing inclusion of celebrities into press releases demonstrates both agencies' campaign to regaining public trust, legitimacy and power through 'trustworthy' public figures. Celebrities visiting Intelligence Community headquarters, as well as intelligence officials referring to celebrities in interviews illustrate the agencies' effort to create a positive public image.

The CIA states:

'Mr. (Daniel) Craig remarked (…) how impressed he was with the commitment and dedication of CIA officers' (CIA, 2018a).

With its press initiative of 'Reel vs Real' the CIA strives to dismantle the heroisation of operations and staff members in Hollywood movies, with CIA officers popularly depicted as 'liberal and cautious', yet determined to fight against a 'terrorist threat' (Cummings, 2018).

This, however, stands in contrast to the CIA's increasing efforts to highlight its historical successes and speaks against such a promoted effort to dismantle its 'hero image'. The frequent reference to past staff members reproduces the image of 'spies and heroes' and enables the CIA to create its own story of historical achievements, absent from the image the US film industry has created. 'Storytelling' under the CIA-promoted hashtag '#Histint', an abbreviation of 'Historic Intelligence', has been given increasing prominence on the CIA's blog. The CIA's strive to position itself within the image of its historical successes demonstrates how successful intelligence operations from the past can be used to legitimise continuous state secrecy.

A practice of including celebrities into public statements was also observed in the case of the NSA. Nevertheless, the NSA's discourse showed a stronger emphasis on its workforce than educating the public on the reality of its activities vis-à-vis their Hollywood depictions, unlike in the case of the CIA. In hosting a performance by the 'America's Got Talent'-singer Benton Blount, the NSA states:

'The stay-at-home dad said that knowing NSA is a military support organization made him a big fan of the agency' (NSA, 2015a).

With specific attention to the emphasis on 'the-stay-at-home dad' and 'big fan of the agency', this quote also highlights the aforementioned recruitment efforts of the NSA to depict it's organisation as 'ideal workplace'. Similarly, publications coded around the theme of 'remembering' show that that the narrative of the NSA's history emphasises the stories of individual staff members alongside its continuous emphasis on its cryptological history (NSA, 2015b). These depict the NSA in a 'heroic' light, especially through press releases about the employment of women, which further points towards a broadening of the agency's recruitment narrative. Interviews with intelligence officials

have been especially common in the publications of the NSA, not only in highlighting its history but also in familiarising the public with its present workforce.

In this manner, both the CIA and NSA can be seen to use transparency in an attempt to re-establish trust with the public, through a process of the 'heroisation' of past staff members, and the use of praise from celebrated US public figures. In its use of celebrities, the NSA, however, shows a greater emphasis on its workforce and recruitment interest than an image revision campaign, like the CIA.

7.6 References to Online Culture

References to the wider online culture were particularly common among the analysed publications of the CIA. As aforementioned, analysing the CIA's transparency narrative demands looking beyond what is being said on transparency directly. A sensitivity towards online trends allows the agency to reach a wider audience and to control its public image. This is illustrated by the following quote from Privacy and Civil Liberties Officer Benjamin Huebner:

'We have to engage where people actually are and where those conversations are happening. (…) That's why we're on social media. It's where a lot of conversations are happening right now' (CIA, 2019d).

The introduction of the 'Q&A' hashtag '#AskMolly' demonstrates such an effort. The pseudonym of the CIA staff member Molly Hale answering the public's question about the CIA illustrates the CIA's effort to 'venture into the social media sphere' (CIA, 2019b). The choice of the pseudonym illustrates how Molly as 'typical American name' strives for 'trust'. The last name Hale acts as 'a tribute to Nathan Hale', who was 'executed for spying' (CIA, 2019b), again illustrating the heroisation of 'spies' within narrating the history of the CIA. The creation of the #AskMolly blog establishes an image of transparency on the part of the CIA by showing a simple way for the public to pose questions to the CIA, just through using the designated hashtag. However, the questions answered under #AskMolly concern the CIA museum, whether or not there is a Starbucks café in the CIA Headquarters and if the CIA has its own library (CIA, 2019c). The #AskMolly does not address any of the substantial questions about the conduct of the CIA and rather "promotes transparency" by dealing with trivial matters. The idea of conveying transparency efforts through a concept like #AskMolly demonstrates the CIA's efforts in reshaping its image. The CIA also seeks to regain the public's trust

through its sharing of stories of the 'K-9 Corps', the CIA's police dogs. Given that a dog represents the 'social identity of the owner' (Sanders, 1990), the language being used for the CIA blog's 'pupdates' is important for the analysis of its image campaign. The CIA praises its police dogs as having spent 'their lives in service to their country' (CIA 2018d) with the intention of reflecting an image of loyalty, faith and honesty on the agency and its officers.

While dogs were also mentioned in NSA press releases, this was comparatively less frequent than in the case of the CIA. Rather, the NSA attempted to engage the public through creating an image of a smart workforce of mathematicians, something that 'every ordinary citizen' could be a part of, for example, by playing the NSA's online puzzles (NSA, 2015h).

The above analysis shows how the agencies aims to connect with the public through the portrayed values of trust, loyalty and accountability. The CIA's focus lies on trust, as shown through its creation of Q&A hashtags and its reporting about its dog force. On the other hand, the NSA attempts to proove accountability through highlighting its 'smart workforce'.

7.7. The Cyber Space Paradox

The 'cyber space paradox' has been a vital part of the NSA's narrative on privacy. This narrative strongly builds on the 'uncertainty' of the cyber space. The securitisation framework is partly sufficient in order to explain the disocurse on 'cyber threats'. The 'cyber threat' follows how security representatives 'recreate the notion of other, otherness and difference' (Alvarez, 2006, 74). The rhetorical positioning depicts the NSA as passive and as 'under attack' in the cyber space; emphasising itself as being just as in-danger as the American public. The subject positioning therefore builds on the NSA as a 'possible victim' of the 'cyber threat', which seeks to create a bridge to the public. In comparison to the 'external threat' of cyber attacks, the surveillance of citizens is depicted as 'lesser evil' (Ignatieff, 2004). The paradox that arises is the NSA's continuous narrative that the public should secure their cyber data whilst on the other hand being the subject of violating privacy and misusing cyber data. The US government emphasises the blurring lines of defining potential criminals, stating that 'friends and foes' all use 'the same communications devices', which further acts in favour of the NSA's rhetoric of alarming the public about the 'unpredictability' of the cyber space (President's Review

Group, 2013). Stating that the nation is unprepared for cyber attacks (NSA, 2015f), points away from the fact that the NSA itself has been a 'threatening' actor as regards privacy protection. The NSA therefore depicts itself as a benign actor in contrast to malign hackers. For example, the NSA addresses the public, stating:

'You are the best defense against bad actors on this planet' (NSA, 2016a).

This shows the increasing cyber-awareness efforts by the NSA to depict itself in a positive light. Press statements such as,

'love and cyber attacks come unexpectedly but at least you can prepare for cyber attacks' (NSA, 2015g),

therefore exemplify the NSA's effort to create of an image of trust through assuring the public of its benevolent cyber security recommendations.

8. Concluding Remarks

The discourse analysis of CIA and NSA websites, press releases and speeches by officials has demonstrated the agencies' narratives on transparency. The CIA and NSA discourses showed differences in the interpretation of the notion of transparency. Whilst the NSA directly discussed transparency with a strong connection to privacy rights post-Snowden from 2013 on, the CIA only started mentioning transparency after 2017. Overall, it was found that the NSA showed a greater emphasis on the public and on shaping the term of privacy together with the public. The CIA, on the other hand, embedded the debate about transparency in its own narrative of a 'sacred mission' with less emphasis on the public. In both cases, however, the creation of the position of the Privacy and Civil Liberties Officers was significant for a more public transparency debate. The Privacy and Civil Liberties Officers of both agencies refrained from taking a clear stance against whistleblowing and leaks and attempted to show dedication to the public and transparency. This suggests that in the cases of both the CIA and NSA, the officers' positions within the agencies are intended to act as a 'bridge' to the public and to create a more 'trustworthy' image of the agencies.

This study has highlighted how, within a liberal democracy, public controversy after whistleblowing has the ability to impact security discourses, as illustrated through the

changing transparency narratives of the agencies. As Masco (2010, 454) suggests, with the rise of new technologies of mass communication, intelligence agencies acquire 'a new kind of power: the ability to create realities'. By reshaping the transparency discourse in their own terms, the agencies have been shown to attempt to create a reality of transparency and thereby uphold their legitimacy. This study has further elaborated the development of intelligence, which leads to the agencies' 'more forward strategy', which aims 'to protect its reputation and promote public understanding of its work' (Aldrich & Moran, 2018, 12).

Justifications of silence simultaneous with a conversation about transparency act as 'political strategy' (Ku, 1998, 182) to re-establish trust in the agencies' conduct. Silence is important not only in relation to the act of whistleblowing, which 'breaks the silence' on illegitimate conduct by the Intelligence Community, but also in relation to how the agencies themselves try to re-shape the discourse by 'breaking the silence' in their own way and thereby regaining 'power over knowledge' (Macdonell, 1986, 62). Consequently, silence in the Intelligence Community's discourse has to be seen as an 'element that functions alongside the things said, with them and in relation to them within over-all strategies' (Foucault, 1979, 27).

The findings on the agencies' narratives of transparency contribute to broaden the securitisation framework in its current theoretical debate concerning the Intelligence Community's speech acts. Whilst the 'war on terror' narrative is still largely prominent in the agencies' discourses, the securitisation framework insufficiently explains recent debates about transparency. The Intelligence Community's nature builds on the maintenance of silence in politics. Today, in a constant speaking world, the agencies have to publicly legitimise their conduct in the context of growing calls for more transparency, as shown through this study's discourse analysis. The American public's demand for the increasing visibility of power consequently impacts the securitising discourse in a manner which requires the Intelligence Community's discourse to be about more than threats, namely the re-establishment of trust in the democratic government (Ku, 1998, 176).

Continuing on what this thesis has suggested, an analysis of the agencies' social media accounts like Twitter and Facebook could further contribute to examining their image campaign and transparency debate, perhaps even focussing on other agencies of the US

Intelligence Community. Furthermore, the elaboration on the changing nature of the Intelligence Community through, *inter alia*, increasing privatisation suggests that the agencies' public rhetoric could further be compared to image campaigns by private security companies.

However, in keeping with Dean's (2002) suggestion, the mere focus on what the Intelligence Community says about transparency dismisses its important contextualisation within the public's 'obsession' of revealing the secret. As Masco (2010, 440) argues, the American public today is 'overdetermined not by the amount of information set free but rather by the political deployment of the secret as idea'. Therefore it is important to uncover the language game played by the Intelligence Community, which continues to produce the paradox of sacred secrets and the availability of all desired information online as long as the public searches enough. This paradox is illustrated by the agencies' attempts to push a narrative of the harmonious coexistence of sacred secrets and visibility in the 21st century.

6. List of References

Primary Sources

CIA (2019a). Balancing Transparency and Secrecy in a Digital Age. Retrieved from https://www.cia.gov/news-information/blog/2019/balancing-transparency-and-secrecy-in-a-digital-age.html.

CIA (2019b). Have a Question About the CIA? Ask Molly! (2019, February 04). Retrieved from https://www.cia.gov/news-information/blog/2019/ask-molly.html.

CIA (2019c). Blog. Retrieved from https://www.cia.gov/news-information/blog/index.

CIA (2019d). Transparency at CIA. (2019, May 01). Retrieved from https://www.cia.gov/news-information/featured-story-archive/2019-featured-story-archive/transparency-at-cia.html.

CIA (2018a) Reel vs Real with Daniel Craig. Retrieved from https://www.cia.gov/news-information/blog/2018/reel-vs-real-with-daniel-craig.html.

CIA (2018b). Message from the Director: Commitment to a Diverse and Inclusive Workplace Free of Harassment and Discrimination. (2018, July 11). Retrieved from https://www.cia.gov/news-information/press-releases-statements/2018-press-releases-statements/commitment-to-a-diverse-and-inclusive-workplace-message-from-the-director.html.

CIA (2018c). CIA Director Gina Haspel's Speech at the University of Louisville. (2018, October 03). Retrieved from https://www.cia.gov/news-information/blog/2018/cia-director-gina-haspels-speech-at-the-university-of-louisville.html.

CIA (2018d). CIA Unveils Memorial to Agency K9s. (2018, September 10). Retrieved from https://www.cia.gov/news-information/blog/2018/cia-unveils-memorial-to-agency-k9s.html

CIA (2017b). Director Pompeo Delivers Remarks at CSIS. Retrieved from https://www.cia.gov/news-information/speeches-testimony/2017-speeches-testimony/pompeo-delivers-remarks-at-csis.html.

CIA (2015a). CIA Vison and Values. Retrieved from https://www.cia.gov/about-cia/cia-vision-mission-values.

CIA (2014a). CIA Launches New Social Media Accounts. Retrieved from https://www.cia.gov/news-information/press-releases-statements/2014-press-releases-statements/cia-launches-new-social-media-accounts.html.

DNI (2017). The FISA Amendments Act: Q&A. Office of the Director of National Intelligence. Retrieved from https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf.

DNI (2019). What We Do. Director of National Intelligence. https://www.dni.gov/index.php/what-we-do/ic-budget.

HSA (2002). Homeland Security Act of 2002. Senate and House of Representatives of the United States of America in Congress. Retrieved from https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.

IC On The Record (2019). Retrieved from https://icontherecord.tumblr.com.

NSA (2017a). Failing to Keep Pace: The Cyber Threat and Its Implications for Our Pr. (n.d.). Retrieved from https://www.nsa.gov/news-features/speeches-testimonies/Article/1608850/failing-to-keep-pace-the-cyber-threat-and-its-implications-for-our-privacy-laws/.

NSA (2016a). NSA Staffer Talks Cybersecurity with Teen Math Phenoms. (2016, August 04). Retrieved from https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1623557/nsa-staffer-talks-cybersecurity-with-teen-math-phenoms/.

NSA (2015a). NSAs Got Talent For Summer Series. Retrieved from https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1626202/nsas-got-talent-for-summer-concert-series/.

NSA (2015b). Symposium for Cryptologic History has its own rich History. Retrieved from https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1626956/symposium-for-cryptologic-history-has-its-own-rich-history.

NSA (2015c). Commitment. (Wayback Machine). Retrieved from https://web.archive.org/web/20150905063343/https://www.nsa.gov/about/commitment/index.shtml.

NSA (2015d). Cryptology, whack-a-mole, & time travel: NSA,s research director on se. (2015, August 18). Retrieved from https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1625769/cryptology-whack-a-mole-time-travel-nsas-research-director-on-securing-cyberspa/.

NSA (2015e). "Our difference is but the thickness of this line." NSA's Pre-Ramadan. (2015, June 18). Retrieved from https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1626755/our-difference-is-but-the-thickness-of-this-line-nsas-pre-ramadan-lecture-lunch/.

NSA (2015f). Steve LaFountain (Dean of the College of Cyber: Building the Next Generation (2015, October 29). Retrieved from https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1625754/steve-lafountain-dean-of-the-college-of-cyber-building-the-next-generation-of-c/.

NSA (2015g). NSA.gov Love Notes. (2015, September 25). Retrieved from https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1626459/nsagov-love-notes/.

NSA (2015h). July 2015 Puzzle Periodical. (2015, July 21). Retrieved from https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1627293/july-2015-puzzle-periodical/.

NSA (2014a). Reagan National Defense Forum: Building Peace Through Strength For American Security. Retrieved from https://www.nsa.gov/news-features/speeches-testimonies/Article/1619392/reagan-national-defense-forum-building-peace-through-strength-for-american-secu/.

NSA (2014b). Live Tumblr Q&A with NSA Civil Liberties & Privacy Officer Rebecca Richards. Retrieved from https://www.nsa.gov/Portals/70/documents/news-features/news-stories/pre-2015/20141124-clpo-tumblr.pdf.

NSA (2013a). Remarks by GEN Keith Alexander, Commander, U.S. Cyber Command (USCYBER. (n.d.). Retrieved from https://www.nsa.gov/news-features/speechestestimonies/Article/1620137/remarks-by-gen-keith-alexander-commander-us-cyber-command-uscybercom-director-n/.

OHCR (2013). The Right to Privacy in the Digital Age. United Nations Human Rights. https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

OIG (2019). Whistleblower Information. National Security Agency Office of the Inspector General. Retrieved from https://oig.nsa.gov/Whistleblower-Information/.

President's Review Group (2013). Liberty and Security in a Changing World. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Rainie, L., & Madden, M. (2015). Americans' privacy strategies post-Snowden. Pew Research Center, Internet Science and Technology. Retrieved from http://www.pewinternet. org/2015/03/16/americans-privacy-strategies-post-snowden.

USA Freedom Act (2015). Uniting and Strengthening America by fulfilling Rights and Ensuring effective Discipline over monitoring Act of 2015. Government Publishing Office. https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.htm

USA Patriot Act (2001). H.R.3162, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001. Retrieved from https://www.congress.gov/bill/107th-congress/house-bill/3162.

USNI (2013). U.S. National Intelligence: An Overview 2013. Director of National Intelligence. https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf.

Secondary Sources

Ackerman, S. (2014, March 14). How the US intelligence community attempts to rebrand itself – on Tumblr. The Guardian. Retrieved from https://www.theguardian.com/world/2014/mar/14/intelligence-community-on-the-record-james-clapper-nsa.

Agamben, G. (2005). The State of Exception. Chicago: University of Chicago Press.

Agamben, G. (1998). Homo Sacer: Sovereign Power and Bare Life. Stanford: Stanford University Press.

Aid, M. M. (2001). The National Security Agency and the Cold War. In Intelligence and National Security, 16(1), 27-66.

Aldrich, R. J. (2002). Hidden Hand: Britain, America and Cold War Secret Intelligence. New York: Overlook.

Aldrich, R. J., (2011). Intelligence. In Williams, P. D. Security Studies; An Introduction. 2nd edn. London: Routledge, 235-249.

Aldrich, R. J. & Moran, C. R. (2018) 'Delayed Disclosure': National Security, Whistle-Blowers and the Nature of Secrecy. In Political Studies, 67(2), 1–16.

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? Journal of Social Issues, 33(3), 66-84.

Alvarez, J. E. (2006) Re-thinking (in)security discourses from a critical perspective. Asteriskos Journal of International and Peace Studies. 1(2), 61-82.

Barnett, C. (2015). On the milieu of security. Dialogues in Human Geography, 5(3), 257-270.

Bellaby, R. W. (2017). The ethics of whistleblowing: Creating a new limit on intelligence activity. Journal of International Political Theory, 14(1), 60-84.

Bellman, B. L. (1981). The paradox of secrecy. Human Studies, 4(1), 1-24. doi:10.1007/bf02127445

Bhambra, G. K., & Shilliam, R. (2009). Silencing human rights: Critical engagements with a contested project. Basingstoke, Hampshire: Palgrave Macmillan.

Bindeman, S. L. (2017). Silence in philosophy, literature, and art. Leiden: Brill-Rodopi.

Bruneau T. C., Dombroski, K. R. (2014) Reforming Intelligence: the challenge of control in the new democracies. Retrieved from: https://calhoun.nps.edu/handle/10945/41971.

Boynton, G. & Richardson, G. W. (2016). Agenda setting in the twenty-first century. In New Media & Society, 18(9), 1916-1934.

Buzan, B., Wæver, O., & Wilde, J. D. (1998). Security: A new framework for analysis. Boulder, CO: Lynne Rienner Pub.

Byman, D. & Wittes, B. (2014). Reforming the NSA: how to spy after Snowden. (Edward Snowden and the National Security Agency). In Foreign Affairs, 93(3), 127-138.

Caldas-Coulthard, C. R. (2003). Cross-Cultural Representation of 'Otherness' in Media Discourse. Critical Discourse Analysis, 272-296.

Chomsky, N. (2017). Noam Chomsky on the Long History of US Meddling in Foreign Elections, Interview by C.J. Polychroniou. Troughout. Retrieved from https://truthout.org/articles/noam-chomsky-on-the-long-history-of-us-meddling-in-foreign-elections/.

Chouliaraki, Lilie and Fairclough, N. (2001). Discourse in late modernity: rethinking critical discourse analysis. Journal of English Linguistics. 29(2). 183-189.

Clinton, R. S. (1990). "The Animal 'Other': Self Definition, Social Identity and Companion Animals". In NA - Advances in Consumer Research, 17(1), 662-668.

Cummings, J. (2016). The CIA Is Not Your Friend. JACOBIN. Retrieved from https://www.jacobinmag.com/2016/12/cia-russia-wikileaks-podesta-trump-clinton-obama

Dillon, M. (1996). Politics of Security: Towards a Political Philosophy of Continental Thought. London: Routledge.

Daugirdas, K. & David Mortenson, J. (2018). Time-Limited Provisions of the Foreign Intelligence Surveillance Act Reauthorized Through 2023. In The American Journal of International Law, 112(2), 303-306.

Dean, J. (2002). Publicity's secret: How technoculture capitalizes on democracy. Ithaca, New York: Cornell University Press.

DeVine, M. E. (2018). Intelligence Community Spending: Trends and Issues. Retrieved from https://fas.org/sgp/crs/intel/R44381.pdf.

Dingli, S. (2015). We need to talk about silence: Re-examining silence in International Relations theory. European Journal of International Relations,21(4), 721-742.

Duyvesteyn, I. (2011) 'Intelligence and Strategic Culture: Some Observations'. In Intelligence and National Security, 26(4), 521-530.

Ellis, W. W. (2010). Us intelligence at the crossroads. In Mediterranean Quarterly, 21(2), 1-11.

Fairclough, N. (1995) Critical Discourse Analysis: The Critical Study of Language. London: Longman.

Fairclough, N. (1992). Discourse and Text: Linguistic and Intertextual Analysis within Discourse Analysis. Discourse & Society, 3(2), 193-217.

Fairclough, N. (1989) Language and Power. London: Longman.

Fenster, M. (2017). The Transparency Fix: Secrets, Leaks, and Uncontrollable Government Information. Stanford: Stanford Law Books.

Fidler, D. P. (2015). The Snowden Reader. Indianapolis: Indiana University Press.

Fierke, K. (2002). Links Across the Abyss: Language and Logic in International Relations. International Studies Quarterly, 46(3), 331-354.

Foucault, M. (1979). The History of Sexuality. London: Allen Lane.

Foucault, M. (1979). Power and Norms. In M. Morries and P. Patton (Eds.), Power, Truth and Strategy (62). Sydney: Feral.

Gleijeses, P. (2016). The CIA's Paramilitary Operations During The Cold War: An Assessment, In Cold War History, 16(3), 291-306.

Guillaume, X. (2018). How to do things with silence: Rethinking the centrality of speech to the securitization framework. Security Dialogue, 49(6), 476-492.

Halmari, H., Virtanen, T. (2015). Persuasion Across Genres: A Linguistic Approach. Amsterdam: John Benjamins Publishing Company.

Hansen, L. (2000). The Little Mermaids Silent Security Dilemma and the Absence of Gender in the Copenhagen School. Millennium: Journal of International Studies, 29(2), 285-306.

Hughes, R. G., Jackson, P., & Scott, L. V. (2008). Exploring intelligence archives: Enquiries into the secret state. Abingdon: Routledge.

Hunter, D., & MacDonald, M. N. (2017). Arguments for exception in US security discourse. Discourse & Society, 28(5), 493-511.

Ignatieff, M. (2004). The Lesser Evil: Political Ethics in an Age of Terror. Princton: Princton University Press.

Janks, H. (1997) Critical Discourse Analysis as a Research. Journal Discourse: Studies in the Cultural Politics of Education, 18(3), 329-342.

Joachim, J., & Schneiker, A. (2012). New Humanitarians? Frame Appropriation through Private Military and Security Companies. Millennium: Journal of International Studies, 40(2), 365-388.

Kaufmann, C. (2004) Threat Inflation and the Failure of the Marketplace of Ideas: The Selling of the Iraq War. In International Security, 29(1), 5-48.

Krzyżanowski, M., & Tucker, J. A. (2018). Re/constructing politics through social & online media. Journal of Language and Politics Re/constructing Politics Through Social & Online Media, 17(2), 141-154.

Ku, A. S. (1998). Boundary Politics in the Public Sphere: Openness, Secrecy, and Leak. Sociological Theory, 16(2), 172-192.

Lashmar, P. (2019). From Silence to Primary Definer: The Emergence of an Intelligence Lobby in the Public Sphere. In Critical Sociology, 45(3), 411-430.

Lidberg, J. & Muller, D. (2018). In the Name of Security – Secrecy, Surveillance and Journalism. London: Anthem Press.

Lipscomb, M. (2012). Abductive reasoning and qualitative research. Nursing Philosophy, 13(4), 244-256.

Lowenthal, M. M. (2017). My take on teaching intelligence: Why, what, and how. Intelligence and National Security, 32(7), 1-9.

Lucas, G. R. (2014). NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden. Ethics & International Affairs, 28(1), 29-38.

MacDonald, M. N., & Hunter, D. (2019). The discourse of security: Language, Illiberalism and Governmentality. Cham, Switzerland: Palgrave Macmillan.

Macdonell, D. (1986). Theories of Discourse. Oxford: Blackwell.

Machin, D., & Mayr, A. (2012). How to do critical discourse analysis: A multimodal approach. Los Angeles: Sage.

Macnish, K. (2016). Government Surveillance and Why Defining Privacy matters in a post-Snowden World. Journal of Applied Philosophy, 35(2), 417-432.

Masco, J. (2010). "Sensitive but Unclassified": Secrecy and the Counterterrorist State. In Public Culture, 22(3), 433-463.

Mccarthy, M. T. (2002). USA Patriot Act. In Harvard Journal on Legislation, 39(2), 435-453.

Miller, S. (1990). Foucault on Discourse and Power. In Theoria: A Journal of Social and Political Theory, 76(1), 115-125.

PEN American Centre (2015). Secret Sources, Whistleblowers, National Security, and Free Expression, Retrieved from https://pen.org/sites/default/files/Secret%20Sources%20report.pdf.

Peirce, C. S. (1998). Deduction, induction and hypothesis. In N. Houser & C. Kloesel (Eds.), The Essential Peirce: Selected Philosophical Writings – Volume 1 (1867–1893). Bloomington: Indiana University Press.

Richelson, J. (2012). The US Intelligence Community, Boulder: Westview Press.

Rovner, J. (2011). Fixing the Facts: National Security and the Politics of Intelligence. Ithaca: Cornell University Press.

Roe, P. (2012). Is securitization a 'negative' concept? Revisiting the normative debate over normal versus extraordinary politics. Security Dialogue, 43(3), 249-266.

Schmitt, C. (1922). Politische Theologie. Vier Kapitel zur Lehre von der Souveränität. Berlin: Duncker & Humblot.

Schneiker, A. (2007). Mercenaries into Businessmen: The Marketing Strategies of Private Military Firms. In Internationale Politik und Gesellschaft, 4(1), 74-89.

Schudson, M. (2004). Notes on Scandal and the Watergate Legacy. In American Behavioral Scientist, 47(9), 1231-1238.

Snowden, E. (2019). Edward Snowden Explains Why the CIA just made an Instagram. Interview by Ben Makuch. Vice. https://www.vice.com/en_us/article/xwnznk/edward-snowden-explains-why-the-cia-just-made-an-instagram.

Sorkin, A. D. (2014). The N.s.a.'s Spying on Muslim-americans. The New Yorker. https://www.newyorker.com/news/amy-davidson/the-n-s-a-s-spying-on-muslim-americans.

Stoycheff, E. (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. Journalism & Mass Communication Quarterly, 93(2), 296-311.

Spivak, G. (1996). The Spivak Reader. New York; London: Routledge.

Thompson, J. A. (2010). Wilsonianism: The Dynamics of a Conflicted Concept. In International Affairs 86(1), 27-47.

Thompson, J. B. (1995). The Media and Modernity—A Social Theory of the Media. Cambridge: Polity Press.

Tidd, J. M. (2008). From Revolution to Reform: A Brief History of U.S. Intelligence. In SAIS Review of International Affairs, 28(1), 5-24.

Walters, W. (2015). Secrecy, publicity and the milieu of security. Dialogues in Human Geography, 5(3), 287-290.

Weber, M. (1958). The Three Types of Legitimate Rule. In Berkely Publications in Society and Institutions. 4(1), 1-11.

Weldes J., Laffey, M, Gusterson, H. & Duvall R. (1999). Cultures of Insecurity: States, Communities, and the Production of Danger. Minneapolis: University of Minnesota Press.

Williams, M. C. (2003). Words, Images, Enemies: Securitization and International Politics. International Studies Quarterly, 47(4), 511-531.

Zeghart, A. (2019). Michael Morell Spies, Lies and Algorithms. Foreign Affairs. Retrieved from https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms