How can intelligence be used for benign purposes, in order to solve current global governance issues?

Date of Submission: 24/7/2023

University of Glasgow ID: 2712429

Dublin City University ID: 21109087

Charles University ID: 14070740

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 24,147 : Pathway A

Supervisor: Marcin Kaczmarski

Table of Contents

Abstract

Intelligence, by its very nature, is an elusive concept (Lundborg,2021,p443; Cornish,2021,p224; Deeks,2016,p599; Tucker, 2014,p10). As a result of its seemingly intangible characteristics, its positive application has gone under-recognised, and its creative application, largely neglected (Stone, 2012; Breakspear, 2012, p. 678). A significant focus on its function through espionage has left the public, and actors alike, hesitant to invest or study further, into its innovation (Glassman, 2012, p. 673; Potter, 1996; Richards, 2010, p. 4). The state-centric focus of literature and observations relating to the intelligence sector, means that its private-sector function is largely neglected, even though it is a fast emerging, and powerful sector (Gill,2013, p93; Lin, 2011, p10;Puyvelde,2019,p21;Adriana,2021, p8). Taken in the context of global governance issues, outlined by the UN Sustainable Development goals, we will see how far that private sector intelligence has come already outside of the remit of the state, and its transformative capacity (UNCD, 2014, p. 4). With any fast-expanding sector, comes its own issues. Lack of regulation of the industry, has contributed to the absence of a universal accountability mechanism, which this dissertation will look to create through an originally developed ethical framework (Yu, 2018; Omand, 2012, p. 38; Rittenburg, 2006, p. 235; Rosenbach, 2009; Crane, 2011, p. 233). 5 private sector companies will be assessed through the ethical framework, displaying the ultimately benign capabilities of the sector. This will show that private sector intelligence helps to balance the asymmetry of the world stage, acting as a key part of global governance itself, and taking on a self-regulatory capacity (UNCD, 2014, p. 4).

Chapter 1

Introduction

The concept of intelligence leaves us with more questions, than answers (Stone, 2012; Breakspear, 2012, p. 678; Colibasanu, 2009, p. 2). Why is intelligence so often associated with malignant practices (Stone, 2012; Breakspear, 2012, p. 678)? Can it be applied to global governance issues in a way that doesn't exclusively function through espionage (Glassman, 2012, p. 673)? Why has its potential not been explored in depth conceptually, much like many other political concepts (Hough, 2011, p. 24)? Why has the potential of private sector intelligence not been explored in-depth in the literature (Hough, 2011, p. 24; Freeman, 2021, p. 4)? Can ethics be applied to such a fast-growing and autonomous sector (Gill,2013, p93; Lin, 2011, p10;Puyvelde,2019,p21;Adriana,2021,p8)? Leading us to the ultimate objective of this dissertation, not only to find some, but to apply them to real life case studies, and provide real world analysis. These will form the basis of our research questions, throughout the piece.

Therefore, by the question *How can intelligence be used for benign purposes, in order to solve global governance issues?* We ultimately mean *How can intelligence be applied ethically and creatively to a context other than espionage, independently from the state, whilst transforming its pervasive and malignant image, and addressing current global issues (Stone, 2012; Breakspear, 2012, p. 678)?*

This introduction sets out to clearly outline the aims, objectives, and relevance of the dissertation, and clarify the research question. The question will then be fully answered in proceeding sections by doing an in-depth review of the literature on both ethics and intelligence to gauge the gaps in the current empirical and theoretical landscape in the intelligence sector. The dissertation then moves on to apply this to five intelligence companies, interviewed through interview methodology, and then applied to grounded theory in order to analysis and theorize research gathered (Holton, 2008, p. 5; BRM, 2006). By definition, Grounded theory is a research process that results in patterns and theories being identified directly from research gathered (Holton, 2008, p. 5). Interview methodology, is the process of interviewing individuals, to gather empirical research (BRM, 2006).

The aims and objectives of this dissertation are to recognise and identify the specific ways that private sector intelligence and their business models lend themselves to positively impacting world issues, so that we can identify the sectors transformative capacity, in the context of global governance issues. This goes hand in hand with its aim to develop an original ethical framework, to measure the positive impact of these businesses, and create a unique accountability mechanism for the intelligence sector, both academic and in the private and public intelligence sphere. This contributes to the pieces objective, to address both the theoretical and empirical facets of the question, and to bring analysis outside of its restrictive and state-centric focus (Gill,2013, p93; Lin, 2011, p10;Puyvelde,2019,p21).

This dissertation will go on to find that intelligence can in fact be used for benign purposes, in order to solve global governance issues, as private sector intelligence provides a key function as a significant point of balance on the world stage, arguably balancing the asymmetry of access to intelligence, as well as moving the sector far outside of the constrictive remit of espionage (Sims, 2006, p. 21; Koniauko, 2023, p. 102). We will find that private sector intelligence now acts as a key point of global governance in itself, and that its very function has become an expression of self-regulation (Deibert, 2022, p. 240; Arnham, 2001, p. 151). This will be found to have natural limitations, as the unentrenched and largely unaccountable ethical framework that is currently in place is shown to be flawed, with the ethical framework developed by this dissertation still necessitating an enforcement mechanism, for it to be fully palpable (Omand,2012,p27;Defao,2007).

The fundamental underlying argumentation of this dissertation, is that as a result of the intelligence sectors outdated image, and negligence in intellectual and empirical analysis, its transformative capacity has gone under recognized and untapped (Hough, 2011, p. 24; Freeman, 2021, p. 4). It's capability to develop other positive functions is therefore obstructed, as theoretical and empirical barriers lie in its way, which this dissertation seeks to ultimately remove, by identifying intelligences positive application in the private sector, and transformative capacity (Betts, 1978, p. 62; Helfont, 2023; Lundborg, 2022, p. 23).

Before we fully begin, we will outline term definitions. By intelligence, we mean "*Information Gathering"* or "*Information, and knowledge about an adversary, obtained through observation, investigation, analysis or understanding."* (Pythian P. G., 2018, p. 62; Warner, 2002, p. 1). These two definitions are both mutually exclusive, and symbiotic, making up for what the other lacks. If we limit intelligence to "*information gathering*", then we neglect the contextual application of information, and if we confine ourselves to Warner's definition, we neglect its use for non-adversarial purposes (Warner M. , 2002, p. 21; Pythian M. , 2013, p. 62). Using the two definitions interchangeably will provide a balanced way of representing these two facets. How intelligence can be used for benign purposes will be assessed and defined through the five companies performance against the ethical framework, which will assess positive applications of intelligence in the context of the intelligence cycle (CIA, 2023). The intelligence cycle, being the process in which information is gathered (CIA, 2023). By benign, we then effectively mean how they make a positive impact, through their application in the intelligence cycle (CIA, 2023).

We also need to clarify what we mean by global governance issues. This dissertation has chosen global governance issues in the context of development, as it complements the aims and objectives of this dissertation: To discover how intelligence can be transformative, in a positive, creative and ethical way. The aims of development goes hand in hand with this, as its core objectives look to improve the infrastructure of the world stage, as well as improve the lives of the individual (UN, 2015). In prioritising brevity, this dissertation has chosen the top three global governance issues to cross analyse with the case studies, and ethical framework.

The UN committee for development has cited these three, as significant areas for concern. "*The current global governance system is not properly equipped to manage the growing integration and interdependence amongst countries*" (UNCD, 2014, p. 4). Which can be summarised as issues arising from interdependence (UNCD, 2014, p. 4). "*The current system is currently marked with asymmetries in terms of access, process and outcomes*" (UNCD, 2014, p. 4). This pertains to the asymmetries of the world stage, which impact the functioning of governance worldwide, as a particular group of world players, effectively hold the majority of the worlds power (Zhu, 2005; Smith, 1996, p. 50). "*Global rules have led to a shrinking of the policy space of national governments, particularly of developing countries in ways that impede the reduction of inequalities within countries and is well beyond what is necessary for an efficient management of interdependence*" (UNCD, 2014, p. 4). This can be said to represent inequalities that have arisen from the decreasing role of the state, and the inevitable emergence of the private sector, as a key part of newfound global governance mechanisms (Frunza, 2021, p. 45; Jackson, 2004, p. 25). These will form the underbelly of our analysis, representing the key markers for global governance transformation.

The relevance of this dissertation can be defined in four stringent ways. Primarily, the malignant image of intelligence has not only restricted its creative application, but de legitimised its operating capacity (Betts, 1978, p. 62; Helfont, 2023; Lundborg, 2022, p. 23). Changing this image and bringing more legitimacy to its actions through ethical accountability, therefore becomes essential to intelligences transformation. Exploring intelligence creatively, becomes exceptionally difficult, when its very function is viewed with suspicion. "*To spy, or not to spy*" is a question that that the public have increasingly been asking themselves, as intelligences malignant image has become more and more pervasive (Hutton, 2009, p. 20). We need only look to the mainstream media in the UK to observe the outrage over MI5's knowledge of the terrorists that were deeply entwined in the Manchester Attacks, and ultimately how preventable this could have been (Hardy, 2023).

On the same topic, the ethical bounds of intelligence are consistently overrun by the very nature of the industry, as the actor who holds the most valuable intelligence, inevitably holds the most power: thus encouraging the circumvention of rules in order to obtain it (Sepper, 2010, p. 3). The Salisbury spy poisoning provides a stark example of this, the brutality of the sector, and its fluctuating moral compass (Gregory, 2022). This is just one of a whole plethora of examples of civilian casualties that have become more and more normalised, hence the term *"collateral damage,"* and desensitisation towards unconventional methods to obtain information (Gregory, 2022). Practices such as this have earned this malignant image, although this can largely be attributed to covert action, which is only one facet of intelligence (Potter, 1996). This is not intelligences only function, yet is the only one that immediately comes to mind. This dissertation will look to address this negative image, by methodically analysing both literature, and real-life case studies of private sector intelligence, outside of the remit of state intelligence, and spying, in order to see its current role, and future capacity in benign activity.

Moving onto our second reasoning for this dissertation, we see that intelligences harsh judgement on the world stage has led to a lack of recognition for its achievements, inevitably inhibiting its future ability to be applied to global issues (Chesterman, 2008, p. 1055; Blicharz, 2003, p. 5). Intelligence failure is the facet of intelligence that is most known, meaning that public support and further investment in mechanisms outside of espionage are unlikely to be suggested in the first place, as positive alternative functions can hardly even be imagined (Betts, 1978, p. 62; Helfont, 2023; Lundborg, 2022, p. 23). This ability to never shy away from controversy, makes it both a point of contention, and ripe for redemption (Wagner, 2003, p. 4). The littering of intelligence failure in the public narrative proves this further, as intelligence success is often kept under wraps, due to its sensitive nature (Betts, 1978, p. 62; Helfont, 2023; Lundborg, 2022, p. 23).

With one of the most recent, and devastating intelligence failures being the August 2021 Taliban takeover of Afghanistan, we can see the agency intelligence holds, as well as this inherent vulnerability to failure (Chesterman, 2008, p. 1055; Blicharz, 2003, p. 5; CFR, 2023). We see this particularly through US forces lack of access to appropriate intelligence, which played a key part in the resulting establishment of the Taliban government (CFR, 2023). However, this focus on failure neglects the scope of the private intelligence sector, and its capacity to outgrow and even outperform state sector functions (Frunza, 2021). We look to address this by exploring its positive impact.

Onto our third logic for the dissertation, we can see that intelligence is grossly limited by its tendency to overstep legality, overriding its lesser known functions that may have positive effects (Joffe, 1999, p. 325; Williams, 2010, p. 19). This places the dissertation within a vital paradigm, intelligence's capacity for 'good', and the malignant impact that naturally emerges through its core function of "*information gathering*"' (Pythian M. , 2013, p. 1). Overstepping of legality and privacy is one example of negative practice taking the limelight, having become an accepted behavioural practice of information gathering (WP, 2013; Freeze, 2014; ECHR, 2022, p. 20). We see this with China, particularly when they were accused of intelligence gathering through corporate entities, leading to the US and even the UK banning business with Chinese tech companies in their supply chains (Pythian P. G., 2018, p. 62; Evans, 2018). This was a result of Chinese spyware microchips, discovered in pentagon computers, and in numerous domestic products (Pythian P. G., 2018, p. 62; Evans, 2018). With such a powerful impact even in a negative way, we can only assume how valuable these intelligence mechanisms can be, when harnessed for good.

Finally, the focus in the literature on the process of intelligence rather than the construct, leaves the creative and ethical use of intelligence, under researched (Bartes,2013,p3; Johnson, 2008,p10). Intelligence tends to refer to "*information gathering"*, representing the process of intelligence rather than the construct of it (Pythian P. G., 2018, p. 62). If we look to the origins and study of intelligence itself we see a conflict between intelligence as an "*art*", and as a "*science*", showing how important the ying and yang of "*construct*" and "*process*" are in counter-balancing one another (Richards, 2010, p. 1). By focusing excessively on "*process*", the literature fails to observe the potential intelligence has to apply itself to areas outside the boundaries of its current processes (Richards, 2010, p. 1). In addition, the "*intelligence cycle*" acts as a central point, and sometimes the only point of analysis (CIA, 2023). The intelligence cycle is effectively a process based analysis that could be more creatively applied, and with which we will base the ethical framework on (Pythian P. G., 2018, p. 62; Bose, 2008, p. 26; Pellissier, 2013, p. 68). We can so easily apply models of intelligence to more pressing issues than espionage, it simply hasn't been given sufficient study, development or recognition.

This leaves the relevance of this dissertation as hard to question, as the sector's last recognised revolution was in response to 9/11, which was limited to the physical amalgamation of intelligence agencies across the US government (Prosner, 2005, p. 10). Rare is it to see literature that hints or explores an intellectual revolution in thinking around the intelligence sector (Wark, 2008, p. 102; Moore, 2009, p. 49; Mconnell, 2007, p. 49). Although this piece will not claim to precipitate an intellectual revolution, it will seek to intellectually, and empirically, reveal a new mode of thinking surrounding the sector.

With the intention of contextually applying this reasoning, we can see the sector empirically revolutionising through private sector intelligence companies with limited recognition, as a result of its lack of affiliation with the state (Singer, 2007, p. 10; Landau, 2005, p. 55; NYT, 2021). For example, in the book "*Corporate warriors: the rise of the privatised military industry*", by Peter Singer, he explores the private sectors intelligence and militarised placement of agents in war zones, and how significant their impact has been in wars such as Afghanistan and Iraq (Singer, 2007, p. 2). This has been dubbed as "*corporate shadow wars*", evading the public, and showing a demonstrable shift in the sector (Mcfate, 2015). This is just one example of a whole host of private sector activity, that goes under the radar (Pegg, 2023; Eventon, 2016, p. 2; Bartlett, 2015, p. 101). On the other hand, limited attention has also been given to innovations that have worked to make a clunky sector, much more efficient and well placed in the modern era, such as the use of private sector satellites, to monitor on the ground conflict by SpaceX corporation in Ukraine (Wirtz, 2018, p. 215; Mikhaylov, 2018; Janyanti, 2023). The sector is also revolutionising through a trend of disclosure, where states are bringing state secrets more and more into the public sphere, since the war in Ukraine (Zegart, 2022). This shows that the intelligence sector is at a pivotal turning point in both empirical senses, with disclosure finally placing it at a crucial point of accountability (Zegart, 2022). This is through its own willingness to bear itself to the public in acts of transparency, leaving it at a perfect intersection for this dissertations research (Zegart, 2022).

This is not to say that the private sector has produced only positive outcomes. The development of Pegasus spyware, a malware that has the ability to take over complete control of hosts phones, has caused a disastrous ripple effect in the industry (Kirkgaessner, 2020; Ingleton, 2022; Manors, 2022). David Leonhardt, reporting for the New York times, has framed this as a way of right-wing governments "*knitting together*" capabilities, with governments such as Hungary, Poland and India investing in its use, and cross collaborating on the project together (Leonhardt, 2022).

This shows intelligences capability to not only revolutionise cyber-warfare, but the global political landscape, itself. Even Amazon founder Jeff Bezos, has emerged as a prominent Pegasus casualty, and arguably, of private sector primacy (Kirkgaessner, 2020; Ingleton, 2022; Manors, 2022). After being sent a scam link, suspected to be from a private sector company in Saudi Arabia, information concerning an ongoing affair was leaked to the media (Kirkgaessner, 2020). The private sector company was assumed to be acting alongside the Saudi Arabian state, in retribution for Bezos pulling out of a lucrative deal, that would have cost the state billions of dollars in losses (Kirkgaessner, 2020). This makes the relevancy of this dissertations exploration of the private sector even more relevant, as we can see even simple issues like spyware, are dangerously underrated. Dr. Liapoulos sees this as a new technological paradigm, emerging in the intelligence sector. "*New capabilities in technology in the intelligence sector, have contributed to the decentralisation, tailored systems and networking capacity*" that effectively challenges the old and hierarchical functions within the old intelligence cycle (Liaropoulos, 2006, p. 7). We will recognise this shift, but keep the intelligence cycle as a key part of our ethical framework, because of its symbolism as a well-known, and universal point of recognition (Pythian M. , 2013, p. 2).

This primacy of the private sector has been dubbed the "*commercialisation of intelligence*", where an essential function of state has transformed into a means for profit (Crane, 2011, p. 233). Its lack of regulation has emerged as a prevalent issue, in lieu of this (Crane, 2011, p. 233). With such sensitive information in the hands of corporations, it does beg the question whether intelligence should be privatised at all (Rathnell, 2007, p. 211; Mills, 1999, p. 10). In response, this dissertation will argue that private sector intelligence is in fact, increasingly relevant, as state functions operate in a state of overwhelm, making outsourcing a necessary solution (Krishnan, 2011, p. 196). Already, the CIA operates with 60% outsourced intelligence meaning that it is a reality, that we already must embrace (Krishnan, 2011, p. 196). This places the dissertations development of an ethical framework as all the more relevant, as private sector intelligence is in need of an accountability mechanism, in order to counter-balance this (Rosenbach, 2009). This also demonstrates the need for shifting intelligences malignant image, because of this negative response to its commercialisation, as the reality is that this is where the sector is heading (Crane, 2011, p. 233). The ethical framework becomes more and more essential, as this migration to private sector intelligence means intelligence increasingly operates within its own security sphere, with the public already seeing it as a lawless and morally ambiguous entity (Leigh, 2015, p. 255).

In summary, the dissertation aims to shift the thinking surrounding intelligence in order to explore its benign application, in opposition to its persistent malignant image, and widen the current scope of intellectual analysis outside of its state centric remit, through recognition of the private sector (Stone, 2012; Breakspear, 2012, p. 678). It will look to apply these business models and case studies to global governance issues, to see how private sector intelligence can transform the global political scene for good. Good will be measured by the universal ethical framework, that has been developed as a benchmark and universal accountability mechanism for the intelligence sector.

This will show that intelligence can indeed, and currently does, a significant amount of transformative actions that are vital in the transformation of world issues, there just has not been enough credit or research dedicated to it (Rathnell, 2007, p. 2; Krishnan, 2011, p. 196). This dissertation hopes to be a part of the impetus required to explore the application of intelligence, more creatively. Rather than its focus on process as mentioned before, seeing how we can apply it outside of its traditional functions within espionage (Richards, 2010, p. 1). Hence, we have provided a distinct and clear outline of the project, contextualising and grounding it within emerging trends, and defending its relevance, whilst also clarifying the research question itself. Term definitions, and a clear statement of aims and objectives, have been identified. This introductory section has sought to introduce the complexity of the subject that follows, and pre-empt any pressing questions that may arise from the first glance.

Chapter 2

Literature Review-General Works on Intelligence

This literature review will show that state-centrism, and perceived malignancy, in the intelligence sector are patterns that consistently emerge in the literature (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25). This will show the interaction between the two, to be strong in their ability to act as a latent self-protection mechanism of state, but weak in their encouragement of a self-perpetuating cycle that places limitations on positive and innovative growth in public and private sector intelligence (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25). This can also be seen through the sectors inadvertent politicisation and glamourisation (FPI, 2023; Wesley, 2010, p. 20; Coletti, 2017, p. 65; Agrell, 2021, p. 25).

As a result, the gaps in the literature can be said to be the lack of positive application of intelligence, exclusion of the private sector from analysis, exploration outside of the remit of espionage, as well as a lack of recognition of non-democracies in analysis (Vitkauskas, 1999, p. 6; IA, 2023). This will inherently tackle the first and last research question *why is intelligence so often associated with malignant practices* (Stone, 2012; Breakspear, 2012, p. 678)? As well as *why has the potential of private sector intelligence not been explored in-depth in the literature,* although this will also be addressed by the case study section, which shows private sector application, in practice *(Hough, 2011, p. 24; Freeman, 2021, p. 4)*?

The literature overwhelmingly places the state at the centre of its analysis (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25). The debate that has emerged as a bi-product of this "*neorealist*" placement of the state as the core actor, has encouraged prominent authors to begin to recognise the rise in powerful and private sector intelligence activity, and naturally challenge this (Morton, 2023; USDJ, 2003, p. 5; Horowitz, 2018, p. 372). Even within this emerging debate, there is a lack of exploration of the empirical reality of the rise of the private sector (Morton, 2023; USDJ, 2003, p. 5; Horowitz, 2018, p. 372). We need only look to the example of BAE systems, a private intelligence and security firm, to see the extent to which private sector intelligence firms, now play a crucial part in the global political landscape (BAE, 2023). The ministry of defence, UK has recently awarded a contract to BAE in order to "*boost technologies for the UK's future combat aircrafts*" (BAE, 2023). This is only one of a whole array of contracts, just in the past few weeks, that represent a significant outsourcing of key government functions (BAE, 2023). Yet a whole host of policy reports, media outlets and published academia, still focuses on the state as the ultimate facilitator of intelligence (News, 2023; Dearden, 2018; Davies, 2002, p. 62; Lahenaman, 2010, p. 201; Caparini, 2007, p. 1).

This dichotomy between theory and reality in the intelligence sector, aptly reflected by Sturgis, is emphasised by him to be symbolic of a latent revolving door between government, and private security firms, that has worked to create a private sector intelligence shadow governance mechanism (Sturgis, 2013). This is strong in demonstrating that the public falsely believes that there is a strong separation between state and private sector, but weak in conveying the reality that they both equally provide powerful, and transient functions. Subsequently, further literature supports this antiquated and state-centric view of the sector (Davies P. , 2002, p. 66; Andrew, 2010, p. 164). As Andrew identifies, there has been a "*under-theorization*" of the sector, placing it in a time-freeze within the cold war time period, where the state was the focal point of analysis (Andrew, 2010, p. 164).

Curtis refreshes the debate, by rethinking the traditional function of state, and reframing government as a "*process*" with multiple entities, rather than a singular omnipotent institution, which provides strong theorization for what intelligence really looks like (Curtis, 1995, p. 575). This can be argued to see the state protecting itself, through keeping some of its functions under wraps (Curtis, 1995, p. 575). If we combine this with "*self-affirmation theory*", we can further theorize the way the state is behaving in self-protection, as it seeks: *"to protect an image of its self-integrity, of its moral and adaptive adequacy. When this image of self-integrity is threatened, they respond in such a way as to restore self-worth*" (Sherman, 2006, p. 183).

Literature that looks outside of the state as the focal point of analysis, gives a strong case for government as both a process with multiple actors, and a self-affirming entity, bridging a gap in the literature that focuses on the state as the ultimate driver of intelligence (Curtis, 1995, p. 575; Sherman, 2006, p. 183; Caparini, 2007, p. 1). By covering up its interweb of functions, this can be said to both protect and limit the state innovating, and from recognition and investment in its benign activity. Equally, however refreshing particular authors are at shifting the debate, a big gap in the literature lies in the state remaining at the centre of analysis (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25) .

Puyvelde identifies the trend of private sector spies for hire, with the motto "*we can't spy if we can't buy*" at the forefront of his analysis (Puyvelde,2019,p218; Chesterman,2008,p1055). As a saying commonly used by politicians, this has been identified as a key indicator for the growth and significance of the private sector, who now act as a central part of state intelligence functions in a mutually beneficial financial partnership (Puyvelde, 2019, p218;Chesterman,2008,p1055). This is a strong observation by Puyvelde, as he identifies this "*commercialisation of intelligence*" (Crane, 2011, p. 233). However, this lacks a more in-depth analysis of this new dynamic between public and private sector, where the public is not fully aware of how the two work together (Puyvelde, 2019,218).

Rather than seeing this as a strategic coveting of the private sector, and a malignant act by state in order to keep functions secret, we can see through alternative literature that this could potentially instead be likened to an emerging self-protectionism mechanism, in the overzealous pursuit of state secrecy (Bellaby, 2019, p. 21). This brings us back to the enduring debate that Hobbes began "*over sovereignty's right to shape citizens' minds"* (Warner, 2022, p. 888). Pointing to a need for accountability to the public, and a gap in the literature where private sector intelligence is so under recognised, that it is commonly seen for its commercial facets, neglecting its transformative capacity (Crane, 2011, p. 233). If we take the NSA surveillance scandal, for example (Sturgis, 2013). Information was collected on US citizens that infringed extensively on the right to privacy (Sturgis, 2013). It emerged that this was being carried out by private sector intelligence firms Booz Allen, Mclean and Va (Sturgis, 2013). Few people had the knowledge that these firms even had the power to carry out these intelligence functions (Sturgis, 2013). The public quite often only come to know of intelligence activity, when it has reached this malignant stage.

State centrism and perceived malignancy can be seen consistently in the literature, interacting through private intelligences dual function as both a "*problem and solution"* for the state (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25). This means that going by the narrative in the literature, the private sectors role can be manipulated to suit the role of the state, but can also challenge, and undermine its activity (Puyvelde,2019,p219). This shows strength in the literatures ability to recognise the malleability of the rise of private sector intelligence, but also that it lacks an understanding of grey areas that have emerged, in parallel to its rise. Adriana partially fills in in this gap empirically, by bringing attention to the *"murky rise of 'risk' practitioners"*, who's role can be defined through their work as intelligence forecasters (Adriana, 2021, p. 12). This demonstrates the grey area that the private sector sits in, in parallel to the state (Adriana, 2021, p. 12).

As Adriana further divulges, the "*professionalization*" of intelligence agents in the public sector, only began recently (Adriana, 2021, p. 13). "*There is little known, about private sector analysts*" (Adriana, 2021, p. 12). Hence, we see limited attention given to the need for professionalization of the sector in the literature, as well as a clear definition of the private sectors role, limits, boundaries and analysis (Adriana, 2021, p. 12). What is particularly missing, is a recognition of how advantageously ambiguous this nature can be, as the state is able to outsource negative intelligence functions to the private sector (Puyvelde,2019,p219). Artificial intelligence development is one of those functions (Chandra, 2021). Chandra fills in the gap that Adriana and Puyvelde left, by signifying this collaborative and chaotic relationship between government and the private sector, specifically bringing our attention to this in the context of contentious AI development (Chandra, 2021).

An example of this can be seen through the association of "*killer drones*" with the Department for Defenses' development of AI technology in America, which has led to many tech employees refusing to work on these projects through ethical grounds, which matches the publics natural hesitation about AI (Chandra, 2021). The outsourcing of this function to the private sector therefore fulfils the governments needs for developing AI, without public accountability. (Chandra, 2021). This points to private sector intelligence companies representing a malleable and interchangeable mechanism that can serve in or against the interests of the state, whilst also hiding in plain sight (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25). The extent to which this could impact society, is however neglected from the literature, as accountability for AI development is separated from the state, and yet is indirectly developed by them (OECD, 2019, p. 1). The strength in this, is the literatures presentation of this as a *government process* that serves to protect the *moral integrity* of the government, although its weakness lie in the ability of this to infringe on legitimacy even more, if the public knew the full extent of private sector outsourcing, by the public sector (Sherman, 2006, p. 183; Curtis, 1995, p. 575).

Literature from the state itself creates its own limitations, through putting barriers in the way of its evolution into other areas of policy (Nicander, 2011, p. 534; Steele, 2023; Mason, 2023). "*In the strategic context, intelligence has little to contribute to foreign affairs, defense, trade and policy strategy* (Steele, 2023)." By excluding itself from entire sectors that are ripe for transformation, we see the limits on innovation it places on itself even in publications like this, which are purposefully striving to promote its innovative qualities (Steele, 2023). Nicander sees this as "*reactive adaptability*", where the intelligence community only innovates when necessary, or in response to a major event (Nicander, 2011, p. 531). This corroborates with Steeles outline of the restrictive political infrastructure that the intelligence community operates from, even from a literary perspective (Nicander, 2011, p. 531; Steele, 2023). This sees the state innovating as a reactive reflex, rather than coming from its own strategic impetus, which can be only presumed to garner critical malignancy, as a result of a lack of foresight in innovation (Nicander, 2011, p. 531; Steele, 2023). We can see the state self-affirming its innovative processes, by approaching it cautiously, in aid of protecting its own vulnerability (Sherman, 2006, p. 183).

In addition, there is significant focus in the literature on western and democratic intelligence as the benchmark for innovation (Richterova, 2020, p. 3; West, 2019, p. 10; Bennett, 2012, p. 24). Simply because a state is undemocratic, does not mean innovation cannot stem from it. Although perhaps, not the most desirable benchmark, there are aspects we can learn from China's intelligence model. "*The historical thrust of Chinese intelligence"* demonstrates rapid innovation over a long period of time, and is an expression of the exponential speed in which they are developing technological intelligence capabilities (Davies,2013,p23). However, the literature also points to China being a prime example of state-centric intelligence, with publications such as "*The Tao of spycraft*", demonstrating that they effectively integrate state intelligence into all areas of political life (Arpin, 2007, p. 2).

We need only look to their domestic intelligence capabilities, to even begin to fathom what they are capable of in foreign missions (Davies,2013,p14). The technology that they have developed, now means that they are able to monitor the emotions of citizens in a variety of its cities, meaning that it can now pre-empt crimes before they have even taken place (Hannas, 2021, p. 11). We can definitively learn from these rapid technological capabilities, although we must also be aware that this also lends itself to automated prejudice and racism, as the algorithms teaches itself to be more alert for repeat criminals: with particular minorities being these repeat offenders (Hannas, 2021, p. 11). The literature therefore stringently points to self-protectionism, through Chinese moves to develop intelligence based population control (Davies,2013,p23; Hanna,2021,p.11;Arpin,2007,p.2).

Intelligences glamourized image is a powerful tool within the literature, that feeds into malignancy and self-protection of the state (Mackrakis, 2023, p. 10; IEEE, 2023; Marie, 2001, p. 2). It naturally restricts the creative application of intelligence, and can be argued to be forcing an unattainable narrative on it (Mackrakis, 2023, p. 10; IEEE, 2023; Marie, 2001, p. 2).

This can be attributed to the cold war time period, when intelligence first boomed, and there was a pressing need for recruitment in the sector due to the existential threat of nuclear weaponry (Britannica, 2023; IEEE, 2023). We need only look to James Bond, to see an exceptionally flowery version of the bureaucratic and sometimes immoral work that necessitates being an intelligence analyst or agent (Britannica, 2023). This is not excluded from the influence of novels, as the author Le Carre reflects the moral ambiguity of the sector, with his main characters overstepping ethical and moral bounds (Carre, 2011, p. 5).

However, this literature lacks nuance. What Mackras, IEEE and Marie all evade, is that it's glamourized image may inadvertently protect the state: as the reality of the sector is never fully known, meaning that it is effectively given an image by the media (Carre, 2011, p. 5; Britannica, 2023). Stevyn Gibson theorizes the intelligence work of the UK, which fits this narrative. Representing the UKs role in intelligence as both "*Global policeman*" and "*networker,*" we can see why it would be beneficial to perpetuate a glamourized image in the literature, when the reality involves fundamental interference in world affairs (Gibson, 2009, p. 100). Another facet that isn't as explored in the literature as it should be, is that a sector who's function by its very nature is not very well known, and who's image is largely constructed by the media and Hollywood lends itself to malignancy, as the empirical reality of intelligence failure, and immoral intentions clashes with the heroic and celebrated image of the industry (Lomas, 2021).

The *"politicisation of intelligence",* a trend consistently debated in the literature, demonstrates the limitations of the state-centric outlook on intelligence (FPI, 2023; Wesley, 2010, p. 20; Coletti, 2017, p. 65; Agrell, 2021, p. 25). As a result of the state's revolving door syndrome with intelligence branches, intelligence agencies struggle to operate fully autonomously, and without the overbearing presence of political incentive and pressure (FPI, 2023). Intelligence products, biasedly selected and encouraged by US and UK government officials, were incriminatingly used to justify the *"war on terror"* (Pillar, 2006, p. 1022). Information that was nothing if not subjective, was taken as an absolute, with Osama Bin Laden's stockpile of weaponry uncertified, yet put to the public as a definitive and devastating justification for the ultimate invasion of Iraq in 2002 (Pillar, 2006, p. 1023).

Yet nowhere in the literature does it mention politicisation as a tool of self-protection, with perceived malignancy making the government sometimes even circumvent the public due to fear of reappraisal, much like when Tony Blair evaded a house of commons vote and went to war with Iraq anyway (Elgot, 2016). This shows the pervasiveness of state-centrism in the literature, and how it feeds into its own malignancy through inadvertent self-protectionism (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25).

Intelligence can therefore be said to be so often associated with malignant practice, because of the neglect of other functions of intelligence outside of the state, limiting its image, as a result of politicisation (FPI, 2023). We can also say that private sector intelligence has been neglected by the literature, because of the benefits of its elusive nature, and the advantageous nature of politicisation (FPI, 2023). This has so often, only projected polarised views of the sector, with either glamourization or failure, littering the news, making it natural that this has resulted in its negative image (Mackrakis, 2023, p. 10; IEEE, 2023; Marie, 2001, p. 2; Vitkauskas, 1999, p. 3; Kendall, 2011, p. 25).

We have analysed this thematically through the empirical and theoretical reality of the public and private sector, a lack of non-western analysis and recognition of stagnant processes, as well as exploring this through innovations, AI, intelligence failure and politicisation (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25; Richterova, 2020, p. 3; West, 2019, p. 10; Bennett, 2012, p. 24; FPI, 2023; Wesley, 2010, p. 20; Coletti, 2017, p. 65; Agrell, 2021, p. 25). All which link back to the same premise: that the literature does not give enough attention to the private sector, and that the current block of literature feeds into a lack of recognition of benign activity, thus limiting future innovation (Vitkauskas, 1999, p. 3; Puyvelde, 2019, p. 2; Kendall, 2011, p. 25; Richterova, 2020, p. 3; West, 2019, p. 10; Bennett, 2012, p. 24; FPI, 2023; Wesley, 2010, p. 20; Coletti, 2017, p. 65; Agrell, 2021, p. 25).

Chapter 2.1

Ethics Literature

There is currently no palpable, and clearly defined ethical framework for intelligence practice, and academia alike (Frisk, 2020, p. 70). This may seem a tricky notion to adopt for the private sector, but that does mean that one should not operate as a core point of accountability. Just as the universal framework for human rights has guided and held many states and companies alike to account, this dissertation argues that an intelligence one is also capable of doing so (UNICEF, 2019; Martin, 2016, p. 16). Although claimed to be by many authors, the frameworks outlined are not keeping pace with the industry (Nolte, 2009, p. 2; Herman, 2010, p. 342; Geldron, 2007, p. 398). By industry, we mean both state and non-state intelligence organisations. However, the need for one is becoming more and more pressing, as intelligence moves outside of the confines of the state, and into unregulated territory (Yu, 2018; Omand, 2012, p. 38; Rittenburg, 2006, p. 235). It is this sections intention to assess the current literature, and semblances of ethical frameworks, as well as answering the research question, can ethics be applied to such a fast-growing and autonomous sector (Gill,2013, p93; Lin, 2011, p10;Puyvelde,2019,p21;Adriana,2021,p8)?. We will begin with a short review of the literature concerned with the specific framework, and then into an outline of the authors code of ethics. We will also be answering why intelligences potential has not been explored in depth conceptually, much like many other political concepts, as another fundamental research question (Hough, 2011, p. 24)?

Ethics can be fundamentally defined by: "*A social, religious, or civil code of behaviour considered correct, especially that of a particular group, profession or individual*." (Omand, 2018, p. 6). This shows the vague, and nascent ambiguity of the definition itself, as ethics is equalised with cultural and social practice, emerging from a specific industry or individual (UNESCO, 2023; Meyer, 2023). This means that it can be confined to a very specific lens, and has the potential to emerge from a restrictive, limiting, or biased source. The emergence of ethical practice, is strongly linked with precedence, meaning that it can be fragile and open to interpretation, reflecting the empirical reality of ethics in intelligence (Omand,2018,p6).

Angela Geldron explores the rough moral framework that currently guides the intelligence sector (Geldron, 2007, p. 398). Her assessment of the current state of ethics, is that it is based on moral precedence, failing to limit aggression, and allowing harmful practice in the process of obtaining information (Geldron, 2007, p. 400; Bailey, 2016, p. 49). A current example of this, being the bugging of the United Nations Security Council, in order to galvanise voting patterns (Geldron, 2007, p. 401). This becomes particularly harmful when these practices are favoured and funded by more powerful states, feeding into the asymmetry of the world stage (Geldron, 2007, p. 401; VoxEU, 2017; UN, 2015).

The very nature of covert intelligence gathering, and any other method of collection than OSINT, lends itself to moral dilemma, as its very nature encourages the challenging of ethics, in order to obtain information (Jackson, 2004, p. 10). *"There are great occasions in which some men are called to great services, in the doing of which they are excused from the common rule of morality."* -Oliver Cromwell (Perry, 1995). This reflects the excusing of unethical behaviour in the name of grand state missions, representing the semblance of an ethical framework that currently guides the intelligence community (Geldron, 2007, p. 400). The notion that the *"rule of law"* can be overridden by exceptional circumstance, makes the intelligence community able to operate within their own security sphere, with their normal mode of operation pertaining to exceptional circumstance (Spracher, 2016, p. 102; Chris, 2016, p. 49).

However, Geldrons' article roots itself in "*Kantian Idealism*", where actors are assumed to be rational and living in mutual respect "*with the general consensus that listening in to one another and stealing each other's secrets, is improper*" (Geldron, 2007, p. 400).Where naturally, they cannot live in mutual respect, if they are able to use harmful practices of obtaining information (Jackson, 2004, p. 10). This also demonstrates the exclusive association of ethics with the west, as Kantian moral values, are equated to Western liberal values, which may be deemed as an extension of the exportation of exclusively western values into yet another code of ethical practice (Myser, 2011, p. 20). Idealism is linked with Realism, to represent judgement of morality through actions and outcomes, realism being the proposed current reality of ethics (Geldron, 2007, p. 398). Geldron equally reflects the disequity between private and public ethics, with "*Raison d'etat*" justifying state action, or the *"ends justify the means,"* which acts as a fragile compass for the sector (Geldron, 2007, p. 400). The moral dilemma she emphasises, at least for democracies, is how to balance the need for security and human rights, without squashing the other (Geldron, 2007, p. 398). S Miller sees that these principles do not actually transfer well to national security, as there is a lack of analysis of the intelligence cycle, and the ethical implications at each stage of it (Miller, 2021, p. 211). This neglect of the intelligence cycle, demonstrates a pertinent gap in the current code of ethics.

Geldrons' observations can therefore be summarised by The *"Just War Doctrine,"* which is ultimately seen as a rule of thumb for the intelligence community, representative of the current moral framework, where states do not go to war or commit harmful intelligence acts, without a *"Just cause"* (Geldron, 2007, p. 398). Bellaby sees the evolution of *"Just war principles",* as both inaccurate and unhelpful, if done in an exacting way (Bellaby R. , 2022, p. 101). He however agrees with the fundamental underlying, and ethical premise, agreeing that they work as a sound moral guide, if taken in the context of intelligence practice, and with flexible application (Bellaby R. , 2022, p. 101). Yet even this can easily be circumvented. If we look to the saying "*one man's terrorist is another man's freedom fighter*," actors are able to neglect human rights in order to squash an enemy, simply by labelling them as an enemy of state (Beydoun, 2022, p. 101).

This can easily be applied to the *"Just war doctrine"*, as states can paint world events as more of a threat than they are, in order to achieve political objectives (Fisher, 2013; Geldron, 2007, p. 398). We need only look to North Korea, to see this in practice empirically, as propaganda videos are faked, in order to justify the regime, and military aggression towards the west (Fisher, 2013). Guantanamo Bay and the case of Shaamima Begum in the UK, also represent the conveniently ambiguous interpretation of human rights when it comes to states dealing with accused terrorists (HRW, 2023). Yet these are the precedents that the intelligence community is faced with.

To provide clarity, we will summarise Geldron's overview of the current ethical framework for intelligence, that currently exists. The *"Just War doctrine"* governs intelligence practice, meaning that the intelligence community is bound by moral precedence that expects actors to only act unethically if the situation requires it, and is exceptional (Geldron, 2007, p. 401; Carnegie, 2023). This is commonly implemented through government intelligence, meaning that it is assumed to be ethical, at least in *"liberal-democratic democracies"* (Phillips N. , 2016, p. 20). Legal, judicial and constitutional constraints emerge from individual nation-states, but are not subject directly to international accountability frameworks, unless there have been severe breaches (Geldron, 2007, p. 397).

These can also be politically driven, and in the interest of the government, as intelligence and governments, are naturally entwined (Geldron, 2007, p. 398). Intangible soft influences such as unpredictable global events, and interests of particular leaders have a significant impact on the ethical practice of the intelligence sector, that cannot be defined by a singular ethical framework (Geldron, 2007, p. 350; George, 2010; OECD, 2009). Intelligence is also synonymous with force, acting as an arm of state, meaning its ethical framework is also reflective of the states (Geldron, 2007, p. 398).

"Ends justify means", motivates intelligence gathering behaviour, meaning that intelligence gathering cannot be done without purpose (Geldron, 2007, p. 400). This can be attributed to the Machiavellian time period, with some even claiming that this is a way of *"lying and then justifying"* by officials (Mintz, 2018). An example given, is of the former director of the CIA, James Clapper, claiming that the CIA were not *"wittingly"* collecting data on millions of Americans in the senate, even though this is a primary function of the organisation (Mintz, 2018). These ethical standards can be summarised by the natural law of individual morality, which interacts with the last resort principle, probability of success, and regard for human consequences as well as discrimination, which all form ethical limits that liberal democracies place on themselves, before overstepping moral boundaries (Geldron, 2007, p. 378). In lieu of this, this still begs the question *"How much, can the Just War, justify?"* (Wells, 1969, p. 819).

The issues that emerge with this framework carry on from these concerns. There is no direct international accountability mechanism for intelligence, putting a variety of barriers in the way of enforcement (Bjorn-Muller-Wille, 2007, p. 100; Born, 2007, p. 24). The framework is completely open to interpretation, and the whims of leaders, governments, or politics (Goldman,2006, 221). Accountability and ethics have emerged with western characteristics, making its application more exclusive (Goldman, 2006, 222). There is also no universal ethical point of reference (Demarest, 1995, p. 321). This framework has also only been devised in the context of foreign espionage, with no reference to the private sector, as an important facet to intelligence (Voelz, 2009, p. 20; Matey G. , 2013, p. 15). Even more shockingly, human rights can be overridden in the event of exceptional circumstance, which can ultimately be an everyday occurrence (Geldron, 2007, p. 401). Overall, these are informal and unentrenched rules of operation which serve to guide the intelligence sector, and arguably avoids holding the intelligence sector fully to account.

Ross Bellaby's Ethical framework is also based on the *"Just war"* principles, although he develops the idea into a notion of "*Just intelligence*" (Bellaby R. , 2012, p. 93; Geldron, 2007, p. 378). He brings attention to one of the biggest ethical conflictions in the intelligence sector:

torture, and the impact of intelligence collection on the individual (Bellaby R. , 2012, p. 93; BU, 2023). He breaks his ethical framework into two distinct parts, harm to the individual and *"Just intelligence"* principles (Bellaby, 2012, p. 93). These are principles based on a set of criteria that comes from the *"Just war"* tradition: just cause, legitimate authority, right intention, last resort, proportionality and discrimination (Bellaby R. , 2012, p. 94; Geldron, 2007, p. 378).

Avoiding harm to the individual, involves recognising individual rights (Bellaby, 2012, p. 94). Joel Feinberg, calls these 'welfare needs' (Bellaby, 2012, p. 95). These can be described as the individuals mental and physical integrity, autonomy, liberty, sense of self and privacy (Bellaby, 2012, p. 93). The ethical response, he summises is "*Primum Non Nocere- First do no harm",* which ultimately means harm as a last resort (Bellaby, 2012, p. 93). Johnson evaluates Bellaby in a number of stringent ways: he compliments him for amalgamating the philosophical and ethical facets of *"Just war"* theory in a competent way, but also criticises his focus of these principles primarily at *collection* phase of the intelligence cycle (Johnson D. , 2015, p. 200). This arguably neglects real life application. Equally, "*first do no harm"* is so commonly violated, that the recent discovery of a Russian spy in a Norwegian university, posing as a researcher in order to obtain and monitor information regarding Arctic security, comes as no surprise (Raw, 2022; Bellaby R. , 2012, p. 95). Unsurprisingly, this disregarded all of the above principles, as colleagues and professors' realities were permanently altered by years of deception, bearing a heavy load on individual rights (Raw, 2022).

Brian Auten examines Bellaby's framework in a distinct way, by showing that Bellaby focuses more on harm to the states right to privacy, than the individual, contradicting his overall message, of rights of the individual (Auten, 2013; Bellaby R. , 2022, p. 93). These breaches of privacy and of individual security, are more common than one might think. A recent example of this, is when undercover police and intelligence officers planted themselves in activist households in Leeds, UK, where they established real relationships with members of households, in order to obtain exclusive information on when the next activist actions may take place (Syal, 2011). The officers even had their own secret families and alternate lives, making this an especially traumatic experience for the victims (Syal, 2011). In response to an influx of media attention, this was put through the justice system in the UK, with the morally abhorrent nature of this finally recognised (Syal, 2011). Many of these incidents will go unchecked, unless the harm to the individual is so public and obvious that it necessitates a stringent response (Liberty, 2022; Syal, 2011). This can be seen through MI5's tribunal by Liberty and

Privacy International, who revealed that they have been breaching privacy laws since 2010, by *"providing false information to unlawfully obtain bulk surveillance warrants against the public,"* but have only been brought to justice now (Liberty, 2022).

Bellabys' intelligence framework can therefore be questioned in a number of ways. How can the individual's level of harm be measured, if it is done through covert action, and rarely comes to the attention of the public (Syal, 2011; Bellaby R. , 2022, p. 93)? In the just principles, how can harmful intelligence practice be a last resort, when many countries are using it pre-emptively and strategically, to gain advantage over one another (Raw, 2022; Bellaby R. , 2022, p. 93; Geldron, 2007, p. 398)? Why is the state again seen as the sole operator of intelligence, with no mention of the private sector? (Bellaby R. , 2022, p. 22). Equally, right intention can easily be faked, with countries making up false 'legitimate' intentions in order to justify actions, and so how can we really say *"Ends Justify Means?"* (Elgot, 2016, p. 75; Geldron, 2007, p. 398). In comparing Bellaby to Geldron however, we see vast improvements from the omnipotence of the *"Just War principles"*: with consideration for the individual, legitimate authority and right intention (Geldron, 2007, p. 398). However, this is again linked exclusively to the moral compass of western, liberal democracies (Bellaby R. , 2012, p. 398). Equally the state is equated with the individual and breaches of privacy, which continues the state-centric narrative (Bellaby R. , 2012, p. 398).

For our third ethical framework of intelligence, we look to the private sector. Maria Morrow covers the rough framework that governs private sector intelligence. One of the universal principles is the illegality of espionage, implemented around the world, although not necessarily fully adhered too (Morrow, 2022, p. 405; Cyphere, 2023; Mcfadden, 2019). "*A step in the direction of codification of these ethics"* is AIRIP's development of a code of conduct for risk intelligence (2015), which represents one of the first codifications of these ethics, emphasising the importance of operating within the organisations code of conduct, objective and unbiased analysis, abiding by the law, and upholding high levels of professional credibility (Morrow, 2022, p. 405; AIRIP, 2023).

In parallel, Maria Morrow emphasises the "*professionalisation"* of the private intelligence sector, where the development of a universally accepted and implemented code of ethics, is nothing short of essential (Morrow, 2022, p. 402). Google's worrying behaviour in 2019, where they were exposed for cyberstalking and bullying on the internet, indicates the vital need for these limitations on the sector (Morrow, 2022, p. 403). Not only this, but the stark rise in artificial intelligence, brings the ethics of the private sector more and more into question, as intelligence capabilities now teter at the brink of developing their own consciousness (College, 2023). Privacy International contests this limited private sector ethical framework, as they flag major issues that are emerging as a bi-product of privatisation that should be regulated, but aren't (PI, 2023, p. 2). For example, the mishaps of Blackcube intelligence, who sent undercover employees to befriend witnesses of Harvey Weinsteins sexual assault (PI, 2023, p. 2). These undercover agents were caught, yet faced limited consequence (PI, 2023, p. 2). As a result, PI would perhaps argue that regulation does not nearly go far enough, particularly in reference to Morrows description of the framework (PI, 2023, p. 2; Morrow, 2022). This private sector framework is also predominantly uncodified, meaning there is limited accountability (Morrow, 2022, p. 401). This leaves it at the peril of mutual trust, and accountability, where naturally, there are no bodies that enforce this (Morrow, 2022).

The issues with both private sector intelligence ethical frameworks, and public sector, are evidently not that dissimilar. Both have a lack of accountability mechanisms in place, even if there are vague laws and conventions surrounding them (Bellaby R. , 2012, p. 93; Geldron, 2007, p. 398; Morrow, 2022). They are overwhelmingly ethically uncodified, operating from an assumption of abiding by precedence and mutual 'trust' (Bellaby R. , 2012, p. 93; Geldron, 2007, p. 398; Morrow, 2022). There is also no universal ethical point of reference, and for states, these practices can quickly be overridden in the event of exceptional circumstance (Bellaby R. , 2012, p. 93; Geldron, 2007, p. 398; Morrow, 2022). This leaves a significant amount open to interpretation, and when dealing with human rights, can have dire consequences (CFRES, 2018).

In one of the most recent propositions of a new ethical framework for intelligence, we look to Cecil Fabre, who through her publication *"Spying through a Glass Darkly",* received praise from MI6's ethics department itself (Fabre, 2022, p. 10). One of the main premises of the book, is Sun tzu's principle that a ruler has an essential duty to "*avoid conflict wherever possible*", where espionage plays a vital role in prevention, as information can be used to pre-empt and prevent it (Fabre, 2022, p. 11; Tzu, 2023). She emphasises that many wars would fail to be prevented otherwise, and that intelligence can be a vital means for peace (Fabre, 2022, p. 11). Philosophers such as Hobbes eagerly agree with this sentiment, as without intelligence agents, "*sovereigns have no more idea what orders need to be given for the defence of their* *subjects than spiders can know when to emerge and where to make for without the threads of their webs*" (Owen, 2022).

She proposes three main approaches to the ethics of espionage. The "*Dirty hands approach*"- or *"ends justify means"* (Fabre, 2022, p. 9; Geldron, 2007, p. 398). The *"Contractarian approach",* where espionages rules only apply to its own players, with the general population excluded, as it continues to operate within its own security sphere (Fabre, 2022, p. 9). Citizens therefore have a social contract with the state to protect them, and they give up their right to transparency (Fabre, 2022, p. 9). Finally, the *"Just War Approach"*, which is subject to two distinct criteria (Fabre, 2022, p. 9). Espionage activities must serve a just cause, and must be conducted ethically (Fabre, 2022, p. 10). In a podcast with Nick Spencer, Fabre and Spencer questioned whether the function of spying can ever truly be ethical, which contradicts the premise of this framework in itself (Spencer, 2023). Fabre answers her own question, with the example below. It is hard for any sector, to be fully ethical (IESE, 2015).

Fabre uses the example of Russia invading Ukraine as an unjust use of espionage, specifically with recent cyber-attacks on SpaceX, as a mechanism that fundamentally aids Ukrainian communications (Fabre, 2022, p. 8; Lynanashock, 2022). Where critiques stray from Fabre's approach, is on the question of morality. Fabre argues that if your community is engaged in treason (unethical behaviour), you should approach it as if you are a non-member (Fabre, 2022, p. 10). Alternatively, what Parry suggests, is to keep ties with the community, in order to prevent further unethical behaviour (Parry, 2006, p. 251). In espionage terms, this translates to integration, rather than separation, in order to achieve objectives. This paints morality in the intelligence sector, as a community effort, rather than anything that a singular framework can achieve.

The issues with this framework are much the same as the previous ones. Although the *"Contractarian approach"* reinforces an elitist and in transparent processes in the intelligence sector, this can be argued to be based on what roughly already exists (Fabre, 2022, p. 10). However, this undermines the current calls from the public for more transparency in the private sector, with the *"Dirty hands",* and "*Just war*" approach, notions that have already been around for a long period of time (Haydon, 2013; Geldron, 2007, p. 398; Bellaby R. , 2022, p. 93). These all also fail to mention the rise in artificial intelligence, non-western countries and the private sector in general (Yu, 2018). Equally, there is a lack of innovation amongst these frameworks, as they have evolved, but in minor ways, leading to the pressing need for a new one.

As a result, we see that there has been a lax attitude towards intelligences exploration conceptually, because of this reliance on precedence, and unentrenched frameworks to guide the sector, as well as an assumption that the *"Just War*" and *"Just Intelligence"* principles, are fit for purpose (Geldron, 2007, p. 11; Bellaby R. , 2022, p. 50). With a lack of awareness about the true functions of intelligence, comes a lack of calls for accountability, and development of these frameworks beyond structures that were better suited to a espionage context (Lundborg,2021,p443; Cornish,2021,p224; Deeks,2016,p599; Tucker, 2014,p10). There is quite evidently also a disparity between theorization and implementation, which could be said to take the impetus and motivation out of doing so. Ethics can therefore be said to be capable of application to such a fast-growing and autonomous sector, it just needs a more stringent and universal framework, which this dissertation will provide.

Chapter 3

Methodology

This dissertation follows a distinct methodology. By methodology, we mean the overarching strategy and rationale of the piece as well as its research processes, and ethical considerations. We have begun by contextualising the debate, and have moved into an in-depth exploration of not only the literature on intelligence, but on ethics too, to justify this pieces ethical grounding, and identify the gaps in the literature. We will then move onto the ethical framework, which is based on the CIA's model of the intelligence cycle, meaning that we can pair both the process and ethical facets of accountability, and transform this into a more palpable framework (CIA, 2023). The intelligence cycle provides stringent markers for transformation within a universally known structure of intelligence gathering, making it a viable structure for the ethical framework (CIA, 2023). We have chosen a international security issue to apply this too, climate change, as this is an example that is limited in politicisation, and will show the ethical framework in action. Terrorism was the original example used, which we changed because of its contentious nature, and vulnerability to being interpreted in a number of different ways.

We will then move onto case study analysis, where 5 businesses were selected for their innovative and positive contributions to transforming global governance issues. These were selected through cold emailing companies that were shortlisted for their contributions, and through extensive searching via LinkedIn. Bias in selection could be argued here, as finding individuals relied on LinkedIn's algorithms, although there was limited alternative to finding contacts.

Company A was chosen for their hybrid intelligence and security consultancy functions, which was unique not only in its constitution, but in its commitment to ethics and transformation of the sector outside of a western centric remit. Company B was chosen for the groundbreaking business model it operates from where transparency of sources works at the centre of its operations, and is also developing its own unique ethical framework. Company C was chosen because of its specialised strategic intelligence capacity and the expertise of the founder who also started their own company. Company D was selected because of its unique contribution to attacking financial crime and commitment to transforming global governance issues, as well as its hybrid HUMINT and OSINT function. Company E was chosen for their exceptionally high standards of analysis, seen through it being awarded the queens award, and its outstanding contributions to the field during the Russia-Ukraine conflict. We interviewed one representative from each company, in order to gain a clear perspective.

Global governance issues were selected in line with the UN development goals through identification that these were already being used as a part of ethical benchmarks for companies in the intelligence sector, with whom we cannot name, as they were a part of our case studies (UN, 2015). This showed that they already carried significant weight, both politically and practically.

We will now move onto how we have developed the ethical framework in line with the intelligence cycle (CIA, 2023). If intelligence is knowledge, *"information gathering"* and many times in the context of an adversary, then our ethical framework should reflect these different processes of intelligence, as well as the construct of it (Pythian P. G., 2018, p. 62; Warner, 2002, p. 1). *"A good starting point for developing an ethical framework, is to look to the notion of intelligence itself."* (Omand, 2018, p. 27). We will also look to critical theory, to develop our originally developed framework (Bean, 2021, p. 467). "*Scholars are increasingly calling for the development of metacognitive perspectives, in which self-reflection, critique, and de-reification of dysfunctional abstractions become pillars of a new approach to intelligence*" (Bean, 2021, p. 467). This will account for the process facet of intelligence, and construct side, but we will add to this, by accommodating the private sector (Richards, 2010, p. 10). This inherently changes the whole construct of intelligence, as it is encouraged to emerge from its exclusive security sphere, and self-reflect through assessing each stage of its processes.

The intelligence cycle will effectively act as a positive measure of intelligence, as we measure business and organisations actions at each stage of the cycle (CIA, 2023). The more stages they conform to ethically, the more benign they can be measured as. We will then be able to measure the companies positive activity via our case studies, with ease, as their contribution at each stage is measured separately, and in detail. Equally, this can easily be applied to the transformation of global governance issues, as the intelligence cycle provides important markers for transformation, if taken alongside tailored and specific ethical considerations (CIA, 2023). It will also act as an important gauge for the *"Just war principles",* which currently have no measurement for when a situation is exceptional, and when escalation should result in the removal of basic rights (Geldron, 2007, p. 11).

We will analyse Canadas wildfires 2023 to empirically apply the ethical framework, so that we can see how it can be applied to a global crisis (GM, 2023). In turn determining how the framework can help provide clarification, and ethical assessment in response to sensitive and contentious climate events, that may not have competent accountability mechanisms already in place.

Canada's wildfires 2023 provides a distinct example of climate crisis, with intelligence gathering at the centre of the country's ability to coordinate prevention (CDP, 2023). With multiple and intangible outbreaks of wildfires occurring simultaneously, the role of intelligence at each stage of the crisis has proved to be crucial, as its sporadic and life-threatening nature, threatened to kill a great number of innocent civilians, just this year (GM, 2023). We can see this particularly, through the outbreak of 169 fires, recorded in Ontario alone (2023) (GM, 2023). As recently as June 6th, there were 31 active fires across Northeastern Ontario, 21 of these are still not under control (GM, 2023). These wildfires have consistently caused millions of dollars' worth of damage, and displaced thousands of civilians (CDP, 2023). Points of escalation have been hard to predict, and fires difficult to control, even with traditional firefighting mechanisms (GM, 2023). These have been directly attributed to the effects of climate change, making it a key part of the global governance landscape, and naturally, a key issue for transformation (CDP, 2023).

We will specifically focus on The WildfireSat mission for the purpose of the empirical application section, as it is a direct response effort to the wildfires, and a cross-collaboration between private and public sector intelligence agencies, that intends to closely monitor, and prevent wildfire escalation by 2029 (GOC, 2023). The aim of the programme is to monitor wildfires on a daily basis, through space satellites (GOC, 2023). This provides us with a unique opportunity to assess its ethical application, at different stages of the intelligence cycle, as there are a diversity of agencies involved, with the project having unique and trailblazing characteristics (GOC, 2023; CIA, 2023). This initiative includes companies such as Spire Global, a Satellite powered data gathering private sector company, Orora-tech, an infrared thermal intelligence company, the EU space agency, Canadian Space Agency and Inter-agency forest fire service, to name a few (GOC, 2023). With such a new initiative, inevitably comes ethical issues which that haven't been found before.

In the analysis section, this dissertation has chosen to use *"grounded theory"* in order to establish patterns and theories from research gathered (Holton, 2008, p. 5). This has been effective in pairing these patterns with global governance issues. As a result, this dissertation has then been able to get an in-depth overview of how intelligence can in fact be applied to global governance issues, whilst recognising its transformative and positive capacity. We will draw on literature in previous sections in order to continue the narrative and apply this to a empirical, and research driven context. We will also take each global governance issue mentioned in the introduction separately, and pair it with a pattern. The piece is then finished by conclusions, which provides a summary of work carried out.

This will lead us to a clear outcome from the dissertation, with an assessment of these companies strengths and limitations, when faced with the ethical framework. This will also give an overview of intelligences benign use, and its functions outside of the state. By choosing both the theoretical and empirical, and deciding not to do a data driven piece, this dissertation has created a more balanced and humanistic research outcome.

This dissertation also recognises that at case study stage, the process could have been improved by reaching out to companies sooner, and establishing relationships pre-emptively, as the research timeline was pushed back due to delayed responses. Equally in the dissertation proposal, the question originally affiliated global governance with particular sectors, for example in the poverty, migration and climate change sector. This turned out to be an unfeasible part of the question as the piece would have to be much longer in order to incorporate all of these facets. Therefore, we have focused on more of a macro-overview of global governance issues, rather than affiliating them with particular sectors.

We came across many issues during this process, with it taking more than a month to receive responses from companies emailed, forms were filled in wrong, and participants dropped out at various stages, leading to dead ends. Nevertheless, trust was built with participants over time, which led to them referring us to colleagues who were willing to participate. The initial interview questions also became less relevant during the interviews, as these questions had been submitted to the ethics committee in January, meaning that the piece had evolved to a stage where some of the questions were less than relevant. Questions such as: what is your personal opinion of the intelligence sector? Were not received well initially by participants, and thus this was excluded from remaining interviews. The intelligence cycle was also not initially mentioned in the lines of questioning, which was an inevitably essential part of this research

(CIA, 2023). Thus, it was important that this was included as a part of the interview, in order to gauge company activity at each stage of the cycle, and their ethical practice in correlation to it (CIA, 2023). We also added in questions concerning which stage of the cycle the companies believed they excelled the most in, and where there was room for improvement, which gave us a better picture of how they are able to operate within the ethical framework (CIA, 2023). As a result, this dissertation has been reflexive in its research processes, and responsive to evolving needs of the project, and interviewees.

There are also naturally ethical considerations that have been taken into account when conducting a research piece of this calibre, and with mixed methodology. By using *"interview methodology*", we have explored ethical considerations by gaining ethical consent from the university and individuals interviewed, and have ensured that all procedures have been followed regarding legality and data collection/storage (BRM, 2006). By reaching out to intelligence companies there was the risk that individuals that those that we sought to interview, may have felt their privacy infringed upon, or that they may be put at risk by being part of this publication. To address this, we have used pseudonyms throughout the study, and have checked consent of the interviewee at each stage of the process so they have had the opportunity to withdraw if needed. This consent has also been extended to the company that they work for, so that both their jobs and reputation were not put at risk, by being a part of the publication. They have also been made aware that data will only be stored for the duration of the project, and the publication held within the university's secure server.

We must also within this, recognise the limitations to our research as a whole. By interviewing private sector intelligence agencies, we gathered incredibly rich research, but by doing so we inevitably have not gathered a fully rounded perspective. Company representatives will naturally defend their organisation, without perhaps, giving a balanced overview of the reality of their operations. As a result, we may have gathered positive examples of intelligence, but potentially not considered negative implications of them, which would entail more extensive research, and reaching out to different categories of interviewees, over a longer period of time. Our ethical framework, may also be difficult to implement, and be subjective when taken within organisations that are looking to rate themselves positively. Our global governance issues, equally, were selected specifically in the context of development, and thus further research may need a broader remit, in order to encompass the breadth of issues that the world is experiencing.

Chapter 4.1

Ethical framework

This dissertations framework as mentioned in the methodology section, provides a distinct basis for analysis, by pairing the intelligence cycle with ethical concerns, in order to assess organisations (CIA, 2023). It is this sections intention to showcase the framework, by explaining each stage of the intelligence cycle, and pairing it with relevant ethical considerations to be applied to an empirical example, in the following section and to finally assess our five companies with. This intends to form a universal point of reference for the intelligence sector going forward, and will empirically answer the research question can ethics be applied to such a fast-growing and autonomous sector (Gill,2013, p93; Lin, 2011, p10;Puyvelde,2019,p21;Adriana,2021,p8)?.

We will assess organisations at *Planning & Direction* stage, by their ability to ethically direct their intelligence gathering, and impact global governance issues positively, shown through how they strategize (CIA, 2023). At *Collection* stage, we will assess them through their methods of them gathering information, how ethical this is, and how far this infringes on the right to privacy (CIA, 2023). They will be assessed at *Processing* stage, through how ethically they process information, and when and if they do so, as well as how (CIA, 2023). At *Analysis & Production* stage, we will assess actors on the ethical nature of how information is made into a product (CIA, 2023). Finally, at *Dissemination* phase, we will assess how ethical their way of distributing intelligence is, and how directly this impacts global governance outcomes (CIA, 2023). We will clarify the stages of the intelligence cycle below, and their relevance to these ethical assessments (CIA, 2023).

Planning & Direction is the first stage of the CIA based intelligence cycle, which in simple terms, means the planning and directing of intelligence gathering (CIA, 2023). The CIA describes this in real terms as "*When we are tasked with a specific job, we begin planning what we'll do and how. We move in a specific direction to get the job done, listing what we know about the issue and what we need to find out. We discuss ways to gather the necessary intelligence*" (CIA, 2023). When paired with ethics, we can assess *planning and direction*, alongside the ability of the organisation to impact global governance issues positively, by planning and creating solutions to global governance issues (CIA, 2023). This will involve their strategic outlook, and empirical capacity to carry out such initiatives (CIA, 2023). This works to counter *"clandestine intelligence gathering"*, or secretive planning and direction of intelligence, as transparency is called for by the public (Goldman, 2005, p5). An example of this positively in action, would be if Crisis24, a Intelligence, risk analysis and operations company, planned to expand their intelligence capabilities to monitor and rescue refugees that were directly impacted by the climate crisis (C24, 2023). This could be measured as ethical planning and direction, on behalf of the company although this dissertation is aware, that there are nuances within this, as we cannot simply deem a company as ethical, because of one action.

Collection is a stage of the intelligence cycle that unsurprisingly, involves how intelligence is gathered (CIA, 2023).**"***We collect information overtly (openly) and covertly (secretly). Reading foreign newspapers and magazine articles, listening to foreign radio, and watching overseas television broadcasts are examples of "overt" (or open) sources for us. Other information sources can be "covert" (or secret), such as information collected with listening devices and hidden cameras. We can even use space age technology like satellite photography. For instance, some analysts could actually view how many airplanes are present at a foreign military base by looking at a picture taken from a satellite in space*" (CIA, 2023)**.** This can be paired with the ethical ways that they gather information. Naturally, this involves avoiding collecting information *"surreptitiously, or intrusively"* (Scott, 1999, p. 34). For example, how far they infringe on the right to privacy (UNICEF, 2019). In practice, this looks like companies such as Erinys, a private security and intelligence company, collecting information on adversaries consensually, and through transparent processes, whilst complying with legal and ethical boundaries (Erinys, 2023).

At *Processing stage*, this concerns how information is processed, and the methods of doing so (CIA, 2023). **"***We take all the information that we have collected and put it into an intelligence report. This information could be anything from a translated document to a description of a satellite photo*" (CIA, 2023).This therefore concerns the ethical implications of when and if intelligence is processed, and the method in which it is done so. Jonson labels this as an expectation that the agent is committed to *"unbiased learning"*, so there not just being an unbiased product, but an unbiased commitment to self-development, and reflection (Jonson, 2018, p. 1). This looks like companies such as G4s, a private security company, processing information that protects source identities, and stores data sensitively, processing data, with integrity, as well as employees taking the onus to develop and engage in ethical initiatives (G4S, 2023).

With *Analysis & Production***,** this can be fundamentally linked to how intelligence is interpreted, and whether it is biased, or done with error (CIA, 2023). **"***During this step, we take a closer look at all the information and determine how it fits together, while concentrating on answering the original tasking. We assess what is happening, why it is happening, what might occur next, and how it affects US interests*" (CIA, 2023). This is paired with the ethical implications of how information is made into a product. Omand would call this *"Building confidence, through oversight and accountability,"* although in this case, is grounded in an analytical context (Omand,2018,p151). This looks like companies such as Kroll, a risk advisory firm, committing to analysis with integrity, without as much bias as possible, whilst formulating products that are deemed to be as neutral and people driven as possible (Kroll, 2023).

How organisations *Disseminate* their intelligence is imperative to ethics, and can be boiled down to how intelligence is distributed (CIA, 2023). "*In this final step, we give our final written analysis to a policymaker, the same policymaker who started the cycle. After reading the final analysis and learning the answer to the original question, the policymaker may come back with more questions. Then the whole process starts over again.*" (CIA, 2023). We can therefore assess the organisations process of dissemination, on how ethical their distribution mechanisms are, and ultimate global governance outcomes. "*The reality of todays world, is that its dauntingly complex,"* and therefore context, and an understanding of the diversity of global and local issues, is just as important as the process itself (Steele, 2023). This looks like companies such as AEIGS, a integrated security firm distributing their intelligence, with integrated and local knowledge in mind, meaning that it is ethically, and contextually applied (Aegis, 2023).

In summary, the ethical framework provides a uniquely process-driven, and ethical benchmark that can be applied to private, and public sector intelligence organisations alike. It develops on the loosely formulated and implemented "*Just war"* and *"Just intelligence"* principles, and even on regulation that has emerged as a bi-product of *"professionalization"*, filling in a substantial accountability gap in the intelligence sector (Geldron, 2007, p. 25; Bellaby R. , 2022, p. 30; Adriana, 2021, p. 8). This shows ethics to be capable of integration in the private intelligence sphere, although this will fundamentally be based on consent, until global accountability mechanisms are put in place.

Chapter 4.2

Empirical Application of framework

The Canada wildfires have placed "*Canada at a tipping point*", where climate change has inevitably fostered the harsh conditions where "*pre-suppression effectiveness*" is becoming less and less effective, as mentioned in the methodology section (Tymstra, 2020, p. 26). This has led to increasingly devastating effects, and a disaster management programme, that is more ineffective than ever, as wildfires rampage through the country (Tymstra, 2020, p. 27; PSC, 2023). This failure is expressed most prominently through the Mitigation stage of disaster relief management, defined as "*structural and non-structural measures, implemented to limit the impact of disasters"* (BCOEM, 2023; Henstra, 2005, p. 303). In comparison with The Emergency Management Strategy for Canada, a resilience framework published as a solution response, the WilfireSat mission provides a much more hands on, and applied approach to mitigation (PSCR, 2019, p. 1).

In response, it is this sections intention to evaluate the WildfireSat mission against the ethical framework, and intelligence cycle, so that we can garner its proposed effectiveness, as a mitigation solution, and in context of the WildfireSat mission, as the most arguably effective resolution (BCOEM, 2023; Henstra, 2005, p. 303). This method of analysing the framework against a real-life example makes it stand out from other frameworks, as up to date and empirical examples were sparingly used in other academics works (Bellaby R. , 2012, p. 20; Morrow, 2022, p. 402; Geldron, 2007, p. 50).

The WildfireSat mission *Plans & Directs* Intelligence ethically by aiming to involve a diversity of bodies in the mission (GOC, 2023; CIA, 2023). This includes the Canadian Space Agency, Natural Resources Canada, Canadian Forest service, Canadian Interagency Forest Fire Service, BC Wildfire Service, Ontario Ministry of Forest Fire service, and private sector agencies such as SpireGlobal, and Orora-Tech (GOC, 2023; SG, 2023). Some may argue in line with the general debate, that government functions should not be outsourced to companies who are less accountable (Krishnan A. , 2007, p. 195; Antara, 2020; Storm, 2018, p. 125). However, as Anna Leander argues, privatised functions of government, are *"as old as private security itself"* (Leander, 2016, p. 57). Meaning that even if the public has not been aware of this, it has already been an integral part of government functions, for many decades (Leander, 2016, p. 58). In the World Bank Report on privatisation, 2013, its findings conclusively showed that by privatising particular government functions, this expedites lengthy and bureaucratic processes, as well as financially and operationally speeding up processes (Kikeri, 2007, p. 101). This has also been shown to reduce workforce labour by 20%, in transitional and developing countries (Mcgettigan, 1999, p. 221).

In the example of the Canadian wildfires, this sentiment is particularly relevant, as time is of the essence when wildfires break out, and less labour force will protect human lives (GOC, 2023). The monitoring of the fires, purely through satellite machinery, is one useful example of this, which may translate into less need for a physical labour force (GOC, 2023; Jackson B. , 2001, p. 5). However, the mission is exclusively advertised as a government mission, leaving the names out of private sector intelligence agencies, which challenges the ethical transparency of its processes (GOC, 2023). This is particularly relevant in the context of the shift in the sector towards being more open with the public in intelligence practice (GOC, 2023; Zegart, 2022). As a result, we can assess that the WildfireSat mission leans toward ethical practice in *planning and direction*, through the mission's diverse constitution, but lacks transparency in its advertisement, challenging its ethical accountability and legitimacy (CIA, 2023; GOC, 2023). This initiative inevitably sets a precedence for future emergency response missions, and intelligences integration into further government mechanisms, hence we can classify this as an integral part of transforming global governance issues.

At *Collection* phase of the intelligence cycle, we can garner that there may be breaches of the right to privacy, through satellite monitoring of the wildfires (CIA, 2023; GOC, 2023). It is inevitable that most pieces of technology have the potential to be hacked, rendering vulnerable information to a potential enemy of state (Hartwig, 2023). A team of hackers have shown this in practice, by hacking the European Space Agency, and introducing malicious code: which also happens to be one of the agencies used by the WildfireSat mission (GOC, 2023; Barr, 2023). However, the accuracy of satellites could counter-balance this, as the protection of lives could be argued to be more important than the chance of being hacked (SSPI, 2023).

Equally, *Collection* by a number of different agencies may also lead to future data breaches (CIA, 2023). WildfireSat will not be fully immune to this, much like in recent and high-profile cases, such as the Indian tv firm Dish that was hacked, leading to the loss of data of 300k employees (IANS, 2023). There is therefore much more chance of this happening, the more data is passed on between agencies (Middleton, 2023). For example, Capita, an intermediary company that acts as the go to outsourcing private company for the private sector and government alike, has recently reported 90 organisational data breaches, related to the company (Middleton, 2023). This leaves the cross pollination of agencies in WildfireSat, as all the more worrying, as infringements on the right to privacy, could reach a much wider berth of audience (Middleton, 2023; GOC, 2023). However, academics argue that data breaches refine processes, and because the European Space Agency is so fresh out of one, this could arguably make them a safer choice (Shankar, 2020, p. 35). Therefore, WildfireSat can be argued to be ethical in the ability of the satellites to save lives, and the reduction of human cost, but troubling in its impact on the right to privacy, which provides us with major concern in reference to previous examples of breaches.

Processing stage, comes with its own qualms, for WildfireSat (GOC, 2023; CIA, 2023). By processing data on carbon emissions from the wildfires, as well as locations open to fire risk, this on one hand does show positive ethical moves, as this is not only progressive when it comes to conforming with local law on climate change, but in falling in line with international climate change agreements on carbon levels (GOC, 2023; UNCC, 2023). Equally, effective processing will also positively impact the health of the population, and prevent property loss, and evacuations if it is able to process as quickly as promised, then it will be a vast improvement from current remote sensing tools in place (GOC, 2023). As a result, its processes are ethical in *what* it is processing, but *how* it is processed, is another matter. By using remote satellites, this will inevitably lead to a loss of jobs, and with such close and continuous monitoring, the trust of the citizens may waver as such a cross agency effort can easily be exploited by a wayward individual (Hughes, 2022; Larkin, 2022). We need only look to Wikileaks and Julian Assange, to measure the profound impact an individual can have (Doherhty, 2023). Assanges leaking of political documents, sent shockwaves through the private and public sector, leading to his arrest (Doherhty, 2023).

"Big data management can be exceptionally challenging" (Nuair, 2020, p. 8). As Suja Nuair rightly points out, when data is processed so fast, much like in WildfireSat, there is always a statistical chance of error, or data breaches (Nuair, 2020, p. 9). Therefore, we may not be able to quantify the risk, and ethical implications of WildfireSat until its release, but what we do

know is that it will be interacting with a vast quantity of sensitive data which comes with risk of breach (GOC, 2023). In addition, there has been much public concern regarding the use of algorithms in new technology, and how this invariably encourages bias (Barn, 2019, p. 1477). For example, in WildfireSat, if there were wildfires occurring in one location repeatedly, resources may be overly syphoned to that area which if in need of redirection to another location, may take a long time to do (GOC, 2023). In response, WildfireSat can be said to be ethical in what they are processing, but the main points of concern are from how they are processing, as their processes can easily be taken advantage of (CIA, 2023).

Analysis & Production is a vital ethical stage, as lives rely on the accurate interpretation of data, and how this is presented cross agency (TA, 2010; CIA, 2023). As Fisher stipulates *"Done wrong, it can be dangerous"* (TA, 2010). Preconceptions, even in a seemingly innocuous topic such as climate change, can cause data collected to be applied improperly (AB, 2022, p. 22). Studies show that there is a significant cognitive bias towards climate change that make people hesitant to act , meaning that even if the data may be showing signs of wildfires, there may be grey areas or analysis bias, when it comes to this analysis leading to action (AB, 2022, p. 22). Reports, such as one published by Maiaa Cook who did an extensive study on intelligence analysis bias, emphasised that graphical analysis, or structured analysis works effectively to remove areas of pervasive bias (Cook, 2008, p. 10). In reference to WildfireSat, this may be hard to implement, due to a range of different agencies working together, with potentially conflicting processes, and ethical concerns.

Where WildfireSats strengths lie at analysis stage, is that in speeding up the process of collection, this leaves more crucial time for analysis. In addition, "*One of the most important functions of intelligence, is to remove ambiguity"* (IRP, 2023). Arguably, with more agencies may also come more scrutiny and thus a more legitimised, and clarifying process (GOC, 2023). As well as this, *"Successfully detecting security threats, requires consistent analysis of identical data"* (Labib, 2022, p. 17780). This makes it arguable that WildfireSats vulnerabilities in analysis, may lie in the training of analysts, extent of bias, and consistency of judgement (GOC, 2023). It is also crucial that they ethically avoid what the US has been doing, by *"blinding itself"* to a wide range of sources, simply because information is so widely available and automated (RAND, 2021). It can therefore be said to be ethical in process, but ambiguous in implementation.

Dissemination stage is a vital ethical stage for the WildfireSat mission (CIA, 2023). Ensuring that intelligence, once collected is distributed amongst agencies, and acted upon in an ethical way is imperative to its success. For example, if false data is distributed, then unnecessary evacuations could take place leading to a significant disruption to lives, including loss of income, damage to health and the trauma of re-location (Mclennan, 2013, p. 20). Equally, if fires go undetected, then there is an obvious, and significant, threat to life. During the Mijas wildfire, near Malaga on July 16th 2023, nearby citizens simply stood and watched the plumes of smoke getting nearer, with little update from the authorities, which shows the impact intelligence can ultimately have (Peter, 2022). There are also real-term patterns where false evacuations, lead to evacuation fatigue, where the public may refuse evacuation if errors keep occurring, over a prolonged period of time (Anguiano, 2018). This makes it vital that *dissemination* phase, is done correctly in order to protect lives and livelihoods (CIA, 2023).

Equally, this shows the WildfireSat mission to be more focused on the process of intelligence gathering, rather than a dissemination, people-focused, and outcome-based approach (GOC, 2023; CIA, 2023). By taking into context distribution and cultural context this would take into consideration, a more outcome, and context-based approach. This is shown through the Protective Action Decision Model, which recognises a *"suite of factors"* that are relevant to action-based evacuation procedures (McCaffrey, 2017, p. 1404). Some being socio-cultural characteristics that make people choose to stay in the home until the danger is entirely apparent, or that makes people may wait until the danger is directly in front of the individual/family before they are willing to evacuate (McCaffrey, 2017; Pohl, 2021).

This means that even if there were exceptionally effective means of collecting intelligence like the WildfireSat mission proposes, its implementation would be largely useless if the socio-cultural precedence's were not properly addressed (Pohl, 2021). In addition, *"Intelligence as a practice is charged with locating and preventing very dangerous threats to both individual lives and the interests of the community across their economic, political, and social needs*" (Bellaby W. , 2022, p. 51). Meaning that there is a whole range of ethical considerations that have not been taken into account, when formulating the basis for WildfireSat (GOC, 2023). The mission can therefore be said to be most vulnerable at *dissemination* phase, as a result of the risks of interaction between process and implementation of the mission, and the extent of impact to life, if done so badly (GOC, 2023; CIA, 2023).

We can therefore conclusively say that the ethical framework has legitimacy in its empirical application, and in the case of the Canada Wildfires 2023, and WildfireSat mission (GOC, 2023). There are a whole array of ethical strengths and implications that we may not have been aware of, if it wasn’t for the application of the ethical framework (GOC, 2023). In summary, the mission shows most ethical concern at *dissemination* phase, because of its focus on the process of intelligence gathering, rather than how it is distributed, and implemented (CIA, 2023; GOC, 2023). In counter-balance, we can say that its strengths lie at *Collection* and *Processing* stage, as the mission will exponentially speed-up processes of wildfire detection and monitoring, that will ultimately save a significant amount of lives, if implemented properly (CIA, 2023; GOC, 2023). However, the mission should be aware of risks such as data breaches, security and asset vulnerabilities, socio-cultural context and implementation, and rigorous and universal processes amongst agencies, in order to maintain sufficient ethical standards.

Chapter 5

Case Studies

"Putting a human face on intelligence" is at the forefront of our agenda in this section, playing a significant part of our narrative, as we explore the intricacies of live private sector companies that are active in positive, and benign contributions to the sector (Cohen, 2010, p. 251). The narrative of this section, is simple. That each company contributes to transforming global governance issues positively, in different ways. The ethical framework will draw these contributions out and show mainly the strengths of each company, although we will also recognise limitations in line with it and ultimately show, just *"how crucial"* private sector intelligence is in transforming global governance issues (Boren, 1991, p. 1993). We focus mainly on the benign characteristics of the companies, because of our commitment to shift the sectors image, to a more positive one. This will also definitively show that this is not *"the end of the intelligence cycle",* as our ethical framework uses this as a significant point of examination, pairing process with ethical consideration (Hulnick, 2014, p. 48). This modernises its function, without losing its recognisability. Our interviews are integrated into the text, as we first explore their overall positive function, and then assess them against the ethical framework itself.

Company A reflects its benign nature, through its positive contributions to the intelligence sector, particularly through its business ethics strategy (Interviewee 1,2023). Our interview was with the CEO of a private sector security consultancy based in Estonia, who has spent over 20 years working in a very senior public sector role before starting their own company (Interviewee 1,2023). Although their company is largely consultancy based, there is an intelligence facet to it, making it an interesting point of analysis, as a hybrid company within the private sector (Interviewee 1,2023). Interviewee 1 showed ethical strength within their strategy, specifically through their commitment to pick and choose clients with the highest ethical and moral upstanding (Interviewee 1,2023). This can be seen in practice through their refusal to work with contentious states such as Russia, who have breached international law to a significant extent because of the Ukraine war (Bellinger,2022,p2; Interviewee 1, 2023). Interviewee 1 also showed that the companies ethical practice aims to uphold similar ethical standards as the public sector, by avoiding politicisation at each stage of the intelligence cycle, misinterpretation of data, as well as a commitment to be selective about how data is collected (CIA, 2023; Interviewee 1,2023).

Retrospectively, we can see that Company A aims to integrate public and private sector ethical processes within the intelligence cycle, making the public-private sector divide less mutually exclusive, (CIA, 2023; Interviewee 1,2023). Politicization and disinformation are two ethical dilemmas that the company is trying to avoid, which can be said to be ineffective uses of the intelligence cycle, that effects both the public and private sector, in similar measure (CIA, 2023; Interviewee 1,2023). This puts a human face to intelligence, as we explore Company A's positive function, without assigning it as an arbitrary good or bad entity, but led by a human, who has natural nuances of opinion and operational practice (Cohen,2010,p251; Interviewee 1,2023).

Company A also recognizes the limitations on these ethical standards, as it may be impossible to fully understand whether a client is wholly ethical, or not (Interviewee 1,2023). As a result, the story of Company As business ethics strategy, is in its positive function of practicing intelligence ethics within the intelligence cycle, without too much divergence from public sector premises, as well as selective processes when choosing clients (Interviewee 1,2023). By adhering to high moral standards, this sets a precedence for global governance issues, such as the asymmetry of the world stage, and the drawing back of the state, as private sector intelligence companies hold each other to account, as a result of holding themselves to account, in the absence of rigorous state guidance (UN, 2015).

If we assess Company A against our intelligence cycle, we can see that at *Planning & Direction* stage it acts benignly, through its core function (CIA, 2023; Interviewee 1,2023). As a Due Diligence, Risk Advisory, and Special Investigations company, the very function of it can be assessed to integrate ethics into its core (Interviewee 1,2023). Company A also sees private sector intelligence itself, as a function of accountability, as security consultancies are entirely based around due diligence and strategic risk, that ultimately help to pre-empt and stringently prevent human rights violations, catastrophic events, and refine company processes in line with international frameworks (Interviewee 1,2023). This interestingly frames private sector intelligence as a part of the accountability framework that this piece identified as missing in the earlier stages of the report.

In reference to *Collection*, Company A sees this as the most important phase of the intelligence cycle for the company, as trusted sources and strict selection of clients is an integral part of its processes (CIA, 2023; Interviewee 1,2023). For example, the company does not deal with controversial countries, and ensures background checks on clients, although this cannot admittedly be foolproof (Interviewee 1,2023). In addition, at *Processing* stage, Company A referred to human trafficking as one of the most threatening and contentious issues effecting the intelligence sector (CIA, 2023; Interviewee 1,2023). The company now takes on work regarding human trafficking for no charge, meaning that intelligence is processed in a way that has a notable and positive effect on global governance issues, as human trafficking is a significant side effect of polarization of the world stage, and in difficulties with development (UN, 2015;Interviewee 1,2023) . The company also has a commitment and awareness to countering disinformation and misinterpretation of data, which is a vital component of processing (CIA, 2023; Interviewee 1,2023).

In regards to *Analysis & Production,* Company A works separately from the public sector, meaning that its nuance lies in that it is also a part of the largely autonomous security sphere that is emerging as a result of privatisation of the sector (CIA, 2023; Interviewee 1,2023). Yet Company A's CEO maintained that the company still uses the framework and principles of the intelligence cycle, in order to guide and analyse intelligence/information appropriately (CIA, 2023; Interviewee 1,2023). This supersedes the view that the private sector goes unchecked, as analysis is structured in a legally inspired and ethically grounded way. Finally, at *Dissemination* stage, the company has taken a calculated risk by basing its operations in Estonia rather than the CEO's home country, the US (CIA, 2023; Interviewee 1,2023). This impacts *dissemination*, as the company has moved into newer and uncharted territory (CIA, 2023; Interviewee 1,2023). However, we can see this as a positive and ethical move, as due diligence and dissemination are more reflexive, enabling the company to knowledge share across continents, which can be said to effectively brings ethical standards together, as a whole (CIA, 2023; Interviewee 1,2023).

It is this dissertations assessment that Company A is strongest on *Collection and Analysis* ethically, as there are stringent processes in place to filter out inappropriate or unethical clients, as well as ethically investing in global governance issues such as human trafficking, of their own accord (CIA, 2023). However, we cannot fail to recognise limitations to this. It is hard to assess the company on empirical practice, and so we may not be able to explore how this is implemented as we are analysing this on more of a process driven line of analysis.

We have consequently explored the narrative that Company A acts benignly, through its core function, and how it does this primarily through its business ethics strategy and processes, which chips away at the malignant and unaccountable image of the emerging intelligence sector

(Stone, 2012; Breakspear, 2012, p. 678). This puts a human face on intelligence, by showing the complex interweb of factors, that ultimately make up the ethical landscape (Cohen, 2010, p. 251).

Company B reflects its benign activity, and positive function, through its commitment to transparency of processes (Interviewee 2,2023). This is shown through it being a Due Diligence and Compliance intelligence company, that sets out to create more ethical processes in the industry, and its commitment to transparency of sources (Interviewee 2,2023). For the purpose of this case study, we interviewed the CEO, who is developing an original ethical framework in order to coordinate all the legal nuances and accountability mechanisms that are already in place in the industry (Interviewee 2,2023). This makes it a very unique point of analysis, as it is one of the only companies this study came across that was actively trying to transform the intelligence landscape, and its ethical make up, to this extent. Before setting up this company, the CEO worked for security consultancies, before wanting to make a positive change themselves (Interviewee 2,2023). This shows a human facet to intelligence, as this process of coming to an ethical code of practice, was based on past experience, and human decision making.

Interviewee 2 showed private sector intelligence to be similar to global governance, characterising them as fundamentally one and the same, particularly in respect to their shared due diligence and human rights function (Interviewee 2,2023). In light of this, the old manual advisory model was said to be becoming less and less relevant, because of its lack of focus on these two notions (Interviewee 2,2023). The combination of human analysis and tech platforms makes their business model an industry leader, with an ethical framework being developed, in order to hold themselves, and others, to account, in order to address ethical issues arising from the integration of tech (Interviewee 2,2023). This models their company, as an accountability mechanism itself. As a result, we can see that one of Company B's most impressive functions within ethics in the intelligence sector, is trying to guide ethical growth internally, and externally, as a response to exponential growth in the industry, which is causing cataclysmic changes to the very fabric of how it operates (Interviewee 2,2023). From the interview, we can assume that private sector intelligence companies act as a consensual accountability mechanism themselves, which can be argued to mean they do not necessitate more stringent ones outside of their own processes (Interviewee 2,2023). As a result, Company B tells a story of its benign function through transparency of sources, development of an ethical framework itself, and guiding other intelligence actors, through its own business model (Interviewee 2,2023).

Assessed against the intelligence cycle with *Planning & Direction,* Company B directs intelligence in a pre-emptive and forward-thinking way, by looking toward the emerging ethical issues within the industry, and adjusting its policies accordingly (CIA, 2023; Interviewee 1,2023). At *Collection* stage, as an organisation that is at the forefront of driving transparency, Company B can be assessed to be a keen player in not only holding itself accountable, but working to support other organisations in doing the same (CIA, 2023; Interviewee 1,2023). It may have been easier for the CEO to stay under the old model of private sector intelligence, instead, they chose a more difficult route in order to make a change in the industry (Interviewee 2,2023). This lends itself to ethical practice, as it encourages legitimacy through transparency (Interviewee 2,2023).

Assessed against *Processing* stage of the intelligence cycle, Company B excels (CIA, 2023; Interviewee 2,2023). As a technological platform that is committed to developing more and more efficient AI, the CEO affirms their commitment to maintaining human analysts alongside development of AI: with these two mechanisms, providing a mutual check on one another (Interviewee 2,2023). This means that intelligence is processed faster, statistically more accurately, and with mutual accountability mechanisms (Interviewee 2,2023). However, how wrong can technology get it when it does go wrong, and to what extent?

In reference to *Analysis & Production,* it comes in different forms at Company B (CIA, 2023; Interviewee 2,2023). Not only is there intelligence products that are pledged to be as unbiased as possible by the CEO, but the company has eagerly been involved in conferences such as the anti-corruption summit (Interviewee 2,2023). There are freely accessible resources and blogs on the company website which explain all the initiatives that the company enthusiastically involves itself in outside of the old intelligence product model (Interviewee 2,2023). This means that the company has a diverse way of analysing and producing intelligence that isn't simply a financial exchange (CIA, 2023; Interviewee 2,2023).

Dissemination phase, is another strong category for Company B, as they develop their own ethical framework, which hopes to have a profound impact on the intelligence industry by doing much like what this dissertation intends: to provide a simple point of analysis and accountability for companies that are having to operate in an increasingly confusing and growing industry (CIA, 2023; Interviewee 2,2023). This dissertation can therefore confidently assess that Company B is strongest in *Collection and Dissemination* phase, as not only have they devised self-accountability mechanisms, but they are actively trying to set a benchmark for other companies (CIA, 2023; Interviewee 2,2023). The ethical framework also sets a strong precedence for the industry, and creatively seeks to address an issue that the company is in no way obliged to do (Interviewee 2,2023). Limitations that the dissertation sees to this, is how technology and human analysts will interact in future, and in turn how accurate and ethical analysis will be, as they forge into uncharted territory.

Therefore, our story of Company B's ethical and benign nature, comes to an end. Having narrated the unique ethical function of their ethical framework, and assessed them against our framework, we have not only got an intimate view of their ethical processes, but of how the intelligence sector is evolving ethically (Interviewee 2,2023). Therefore, Company B's positive and benign function, can be attributed to its transparency of processes, which can be argued to have the biggest impact on global governance issues, as they will set an example for other companies (Interviewee 2,2023). We have also brought the human factor into our analysis, by examining the CEO's decision-making processes with ethics, which may not have been achieved by an organisation alone (Interviewee 2,2023).

Company C's benign function, can be defined by the onus it places on itself to evolve ethically (Interviewee 3,2023). The company has taken the initiative to develop a new accountability mechanism, as an internal memo (Interviewee 2,2023). This may seem innocuous at first, but this is a big stride for the industry, as it limits the use of AI or generative tools in order to collect intelligence for the company, ensuring that clients receive trusted and ethical intelligence, that is centred around accuracy (Interviewee 3,2023). For the purpose of the case study, we interviewed a senior lead analyst who is also a founder of their own intelligence company (Interviewee3,2023). Company C is a Strategic Intelligence and Advisory Firm, that from an ethical point of view, excels in supply chain analysis for firms such as Amazon, where they ensure environmental concerns are mitigated by intelligence gathered (Interviewee 3,2023). This also fundamentally helps companies look after each other, and transform global governance issues through in-depth and consensual accountability incentives (Interviewee 3,2023).

The company also sees ethics as a self-imposed obligation rather than something that should necessitate extensive international legal regulation (Interviewee 3,2023). Interviewee 3 mentioned that they have clear moral boundaries, in order to implement this sentiment

(Interviewee 3,2023). For example, you are explicitly banned from impersonating another individual during intelligence gathering (Interviewee 3,2023). Uncredible sources are also not allowed, in order to ardently avoid misinformation and disinformation, which are a growing issue (Interviewee 3,2023). Embedded Analysts are also trained alongside local teams, in order to integrate business functions ethically and ensure intelligence gathering is done with context in mind (Interviewee 3,2023). This shows the human facet intelligence, as AI is limited, and ethical boundaries self-imposed, meaning that there is strong confidence in individual morality (Interviewee 3,2023). This could be argued to lack stringent accountability, however.

How the company *Plans and directs* intelligence can be seen through how the company co-ordinates information gathering in line with client demand, which goes hand in hand with global governance issues (CIA,2023, Interviewee 3,2023). As a strategic firm, it also endeavours to pre-empt client needs in future which also in turn links to global governance issues (Interviewee 3,2023). In lieu of *Collection* stage, Company C prides itself on discernment of sources, but also on local knowledge (CIA,2023, Interviewee 3,2023). As C-suite executives in the company are less likely to understand the cultural nuances of information gathered, this is a vital, and essential ethical component of the *collection* stage (CIA,2023, Interviewee 3,2023).

With *Processing* stage, the company regulates itself even further, by limiting use of AI, in order to counter disinformation, and provide legitimate human analysis and counter disinformation (CIA,2023, Interviewee 3,2023). However, the company also recognises that this is almost impossible to completely counter, as one person's interpretation of data, can be completely different to another's (Interviewee 3,2023). Through *Analysis & Production* the team at Company C, work largely independently to analyse and produce reports which means that the team are to a certain extent protected from group think, but the flip side to this is that their may be barriers to accountability is team members are not working together to provide opposing opinions (CIA,2023, Interviewee 3,2023).

Dissemination at Company C is very stringently centred on the client relationship, and the impact of their analysis (CIA,2023, Interviewee 3,2023). Because of this, they naturally hold themselves to higher standards ethically because of the repercussions of creating a sub-standard product (Interviewee, 3,2023). Company C is strongest at *processing and collection stage* because of its emphasis on local knowledge, relationships with contacts outside of the company and the speed in which it came up with a framework in order to counter issues arising from the rise in AI (CIA,2023, Interviewee 3,2023). However, the dissertation does see limitations to this. As with all the companies, the matter of producing unbiased analysis is almost impossible to mitigate.

It's clear that through our narrative and analysis, that Company C centers self-regulation at the heart of how it operates ethically, making that its primary benign function (Interviewee 3,2023). Moral boundaries are at the epicenter of its function, with the client relationship fundamentally holding itself to account as business would not continue to come in if high standards were not adhered to (Interviewee 3,2023). The company takes a macro and micro perspective by embedding analysts and understanding the local and global impact of their analysis, which also brings a human facet to its operational capacity (Interviewee 3,2023).

Company D represents benign practice, by basing the majority of its functions around tackling specific global governance issues, such as financial crime (Interviewee 4, 2023). Its fundamental function, is as a financial crime risk company, using a unique technological platform in order to gather intelligence and create products for clients(Interviewee 4, 2023). This plays a demonstrable part in the ethical evolution of the intelligence industry, and in combatting key global governance issues, as the very constitution of the company is a transformative mechanism in itself (Interviewee 4, 2023). It works to tackle financial crime in specialist areas such as Money laundering, Sanctions, Bribery and Corruption, Fraud, Tax evasion, to name a few (Interviewee 4, 2023).

We interviewed the companies head of investigations, for the purpose of this case study (Interviewee 4, 2023). The interviewee mentioned that they operate ethically within the UN Sustainable Development Goals, and their function reflects ethical accountability, as they work on both micro and macro issues that could easily transform into a prevailing global governance issue (UN, 2015; Interviewee 4,2023). Interviewee 4 mentioned that the EU is specifically requesting due diligence functions within companies, and thus the interviewees company function, is all the more relevant (Interviewee 4, 2023). The company also brings the human factor into its operations, by its use of HUMINT making the human face of intelligence, all the more relevant (Interviewee 4, 2023).

In reference to *Planning & Directing* intelligence, Company D was exceptionally reflective in its processes (CIA,2023; Interviewee 4,2023). It gave the example of a client who is a venture capital firm in Sub-Saharan Africa, who plans and directs investments in local start-ups, aiming at benefitting and growing the local community (Interviewee 4, 2023). Even though the premise of this is very positive, Company D stressed that the potential for corruption in these financial exchanges is very high and therefore the company plays an important role in bringing the issues to light for the client (Interviewee 4, 2023). As a result, Company D *plans and direct*s information gathering in a way that is multi-faceted, and balanced as it looks into issues from all angles by helping companies be self-reflective even if their intentions are completely good (Interviewee 4, 2023).

With *Collection***,** Company D is the only company interviewed that also engages in HUMINT (CIA,2023; Interviewee 4,2023). Some may say that the ethical implications of HUMINT in the private sector may be huge, after discusses this as a process of collection, the company representative gave assurance that HUMINT looks more like the processes of journalism, with consensual interviews and investigations taking place, rather than any crossing of boundaries with the right to privacy (Interviewee 4, 2023).

Issues were mentioned by Company D with *Processing,* which also effects most intelligence companies, as when data is stored it can at any time be seized by law firms and thus sensitivity and ethics of data storage and processing is of the utmost importance (CIA,2023; Interviewee 4,2023). Company D stipulated that they haven't got access to huge financial resources, and therefore they are unable to go to third party data sources, or get much third party involvement in general- thus impacting their *Analytical and produc*tive capability (CIA,2023; Interviewee 4,2023). We can see this as the company having more exclusive control over its analytical processes, as its ethical information gathering is largely in its own hands.

This dissertation assesses that Company D scores highly on *Dissemination* also, as it has its own board of ethics, and is also registered as a B Corp, meaning that it can be internally and externally assessed to be having a profound global impact, and stringent information gathering processes (CIA,2023; Interviewee 4,2023). However, Company D can be assessed to be strongest at *Planning and direction* stage and *Dissemination*, as its very function is based on ethical practice, holding itself to high ethical standards both internally and externally (CIA,2023; Interviewee 4,2023). It is exceptionally difficult to gain B Corp verification, and thus we can assess this company scores higher in ethical practice than its peers, due to the stringent regulations surrounding this (Interviewee 4, 2023). Particularly maintaining this, alongside having an integrated HUMINT function (Interviewee 4, 2023). Its limitations, lie in its exclusive addressing of financial crime (Interviewee 4, 2023). This may lead to a neglect of other pertinent global governance issues.

Within our story, we see Company D providing a vital ethical function, as it places its operational capacity at the nucleus of global governance issues, whilst also understanding implications of issues on a micro, and local level (Interviewee 4, 2023). It is therefore proactive in its ethical practice, as it seeks to support ethical practice in the industry through its day to day functions, and strict code of practice (Interviewee 4, 2023). It has identified financial crime as a key perpetrator of illicit activity, focusing on this as its specialism meaning that it does not ethically spread itself too thin(Interviewee 4, 2023). The human factor, comes from its HUMINT function, which ethically enables human decisions that would otherwise be automated (Interviewee 4, 2023). Limitations to this, can be said to be that even though its analytical processes do not involve as many third-party data sources, this could also lead to an echo chamber of data collected, potentially leading to unconscious bias in future products.

Company E is a Global Risk Analysis company that uses embedded operations, threat monitoring and reputation risk services within a strategic advisory capacity (Interviewee 5,2023). It has won the Queens Award for services gathering intelligence (Interviewee 5,2023). Its ethical boundaries are stringent, having developed its own internal framework, which makes it's benign nature better attributed to its ability to hold itself accountable, and contribute ethically high standards of work (Interviewee 5,2023). It is a market leader in networking and knowledge sharing in the industry as well as creating an exceptionally high standard of product through practical and solution orientated products (Interviewee 5,2023). For the purpose of this interview, we interviewed an Embedded Intelligence Analyst who represented the company (Interviewee 5,2023). The human factor during this interview, came from the humanistic analysis that the interviewee provided about ethics in relation to diversity and inclusion, which no other company provided (Interviewee 5,2023).

Company E brings up important and prevalent ethical issues in the intelligence industry which also impacts this company, one in particular being a lack of diversity and inclusion, which inevitably has the potential to lead to biased intelligence gathering, and processes (Interviewee 5,2023). They use the example of attending conferences, and there being a lack of representation, particularly of black women (Interviewee 5,2023). Female representation is seen as a particularly prevalent issue, in reference to accessibility to senior positions.

Equally regional desk analysts may not even be individuals from that region (Interviewee 5,2023). For example, a middle east regional analyst may not be from the Middle East (Interviewee 5,2023). They mentioned that barriers to representation, lie in the intensity of the industry, and that being difficult in order to have a work life balance (Interviewee 5,2023). This rests on the client led nature of the industry, but also that it is impossible to predict when cataclysmic political events will take place, meaning that it is difficult for family led individuals, which can disproportionately effect women (Interviewee 5,2023). Interviewee 5 also mentions that there is a lack of visibility of the risk sector for minorities, as this is rarely included in career talks or services at university (Interviewee 5,2023). This sees Company E representing a positive function of intelligence, through self-reflection, and being unafraid of pointing out weaknesses in processes of the sector in general (Interviewee 5,2023).

Company E *Plans and directs* its intelligence in a way that responds imminently to unravelling political situations, as well as being ready for future occurrences by maintaining exceptionally well trained and specialised teams that collaborate and knowledge share, industry wide (CIA,2023; Interviewee 5,2023). This makes it reflexive in its ability to *plan and direct* intelligence, by its responsiveness and predictive capacity to world events, and therefore more ethical, as its mechanisms support its ability to engage and respond to world events (Interviewee 5,2023). As the company representative mentioned, *Collection* can be difficult when the team has a lack of diversity across the industry (CIA,2023; Interviewee 5,2023). Hence information that may be gathered on say, Africa may not be collected by someone from the region, meaning it has the potential to be misconstrued, or the nuances missed (Interviewee 5,2023). However, the representative did mention that there is a cross pollination between analysts on different client contracts, meaning that knowledge is shared in an effective and collaborative way that could potentially seek to fill in the gaps (Interviewee 5,2023).

From the interview, Company E is a market leader in *processing* intelligence in a very time efficient way, which could be deemed as more ethical because of response times saving lives (CIA,2023; Interviewee 5,2023). Company E's representative stated that this was the companies area of strength ethically as *Analysis* has been rated by clients as reflective of an exceptionally high standard (CIA,2023; Interviewee 5,2023). This accuracy and reputational feedback can be associated with a higher standard of ethics, as they are rated both by the Queens award, and by clients, as leading the way with their products (Interviewee 5,2023). Another area of strength for the company is *Dissemination*, as their intelligence was vital in the emergence of the Ukraine/Russian conflict, meaning that they have ethically applied themselves to pertinent global issues and successfully been a part of transforming issues on the world stage, in a positive way (CIA,2023; Interviewee 5,2023).

Company E demonstrates how an efficiency of processes, can positively impact ethical standards and that important indicators of a companies standard of ethics is not only external awards, but an ability to make an impact on the world stage and in the strength of client relationships (Interviewee 5,2023). The representative was the most reflective out of the interviewees, highlighting that diversity and representation may have a huge impact on the ethical operational capacity of the industry as a whole, which added an interesting layer of analysis to the report (Interviewee 5,2023). It has also provided a unique point of analysis for ethical issues surrounding intelligence, instead of a process driven answer the representative provided a people driven one which makes this research much more well-rounded and human orientated, giving us a deeper insight into the cultural and practical issues surrounding intelligence (Interviewee 5,2023). The company therefore provides high ethical standards through its rigorous recruitment program, in-house training and multi-faceted product which represent its benign function (Interviewee 5,2023). Limitations to this have been seen through accessibility to the company, and sector for minorities, and regional analyst integration (Interviewee 5,2023).

As a result, we see all of these case studies representing a positive function of intelligence, and their storyline within the intelligence cycle, in the context of our ethical framework (CIA, 2023). Company A, with its morally founded business strategy and its strength at Collection and Analysis stage, which can be seen through its selective processes when it comes to clients, and its emphasis on trusted sources (CIA,2023; Interviewee 1,2023). We have equally explored Company B's narrative and commitment to transparency of processes, and the major leaps it has been taking, to transform the intelligence sector, and support a universal accountability framework (Interviewee 2,2023). Its strength at *Collection and Dissemination* phase, seen through its embedded self-accountability mechanisms, and source legitimacy and transparency (CIA,2023, Interviewee 2,2023).

Company C also assumes a positive role in the industry, through embedding analysts to address ethical issues and macro and micro global governance issues (Interviewee 3,2023). Its strengths have been shown to lie at processing and collection stage because of its ability to mitigate ethical issues with its business relationships, and ultimately self-reflect (CIA,2023; Interviewee 3,2023). Company D's commitment to ethics and narrative within it, stems from the way the business is constituted around fundamentally tackling major global governance issues, such as financial crime (Interviewee 4,2023). We see this as them being strong at *Planning and Direction*, and *Dissemination* phase because of its function being certified externally and internally, at high standards of ethical practice, and its product directly impacting global governance issues (CIA,2023, Interviewee 4,2023). Company E also takes on a positive role, by leading the market in analysis during global crisis, and being reflective in their own areas of weakness (Interviewee 5,2023). Its efficiency of processes, represents a positive ethical role, in itself, reflecting its strongest facet in the ethical framework (Interviewee 5,2023). We also recognise that all have limitations to these benign functions, yet the aim of this section was to shift the focus to positive functions of the sector. This shows private sector intelligence, to be a positive contributing factor to transforming global governance issues, and that the intelligence cycle still has significant merit in ethical assessment (CIA, 2023).

Chapter 6

Analysis of Case Studies and application to global governance issues

"*The current global governance system is not properly equipped to manage the growing integration and interdependence amongst countries*" (UNCD, 2014, p. 4). As one of the prevailing global governance issues from the introductory chapter, we can pair this with the pattern and theory from the case studies, that private sector intelligence companies are now forming a latent part of the global governance system and are helping governments and private sector clients alike, to increase information sharing, and positive interdependence across borders (Forman, 2006, p. 55). We can theorize this, to be helping clients to strategically deal with threats and issues emerging from increasing integration (UNCD, 2014, p. 4). We will also look to answer one of the fundamental research questions: *can intelligence be applied to global governance issues in a way that doesn't exclusively function through espionage (Glassman, 2012, p. 673)?*

This shows Adriana's description of *"the murky rise of risk practitioners"* to neglect this positive macro application of the intelligence industry, the many positive facets of intelligence companies and their analysts, and their ability to transform global governance issues (Adriana, 2021, p. 10). As Matey rightly stipulates "*the proper application of the principles of intelligence can encourage better decision-making capabilities, particularly in response to global crisis, and the complexities of the world at present"* (Matey G. , 2013, p. 272). In practice, we see all 5 companies contributing positively to issues arising from interdependence (Interviewee 1,2023; Interviewee 2;2023; Interviewee 3;2023;Interviewee 4;2023;Interviewee 5;2023). Company A addresses the ethical and global issue of an increase in potentially malignant clients due to cross-border security threats and interdependence (UN,2015; Interviewee 1,2023). They address this by a selective process with initial vetting process of clients and by not engaging in clients that are involved in interdependent global issues, such as Russia (Interviewee 1,2023).

Company B does this through its integration of global and local ethical frameworks into its operations, which is an important part of upholding the legal and ethical fibre of the industry, and of acting as a barrier to global governance issues and integration, as the mix of legal and ethical standards become more and more hard to understand, and operate within (Interviewee 2,2023). Company C and D does this, through applying themselves to interdependent and cross border global governance issues, such as financial crime and the rise in AI, and Company E does this through integrating their intelligence gathering processes with local security operation centres meaning that they are encouraging positive interdependence through knowledge sharing (Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). This puts a human face to private sector intelligence, digressing from its surface-level *"commercialisation",* in the literature (Crane, 2011, p. 233).

As a result, we can see beneath the confines of intelligences glamourized image, and reveal its positive functions (Marie, 2001, p. 2). Equally, in reference to earlier literature that pointed to the vital need for innovation and creativity in the intelligence sector, we can see how these companies attack these global governance issues, in ultimately creative and responsive ways, and how their processes can continue to be applied to new threats that will continually emerge from the constantly evolving global scene (Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). Hence the continued threats of both Russia and China that have continued to emerge due to interdependence, and the prevalent "*cyber cold war*" mentioned by Mueller, can be addressed in part by the intelligence gathering processes of these companies, and their embedded ethical protocol (Mueller, 2013, p. 20).

Our second global governance issue "*The current system is currently marked with asymmetries in terms of access, process and outcomes*" reveals the ability of private sector intelligence to add to a re-balance of this asymmetry, by encouraging similar access to intelligence products, rather than more powerful states harbouring the majority of intelligence through secretive government mechanisms (UN, 2015). However, some may argue that this further plays into asymmetries on the world stage, as those with more resources, are able to access more intelligence products, through a handful of powerful intelligence companies (Shorrock, 2018). In response, this dissertation would argue even if that is the case, private sector intelligence companies do provide a role of morality, where they re-balance the world stage, by refusing to engage with actors engaging in foul play (Ventura,2023; Interviewee 1,2023). Therefore, private sector intelligence can be argued to have a lasting impact on the asymmetry of the world stage, which may even work to counter-balance the omnipotence of the US in the intelligence sector (Johnson,1996,p23)

Consequently, this also reframes the notion of intelligence failure (Lomas, 2021). Failure in the private sector can be attributed to a particular company rather than an entire state, which can be argued to contribute better to peace, as company culpability holds much less of a devastating effect (Sturgis, 2013). Equally, this demonstrates the malleability of the *"commercialisation of intelligence",* and how it can be applied in a positive way, providing an arbitrary, and hopefully neutral function, on the world stage (Crane, 2011, p. 233). Take the company Sibylinne, for example (Sibylinne, 2023). By covering a range of different sectors as a security consultancy, they cover a wide berth of intelligence knowledge, meaning that they can knowledge share between projects, and exchange expertise in an equalising way (Sibylinne, 2023). This shows how the private sector can bridge the gap in asymmetry (UN, 2015).

Company A addresses asymmetry by placing its operations outside of traditional powers, meaning that it helps by its very existence, to re-balance intelligence gathering functions, and infrastructure on the world stage (Birdsall,2003; Interviewee 1,2023). Company B works towards this, through its pursuit of transparency of sources, meaning that it addresses imbalances when it comes to source acquisition, and as a consequence, sets a self-regulating and ethical benchmark that equally applies to all clients (Interviewee 2,2023). Company C does this by tackling issues that do not discriminate, meaning its function as an intelligence gathering consensual accountability mechanism aids the re-balancing of asymmetrical global players (Interviewee 3,2023). Company D also does this, through its due diligence practice. By these companies taking on these functions, working towards self-imposed accountability, this sets a standard for the industry, and its *"professionalization"* (Morrow,2022,p2; Interviewee 4,2023).

As a result, companies race to raise their standards, much like in the 'competitive business model', where in order to stand out from one another and remain market leading, they must do better than one another (CP, 2023). Meaning that all clients have to embed accountability mechanisms, and this does not effectively discriminate in favour of asymmetrical actors. Company E does this by creating products that unite rather than divide, as global issues are addressed equally and with balanced urgency (Interviewee 5,2023).

Moving on to our third global governance issue, we can see that private sector intelligence companies and issues concerning the shrinking of government mechanisms and lack of regulation in the emerging intelligence industry, are addressed by companies self-regulating (Crane,2011;p3; Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). This prognosis is backed up by literature such as *"A public role* *for the private sector",* where self-regulation is seen as a necessity for the private sector, because of the states shrinking role (Haufler, 2001, p. 6).

This is done by creating stringent ethical benchmarks and operating procedures, which in turn are held accountable by clients. "*Global rules have led to a shrinking of the policy space of national governments, particularly of developing countries in ways that impede the reduction of inequalities within countries and is well beyond what is necessary for an efficient management of interdependence*" (UNCD, 2014, p. 4). This global governance issue is of course, not solved by private sector intelligence, but the pattern and impetus of these companies in managing interdependence and regulating themselves can be argued to be more functional than was previously thought, prior to conducting this dissertation (Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). Bob Constantain sees this management of interdependence as a *"regional tool"*, where mutual technology, and private-public sector partnerships will define the emerging political landscape (Constantain, 2010, p. 71). This is effectively what private sector intelligence, is doing anyway.

As a bi-product, we can see small steps in the direction of transforming intelligences perceived, malignant image, as private sector intelligence takes its own initiative to be a functioning part of the global governance system (Hutton, 2009,p22; Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). This goes hand in hand with tackling politicisation and state-centrism, as we recognise the latent role that private sector intelligence, has in fact been playing at holding even the state to account through its due diligence function and overtaking it in positive and creative intelligence functions which can be observed, through our case studies (FPI, 2023; Wesley, 2010, p. 20; Coletti, 2017, p. 65; Agrell, 2021, p. 25). We can also observe that not only have private sector intelligence companies created their own ethical and governance mechanisms, but they have notably added to the current lacking global and ethical framework by addressing ethical issues not just theoretically, but in practice also (Pun,2023; Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023) .

Company A tackles the lack of government regulation of the industry through taking its own initiative, and owning its intelligence cycle to make it the best it can be, for its clients (Pun,2023; CIA, 2023; Interviewee 1,2023). Whereas company B stands out, by developing its own originally developed ethical framework which will help to regulate other companies and state intelligence functions, alike: which has been much demanded by academics within the intelligence industry (Bellaby,2012, p24; Interviewee 2,2023). However, we must also say, that this cannot substitute regulation completely, and as the continued emergence of the industry rapidly increases, this dissertation would recommend both a state and private sector accountability mechanism that coalesces and that provides empirical consequences, for digression (Morrow, 2022). Company C, D and E also positively contribute to this pertinent global governance issues, by either working in parallel or in cohesion with government functions, in order to manage interdependence positively (Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023).

However, there are limitations to this. As Hutton identified earlier on in this piece and the companies themselves, in the case study research, there are teething issues with such rapid professionalization (Hutton, 2009, p. 10). The intelligence sector is consistently enmeshed with intelligence failures that have a profound global impact, and some intelligence companies do in fact overstep ethical and moral boundaries in the pursuit of profit (Betts, 1978, p. 62; Helfont, 2023; Lundborg, 2022, p. 23). The companies themselves have admitted that there is a real need for a consolidation of intelligence legislation and benchmark for the industries empirical operations, as it is inevitable that some will take advantage of the lack of clarity with this (Bellaby,2012,p24; Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). As Voelz points out, the widening berth of contracted labour in the emerging private sector intelligence community, poses similar due diligence issues as when corporations move their supply chains abroad, and outsource vital functions (Voelz, 2009, p. 587). Therefore, who is holding these people to account, in a sector that has been used to operating in its own sphere for many decades (Leigh, 2015, p. 255)? Hence, we must take intelligences positive functions, in the context of its weaknesses, in order to encourage accountability and continued transparency.

As a result, our analysis produces a telling story: that intelligence can in fact be used for benign purposes and be applied to global governance issues. There is evidently no way that the intelligence sector alone can solve global governance issues, but we can see that contrary to the literature, intelligence companies have played a significant role in transforming these global governance issues through competent self-regulation, and acting as a consensual accountability mechanism for clients, who naturally compete to provide the highest ethical standard of practice (Stone, 2012; Breakspear, 2012, p. 678; Colibasanu, 2009, p. 2). What’s missing, is naturally entrenched legislation and accountability frameworks (Pun, 2023).

We also see through this analysis, that crucial factors such as transparency of sources, client selection, and making intelligence accessible to a range of clients plays a part in levelling the global playing field and addressing issues concerning interdependence and lack of regulation in the industry (UN,2015; Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). In answer to the research question, we can see that intelligence can quite obviously be applied to significant global governance issues, that are outside the remit of espionage and as a result, can have a profound global impact (Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). The main patterns and theories identified through grounded theory, are that private sector intelligence companies are now forming a latent part of the global governance system, levelling the playing field, and self-regulating which make up the persistent factors that show intelligence to be a growing industry, with positive facets (Holton, p8; Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023).

Chapter 7

Conclusion

It’s natural to finish this dissertation with a summary of answers to questions asked at the beginning of this piece. In summary, intelligence is often associated with malignant practices because of it direct, and consistent association with intelligence failure and espionage which answers the first question: Why intelligence is so often associated with malignant practices (Stone, 2012; Breakspear, 2012, p. 678)? By exploring its positive application through the private sector, and its impact on global governance issues, we have been able to see its transformative function, whilst also bearing in mind its limitations (UN, 2015). This goes hand in hand with the next question: Can it be applied to global governance issues in a way that doesn’t exclusively function through espionage (Glassman, 2012, p. 673)? We have established through our case studies, that this is certainly the case, and that they are contributing exceptionally transformative and useful functions to global governance issues that aren’t just through espionage. With our next two questions: Why has the potential of private sector intelligence not been explored in-depth in the literature, and conceptually (Hough, 2011, p. 24; Freeman, 2021, p. 4)? We have established that this is down to a literary freeze of the sector in the cold war time period, as well as a lack of investment in funding and research (Andrew, 2010, p. 164).

We have taken five case studies and explicitly seen how intelligence functions outside of the remit of espionage, with Company A being a private sector security consultancy with hybrid intelligence functions, Company B being a due diligence and compliance intelligence company, C being a Strategic and intelligence advisory firm, D being a financial crime risk firm, and E being a Global Risk Analysis company (Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). We have utilised grounded theory in order to discover these patterns of intelligence gathering outside of espionage and these firms impact on global governance issues (Holton, 2008, p. 8). We can surmise that intelligence companies are now an important part of the global governance scene itself, as they work to level the asymmetrical world stage, and fundamentally self-regulate at this stage of their professionalization (Deibert, 2022, p. 240; Larkin, 2022; Sims, 2006, p. 8; Koniauko, 2023, p. 100).

We have also seen that the current accountability mechanisms in place for the sector are simply not fit for purpose, verified by the companies themselves (Rosenbach, 2009). This places the ethical framework developed by this piece, as all the more crucial, as it acts as a gauge for where the companies excel, and their operational weaknesses in line with the intelligence cycle, which in turn significantly impacts global governance issues (CIA, 2023; UN, 2015). Naturally answering the question Can ethics be applied to such a fast-growing and autonomous sector (Gill,2013, p93; Lin, 2011, p10;Puyvelde,2019,p21;Adriana,2021)? We have also recognised that this is difficult to fully entrench, although the impetus of the sector to self-regulate could balance this out as companies actively seek to hold themselves to account (Deibert, 2022, p. 240; Arnham, 2001, p. 151).

We have therefore also explored its potential conceptually, and discovered why it has not been explored conceptually previously, through the ethical framework developed, and empirical analysis. This was shown specifically through its application to the example of the WildfireSat mission, as an interagency attempt to prevent Canada Wildfires (GOC, 2023). This has aptly assessed the ethical implications of this mission, and has shown the framework to be operational when applied to a diversity of contexts (GOC, 2023).

Therefore, the aims of this dissertation have been fulfilled in a number of different ways. We have recognised and identified specific ways that private sector intelligence and their business models lend themselves to positively impacting world issues (Interviewee 1,2023; Interviewee 2,2023; Interviewee 3,2023; Interviewee 4,2023; Interviewee 5,2023). This has been shown through analysis of the five businesses, with an in-depth analysis of their impact on global governance issues. We have developed an original ethical framework to measure the impact of these businesses, and future ones bridging a gap in the intelligence sector that has not been bridged before (Bellaby R. , 2012, p. 75). This has also been applied to a international security issue, to show further real-world application. We have consequently addressed both the theoretical and empirical facets of the question, by an extensive review of the literature, and an in-depth case study analysis.

There are of course, broader implications to this research. By reframing the narrative of intelligence to a positive one, we have begun the impetus required to recognise it for its achievements, rather than saddling it with a negative and elusive image that encourages it to operate underground (Stone, 2012; Breakspear, 2012, p. 678). By doing so, we have set the scene for further innovation and research, that comes with a sector that is perceived as more benign. We have also established an ethical framework that can be used as a universal point of reference, and accountability mechanism which will work to make the sector, more transparent.

We have also recognised the gaps in the literature, and analysed current ethical frameworks, which will encourage further theorization of the sector. By using real life case studies, we have also gained live examples of current private sector intelligence activity, which gives the research significant legitimacy.

We can therefore surmise that intelligence, can in fact be used for benign purposes in order to solve current global governance issues. These global governance issues being the asymmetry of the world stage and increasing interdependence, as well as a concerted shrinking of national policy space leading to a largely unregulated emergence of the private intelligence sphere (UN, 2015). Private sector intelligence has been argued to positively contribute to these issues transformation, by self-regulation, consensual accountability mechanisms and aiding the evolution of the sector outside of the remit of espionage, as well as equalising imbalances in client's access to intelligence (Deibert, 2022, p. 240; Arnham, 2001, p. 151). Hence, we can see that private sector intelligence can continue to contribute positively to emerging world issues, if it continues to be applied properly, and with proper intention. We have also recognised that this has limitations, and the lack of entrenched framework, poses an imminent problem to the operational legitimacy of the sector (Omand,2012,p27;Defao,2007).

Bibliography

Advisory Board. (2022). *Addressing Cognitive Bias in Climate Change.* Michigan: Advisory Board. 22-56

Adriana, M. (2021). *The Professional Identity of Security Risk .* Portsmouth: University of Portsmouth 2-221

Aegis (2023) [Online] *Integrated Security*. Retrieved from AEIGS: https://www.aegissecurity.co.uk/ [Accessed 23 June 2023]

AEIGS. *Security and Investigations*. Retrieved from AEIGS: https://aegis.com/ [Accessed 16 June 2023]

Intelligence Africa (2023) [Online] *About Us*. Retrieved from Intelligence Africa: https://intelligenceafrica.com/Home/About [Accessed 01 May 2023]

Agrell, W. (2021). *Avoiding politicisation.* Oxford: Routledge.p25-30

Amnesty International (2023). [Online] *Torture*. Retrieved from Amnesty International: https://www.amnesty.org/en/what-we-do/torture/ [Accessed 15 May 2023]

Association of Risk Intelligence Professionals. (2023) [Online] *What is AIRIP?* Retrieved from Association of Risk Intelligence Professionals: https://www.airip.org/page/about [Accessed 03 May 2023]

Albrecht, P. (2017). *An Untapped resource: African forces in intelligence gathering: Inequality in Minusma.* Geneva: DISS Policy brief. 1-10

Andrew, C. (2010). Intelligence, International Relations and 'Under-theorisation'. *Intelligence and National Security*, 170-184.

Anguiano, D. (2018) [Online] *'Evacuation fatigue': Danger after people flee wildfires five times in two years*. Retrieved from Guardian: https://www.theguardian.com/us-news/2018/nov/13/california-wildfires-evacuation-fatigue-paradise-camp-fire [Accessed 20 July 2023]

Antara.(2020) [Online] *In & Out: The Dilemma of Competitive Intelligence outsourcing, solved*. Retrieved from Antara Information Technology: https://www.antara.ws/en/blog/in-out-the-dilemma-of-competitive-intelligence-outsourcing [Accessed 03 April 2023]

British Army.(2023) [Online] *Artificial Intelligence used on British Army operation for the first time*. Retrieved from Army be the best: https://www.army.mod.uk/news-and-events/news/2021/07/artificial-intelligence-used-on-british-army-operation-for-the-first-time/ [Accessed 01 January 2023]

Arnham, R. (2001). Business War: Economic Espionage in the US and European Union and the need for greater trade secret protection. *NCJ International*, 150-154.

Arpin, J. (2007). *The Tao of Spycraft: Intelligence Theory and.* Chicago: Naval War College Review.2-23

Auten, B.(2013) [Online]. *Examining Just Intelligence theory*. Retrieved from Political theology: https://politicaltheology.com/examining-just-intelligence-theory/ [Accessed 16 April 2023]

BAE.(2023) [Online]. *New multi-million pound investment to boost technologies for the UK's future combat aircraft*. Retrieved from BAE Systems: https://www.baesystems.com/en-uk/article/new-multi-million-pound-investment-to-boost-technologies-for-the-uk-s-future-combat-aircraft [Accessed 02 April 2023]

Bailey, C. (2016). The Moral-Ethical Domain and the Intelligence Practitioner. *American Intelligence Journal*, 49-58.

Barn, B. (2019). Mapping the public debate on ethical concerns: algorithms in mainstream media. *Journal of Information, Communication and Ethics in Society*, 1477-996.

Barr, K. (2023) [Online] *Hackers Take Control of Government-Owned Satellite in Alarming Experiment*. Retrieved from Gizmodo: https://gizmodo.com/hackers-control-government-owned-satellite-test-esa-1850383452 [Accessed 15 February 2023]

Bartes, F. (2013). *Five-phase Model of Intelligence* . Brussels: University of Agriculture. 3-31

Bartlett, J. (2015). Under the radar: How people keep security agencies in check. *Index on Censorship*, 101-105.

Bexar County Office of Emergency Management. (2023) [Online]. *The Five Phases of Emergency Managemen*t. Retrieved from Bexar County: https://www.bexar.org/694/Five-Phases#:~:text=Mitigation%20involves%20structural%20and%20non,and%20clearing%20areas%20around%20structures. [Accessed 10 July 2023]

Bean, H. (2021). Critical intelligence studies: introduction to the special issue. *Intelligence and National Security*, 467-475.

Bellaby. (2019). *Too many secrets? When should the intelligence community be allowed to keep secre ts?* . Sheffield: University of Sheffield. 21-35

Bellaby, R. (2012). Whats the harm? the ethics of intelligence collection. *Intelligence and National Security*, 93-117.

Bellaby, R. (2022). Intelligence and the just war . *Taylor & Francis*, 93-115.

Bellaby, W. (2022). Redefining the security paradigm to create an. *Intelligence and National Security*, 101-121.

Bellinger, J. (2022). How Russia's Invasion of Ukraine Violates International Law. *Council on Foreign Relations*, 2-10.

Bennett, R. (2012). *Espionage: Spies and Secrets.* Chicago: Chicago University Press.24-27

Betts, R. (1978). *Analysis, War and Decision, why intelligence failures are ineveitable.* Atlanta: Brookings institution. 60-151

Beydoun, K. (2022). On Terrorists and Freedom Fighters. *Harvard Law Review*, 101-110.

Birdsall, N. (2003) [Online] *Asymmetric Globalization: Global Markets Require Good Global Politics*. Retrieved from Brookings: https://www.brookings.edu/articles/asymmetric-globalization-global-markets-require-good-global-politics/ [Accessed 05 July 2023]

Bjorn-Muller-Wille. (2007). Improving the democratic accountability of EU intelligence. *Intelligence and National Security*, 100-128.

Blicharz, M. (2003). *Role of Industrial Espionage and Business.* Oxford: academia.edu. 1-10

Boren, D. (1991). The intelligence community: how crucial. *Foreign Affairs*, 1991-1993.

Born, H. (2007). Intelligence Accountability. In L. Johnson, *Handbook for Intelligence*. Oxford: Oxford University Press. 24-26

Bose, R. (2008). Competitive Intelligence Process and tools for intelligence analysis. *Industrial Management and Data Systems*, 25-37.

Breakspear, A. (2012). A New Definition of Intelligence. *Intelligence and National Security*, 678-693.

Britannica. (2023) [Online] *Intelligence in the Modern Era*. Retrieved from Britannica: https://www.britannica.com/topic/intelligence-international-relations/Intelligence-in-the-modern-era [Accessed 02 February 2023]

Business Research Methodology. (2006) [Online] *Interviews*. Retrieved from Business Research Methodology: https://research-methodology.net/research-methods/qualitative-research/interviews/ [Accessed 03 March 2023]

Bournemouth University.(2023) [Online]. *Professor discusses legal and ethical issues revealed in report on CIA's use of torture*. Retrieved from The Record: https://www.bu.edu/law/record/articles/2014/professor-discusses-legal-and-ethical-issues-revealed-in-report-on-cias-use-of-torture/ [Accessed 15 February 2023]

Crisis24.(2023) [Online]. *Solutions & Expertise*. Retrieved from Crisis24: https://crisis24.garda.com/ [Accessed 30 March 2023]

Caparini, M. (2007). *Controlling and Overseeing Intelligence Services in Democratic States.* Oxford: Routledge. 1-152

Carre, L. (2011). *Tinker, Tailor, Soldier, Spy.* London: Penguin Books. 5-27

Critical Disaster Programme. (2023) [Online] *2023 North American Wildfires*. Retrieved from CDP: https://disasterphilanthropy.org/disasters/2023-north-american-wildfires/?gclid=CjwKCAjw-7OlBhB8EiwAnoOEkw8ap6q1l7d9QcW4Niny_GRDdl0vYNKenO92-n637NGVGOmPiF2AzRoCt5UQAvD_BwE [Accessed 14 February 2023]

Cerulus, L. (2022) [Online]. *Could cyberattacks break Putin's will? Western leaders weigh options amid fear of escalation*. Retrieved from politico: https://www.politico.eu/article/west-cyber-operation-force-russia-back-off-ukraine/ [Accessed 03 April 2023]

Council On Foreign Relations. (2023) [Online].*The Taliban in Afghanistan*. Retrieved from The Council on Foreignn Relations : https://www.cfr.org/backgrounder/taliban-afghanistan [Accessed 30 June 2023]

Centre For Research and Evidence On Security Threats.(2018) [Online]. *Intelligence Ethics: Not An Oxymoron*. Retrieved from Centre for Research And Evidence On Security threats: https://crestresearch.ac.uk/comment/intelligence-ethics-not-an-oxymoron/ [Accessed 02 July 2023]

Chandra, B. (2021) [Online] *Collaboration or Chaos: Two futures for Artifical Intelligence and US National Security*. Retrieved from Modern War Institute: https://mwi.usma.edu/collaboration-or-chaos-two-futures-for-artificial-intelligence-and-us-national-security/ [Accessed 01 January 2023]

Chesterman, S. (2008). We Can't Spy … If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'. *Journal of European international Law*, 1055-1754.

Chris. (2016). The Moral-Ethical Domain, and the Intelligence Practioner. *Christopher Bailey*, 49-58.

Christafis, A. (2015) [Online] *It looked like a battlefield': the full story of what happened in the Bataclan*. Retrieved from the guardian: https://www.theguardian.com/world/2015/nov/20/bataclan-witnesses-recount-horror-paris-attacks [Accessed 03 May 2023]

Central Intelligence Agency. (2023) [Online] *CIA government website*. Retrieved from the intelligence cycle: https://www.cia.gov/spy-kids/parents-teachers/docs/Briefing-intelligence-cycle.pdf [Accessed 19 July 2023]

Cohen, R. (2010). Putting a Human and Historical Face on Intelligence Contracting. *ScienceDirect*, 232-251.

Coletti, G. (2017). Politicising intelligence: What went wrong with the UK and US assessments on Iraqi WMD in 2002. *Journal of Intelligence History*, 65-78.

Colibasanu, A. (2009). Between Intelligence and Espionage in the Contemporary Business Environment. *Ekonomika a Management*, 1-10.

Christchurch College. (2023) [Online]. *Will AI ever be conscious?* Retrieved from University of Cambridge: https://stories.clare.cam.ac.uk/will-ai-ever-be-conscious/index.html [Accessed 21 July 2023]

Constantain, B. (2010). Interdependence Between Public and Private Sector in Services - a Regional Development Tool. *Bucharest Academy of Economic Studies*, 50-71.

Cook, M. (2008). *Human Factors: the journal of human factors and ergonomics Society.* Cambridge: Sage Publications. 9-49.

Cornish, P. (2021). *The Oxford Handbook of Cyber Security.* Oxford: Routledge. 219-328

Competition Policy. (2023) [Online] *Why is competition policy important for consumers?* Retrieved from Competition Policy: https://competition-policy.ec.europa.eu/about/why-competition-policy-important-consumers_en#:~:text=Better%20quality%3A%20Competition%20also%20encourages,or%20friendlier%20and%20better%20service. [Accessed 01 May 2023]

Crane, A. (2011). In the Company of Spies: when competitive intelligence gathering becomes industrial espionage. *ScienceDirect*, 233-240.

Curtis, B. (1995). Taking the State Back Out: Rose and Miller on Political Power. *British Journal of Sociology*, 575-589.

Cusack, J. (2010) [Online] *The Intelligence Challenge: Lessons from the Private Sector*. Retrieved from Harvard Business Review: https://hbr.org/2010/11/intelligence-failure-what-the [Accessed 05 June 2023]

Cyphere. (2023) [Online]. *What is Corporate Espionage? Types, Examples and Myths*. Retrieved from cyphere: https://thecyphere.com/blog/corporate-espionage/#:~:text=Yes%2C%20corporate%20espionage%20is%20illegal,make%20you%20face%20criminal%20prosecution. [Accessed 17 July 2023]

Davies, P. (2002). Ideas of intelligence. *Harvard International Review*, 62-66.

Dearden, L. (2018). *Children being used to spy on terrorists, drug dealers and grooming gangs by British security services.* London: Independent Newspaper Report.

Deeks, A. (2016). Confronting and Adapting: Intelligence Agencies and National Law. *Virginia Law Review*, 599-685.

Defaeo, M. (2007) [Online] *What international law controls exist or should exist on intelligence operations and their intersections with criminal justice systems ?* Retrieved from Cairn: https://www.cairn.info/revue-internationale-de-droit-penal-2007-1-page-57.htm [Accessed 05 May 2023]

Deibert, R. (2022). Subversion Inc: the age of private espionage. *Journal of Democracy*, 213-240.

Demarest, G. (1995). Espionage in International Law. *HeinOnline*, 321-325.

Derian, J. D. (2008). Anti-diplomacy, intelligence theory and surveillance practice. *Intelligence and National Security*, 29-51.

Devlin, J. (1997) [Online] *Western Intelligence - Nothing More Than A Cold War Relic?* Retrieved from Journal of International Affairs: http://www.inquiriesjournal.com/articles/1167/western-intelligence--nothing-more-than-a-cold-war-relic [Accessed 03 February 2023].

Doherhty, B. (2023) [Online]. *Julian Assange 'dangerously close' to US extradition after losing latest legal appeal*. Retrieved from Guardian: https://www.theguardian.com/media/2023/jun/09/julian-assange-dangerously-close-to-us-extradition-after-losing-latest-legal-appeal [Accessed 06 February 2023].

European Court of Human Rights. (2022). *Mass Surveillance.* Brussels: European Court of Human Rights 2-20.

Elgot, J. (2016) [Online] *Tony Blair could face contempt of parliament motion over Iraq war*. Retrieved from The Guardian: https://www.theguardian.com/politics/2016/jul/10/tony-blair-contempt-motion-iraq-war-mps [Accessed 29 May 2023]

Erinys. (2023) [Online] *About Us*. Retrieved from Erinys International: https://www.erinys.net/ [Accessed 07 March 2023]

Evans, M. (2018). *China accused of planting spy chips in Pentago computers.* New York: The Times Newspaper.

Eventon, R. (2016). *Above the Law, Under the Radar.* Swansea: Swansea University. 1-23

Fabre, C. (2022). *Spying through a glass darkly.* Oxford: Oxford University Press 10-16

Federal Bureau of Investigation. (2023) [Online] *Major Cases*. Retrieved from FBI Counterintelligence: https://www.fbi.gov/investigate/counterintelligence/major-cases [Accessed 01 February 2023]

Fisher, M. (2013). *North Korean propaganda video 'explains' what life is really like in Western countries.* Washington: Washington Post Newspaper.

Forman, S. (2006). New Coalitions for Global Governance. *Global Governance*, 51-72.

Foreign Policy Institute. (2023) [Online] *Politicisation of the intelligence community is extremely dangerous*. Retrieved from Foreign Policy Institute: fpri.org [Accessed 30 May 2023].

Freeman, B. (2021). *The role of the private.* New York: International Law Programme and Asia-Pacific Programme. 4-64

Freeze, C. (2014). *Privacy or national security: Have spy agencies gone too far?* NYC: The globe and Mail Newspaper.

Frisk, R. (2020). From Samurais to Borgs: Reflections on the. *International Journal of Intelligence and*, 70-96.

Frunza, M. (2021) [Online] *The Rise of Private Intelligence*. Retrieved from IntelBlitz: https://schwarzthal.tech/en/research/intelblitz-38-the-rise-of-private-intelligence [Accessed 17 January 2023].

G4S. (2023) [Online] *G4S*. Retrieved from who we are: https://www.g4s.com/en-gb [Accessed 15 June 2023].

Geldron, A. (2007). Just War, Just Intelligence: An Ethical Framework for Foreign Epionage. *International Journal of Intelligence and Counter-Intelligence*, 398-434.

Gentry, J. (2008). Intelligence Failure Reframed. *Political Science Quarterly*, 247-270.

Gibson, S. (2009). Future roles of the UK intelligence system. *Cambridge University Press*, 100-110.

Gill, P. (2013). The Implications of Intelligence Practice Within and Beyond the State: An Analytical Model. *Journal of Regional Security*, 93-110.

Gill, P. (2019). *Intelligence theory: key questions and debates.* Oxford: Routledge. 200-205

Glassman, M. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *ScienceDirect*, 673-682.

Global Medic. (2023) [Online] *Canada Wildfires 2023*. Retrieved from Global Medic: https://globalmedic.ca/canada-wildfires-2023/?gclid=CjwKCAjw-

7OlBhB8EiwAnoOEkwUf7nSUKElyGhbnJMdGGIREv7JW3pGwV5MKy0vFw-0R0CRZKfyooxoCYNAQAvD_BwE [Accessed 20 July 2023].

Government of Canada. (2023) [Online] *WildFireSat: Enhancing Canada's ability to manage wildfires*. Retrieved from Government of Canada: https://www.asc-csa.gc.ca/eng/satellites/wildfiresat/ [Accessed 01 February 2023].

Goldman, J. (2006). *Ethics of Spying: A Reader for the Intelligence Professional, Volume 1.* Maryland: Scarecrow Press. 22-250.

Goldman, J. (2010). *Ethics of spying: A reader for the intelligence professional.* Oxford: University of Oxford Press.5-23.

Gregory, A. (2022). *What happened in the Salisbury Poisonings?* Oxford: The Independent Newspaper.

Hannas, W. (2021). *China's Quest for Foreign Technology: Beyond Espionage.* New York: Routledge. 7-45.

Hardy, J. (2023) [Online] *MI5 chief 'profoundly sorry' agency did not prevent Manchester Arena attack*. Retrieved from The Telegraph: https://www.telegraph.co.uk/news/2023/03/02/mi5-missed-significant-opportunity-prevent-manchester-arena/ [Accessed 01 April 2023].

Harknett, R. (2011). The Struggle to Reform Intelligence after 9/11. *Public Administration Review*, 700-706.

Hartwig, B. (2023) [Online] *Cybersecurity and New Technologies*. Retrieved from Hackr: https://hackr.io/blog/cybersecurity-and-new-technologies [Accessed 19 March 2023].

Haufler, V. (2001). *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy.* Routledge: Oxford. 6-28.

Haydon, M. (2013) [Online] *Former NSA chief: western intelligence agencies must be more transparent*. Retrieved from the Guardian: https://www.theguardian.com/world/2013/sep/30/nsa-director-intelligence-public-support [Accessed 03 June 2023].

Helfont, S. (2023) [Online]. *The Iraq wars Intelligence failures are still misunderstood*. Retrieved from war on the rocks: https://warontherocks.com/2023/03/the-iraq-wars-intelligence-failures-are-still-misunderstood/ [Accessed 04 June 2023].

Henstra, D. (2005). Canadian Disaster Management Policy: Moving toward a Paradigm Shift? *Canadian Public Policy / Analyse de Politiques*, 303-318.

Herman, M. (2010). Ethics and Intelligence after September 2001. *Intelligence and National Security*, 342-358.

Holton, J. (2008). Grounded Theory as a General Research Methodology. *Grounded theory, an International Review*, 5-50.

Horowitz, M. (2018). *American Defense Policy.* New York: John Hopkins University Press.370-373.

Hough, M. (2011). The conceptual structuring of the intelligence and counterintelligence processes: enduring holy grails or crumbling axioms --quo vadis? *Strategic Review for South Africa*, 20-25.

Human Rights Watch. (2023) [Online] *Shamima Begum Ruling a Dark Stain on The UK Jusstice System*. Retrieved from Human Rights Watch: hrw.org [Accessed 05 May 2023].

Hughes, O. (2022) [Online] *Automation could make 12 million jobs redundant. Here's who's most at risk*. Retrieved from ZDNet: https://www.zdnet.com/article/automation-could-make-12-million-jobs-redundant-heres-whos-most-at-risk/ [Accessed 02 June 2023].

Hulnick, R. (2014). *The future of the intelligence process: The end of the intelligence cycle?* Oxford: Routledge. 42-49.

Hutton, L. (2009). To spy or not to spy? Intelligence and democracy in South Africa. *Institute for Security Studies Monograph*, 20-43.

India Times. (2023) [Online] *Satellite TV firm Dish confirms ransomware attack, loses data of 300K workers*. Retrieved from Economic Times: https://hr.economictimes.indiatimes.com/news/industry/satellite-tv-firm-dish-confirms-ransomware-attack-loses-data-of-300k-workers/100490123 [Accessed 21 March 2023].

Institute for Electrical and Electronic Engineers. (2023) [Online] *Competitive intelligence on the World Wide Web*. Retrieved from IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/799128 [Accessed 20 February 2023].

IESE University of Nevarra. (2015) [Online] *Why is it hard to be ethical in business?* Retrieved from IESE Business School: https://blog.iese.edu/ethics/2015/07/09/why-is-it-hard-to-be-ethical-in-business/ [Accessed 12 July 2023].

Ingleton, D. (2022) [Online]. *A year on from the Pegasus project, governments still have access to surveillance technology*. Retrieved from The Guardian: https://www.theguardian.com/commentisfree/2022/jul/18/pegasus-project-surveillance-tech-spying-nso-group [Accessed 04 April 2023].

IRP Intelligence Threat Handbook. (2023) [Online] *Operations Security*. Retrieved from Intelligence Collection Activities and Disciplines: https://irp.fas.org/nsa/ioss/threat96/part02.htm [Accessed 20 June 2023].

Jackson, B. (2001). *Protecting Emergency Responders: Lessons.* Chicago: Rand Corporation. 25-30

Jackson, P. (2004). *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows.* Oxford: Routledge.7-14.

Janyanti, A. (2023) [Online] *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?* Retrieved from Harvard Kennedy School: https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose [Accessed 03 May 2023].

Joffe, A. (1999). Dismantling intelligence agencies. *Crime,Law and Social Change*, 325-346.

Johnson, D. (2015). Review of The Ethics of Intelligence: A New Framework. *Global Security and Intelligence Studies*, 200-204.

Johnson, L. (1996). *Secret Agencies: U.S. Intelligence in a Hostile World.* Yale: Yale University. 21-23.

Johnson, L. (2007). *Handbook of Intelligence Studies.* Oxford: Routledge.

Johnson, L. (2008). Decision costs in the intelligence cycle. *Journal of Strategic Studies*, 318-335.

Johnson, L. (2008). *Sketches for a theory of strategic intelligence.* Oxford: Routledge. 2-17

Jonson. (2018). Spies and scholars in the United States: winds of ambivalence in the groves of academe. *Intelligence and National Security*, 1-21.

Kendall, W. (2011). The Function of Intelligence. *Cambridge University Press*, 25-37.

Kikeri, S. (2007). *Privatisation in competitive sectors.* Washington: World Bank.2-21.

Kirkgaessner, S. (2020) [Online] *Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince'*. Retrieved from Guardian: https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince [Accessed 01 February 2023].

Kolb, D. (2023) [Online] *A Global Environmental Monitoring System? Dream? Or Reality?* Retrieved from traversals: https://traversals.com/blog/ [Accessed 05 March 2023].

Koniauko, V. (2023). From the "Rush to Ethics" to "the rush to governance" in Artificial Intelligence. *Information Systems Frontiers*, 101-115.

Krishnan, A. (2007). The Future of U.S. Intelligence Outsourcing. *The Brown Journal of World Affairs*, 195-211.

Krishnan, A. (2011). The future of intelligence outsourcing. *The Borwn Journal of World Affairs*, 195-211.

Kroll. (2023) [Online] *Stay ahead with Kroll*. Retrieved from Kroll: https://www.kroll.com/en [Accessed 18 July 2023].

Labib, A. (2022). Analysis of noise and bias errors in intelligence information systems. *National Library of Medicine*, 1775-17780.

Lahenaman, W. (2010). The Need for a New Intelligence Paradigm. *International Journal of Intelligence and Counter Intelligence*, 201-225.

Landau, S. (2005). Under the Radar: NSA's Efforts to Secure. *Journal of National Security Law and Policy*, 50-56.

Larkin, C. (2022) [Online] *Building trust in Space Tech*. Retrieved from EY: https://www.ey.com/en_au/space-tech/building-trust-in-space-tech [Accessed 22 June 2023].

Leander, A. (2016). *Routledge Handbook of Private Security Studies.* Routledge: Oxford. 51-67

Leigh, I. (2015) [Online] *Legal Standards and Best Practice for Oversight of Intelligence Agencies.* Oslo: Parliament of Norway. Retrieved from Parliament of Norway. [Accessed 03 February 2023].

Leonhardt, D. (2022). *How Pegasus's Spyware Changed Global Intelligence.* New York: New York Times Newspaper.

Liaropoulos, D. A. (2006). *A Revolution in Intelligence Affairs? .* Athens: Research Institute for European and American Studies. 7-35.

Liberty. (2022) [Online]. *MI5 Breached Surveillance Laws For a Decade:* tribunal told. Retrieved from LIBERTY: https://www.libertyhumanrights.org.uk/issue/mi5-breached-surveillance-laws-for-more-than-a-decade-tribunal-told/ [Accessed 30 February 2023].

Lin, L. (2011). *State-centric Security and its Limitations: the case of transnational organized crime.* Athens: Research Institute for European and American Studies.8-10.

Lomas, D. (2021) [Online]. *Forget James Bond? Public Perceptions of UK Intelligence*. Retrieved from RUSI: https://rusi.org/explore-our-research/publications/commentary/forget-james-bond-public-perceptions-uk-intelligence [Accessed 06 June 2023].

London School of Economics. (2023) [Online]. *The current debate over U.S. intelligence is missing the larger problem, the intelligence community's inability to think big.* Retrieved from LSE Blog: https://blogs.lse.ac.uk/usappblog/2013/11/08/intelligence-community-think-big/ [Accessed 21 February 2023].

Lucas, E. (2019) [Online] *Changes in technology, politics, and business are all transforming espionage. Intelligence agencies must adapt—or risk irrelevance.* Retrieved from Foreign Policy: https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/ [Accessed 25 March 2023].

Lundborg, T. (2021). Secrecy and Subjectivity: Double Agents and the Dark Underside of the International System. *International Politcal Sociology*, 443-459.

Lundborg, T. (2022). The politics of intelligence failures: power, rationality, and the intelligence process. *Intelligence and National Security*, 20-25.

Lynanashock, L. (2022) [Online] *The Hacking of Starlink Terminals Has Begun*. Retrieved from Wired: https://www.wired.co.uk/article/starlink-internet-dish-hack [Accessed 19 July 2023].

Mackrakis, K. (2023). *Espionage: A Concise History.* Oxford: Routledge. 10-21.

Manors, K. (2022) [Online] *Pegasus: What you need to know about Israeli spyware*. Retrieved from Aljazeera: https://www.aljazeera.com/news/2022/2/8/what-you-need-to-know-about-israeli-spyware-pegasus [Accessed 17 March 2023].

Marie, R. (2001). *Bodies of evidence: Images of women in spy films.* Michigan: University of Michegan Press. 2-20.

Martin, D. S. (2016). *Spying in a Transparent World: Ethics and Intelligence in the 21st Century.* Geneva: Geneva Papers. 10-24.

Mason, D. L. (2023) [Online] *National Security Innovation: Creating new capabilities for the future*. Retrieved from Centre for emerging technology and security: https://cetas.turing.ac.uk/publications/national-security-innovation-creating-new-capabilities-future [Accessed 17 June 2023].

Matey, G. (2013). The Use of Intelligence in the Private Sector. *International Journal of Intelligence and Counter Intelligence*, 272-287.

McCaffrey, S. (2017). Should I Stay or Should I Go Now? Or Should I Wait and See? Influences on Wildfire Evacuation Decisions. *Risk Analysis An International Journal*, 1390-1404.

Mcfadden, C. (2019) [Online] *5 Famous Cases of Industrial Espionage*. Retrieved from Interesting Engineering: https://interestingengineering.com/lists/5-famous-cases-of-industrial-espionage [Accessed 30 January 2023].

Mcfate, S. (2015) [Online] *Shadow Wars: The world of military contracting*. Retrieved from World Affairs: https://www.worldaffairs.org/video-library/media-by-region/latin-america-caribbean/event/1425 [Accessed 20 May 2023].

Mcgettigan, D. (1999). *Privatization in Transition Countries: Lessons of the first decade.* Chicago: International Monetary Fund. 220-251.

Mclennan, J. (2013). *"Should We Leave Now?": Behavioral Factors in Evacuation Under Wildfire Threat.* Brisbane: University of Southern Queensland. 1-20.

Mconnell, M. (2007). Overhauling Intelligence. *Foreign Affairs*, 49-58.

Meyer, M. (2023) [Online] *Ethical Relativism*. Retrieved from Markulla Centre for Applied Ethics: https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/ethical-relativism/ [Accessed 18 June 2023].

MI5. (2023) [Online] *Historical spy cases*. Retrieved from MI5: https://www.mi5.gov.uk/historical-spy-cases [Accessed 01 January 2023].

Middleton, J. (2023) [Online] *Capita cyber-attack: 90 organisations report data breaches*. Retrieved from The Guardian: https://www.theguardian.com/business/2023/may/30/capita-cyber-attack-data-breaches-ico [Accessed 02 February 2023].

Mikhaylov, S. (2018) [Online] *Artificial intelligence for the public sector: opportunities and challenges of cross-sector collaboration*. Retrieved from Royal Society of Publishing: https://royalsocietypublishing.org/doi/full/10.1098/rsta.2017.0357 [Accessed 23 March 2023].

Miller, S. (2021). Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity. *Social Epistemology*, 211-231.

Mills, G. (1999). *The privatisation of Security in Africa.* Oxford: Routledge. 9-14.

Mintz, S. (2018) [Online]. *Do the Ends Justify the Means?* Retrieved from Ethics Sage: https://www.ethicssage.com/2018/04/do-the-ends-justify-the-means.html [Accessed 22 July 2023.]

Moore, D. (2009). *Sensemaking: A Structure for an Intelligence Revolution.* Chicago: Chicago University Press. 30-98.

Morrow, M. (2022). Private sector intelligence: on the long path of professionalization. *Intelligence and National Security*, 402-420.

Morton, A. (2023) [Online] *The Anarchy Problematique and Sovereignty: Neo-Realism and State Power*. Retrieved from Theorising the international: https://sites.google.com/site/irtheoryresource/home/neo-realism-2 [Accessed 09 June 2023].

Mueller, M. (2023) [Online] *Are we in a digital cold war?* Retrieved from Internet Governance: Internetgovernance.org [Accessed 04 April 2023].

Myser, C. (2011). *Bioethics around the Globe.* Oxford: Oxford University Press. 5-21.

Newkirk, A. (2020) [Online] *The Rise of the Fusion-Intelligence Complex: A critique of political surveillance after 9/11*. Retrieved from Surveillance and Society: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3473 [Accessed 15 July 2023].

Sky News. (2023). *Islamic State leader in Syria killed by Turkish intelligence services, says President Erdogan.* Chicago: Sky News.

Netwatch Global. (2023) [Online] *About us*. Retrieved from Netwatch Global: https://www.netwatchglobal.com/ [Accessed 05 January 2023].

Nicander, L. (2011). Understanding Intelligence Community Innovation in the Post-9/11 World. *International journal of intelligence and counter-intelligence*, 534-568.

Nolte, W. (2009). Ethics and Intelligence. *Joint Force Quarterly*, 1-8.

Nuair, S. (2020). A review on ethical concerns in big data management. *International Journal of Big Data Management*, 8-25.

NewYorkTimes (2021) [Online]. *Intelligence Agencies Pushed to Use More Commercial Satellites*. Retrieved from New York Times: https://www.nytimes.com/2021/09/27/us/politics/intelligence-agencies-commercial-satellites.html [Accessed 01 April 2023].

Organisation for Economic Co-operation and Development. (2019). *OECD Working Papers on Public Governance.* Chicago: OECD.1-128.

Omand, D. (2012). *Intelligence and National Security*, 38-63.

Omand, D. (2018). *Principled spying: the ethics of secret intelligence.* Oxford: Oxford University Press.3-200.

Osborne, D. (2006). *Out of Bounds: Innovation and Change in Law Enforcement Intelligence Analysis.* Washington : Joint military college. 2-103.

Owen, A. (2022) [Online] *the ethics of espionage*. Retrieved from Areo Magazine: https://areomagazine.com/2022/12/07/the-ethics-of-espionage/ [Accessed 21 January 2023].

Parry, J. (2006). *Extended review of 'Through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence' by Cécile Fabre.* London: London School of Economics. 245-296.

Peace Building Support Office UN. (2022) [Online]. *U.S. intelligence agencies review what they got wrong on Russia's invasion of Ukraine*. Retrieved from PBSO News hour: https://www.pbs.org/newshour/nation/u-s-intelligence-agencies-review-what-they-got-wrong-on-russias-invasion-of-ukraine [Accessed 19 June 2023].

PCU3ED. (2023) [Online]. *The 4 essential steps of the Risk Management Process are:*. Retrieved from Mi-GSO: https://www.migso-pcubed.com/blog/risk-management/four-step-risk-management-process/ [Accessed 18 June 2023.]

Pegg, D. (2023) [Online]. *Revealed: the hacking and disinformation team meddling in elections*. Retrieved from the Guardian: https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan [Accessed 05 February 2023].

Pellissier, R. (2013). towards a universal competitive intelligence model. *South African Journal of Information Studies*, 53-78.

Perry, D. (1995) [Online]. *Repugnant ethics*. Retrieved from Markkula Centre for applied ethics: https://www.scu.edu/ethics/focus-areas/more-focus-areas/resources/repugnant-philosophy/ [Accessed 04 March 2023].

Peter, L. (2022) [Online]. *Heatwave: More evacuations as Mediterranean wildfires spread*. Retrieved from BBC News: https://www.bbc.co.uk/news/world-europe-62196045 [Accessed 15 July 2023].

Pfaff, T. (2006). The ethics of espionage. *Journal of Military ethics*, 1-15.

Phillips, N. (2016). *"Were the ones that stand up and tell you the truth". Necessity of Ethical Intelligence Services.* Columbia: Salus Journal.

Phillips, P. (2022). Information, Uncertainty & Espionage. *Review of Austrian Economics*, 10-21.

Privacy International. (2023). *Briefing: Controlling the UK's private Intelligence Industry.* Chicago: Privacy International.1-11.

Pillar, P. (2006). Good literature and bad history the 9/11 commissions tale of strategic intelligence. *Intelligence and National Security*, 1022-1044.

Pohl, K. (2021) [Online]. *The unequal impacts of wildfire*. Retrieved from Headwater Economics: https://headwaterseconomics.org/natural-hazards/unequal-impacts-of-wildfire/ [Accessed 23 June 2023].

Potter, Z. (1996) [Online]. *Covert Action: the Delicate Balance*. Retrieved from Intelligence reform in the post cold war era: https://irp.fas.org/eprint/snyder/covertaction.htm#:~:text=The%20Intelligence%20Authorization%20Act%20of%201991%20officially%20describes%20covert%20action,be%20apparent%20or%20acknowledged%20publicly.%22 [Accessed 21 March 2023].

Prosner, R. (2005). *Preventing Suprise attacks in the wake of 9/11.* Chicago: Chicago University Press.3-10.

Public Safety Canada. (2023) [Online]. *Public Safety Canada*. Retrieved from Government of Canada: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgncy-mngmnt-strtgy/index-en.aspx [Accessed 19 June 2023].

PSCR Public Safety Canada. (2019). *Toward a Resilient 2030.* Ottawa: Public Safety Canada.20-25.

Pun, D. (2023) [Online]. *Rething Corporate espionage in the modern era*. Retrieved from University of Chicago Law School: https://cjil.uchicago.edu/print-archive/rethinking-espionage-modern-era [Accessed 19 April 2023].

Puyvelde, D. (2019). *Outsourcing US Intelligence.* Edinburgh: Edinburgh Unviersity Press. 19-57.

Puyvelde, D. (2019). *Outsourcing US intelligence Contractors and government acocutability.* Edinburgh: Edinburgh University Press. 210-255.

Pythian, M. (2013). *Understanding the Intelligence Cycle.* Cambridge: Cambridge Polity Press.1-100.

Pythian, P. G. (2018). *Intelligence in an insecure world.* Cambridge: Polity Press.59-63.

Rand corporation. (2021) [Online}. *The Intelligence Community's Deadly Bias Toward Classified Sources*. Retrieved from Rand Corporation: https://www.rand.org/blog/2021/04/the-intelligence-communitys-deadly-bias-toward-classified.html [Accessed 21 April 2023].

Rathnell, A. (2007). Privatising Intelligence. *Cambridge Review of International Affairs*, 199-211.

Raw, E. (2022). *Norway's Russian spy scandal should be a warning to all universities.* New York: The Financial Times Newspaper.

Rescher, N. (2017). *Espionage, Statecraft and the theory of reporting.* Pittsburugh: University of Pittsburugh Press. 1000-1003.

Richards, J. (2010). *The Art and Science of Intelligence Analysis.* Oxford: Oxford University Press.1-50.

Richterova, D. (2020). An Introduction: The Secret Struggle for the Global South – Espionage, Military Assistance and State Security in the Cold War. *The International History Review*, 1-11.

Rittenburg, T. (2006). An Ethical Decision-Making Framework for Competitor Intelligence Gathering. *Journal of Business Ethics*, 235-245.

Robotics, S. (2017) [Online]. *AEGIS autonomous targeting for ChemCam on Mars Science Laboratory: Deployment and results of initial science team use*. Retrieved from ScienceRobotics: https://www.science.org/doi/abs/10.1126/scirobotics.aan4582 [Accessed 01 April 2023].

Rosenbach, E. (2009) [Online]. *The Role of Private Corporations in the Intelligence Community*. Retrieved from Harvard Kennedy School: https://www.belfercenter.org/publication/role-private-corporations-intelligence-community [Accessed 03 April 2023].

Sageman, M. (2014). The Stagnation in Terrorism Research. *Terrorism and political violence*, 565-580.

Scott, R. (1999). Territorially Intrusive Intelligence Collection and International Law. *HeinOnline*, 23-35.

Sepper, E. (2010). Democracy, Human Rights and Intelligence Sharing. *HEINOnline*, 3-8.

Space Global. (2023) [Online]. *OroraTech and Spire Global partner to tackle wildfires for CSA*. Retrieved from SpaceWatch Global: https://www.google.com/search?q=spaceglobal&ei=z_GwZN6ML9yehbIPuOa82AI&start=0&sa=N&ved=2ahUKEwiesIKuz42AAxVcT0EAHTgzDys4FBDy0wN6BAgDEAQ&biw=1331&bih=793&dpr=1.88 [Accessed 21 April 2023].

Shankar, N. (2020). Surviving Data Breaches: A Multiple Case Study Analysis. *Journal of Comparative International Management*, 35-54.

Sherman, D. (2006). The Psychology of Self-defense: Self-Affirmation Theory. *Advances in Experimental Pyschology*, 183-242.

Shorrock, T. (2018) [Online]. *5 Corporations Now Dominate Our Privatized Intelligence Industry*. Retrieved from The nation: https://www.thenation.com/article/archive/five-corporations-now-dominate-our-privatized-intelligence-industry/ [Accessed 21 April 2023].

Sibylinne. (2023) [Online]. *About us*. Retrieved from Sibylinne: https://www.sibylline.co.uk/ [Accessed 19 July 2023].

Sims, J. (2006). Foreign Intelligence Liason: Devils, Deals, Details. *International Journal of Intelligence*, 21-50.

Singer, P. (2007). *Corporate Warriors: The Rise of the Privatized Military Industry.* Oxford: Oxford University Press. 10-50.

Smith, D. (1996). *Third World Cities In Global Perspective: The Political Economy Of Uneven Urbanization.* Oxford: Routledge. 31-50.

Spencer, N. (2023) [Online]. *Can Spying ever be ethical? In conversation with Cecil Fabre*. Retrieved from theos: https://www.theosthinktank.co.uk/comment/2022/05/10/can-spying-ever-be-ethical-in-conversation-with-ccile-fabre [Accessed 01 April 2023].

Spracher, W. (2016). Mired in Gray: Juggling Legality, Lawfulness, and Ethics as an Intelligence Professional. *American Intelligence Journal*, 96-103.

Space and Satellite professional international. (2023) [Online]. *How Space Saves Lives*. Retrieved from SSPI: https://www.sspi.org/cpages/how-space-saves-lives#:~:text=Weather%20satellites%20provide%20the%20data,direct%20people%20away%20from%20danger. [Accessed 02 April 2023].

Steele, R. (2023) [Online]. *the new craft of intelligence*. Retrieved from http://www.jar2.com/2/Intel/CIA/OSS/oss.htm [Accessed 04 April 2023].

Stone, M. (2012) [Online]. *MI6 Spy Death: More Questions Than Answers*. Retrieved from Sky News: https://news.sky.com/story/mi6-spy-death-more-questions-than-answers-10479459 [Accessed 05 June 2023].

Storm, J. (2018). Outsourcing Intelligence Analysis: . *Journal of National Security and Law*, 125-127.

Sturgis, S. (2013) [Online]. *The 'shadow intelligence agency' behind the NSA surveillance scandal*. Retrieved from Facing South: https://www.facingsouth.org/2013/06/the-shadow-intelligence-agency-behind-the-nsa-surv.html-0 [Accessed 18 March 2023].

Syal, R. (2011). *Undercover police: Officer A named as Lynn Watson.* Leeds: The Guardian Newspaper.

The Atlantic. (2010) [Online]. *The Dangerous Science of Intelligence Analysis*. Retrieved from The Atlantic: https://www.theatlantic.com/politics/archive/2010/07/the-dangerous-science-of-intelligence-analysis/60488/ [Accessed 04 April 2023].

Thales. (2023) [Online]. *Building a future we can all trust*. Retrieved from Thales: https://www.thalesgroup.com/en [Accessed 17 April 2023].

Thomas, M. (2007). *Empires of Intelligence: Security Services and Colonial Disorder after 1914.* Californa: University of Californa.93-201.

Traversals. (2023) [Online]. *Make Intelligence Driven Decisions*. Retrieved from Traversals: https://traversals.com/ [Accessed 21 April 2023].

Trujillo. (2012). Are Intelligence Failures Inevitable? *E-international Relations*, 1-10.

Tucker, D. (2014). *The End of Intelligence: Espionage and State Power in the Information Age.* Stanford: Stanford University Press. 7-10.

Tymstra, C. (2020). Wildfire management in Canada: Review, challenges and opportunities. *ScienceDirect*, 20-27.

Tzu, S. (2023) [Online]. *Winning Without Conflict*. Retrieved from the art of war: https://scienceofstrategy.org/main/content/winning-without-conflict [Accessed 29 April 2023].

United Nations. (2015) [Online]. *Sustainable Development Goals*. Retrieved from Concern World Wide: https://www.concern.org.uk/news/explained-sustainable-development-goals?gclid=EAIaIQobChMIx8DXuICB_gIVQoxoCR3nIgVuEAAYAiAAEgINkvD_BwE [Accessed 28 April 2023].

United Nations Committee For Development. (2014). *Global Government and Global Rules for Development in the post-2015 era.* Geneva: United Nations Committee for Development. 1-20.

UNESCO World Heritage. (2023) [Online]. *Ethics and Intangible Cultural Heritage*. Retrieved from unesco intangible world heritage: https://ich.unesco.org/en/ethics-and-ich-00866#:~:text=Ethics%20refers%20to%20norms%20of,a%20human%20or%20cultural%20perspective. [Accessed 20 April 2023].

United Nations Childrens Fund. (2019) [Online]. *International Human Rights Framework*. Retrieved from UNICEF: https://www.unicef.org/armenia/en/stories/international-human-rights-framework [Accessed 23 April 2023].

Uras, U. (2015) [Online]. *Turkey: We warned France twice about Paris attacker*. Retrieved from Al Jazeera: https://www.aljazeera.com/news/2015/11/16/turkey-we-warned-france-twice-about-paris-attacker [Accessed 21 March 2023].

United States Department of Justice. (2003). *Engaging the Private sector to promote homeland security.* Colarado: Department of Justice. 5-30.

Ventura, L. (2023) [Online]. *Top 100 Richest Countries In The World*. Retrieved from Global Finance: https://www.gfmag.com/global-data/economic-data/worlds-richest-and-poorest-countries [Accessed 19 March 2023].

Vitkauskas, D. (1999). *The Role of a Security Intelligence Service in A Democracy.* Chicago: NATO.1-101.

Voelz, G. (2009). Contractors and Intelligence: The Private Sector in the Intelligence Community. *Journal of Intelligence and Counter Intelligence*, 1-25.

VoxEU. (2017) [Online]. *Dirty work: Buying votes at the UN Security Council*. Retrieved from CEPR: https://cepr.org/voxeu/columns/dirty-work-buying-votes-un-security-council [Accessed 01 June 2023].

Wagner, R. (2003). *Controversies in Competitive Intelligence: The Enduring Issues.* Chicago: Praeger Publishers.1-17.

Wark, W. (2008). Introduction: The study of espionage: Past, present, future? *Intelligence and National Security*, 101-150.

Warner. (2022). Leviathan’s Heirs: sovereignty, intelligence, and the modern state. *Intelligence and National Security*, 888-902.

Warner, M. (2002). *Wanted: A Definition of Intelligence.* Washington: CIA.1-201.

Wells, D. (1969). How Much Can "The Just War" Justify? *The Journal of Philosophy*, 819-829.

Wesley. (2010). *The politicisation of intelligence.* London: Penguin. 19-331.

West, N. (2019). *MI5: British Security Service Operations, 1909–1945: The True Story of the most secret counter-espionage in the world .* Barnsley: Frontline Books. 2-11.

Williams, R. (2010). (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action. *HeinOnline*, 19-25.

Wirtz, B. (2018). Artificial Intelligence and the Public Sector—Applications and Challenges. *International Journal of Public Administration*, 212-250.

Washington Post Newspaper. (2013). *NSA broke privacy rules thousands of times per year, audit finds.* Washington: the Washington Post Newspaper.

Yu, H. (2018) [Online]. *Building Ethics into Artificial Intelligence*. Retrieved from Cornell University: https://arxiv.org/abs/1812.02953 [Accessed 09 July 2023].

Zegart. (2022) [Online]. *Open Secrets*. Retrieved from Foreign Affairs: https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart [Accessed 24 June 2023].

Zegart, A. (2019). Spies, Lies and Algorithms: Why US intelligence agencies must adapt or fail. *Foreign Affairs*, 85-97.

Zhu, A. (2005) [Online]. *Neoliberalism, Global imbalances, and Stages of Capitalist Development*. Retrieved from Ideas Repec: https://ideas.repec.org/p/uma/periwp/wp110.html [Accessed 01 July 2023].