What's the Harm? The Ethics of Intelligence Collection

Ross W. Bellaby

Thesis submitted in fulfilment of the requirements for the degree of PhD

Department of International Politics
Aberystwyth University
June 13th, 2011

DECLARATION

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed ..... (Ross W. Bellaby)

Date .....

STATEMENT 1

This thesis is the result of my own investigations, except where otherwise stated. Where *__correction services__ have been used, the extent and nature of the correction is clearly marked in a footnote(s).

Other sources are acknowledged by footnotes giving explicit references.

A bibliography is appended.

Signed ..... (Ross W. Bellaby)

Date .....

[*this refers to the extent to which the text has been corrected by others]

STATEMENT 2

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed ..... (Ross W. Bellaby)

Date .....

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loans after expiry of a bar on access approved by Aberystwyth University.

Signed ..... (Ross W. Bellaby)

Date……..

Summary

As the professional practice of intelligence collection adapts to the changing environment of the twenty-first century, many academic experts and intelligence professionals have called for a coherent ethical framework that outlines exactly when, by what means and to what ends intelligence is justified. Recent controversies, including reports of abuse at Guantanamo Bay and Abu Ghraib, allegations of extraordinary rendition programmes and the ever-increasing pervasiveness of the 'surveillance state', have all raised concerns regarding the role of intelligence in society. As a result, there is increased debate regarding the question of whether or not intelligence collection can be carried out ethically. This thesis will tackle this question by creating an ethical framework specifically designed for intelligence that is capable of outlining under what circumstances, if any, different intelligence collection activities are ethically permissible.

This thesis argues that there is a tension presented by intelligence collection between the damage that it can cause and the important, ethical role it can play in the political community. In order to deal with this tension the ethical framework proposed in this thesis is comprised of two parts. The first part is designed to recognise those features of intelligence that might be considered ethically unacceptable by highlighting the 'harm' it can cause. Once the harm is understood, the second part of the ethical framework establishes a set of Just Intelligence Principles that can outline if and when the harms caused are justified. These Just Intelligence Principles are developed by drawing upon the just war tradition and its criteria of just cause, legitimate authority, right intention, last resort, proportionality and discrimination. By placing the harm that intelligence can cause into context with the Just Intelligence Principles it is possible to limit the use of intelligence while recognising the important role it plays in protecting the political community.

Once the ethical framework has been established in Chapter One it is then applied to a range of intelligence collection activities in Chapters Two, Three, Four and Five. This thesis will examine three of the most prominent collection disciplines in the field of intelligence studies: imagery intelligence, signals intelligence and human intelligence. By applying the ethical framework established in the beginning of the thesis to these three important intelligence collection disciplines, it is possible to better understand the ethical framework.

The main argument of this thesis will be that the most appropriate ethical framework for intelligence collection is one which is able to recognise that intelligence collection does indeed cause harm, but that sometimes this harm is necessary in order to protect the political community.

Acknowledgements

The first acknowledgments of this thesis must go to my outstanding supervisors, Professor Toni Erskine and Professor Peter Jackson. As a team they have proved to be one of the best, providing me with unending encouragement, enthusiasm for my project, interesting and engaging academic debate and the type of support that I could not have lived without. Their meticulous reading of my work, intellectual acuity and their support to develop and grow in my own way has not only helped this immediate piece of work but has given me confidence in my ability as a researcher and as a writer to take me far beyond what I have achieved here.

Other members of the department that I would like to extend a special acknowledgement to include Professor Len Scott and Professor Martin Swinburn Alexander. Len has always been an important supporting force for me and my project during my years at Aberystwyth. From the initial days of developing my project all the way through to the end Len has been unceasing in his interest and support, something which has been a great source of strength to me. I must also extend my unending gratitude to Martin for his role in my life during my postgraduate years. While my PhD is the summation of my research here at Aberystwyth, it does not reflect the utter joy I have had as a tutor within the department and it is in this area that Martin has been my mentor and friend. Martin has not only shown to me what it means to be an outstanding lecturer and tutor, but also what it means to act as a role model for those we teach and who come to rely on us. If I become half the true academics that Len and Martin represent then I will be fortunate.

To my friends and loved ones I cannot say enough. Lisa Denney and Matthew Fluck, thank you for being there for me through my PhD and for providing me with coffee and cake on a regular basis – we will always be Office No.1 no matter where we end up. To Andy, Halle and Aoileann, thank you for always making me laugh, showing me love and for chasing away Aberystwyth's most persistent grey skies. To Chris, Alison, David, Tom and Pat, even though you are now far away, memories of you keep me warm. And to everyone else who I do not have space to mention – I thank you all for never asking me to explain my PhD, but always asking me how I am.

Finally, I dedicate this piece of work to my family – Judith, Keith, Tamasine and Robbie. You have all been there for me over these many years and have only ever wanted me to be happy in anything that I do. You are my unending support, whose voice, humour and love has kept me going through all I have ever tried to do. We are the collective and we will never be broken. Your unconditional love and guidance has made me what I am today and I cannot thank you enough for that. Thank you, everyone.

Contents

Table of Figures

List of Abbreviations

ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ASU	Active Service Unit
CCTV	Closed Circuit Television
CEOP	Child Exploitation and Online Protection Centre
CIA	Central Intelligence Agency
CONUS	Continental United States Intelligence Programme
COPA	Child Online Protection Act
CPGB	Community Party of Great Britain
CSIS	Canadian Security Intelligence Service
DARPA	American Defence Advanced Research Projects Agency
DCRI	Direction Centrale du Renseignement Intérieur (Central Directorate of Interior Intelligence)
ECHR	European Convention of Human Rights
EHRC	Equalities and Human Right Commission
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FSB	Federal Security Service
GCHQ	Government Communications Headquarters
HSI	Hyper-Spectral Imagery
HUMINT	Human Intelligence
HVA	Hauptverwaltung Aufklärung (Main Reconnaissance Administration)
IIEA	International Intelligence Ethics Association
IMINT	Imagery Intelligence
IP	Internet Protocol

ISP	Internet Service Provider
MASINT	Measurement Signals Intelligence
MI5	Security Service
MSI	Multi-Spectral Imagery
MSS	Chinese Ministry of State Security
NDNAD	National DNA Database
NSA	National Security Agency
PACE	Police and Criminal Evidence Act
RIPA	Regulation of Investigatory Powers Act
RUC	Royal Ulster Constabulary
SDP	Socialist Democratic Party
SIGINT	Signals Intelligence
SIS / MI6	Secret Intelligence Service
TIA	Total Information Awareness

Introduction

As the professional practice of intelligence adapts to the changing environment and new threats of the twenty-first century, many academic experts and intelligence professionals have stressed the need for a coherent ethical framework that outlines exactly when, by what means, and to what ends intelligence is justified. Recent controversies, including reports of abuse at Guantanamo Bay and Abu Ghraib, allegations of extraordinary rendition programmes and the ever-increasing pervasiveness of the 'surveillance state', have all raised questions regarding the role of intelligence in society. In 2005, the Parliament Assembly of the Council of Europe adopted a recommendation that called for the drafting of a European code of intelligence ethics.[1] In 2007, the European Council's Rapporteur reported on the issue of secret detentions and underlined the need for security services to be "subjected to codes of conduct, accompanied by robust and thorough supervision".[2] Furthermore, the 2009 UK House of Lords report, *Surveillance: Citizens and the State*, highlighted significant anxiety regarding the possible threat surveillance poses to individual privacy. The report highlighted the need to review CCTV camera usage, internet traffic monitoring, DNA databases and wiretaps, questioning what role these activities should play in a Western liberal society.[3] Clearly, there is debate regarding the question of whether or not intelligence collection can be carried out ethically.

The reason why no ethical framework has previously been established for intelligence is the result of a combination of factors. For the intelligence service itself, one of its most important concerns is being able to keep what it does secret, meaning that its people, tactics and general activity is kept out of sight, and therefore, in many instances, out of mind. As a result, there has been no explicit call for an ethical review of intelligence as many people were unaware of the type of activities being carried out. Added to this is the brief professional history of intelligence meaning that it has not had the long history to support an

---

[1] Parliamentary Assembly of the Council of Europe *Democratic Oversight of the Security Sector in Member States* Recommendation Doc.1713 (Strasbourg, 23 June 2005) §5 p.2
Available at http://assembly.coe.int/Documents/AdoptedText/ta05/EREC1713.htm Accessed April 2008

[2] Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs *Secret Detentions and Illegal Transfers of Detainees by Council of Europe Member States* Doc.11302 (Strasbourg 11th June 2007) §18 p.9
Available at http://assembly.coe.int/Documents/WorkingDocs/Doc07/edoc11302.pdf Accessed April 2008

[3] House of Lords: Select Committee on the Constitution *Surveillance: Citizens and the State* 2nd Report of Session 2008–09 (6th Feb. 2009) §70, 84 pp.20, 22 Available at
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/surveillance_report_final.pdf Accessed 9th July 2009. Also see Rose, C., Chief Surveillance Commissioner *Report on Two Visits by Sadiq Khan MP to Babar Ahmad at HM Prison Woodhill* Presented to Parliament by the Secretary of State for the Home Department (February 2008) Cmnd.7336.
Available at http://www.official-documents.gov.uk/document/cm73/7336/7336.pdf Accessed 16th April 2008

ethical code of conduct like that seen with some of the other professions such as medicine and law. Furthermore, there has also been a resistance to developing an ethical code for intelligence from the fear that any restrictions on its use will only impede its effectiveness. In combination, these factors have meant that there has previously been little drive for establishing any coherent, systematic or rigorous ethical framework.

However, it can be argued that this lack of ethical code for intelligence is not only unacceptable but indeed folly. No longer can intelligence remain in the shadows, free to act as it wishes. No activity can claim exemption from ethical review, no matter the circumstances. Public reactions to recent controversies such as those mentioned have demonstrated that people are no longer willing to allow intelligence agencies to carry out activities without some guarantee that what they are doing is indeed ethical. People need to be assured that not only are they being protected but that their protectors are acting in accordance with ethical standards, even if they cannot directly witness it.

This means that if intelligence is to enjoy the trust of those people it is charged with protecting then it must make explicit that it is acting in an ethical way. Clearly, there is a need for a framework that outlines when intelligence is ethically acceptable. What is less clear, however, is what standards the intelligence community should be held to. There has been little academic work that has fully outlined any ethical framework designed specifically to deal with intelligence. This thesis, therefore, will create an ethical framework appropriate for intelligence in order to answer the central research question, 'how is intelligence collection to be ethically evaluated?'

Concerns

The significance of this question has been emphasised by recent intelligence-related incidents that left have many wondering whether current legal restrictions are sufficient. Inhumane treatment of Binyam Mohamed at Guantanamo Bay, in Pakistan and Morocco, and his claims that he was subject to a CIA-run extraordinary rendition program have, for example, caused public outcry and has forced the British government to announce a judge-led inquiry into how and why such activities were allowed to happen.[4] Furthermore, in American politics, the issue of what counts as legitimate treatment of terrorist suspects held centre stage for much of the

[4] Intelligence and Security Committee *Rendition* (July,2007) cm.7171
Available at http://www.fas.org/irp/world/uk/rendition.pdf Accessed 7th December 2010. Also see Grey, S. *Ghost Plane: The True Story of the CIA Torture Program* (New York: St. Martin's Press, 2006) p.53

Bush Administration and casts a long shadow over the Obama Administration.[5] These controversies have sparked increased debate over the ethical issues associated with torture, questioning when, if ever, such action is appropriate.

Another concern is the growing ability and tendency of intelligence and security services to intercept, monitor, and retain personal data in an increasingly computerised world. Surveillance has become a distinguishing feature of modernity: "Over the years surveillance has become increasingly systematic and embedded in everyday life, particularly as state agencies consolidate their position and recognise the administrative benefits".[6] However, in the face of this boom in surveillance technology, there has been significant anxiety regarding the possible threat these surveillance practices pose to individual privacy.[7] Surveillance, as a result of the developments in information and communication technologies, has reached unprecedented levels in its ability to monitor the individual, with, it would seem, no matching revolution in the rules limiting its use. These concerns have forced intelligence practices into the light, making clear the powerful tools intelligence organisations have at their disposal and, if not used properly, the potential they have to cause severe harm.

Impetus

There are three types of impetus for this project. The first one is associated with practical concerns. It is feared that unethical intelligence can or will lead to bad intelligence. Intelligence carried out unethically will cause a brain-drain from organisations as individuals will either turn away from the organisation or feel that they do not want to join an organisation engaging in egregious activities. Richard Dearlove, the former Chief of the Secret Intelligence Service, remarks how "potential recruits would come to us because they believed in our cause . . . This made our work much easier".[8] Furthermore, there is also the fear that unethical intelligence is likely to attract the wrong sort of cooperation from informants. Treating someone in an unethical way runs the risk of annoying, hurting,

[5] See Anderson, K. 'What to do with Bin Laden and Al Qaeda Terrorists?: A Qualified Defence of Military Commissions and United States Policy on Detainees at Guantanamo Bay Naval Base', *Harvard Journal of Law and Public Policy* Vol.25 No.2 (2001) pp.591-635; Clover, J. S. '"Remember, We're the Good Guys": The Classification and Trial of the Guantanamo Detainees' *South Texas Law Review* Vol.45 No.1 (2003) pp.351-395; Dershowitz, A. *Why Terrorism Works: Understanding the Threat, Responding to the Challenge* (London: Yale University Press, 2002)

[6] Ball, K. and Webster, F. 'The Intensification of Surveillance' in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age edited* by Ball, K. and Webster, F. (London; Sterling, VA: Pluto Press, c2003) p.1

[7] House of Lords *Surveillance* (2009), §70, 84 pp.20, 22

[8] Fallows, J. 'Foreword' in *Brave New War: The Next Stage of Terrorism and the End of Globalization* by Robb, J. (Hoboken, NJ: John Wiley and Sons 2007) p.vi

upsetting or distressing the very people from whom one is trying to get information. Former CIA officer John Hedley notes that, "An agent who hates and fears his case officer is not likely to be reliable or helpful".[9] This can result in a counterproductive relationship. These are, however, practical concerns: arguments to act ethically based on notions of efficient intelligence production. Although they are interesting arguments and lend strength to the belief that intelligence agents should act ethically, they are not in themselves the main concern of this thesis. They argue that one should act ethically because it is beneficial to do so, rather than because there is an imperative to act ethically.

The second type of impetus is the result of the argument that democratic nations, by virtue of being such, have an obligation to act ethically. Loch Johnson, for example, argues that, "The United States is a democracy, with a proud tradition of fair play in international affairs and a desire to be a respected world leader – not just for our military and economic might, but for our embrace of human values as well".[10] There is a concern, therefore, regarding how intelligence agencies in democratic societies can carry out their activities while still maintaining the ethical norms that their society embodies. Again, however, while this argument supports the belief that democratic states should act ethically if they are to reflect some of the norms they claim to uphold, it does not offer any limits on non-democratic states whose intelligence agencies, it can be argued, should equally be the subject of ethical scrutiny.

As such, the position that is held in this thesis is that regardless of practical concerns or whether a state is democratic or authoritarian, ethical standards cannot be ignored. Ethics permeates every aspect of life, both at the state and individual level, and as such no activity can purport to be exempt from ethical evaluation. This position was argued by Michael Quinlan who has, on numerous occasions, made it clear that intelligence cannot ignore ethical concerns. In *Just Intelligence: Prolegomena to an Ethical Theory*, Quinlan argued that,

> We can no more step outside ethics than we can opt out of the force of gravity. There is no area of human activity, whether public or private, collective or individual, that has an *a priori* entitlement to require the moralist to be silent. If the effective practice of intelligence raises awkward ethical questions, we are obliged ultimately to face them.[11]

---

[9] Quoted in Olson, J. M. *Fair Play: The Moral Dilemmas of Spying* (Washington, D.C.: Potomac Books Inc., 2006) p.48

[10] Johnson, L. 'Ethical Intelligence: A Contradiction in Terms?' in 'A Symposium on Intelligence Ethics' *Intelligence and National Security Special Issue* Vol.24 No.3 (2009) p.366

[11] Quinlan, M. 'Just Intelligence: Prolegomena to an Ethical Theory' *Intelligence and National Security* Vol.22 No.1 (2007) p.2

Quinlan reiterated this point in a BBC Radio Four interview when he stated that, "I regard any human activity as liable to be judged at the bar of morality. And that's especially true of activities like armed conflict and intelligence".[12] Michael Herman, who served as a British intelligence professional from 1952 to 1987 and former Secretary to the Joint Intelligence Committee, argues a similar point stating that, "most of us – though not arch-realists – feel that states' actions have an ethical dimension in the same way as any other human activity. There is no reason why government intelligence should be excluded".[13] Intelligence operatives must be aware of what ethical standards are expected of them and they must adhere to them regardless of the type of society to which they belong or other, practical, concerns.

A Review of the Literature: The Current Position

Despite claims to being the second oldest profession, the actual professionalization and institutionalisation of intelligence has a relatively young history. It is only in the past hundred years that states have come to use and rely on their intelligence communities in a systematic way. Regardless of whether the short- or long-view is taken, however, it is clear that evidence of any rigorous, systematic, or extended evaluation of the role that ethics does or should play in intelligence is virtually non-existent. Years nestled in the shadows have left the field of intelligence out of sight and out of mind. Indeed, as intelligence moves into the twenty-first century there is little work, whether from the intelligence agencies, government officials, or academic sources that explores the role of ethics in intelligence.

Literature on 'Intelligence Ethics': A Cross-Profession Demand?

A cursory glance at publications of the world's main intelligence communities is one reflection of the current lack of work on ethics in intelligence. British intelligence agencies such as the Security Service (often referred to as MI5), Government Communications Headquarters (GCHQ) and the Secret Intelligence Service (SIS or MI6); American intelligence organisations such as the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA) and the National Security Association (NSA); the Canadian Security Intelligence Service (CSIS); the Australian Secret Intelligence Service (ASIS) and the Australian Security Intelligence Organisation (ASIO) offer little in the way of outlining

[12] Quinlan, M. BBC Radio Four *Analysis*: *Secrets and Mysteries Broadcast Date: 19th April 2007 CD number: PLN716/07VT1015*

[13] Herman, M. 'Why Should Intelligence Professional Attend to Intelligence Ethics?' in 'A Symposium on Intelligence Ethics' *Intelligence and National Security Special Issue* Vol.24 No.3 (2009) p.382

the ethical codes to which they adhere. For example, the SIS website only references the oversight mechanisms that it must adhere to when searches into the limits placed on its activity are made: "Like any other part of Government, SIS is subject to UK law, as are SIS members of staff".[14] Formal-legalistic controls have thus dominated the concerns for limiting the use of intelligence: "measures to enhance congressional control, familiarise executive controls and reorganise the intelligence bureaucracy have been particularly popular subjects for debate... in their ability to control intelligence".[15]

This is not to say that rules of law do not play a vital role in establishing limits on intelligence activity. Indeed, law and oversight mechanisms would be the main articulation and actualisation of the relevant ethical framework. Rather the problem is that there seems to be no explicit effort to outline the ethical basis of these legal rules and norms. The cart, in this instance, seems to have been put before the horse. Laws can be used as a reflection of ethical arguments rather than using legal rules as a *de facto* expression of what activities are ethical. While it can be argued that things that are ethical can (and often should) be reflected in law, this is not to say that those things set out in law are by virtue of this position ethical. Indeed, "laws and regulations sometimes provide the solution to the problem but rarely answers to ethical dilemmas".[16]

What little work there is, however, is the result of a general cross-profession demand from government officials, intelligence professionals and academics for a greater focus on the of role of ethics in intelligence. For example, a central objective of the 2002 Gregynog conference held by the Centre for Intelligence and International Security Studies at the University of Wales, Aberystwyth, was to better integrate normative questions into the study of intelligence and has remained a continuing concern for the centre, illustrated by key contributions to the 2004 collection published in *Intelligence and National Security.*[17] Also, recent years have seen the formation of the International Intelligence Ethics Association (IIEA) whose central aim was to combine the efforts of both intelligence professionals and theorists in developing a broad understanding of ethics in the professional of intelligence. In

---

[14] Secret Intelligence Services Website *Legislation and Accountability* https://www.sis.gov.uk/about-us/legislation-and-accountability.html Accessed 1st March 2011. The American intelligence community is similar, publishing its legal oversight mechanisms. See Central Intelligence Agency Website *Intelligence Oversight* https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/intelligence-oversight/ Accessed 1st March 2011

[15] Hastedt, G. *Controlling Intelligence* (London: Cass, 1991) p.97

[16] Shpiro, S. 'Intelligence Ethics in Israel: Why Do We Need Intelligence Ethics' in 'A Symposium on Intelligence Ethics' *Intelligence and National Security Special Issue* Vol.24 No.3 (2009) p.368

[17] Herman, M. 'Ethics and Intelligence after September 2001' *Intelligence and National Security* Vol.19 No.2 (2004), pp.342-58; and Erskine, T ''As Rays of Light to the Human Soul?' Moral Agents and Intelligence Gathering' *Intelligence and National Security* Vol.19 No.2 (2004) pp.359-81

accordance with this aim, the IIEA has held a series of cooperative conferences in both America and the United Kingdom from 2006-2011 as well as establishing the *International Journal of Intelligence Ethics* in 2010. Both these organisations and journals have drawn and integrated the views and works of intelligence professionals, academics and government officials. This has resulted in a broad recognition of the importance ethics can or should play in intelligence and even some tentative moves towards producing some bodies of work that reflect this new orientation. However, much of the work done in this field is centred on expressing the general desire that an ethical framework for intelligence should be established. Indeed, Michael Quinlan, David Omand and Michael Herman, all of whom have highly distinguished careers in intelligence, defence and government, have expressed the need for an explicit review of the place ethics should have in intelligence. Herman notes the "ethical baggage" intelligence collection carries with it; Omand observes the real dilemma for intelligence agencies in defining the "acceptable boundaries of their conduct"[18]; and Quinlan bemoans that "There are aspects of the intelligence business, as practised by all major countries, that seem notably disreputable by the behavioural standards of normal human settings".[19] In addition to this, Kent Pekel, who spent time interviewing CIA employees on their views regarding the role of ethics in their jobs, notes that "many of the people I interviewed felt that the CIA too largely had taken a passive approach to integrity [and ethics more broadly]... most felt the issue had not been addressed or only addressed within the legal framework of compliance".[20]

Ethical Philosophy: Possible Avenues and First Steps

In order to better understand the role of ethics in intelligence it is important to review some of the appropriate ethical theories, examining what conclusions they make and what they would mean for intelligence. Toni Erskine provides an illuminating summary of how three important ethical traditions – realist, consequentialist and deontological – might be applied to intelligence in her article *Rays of Light to the Human Soul*.[21] Erskine starts by challenging those that would equate realism with an amoral position and argues that Hobbesian realism rests on the moral duty of the sovereign to protect the political community: "This ethical realist position may lend legitimacy to any means of conducting external intelligence

[18] Omand, D. 'The Dilemmas of Using Secret Intelligence for Public Security' in *New Protective State: Government, Intelligence and Terrorism* edited by Hennessy, P (London: Continuum, 2007) p.148
[19] Quinlan, M. 'Just Intelligence' (2007) p.1
[20] Pekel, K. 'Integrity, Ethics and the CIA: The Need for Improvement' *Central Intelligence Agency Washington Dc Center for The Study of Intelligence* (1998) p.2
[21] Erskine, T. 'Rays of Light' (2004)

activities (that serve the interest of the state)".[22] The resulting argument is that intelligence activities are justified if they serve the well-being of the state. However, Erskine argues that this is a position that does not necessarily leave much room for rights other than those the state might deem expedient.[23] Erskine does note that limits on intelligence can be established by a realist ethic in the form of reciprocal agreements, "if they were motivated by the desire to protect the members of one's own political community from intrusive methods of collection".[24] However, Erskine also argues that such restraint can be unilaterally rescinded given that, "adherence to such constraints would necessarily remain dependent upon subjective and fluid interpretations of the national interest".[25] Therefore, the realist ethic would not offer the limits on intelligence that this thesis would argue are required.

The second approach, consequentialism, judges actions by the value of their consequences and (compared with realism) is extended to include the interests of those outside the immediate national political community. In its standard form, consequentialism as a moral theory can be seen to conclude that the rightness or the wrongness of an action is determined by the results that flow from it. All consequentialist theories accord some fundamental role to the question of which states of affairs are best, and that the ethically correct course of action is determined by the relevant consequences. Erskine characterises the consequentialist approach as consistent with that made by Herman in his article *Ethics and Intelligence After September 2001* when he argues that "intelligence has to be judged in the first instance on its manifest consequence".[26] This position supposes an "ethical balance sheet" where knowledge and activities can be examined separately, and then can be integrated together to make a judgement on the overall outcome of an action.[27] Erskine argues that the consequentialist position has a global focus that takes into account the good intelligence causes is for all states, not just those that directly benefit from the information.[28] For example, Herman's consequentialist ethical framework for intelligence takes the position that "governments drawing on a standard of intelligence knowledge tended to behave as more responsible members of the international society than those that had to manage without it, or

[22] Erskine, T. 'Rays of Light' (2004) p.365
[23] Erskine, T. 'Rays of Light' (2004) p.365.
[24] Erskine, T. 'Rays of Light' (2004) p.365 Erskine goes into greater depth on this, what she calls a 'communitarian realist' approach to restraint in war in 'Embedded Cosmopolitanism and the Case of War: Restraint, Discrimination and Overlapping Communities' *Global Society* Vol.14 No.4 (2000) p.580
[25] Erskine, T. 'Rays of Light' (2004) p.366
[26] Herman, M. *Intelligence Services in the Information Age: Theory and Practice* (London: Frank Class, 2001) p.202.
[27] Erskine, T. 'Rays of Light' (2004) p.366
[28] Erskine, T. 'Rays of Light' (2004) p.367

chose to do so – less ignorant, less insensitive and (I would now add of democratic states) less impetuous".[29] According to this consequentialist position, intelligence activities would be acceptable if they maximise the good through balancing the benefits of increased knowledge against the costs of how the intelligence information might have been acquired.[30] The difficulty with this position resides in the highly complex computations of goods and harms required in order to draw up Herman's ethical balance sheet. The first issue this position raises is in determining what should count as the relative good and detrimental consequences of intelligence, something which is "a challenging – and some might argue impossible – endeavour".[31] A second issue is whether the ends one was aiming for are ever actually achieved, and how one can tell when this is so.[32] Quinlan cautions that, "it is... hard even with hindsight to measure the reality and scale of the possible benefits in any concrete way and to bring them into common calculus with costs".[33] Furthermore, one distinctive mark of consequentialist theories is that they regard the value of an action to be determined by their consequences, which means that value of something is not intrinsic to it. If this was so, then there would be no way to actually accord anything with real value: "presumably there are some types of thing which have non-consequential value, and also some things have value because they are instances of those types".[34] As Erskine notes, this position ignores those important ethical arguments that "would deny that such moral considerations could be 'calculated' at all and would consider certain acts to be intrinsically wrong".[35]

Clearly, a simple utilitarian balance sheet will not suffice. However, according to Erskine's third approach, the deontological, there is no need for such calculations as this position argues that some actions are simply prohibited as a result of the activity's inherent immorality. Often referred to as the 'absolutist' position, deontology argues that some acts are an unconditionally morally wrong "all the way down"[36], regardless of the consequences. The dominance of deontology in ethical and political thought is evidenced in those international laws that are concerned with the equal treatment of individuals and other groups: Article 2b of the 1948 Convention on the Crime of Genocide, and Article 1 of the

[29] Herman, M. 'Intelligence after September 2001' (2004) p.345
[30] Erskine, T. 'Rays of Light' (2004) p.367
[31] Erskine, T. 'Rays of Light' (2004) p.368
[32] Erskine, T. 'Rays of Light' (2004) p.368
[33] Quinlan, M. 'The Future of Covert Intelligence' in *Agents for Change: Intelligence Services in the 21st Century edited by* Shukman, H. (London: St Ermin's Press 2000) p.69
[34] Smart, J. J. C. and Williams, B. *Utilitarianism: For and Against* (London: Cambridge University Press, 1973) p.83
[35] Erskine, T. 'Rays of Light' (2004) p.368
[36] Darwell, S. 'Introduction' in *Deontology* edited by Darwell, S. (Oxford: Blackwell, 2002) p.1

1993 Elimination of Violence against Women, as well as the 1984 Convention against Torture; all of which assume the position that these laws are never, under any condition, to be violated.[37] Erskine explores deontology through Immanuel Kant's "categorical imperative", according to which for something to be ethical "one must act only in such a way that the principle guiding one's action might coherently become universal law" and "one must treat other rational actors as having value as ends in themselves, rather than solely as means to an end".[38] Erskine argues that since many intelligence practices necessarily involve deception, they cannot be universalised, in that the "universalised version of deceiving others is that everyone deceives. In such a world, both truth and deception lose all meaning".[39] Furthermore, Erskine argues that intelligence would fail the second formulation of Kant's categorical imperative given that any "attempt to deceive another in order to obtain intelligence would involve treating this other as a tool, thereby contravening Kant's demand that the person be respected".[40] Many aspects of intelligence collection, according to the deontological position, would therefore be prohibited absolutely as any deployment of deception, manipulation or coercion, fail to meet deontological standards.

The question for deontology, however, is how absolute are these *absolute* prohibitions? For example, the most plausible candidate to be regarded as an absolute right – the right to life and the negative duty to refrain from killing – can be, and has been, overridden.[41] Laws of War and laws in domestic society have long justified killing in order to prevent someone from killing another, innocent, person; or if they are engaged in combat with an unjust aggressor; or even if the failure to kill will lead to the death of more innocent persons.[42] What happens if rights come into conflict with each other? Surely some rights will be violated eventually? Should the prohibition be taken as far as Kant does with his 'murder at the door' scenario; is it the correct course to tell the truth to someone who asks for your neighbour after expressing the desire to kill that neighbour, as Kant's absolute prohibition on

[37] For example, the Convention Against Torture states that "No exceptional circumstances whatsoever, whether a state of war or a threat of war, internal political instability or any other public emergency, may be invoked as a justification of torture." (1984) Part 1 Art. 2 § 2. Evans, M. D. *International Law Documents* 8th edition (London: Blackstone Press, 2007) p.309
[38] Erskine, T. 'Rays of Light' (2004) p.371-372
[39] Erskine, T. 'Rays of Light' (2004) p.372
[40] Erskine, T. 'Rays of Light' (2004) p.372
[41] Gewirth, A. 'Are There Any Absolute Rights' *The Philosophical Quarterly* Vol.31 No.122 (1981) p.1
[42] See Thomson, J. J. 'Self-Defence' *Philosophy and Public Affairs* Vol.20 No.4 (1991) pp.283-310.

lying would have argued?[43] Surely, there are times when these types of activity are ethically justified.

What should be clear, therefore, is that there is indeed a drive for an ethical framework for intelligence but that from the outset the necessary tools are not apparent. Erskine's and Herman's work, among others,[44] examine some of the key ethical schools of thought and outline how they would broadly look if applied to intelligence. While these works highlight the strengths and weaknesses of each of the ethical schools, what is lacking is any true consensus on what the most appropriate ethical framework actually is. It can be argued that realism, consequentialism and deontology all have important things to say for intelligence, but none of them are totally appropriate. Therefore, there is need for an ethical framework that is able to incorporate the strengths of these positions while compensating for their weaknesses.

The Oxymoron: A Problem with 'Intelligence Ethics'

Of course, first it must be questioned why should one bother in establishing and applying an ethical framework to intelligence? As Allen Dulles, once the head of the United States Central Intelligence Agency (CIA) and principal intelligence advisor to the President and the National Security Council, argued in 1963, "The last thing we can afford to do today is to put our intelligence in chains".[45] Indeed, many feel that the ability of the hijackers to carry out their attack in September 2001 highlights not only the threats faced in the twenty-first century but also the fear that any restrictions on intelligence are likely to interfere with its effectiveness and therefore increase the possible success of further attacks. There are those who therefore argue that intelligence should not be subjected to an ethical framework that dictates what activities are acceptable for it would just hinder its practice.

Furthermore, there are those who argue that any project that aims to apply ethics to intelligence is oxymoronic.[46] The job of intelligence in many instances is to collect

---

[43] See Cholbi, M. 'The Murderer at the Door: What Kant Should Have Said' *Philosophy and Phenomenological Research* Vol.59 No.1 (2009) pp.17-46; Isenberg, A. 'Deontology and the Ethics of Lying' *Philosophy and Phenomenological Research* Vol.24 No.4 (1964) pp.463-480; and Mahon, J. E. 'Kant and the Perfect Duty to Others Not to Lie' *British Journal for the History of Philosophy* Vol.14 No.4 (2006) pp.653-685

[44] Grendron, A. 'Just War, Just Intelligence: An Ethical Framework for Foreign Espionage' *International Journal of Intelligence and Counter Intelligence* Vol.18 No.3 (2005) pp.398-434; Pfaff, T. and Tiel J. 'The Ethics of Espionage' *Journal of Military Ethics* Vol.3 No.1 (2004) pp.1-15

[45] Dulles, A. *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering in a Free World* (Guildford: Lyons Press, 2006) p.265

[46] Claridge, D. quoted in Quinlan, M. 'Just Intelligence' (2007) p.1; Jones, J. M. 'Is Ethical Intelligence a Contradiction in Terms?', in *Ethics of Spying: A Reader for the Intelligence Professional Volume 2* edited by Goldman, J. (Plymouth: Scarecrow Press, 2010) p.21

information that other actors would wish to keep secret. Intelligence therefore can engage in the practice of stealing secrets, bribery, manipulation, deception, interception of personal communications, surveillance and interfering with private property in order to overcome the efforts of one's target. The world of intelligence is therefore, by necessity, an unsavoury business. As a result, many writing on this subject have argued that since intelligence must engage in these types of activities as an inherent part of its profession, it cannot be reconciled with the ethical standards seen in everyday life: "Effective espionage requires intelligence officers to deceive, incite, and coerce in ways not acceptable for members of the general public"[47]; "intelligence carries an ethical baggage with it or – to be more accurate – a baggage of unworthiness".[48] The argument, therefore, is that it is both unhelpful and redundant to attempt to apply ethical considerations to a field such as this. As a *New York Times* reporter put it, "is there such a thing as an ethical spy?"[49]

However, by claiming that intelligence is an activity that is inherently unethical and so should exist outside the realm of ethical discourse lest the activity be banned outright, is to ignore the important role that ethics plays in the life of the individual and the political community, as well as the ethical role that intelligence itself can play. This means, first, recognising the fact that intelligence cannot exist outside the purview of ethical evaluation. No activity can. It can argued, therefore, that intelligence agencies must be brought out of the shadows, to some extent at least, and be made to respect ethical norms. This is not to say that intelligence should no longer be kept as secret as possible. Such an argument would be naive. Intelligence does deal with threats that are hidden and therefore intelligence itself must retain the ability to remain secret. In an interview on BBC Radio Four, Shami Chakrabarti, Director of human rights organisation Liberty, accepted that indeed there would always be a secret sphere when it comes to intelligence, but that it is because of this fact that it is here "that the ethical framework kicks in. That is where we all have to trust and rely on the ethical integrity of the services".[50] Indeed, it is because intelligence is secret that "the public need perhaps more assurances than it used to need that these activities are being conducted both well in professional terms and justifiable in moral terms".[51]

Second, failure to acknowledge the importance of ethics in intelligence means failure to recognise the ethical role intelligence plays within a political community. Secret

[47] Pfaff, T. and Tiel, J. R. 'The Ethics of Espionage' (2004) p.1
[48] Herman, M. 'Intelligence after September 2001'(2004) p.342
[49] Shane, S. 'Outfitting Spies with New Tools: Moral Compass' *New York Times* 28th Jan 2006 A1
[50] *Chakrabarti, S.* BBC Radio Four *Analysis*: *Secrets and Mysteries Broadcast Date: 19th April 2007 CD number: PLN716/07VT1015*
[51] Quinlan, M. BBC Radio Four *Analysis*: *Secrets and Mysteries 2007*

intelligence is still needed and depended upon, a dependency that is currently driven by the emergence of diverse and asymmetric threats from international terrorist networks and sub-state actors, as well as the various already established threats, including domestic crime and social unrest, state actors, foreign espionage and international instability. It can hardly be argued that intelligence is not a vital tool for protecting the political community from a variety of truly dangerous threats. Moreover, this particular role has an important ethical dimension to it. The political community has an ethical obligation to act so as to protect its people. This idea, as an ethical position, is the result of two important arguments. The first argument is based on the ontological justifications whereby the ethical argument for the individual defending himself is extrapolated 'up' onto the state. The second moral argument is based on the contention that "allows one to justify courses of action with reference to the good of the political community" and "maintains that acting in the national interest is itself complying with a moral principle".[52] That is, protecting the political community is a moral good in and of itself. Michael Walzer explains citizens' historical willingness to defend their state is an outgrowth of their natural attachment to their political community. He argues that the shared experiences and cooperative activity seen in a political community shape a common life that is very valuable to its members. For this reason, he assumes that most states are valuable to their citizens, unless circumstances indicate otherwise.[53] That is, "when states are attacked, it is its members who are challenged, not only in their lives, but also in the sum of things they value most, including the political association they have made".[54]

Finally, those that claim that intelligence is inherently unethical because its actions clash with everyday ethical standards fail to understand that such ethical measures cannot be transposed on to a special activity such as intelligence. That is, not only is it unhelpful to apply everyday moral discourse to the use of intelligence but it is also inappropriate. Intelligence collection when practiced in order to protect the political community is not an ordinary activity. It has a special role to play and therefore requires special ethical consideration. As Omand argues, "we have to accept that the realm that intelligence operates in is, of course, a zone where ethical rules that we might hope to govern our private conduct as individuals cannot apply".[55] Instead, one must establish an ethical framework that recognises the special role intelligence plays as protector of the political community as well

[52] Erskine, 'Rays of Light' (2004) p.364
[53] Walzer, M. *Obligations: Essays on Disobedience, War, and Citizenship* (Cambridge, MA: Harvard, 1970) p.98
[54] Walzer, M. *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: BasicBooks, 2000) p.53
[55] Omand, D. 'Dilemmas of Secret Intelligence' (2007) p.156

as potential instigator of harm. Similar to the use of military force in times of war, where it is argued that war represents such an extraordinary case that everyday ethical principles would simply be inapplicable, so too can intelligence be considered as an extraordinary case. Intelligence raises a set of important ethical issues that everyday ethical discourse is inappropriate for dealing with. Therefore an ethical framework created specifically for intelligence must be established that can engage with the particular issues it brings to the fore.

The Answer

In reviewing realist, consequentialist and deontological schools of thought, it is clear none provide a suitable ethical framework for evaluating intelligence collection. The contribution of each of the three positions is not in debate, and the general importance of them is, as noted, reflected in both domestic and international law. However, none provide a suitable match for the specific issues associated with intelligence. It has been argued that intelligence has an incredibly important role to play in protecting the political community, something that deontology and consequentialism cannot suitably reflect. Realism and consequentialism do not provide, it can be argued, the appropriate restrictions or limits on the damage that intelligence can cause. As such, the most appropriate ethical framework for intelligence is one able to combine parts of both the consequentialist and deontological schools while highlighting the important role of the political community as an ethical good as argued by the realists. Thus, this project will create an ethical framework that is able to balance the good associated with intelligence's role in protecting the political community while also limiting undue levels of damage.

The first part of the ethical framework will argue that the reason why intelligence collection might be considered ethically unacceptable is because of the 'harm' it can cause the individual. That is, intelligence can come into conflict with an individual's core interests and in doing so prevents him from continuing with his other, less fundamental interests. By understanding this negative aspect of intelligence is it then possible to determine if and when intelligence collection is justifiable. In order to achieve this, the second part of the ethical framework will argue for a set of Just Intelligence Principles. These principles are a set of criteria based on the just war tradition that, by making reference to the principles of just cause, legitimate authority, right intention, last resort, proportionality and discrimination, make it possible to understand if and when the harm caused by intelligence is justified.

Methodology

In order to answer the central research question of this thesis the methodology will involve three important aspects. The first aspect is a philosophical study in order to establish an appropriate ethical framework for intelligence collection. By reviewing the current ethical debate it has been demonstrated that realism, consequentialism and deontology are three ethical theories that each offer something important to the emerging field of intelligence ethics. It was also noted, however, that even though they each raised important points, none could offer a complete answer for the development of an ethical framework for intelligence. Establishing an appropriate ethical framework requires investigating and incorporating the relevant aspects of these quite diverse ethical schools into a single ethical framework. That is, paying attention to the ethical importance of the political community, acknowledging the good that intelligence can cause, and the necessity of placing certain prohibitions. In incorporating these three main points it is clear that the ethical theory will draw from both the cosmopolitan and communitarian bodies of literature. The methodology for developing the appropriate ethical framework will therefore stress the ethical importance of all individuals and the affect that intelligence can have on the human condition, while balancing this against the important contribution of the communitarian school; namely that the political community plays a vital ethical role in an individual's life and therefore requires protection. This pluralistic approach of incorporating various and diverse ethical theories means that it is possible to develop an ethical framework that is able to balance aspects of each of the different ethical schools that would have otherwise been in conflict.

The second aspect of the methodology will focus on the intelligence side of the project. Obviously, any work into intelligence will have several inherent obstacles to carrying out the research. As already noted, intelligence is inherently secretive. Letting intelligence become too public raises the prospect of putting operations in jeopardy. Furthermore, it is essential to keep one's methods secret given that if they were to become public it would give opportunity for other actors to devise systems that circumvent the effectiveness of the operation. Therefore its methods, people, targets, operations and procedures are tightly guarded secrets. From a methodological position, any research project that focuses on an area that is inherently secretive means that sources are scarce. Quinlan notes that "there are mountains of vivid fiction, a certain amount of conjecture and hint, and some wary memoir-writing, but the vast majority of citizens do not know and cannot readily find out in any specific, comprehensive and dependable way precisely what intelligence professionals do in

concrete day to day operational terms".[56] However, in order to create an ethical framework for evaluating intelligence activities then, by necessity, one must be aware the type of activities employed.

Fortunately, this does not mean that research into intelligence is totally unfeasible. Even Quinlan, who noted the difficulty of research within the field of intelligence, observed that "we can with reasonable confidence say a number of descriptive things about intelligence work".[57] The aim of this project is not to uncover individual instances of intelligence abuse or to delve into the history of specific cases, but rather to get a better understanding of the type of actions used. Therefore, this project will benefit from the already established historical and contemporary literature on intelligence. For example, *Defence of the Realm: The Authorised History of MI5* by historian Christopher Andrew[58] provide an interesting insight into what type of activities the agencies themselves are willing to acknowledge. Pivotal academic works based on extensive archival research also provide a great deal of information. Other useful sources on intelligence are works based on documents brought in by defectors. Similar sources can also include the memoirs of defectors or ex-intelligence officers who have written about their experiences. Some of the main examples include *The Mitrokhin Archive* written by defector Vasili Nikitich Mitrokhin,[59] *Defending the Realm* by ex-MI5 intelligence operative David Shayler,[60] and *Memoirs of a Spymaster* by Markus Wolf, former head of the East German intelligence agency the HVA.[61] Finally, some examples of intelligence collection activities have become public knowledge as a result of their use by the police and commercial actors. Obviously, when dealing with these types of sources there is always trepidation at their veracity. Intelligence agencies are not likely to authorise the release of information on methods that would put current practices and individuals in danger; while memoirs and autobiographies can carry the weight of the writer's own bias to convey themselves in a certain way.[62] One of the main aims of this thesis is to apply the ethical framework developed to a variety of different intelligence collection activities in order to

[56] Quinlan, M. 'Just Intelligence' (2007) p.3
[57] Quinlan, M. 'Just Intelligence' (2007) p.4
[58] Andrew, C. *Defence of the Realm: The Authorised History of MI5* (London: Penguin Books, 2010)
[59] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane, 1999)
[60] Hollinsworth, M. and Fielding, N. *Defending the Realm: MI5 and the Shayler Affair* (London: André Deutsch, 1999)
[61] Wolf, M with McElvoy, A. *Memoirs of a Spymaster: The Man Who Waged a Secret War Against the West* (London: Pimlico, 1998)
[62] For more on research into intelligence the problems associated with it see Hughes, R. G. and Scott, L. ''Knowledge is Never Too Dear': Exploring Intelligence Archives' in *Exploring Intelligence Archives: Enquiries into the Secret State* edited by Hughes, R. G., Jackson, P. and Scott, L. (Abingdon, Oxon, England; New York : Routledge, 2008) pp.13-40

make statements about under what circumstances they can, if ever, be justified. In order to examine a variety of different intelligence collection activities the examples are drawn from a range literature sources. However, this thesis does not seek to make any statement on the veracity of these literature sources and indeed they may well be unreliable. Indeed, take the *The Mitrokhin Archive* for example, the result of Vasili Mitrokhin's collection of materials from the KGB's foreign intelligence archives and defection to Britain. While this work is used throughout the thesis its use makes no direct claim on the reliability of Mitrokhin's own account or the documents he provided. Information supplied by such defectors can be shaped by the personal aims, needs and desires of the provider and as such can offer a distorted view. Indeed, as J. Arch Getty points out, "Mitrokhin was a self-described loner with increasingly anti-Soviet views who probably did not enjoy the confidence of his bosses… Maybe such a potentially dubious type (in KGB terms) really was able freely to transcribe thousands of documents, smuggle them out of KGB premises… all without detection by the KGB... but they do not much reassure professional historians worried about verifying sources. It may all be true. But how do we know?".[63] Therefore, the cases are hypothetical stories used as a basis for the discussion of the principles of harm and are not meant to strengthen scholars' knowledge of a particular range of information. Indeed, it would be possible to develop purely hypothetical cases to examine the ethical issues that intelligence might cause. However this method was avoided in order prevent the problems associated with manufacturing cases to support or reject certain positions or conclusions. Therefore, the intelligence literature is used as a base in order to illustrate various ethical calculations, though the discussions put forward make no claims about the historical reliability of the cases as a whole.

The third aspect of the methodology will involve combining the ethical theory with the research done on intelligence activities. This will involve using previously considered moral and theoretical judgements to which the different intelligence activities can then be applied. By exploring the relevant background and advancing philosophical arguments intended to bring out the relative strengths and weaknesses, it will be possible to demonstrate whether or not the ethical framework is applicable and internally coherent.[64]

---

[63] Getty, J. A. 'Christopher Andrew and Vasili Mitrokhin. The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*' The American Historical Review* Vol.106 No.2 (2001) p.684

[64] See Daniels, N. 'Wide Reflective Equilibrium and Theory Acceptance in Ethics' *The Journal of Philosophy* Vol.76 No.5 (1979) pp.256-282; DePaul, M. R. 'Two Conceptions of Coherence Methods in Ethics' *Mind* Vol.96 No.384 (1987) pp.463-481; and Haslett, D. W. 'What is Wrong with Reflective Equilibrium' *The Philosophical Quarterly* Vol.37 No.148 (1987) pp.305-311

Intelligence as Collection

One important step in a project such as this is recognising that intelligence as a field of study is incredibly broad, encompassing a diverse range of activities. This means that it is necessary to limit the scope of the thesis in order to allow for an appropriately in-depth analysis. How the field of intelligence is understood and how that field is engaged with – its boundaries, methods, targets, main concerns, et cetera – will affect the limits of any investigation.

As a field of study intelligence is often broken into an 'intelligence cycle' that outlines the process by which information is acquired, converted into its finished product and made available to policy makers. Generally the cycle is comprised of five steps: planning and direction, collection, processing, analysis, and production and dissemination. This project will focus on the collection phase by creating an ethical framework for determining if and when the actions employed to gather information are ethical. Focusing on a single phase of the intelligence cycle is important for several reasons. First, in order to create an ethical framework appropriate for intelligence a common thread between the different cases must be drawn so as to create a framework that can be applied to different instances while still being consistent. By focusing on a single section of the intelligence cycle it is possible to draw several underlying assumptions associated with the phase. Furthermore, the collection phase is often seen as one of the most important of the intelligence cycle, the "bedrock of the intelligence system" absorbing the majority of the allocated resources.[65] For example, the Church Committee commented that 90% of the resource allocation was devoted to the collection phase in the 1970s.[66] Moreover, it is the collection phase of the intelligence cycle that has recently come under increased scrutiny. The issues presented at Abu Ghraib and Guantanamo Bay, the programs of extraordinary rendition, and the rise of the surveillance state are each related to the way in which intelligence agencies collect information. What methods, targets and limitations should be put on this initial phase are the key concern for many and, so, must be addressed before the other phases.

In the literature intelligence collection is often broken into three different 'disciplines', grouped according to methods used: imagery intelligence (IMINT), signals intelligence (SIGINT), and human intelligence (HUMINT). These groupings are often in accordance with underlying, common aspects of the intelligence collection activity.

[65] Lowenthal, M. *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003) p.53
[66] Church Committee *Final Report* Book 1 p.344
Available http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm Accessed 4th April 2009

Therefore, by breaking the structure of the thesis along the lines of the collection disciplines it is possible to address some of the central aspects of the collection discipline.

Throughout the thesis the main focus will be state-run intelligence institutions. While it can be argued that there are other actors who carry out intelligence – private companies working for both the state and for private concerns – the field of intelligence is still dominated by state intelligence agencies. It should be noted that this is not meant to remove from the analysis some political communities that are not states. Indeed, in many respects it is the political community that is the important body. Yet in regards to intelligence collection, the state is the main provider and representative of the political community. Given that the field of intelligence is currently heavily dominated by state institutions, they will be the main focus.

Therefore, the types of issues and ethical questions being addressed in this thesis take the assumption that intelligence is being collected by official state organisations with the aim of protecting the political community from various threats. This means that intelligence carried out by private actors will not be considered. Many companies spend a considerable amount of energy and capital on collecting information. However, the end to which they collect this information is fundamentally different than that held by the state. This means the ethical quality of their activities involves a different set of questions, far outside the direct purview of this thesis. As such, the types of organisations that will feature in this project are those whose task is the collection of intelligence on behalf of the political community. This in itself is still quite broad as it can include those who would be directly considered to be members of the 'intelligence community', for example the British Security Service, Government Communications Headquarters, and Secret Intelligence Service, as well as police-type organisations such as the Police, Special Branch, Customs and Excise, and the Serious Organised Crime Agency.[67] All of these different organisations collect information on the intentions and capabilities of a large range of different actors in order to protect the political community from a variety of threats: "To Seek. To Know. To Forewarn".[68]

[67] It should be noted at this point that there is a difference between collecting 'intelligence' and collecting 'evidence'. That is, collecting intelligence carries no inherent necessity that it can be used in a court of law, where as evidence does. As a result, there are different and established criteria for deciding if and when the information collected can count as evidence or intelligence according to the relevant law. What must be understood, therefore, is that while intelligence can be collected by all these organisations, not all of it can be used in courts. Intelligence is used to help further investigations while evidence is used to help in a court. Indeed, intelligence information might be as simple as a telephone number or an address to check, and often does not come with a certificate of authenticity. For more on standards of evidence see Huxley, P. *Blackstone's Statutes on Evidence 11th Edition* (Oxford: Oxford University Press, 2010).

[68] Motto of the Security Division, Singapore's external security division.

At this point it is worth noting which intelligence communities will be the focus of the thesis. Obviously there will be more information on some of the intelligence institutions as compared to others, and some organisations might favour one set of activities over another, but the variety only serves to support the methodology used. This means that naturally the British, American and Soviet bloc intelligence communities will feature heavily as they have the largest literature published on their activities for various reasons. However, what should be noted early is that the ethical conclusions made are not, therefore, bound to these specific states and can be extrapolated onto different systems.

Structure

After taking into account all of the above considerations the structure of the thesis will be as systematic as possible. This means, that any ethical framework put forward must be established early and then applied to a series of different illustrative examples designed to explore how the theory would act in reality as well as testing it to ensure that it is internally coherent and based on reason. Therefore, the first substantive chapter will create the relevant ethical framework taking into account both the moral end to which intelligence is destined while providing a limit on the damage it can cause. Once the ethical framework has been established in Chapter One it will be applied to a series of illustrative examples. By doing this in a rigorous, systematic and coherent way the ethical framework is tested from various angles to ensure that it is internally coherent. It is essential to ensure that the ethical framework developed can be applied to a range of intelligence collection activities, rather than just fitting a specific case at a specific point in time. The following chapters will then apply the ethical framework to the major collection disciplines mentioned. Chapter Two will apply the ethical framework to imagery intelligence, Chapter Three will focus on signals intelligence and Chapters Four and Five will examine the ethical use of human intelligence. In each of the collection chapters the same structure will be used. First each chapter will outline what distinguishes the intelligence collection discipline from the other while also discussing what activities are included in the discipline. Once the respective intelligence activities are established in Section One, Section Two of each chapter will explore some of the ethical concerns that this intelligence discipline is likely to cause. Section Two is designed to go into greater depth in regards to the ethical questions, highlighting what issues are of specific concern for the collection discipline and how they relate to the ethical framework established in Chapter One. Therefore Section Two will provide the relevant tools for a more in-depth ethical evaluation. Section Three and Four will then use these tools to

evaluate the intelligence collection discipline by applying them to a series of explorative examples. The examples are not designed to be case studies *per se*, but are designed to create a better understanding of how the ethical framework might work in practice. Finally, each Chapter will conclude by outlining if and when the various intelligence collection activities are ethically permissible. The thesis will conclude by arguing that the ethical framework developed is appropriate for intelligence collection because it is able to balance the ethical good that intelligence can produce while placing appropriate limits on the harm it can cause.

Chapter One: Harm, Just War and a Ladder of Escalation

At the centre of the topic of 'intelligence ethics' is the tension between the belief that there are aspects of the intelligence business that seem "notably disreputable"[1] and the argument that without secret intelligence states cannot "understand sufficiently the nature of some important threats".[2] Indeed, it can be argued that over the last century intelligence has become one of the most vital tools a political community has in providing timely information designed to serve and protect and, as such, has become central to the ethical good represented by the protecting the political community. However, it can also be argued that the damage that intelligence can cause means that there should be limits on its use. Any ethical framework advanced for intelligence collection must, therefore, be able to explicitly balance the ethically unacceptable status or 'baggage of unworthiness' of intelligence with the positive role it plays in protecting the political community.

In order to deal with this tension the ethical framework that will be proposed in this chapter is comprised of two parts. The first part is designed to recognise those features of intelligence that might be considered ethically unacceptable by highlighting the 'harm' it can cause. Once the harm is understood, a set of Just Intelligence Principles will be established which outline if and when the harms caused are justified. These Just Intelligence Principles will be developed by drawing upon the just war tradition and its principles of just cause, legitimate authority, right intention, last resort, proportionality and discrimination. By balancing the harm that intelligence can cause with the Just Intelligence Principles it is possible to both limit the use of intelligence while that the appropriate protection of the political community it ensured.

This chapter is separated into three sections. The first deals with the notion of harm, outlining what it means to cause harm to someone so that it is about them that is ethically undesirable. The second section will outline the just war tradition and its principles, demonstrating how they can be interpreted for intelligence collection. Finally, the last section will bring the two previous sections together by placing the categories of harm and the Just Intelligence Principles into a single ethical framework, the Ladder of Escalation, so as to demonstrate how they interrelate.

---

[1] Quinlan, M. 'Just Intelligence: Prolegomena to an Ethical Theory' *Intelligence and National Security* Vol.22 No.1 (2007) p.1

[2] Omand, D. 'Reflections on Secret Intelligence' in *The New Protective State: Government, Intelligence and Terrorism* edited by Hennessy, P. (London: Continuum, 2007) p.116

Section One: What's the Harm?

It can be argued that the practice of intelligence collection involves actions that can cause harm to those it targets, the intelligence practitioners that engage in it, and even the rest of society. By providing the philosophical underpinnings for an account of what it means to cause unacceptable harm it is possible to illustrate the potential objectionable nature of intelligence collection. This notion of harm offers the benefit of being able to highlight what is ethically unacceptable about a range of divergent activities by making reference to the effect they have on the individual's most fundamental interests. This section will argue that by recognising the inherent value of all humans and the bare minimum standard that being human demands it is possible to understand how and in what ways all individuals can suffer harm.

Primum Non Nocere – Above All, Do No Harm

Many moral philosophers, including David Ross, Andrew Linklater and Brian Barry, have argued that the ethic of 'do no harm' should form the bedrock for those rules designed to govern relations between both individuals and societies. Linklater argues that, "the principle 'above all do no harm' should be regarded as the most fundamental and least demanding way in which citizens of one state can respect duties to humanity".[3] Indeed, Linklater maintains that "No society – not even the most cruel or violent – can survive unless most people internalise the principle that they should not inflict unnecessary harm".[4] As a result, every society has developed certain conventions against harm, designed to identify the most serious forms of injury that can befall members of the community and to set them as prohibited.[5] It is not that these harm conventions require societies or their members to act selflessly, but obliges them not to cause unnecessary harm. These harm conventions intercede "between the capacity to injure and the condition of vulnerability to... suffering that is specific to the human species".[6] The primacy, and what Linklater calls the "relative ease", with which many societies have been able to reach agreements about the most basic harms is reflected in those

[3] Linklater, A. 'Citizenship, Humanity and Cosmopolitan Harm Conventions' *International Political Science Review* Vol.22 No.3 (2001) p.262; Also see Barry, B. 'Some in the Disputation Not Unpleasant' in *Impartiality, Neutrality and Justice: Re-Reading Brian Barry's Justice as Impartiality* edited by Kelly, P. (Edinburgh: Edinburgh University Press, 2000) p.233; Ross, W. D. *The Right and The Good* (Oxford: Clarendon Press, 1930) p.22.

[4] Linklater, A. *The Problem of Harm in World Politics: Theoretical Investigations* (Cambridge: Cambridge University Press, 2011) p.29

[5] Linklater, A. 'Citizenship' (2001) p.264

[6] Linklater, A. *The Problem of Harm* (2011) p.30

domestic and international laws intended prevent or regulate injury and to enable the individual to experience as much of the good life as possible.[7]

The first step in establishing an ethic against harm begins with the realisation that individuals have certain requirements that are both 'vital' to them and vulnerable to outside interference. Joel Feinberg argues that in an individual's life there exist two types of interests. First are those interests that can be described as the more 'ultimate' aspirations, goals, needs and activities. These interests are shaped by an individual's version of the good life, that is, how he wants to live both his day to day life and the long-term goals he wants to achieve. These interests might include, for example, "producing works of art or literature… achieving high professional office, successfully raising a family", or just living his day to day life unhindered.[8] However, in order for these ultimate or higher interests to be attainable, other, non-ultimate and more fundamental, interests need to be first satisfied. This second category of interests forms the prerequisites or preconditions that must exist if an individual is to fulfil his more ultimate goals. These are his 'vital interests'. They are the fundamental requirements that an individual must have satisfied if he is to fulfil his own particular version of the good life. Feinberg calls these requirements "welfare interests" and John Rawls calls them "primary goods", but essentially they both amount to the same thing, that is, regardless of what conception of the good life the individual holds or what his life plans might be in detail, these preconditions must be satisfied first in order to achieve them.[9] If these vital interests fall below a threshold level, the ability to realise the more ultimate needs, goals or activities can become dramatically hindered. In this way, these interests are the most important interests a person has, and thus cry out for protection.

'Harm', therefore, can quite simply be defined as the violation of an individual's most vital interests. These interests have intrinsic value and damaging them can cause harm regardless of the repercussions. That is, even if, on balance, the individual does not experience the harm in a "tangible and material" way, he can still be said to be harmed since his vital interests have been violated or wronged.[10]

---

[7] Linklater, A. *The Problem of Harm* (2011) p.48. For example: Article 2b of the 1948 Convention of the Suppression and Punishment of Crime of Genocide; Article 2a on the Convention of the Suppression and Punishment of Crime of Apartheid; Article 1 of the 1993 UN General Assembly Resolution adopting the Declaration on the Elimination of Violence Against Women; Article 1 of the 1984 Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. Evans, M. D. *International Law Documents* 8th edition (London: Blackstone Press, 2007) p.39, p.309

[8] Feinberg, J. *Moral Limits of the Criminal Law: Vol.1 Harm to Others* (Oxford: Oxford University Press, 1984) p.37

[9] Feinberg, J. *Harm to Others* (1984) p.37; Rawls, J. *Theory of Justice* (Cambridge: Harvard University Press, 1971) p.62

[10] Feinberg, J. *Harm to Others* (1984) p.35

While John Mackie argues that there should be some scepticism about any idea of objective values or cross-cultural statements regarding what it means to harm someone and what values should or should not be respected as important to the individual, especially since their content will vary greatly depending on one's culture[11], it can be argued that it is still possible to outline those interests that are vital to all human beings regardless of what conception of the good life they might hold. Linklater makes this point by drawing on three overlapping arguments. Linklater starts with the recognition that all human beings are vulnerable to physical and mental attack as a result of the natural condition of the human body, that "On the one side [of the harm principle] there exist basic universals such as human frailty (the susceptibility of people as embodied selves to bodily pain and mental anguish, inevitable physical decline and death)".[12] It is because of the fundamental nature of what it means to be a human being that the harm principle first finds its footing, for it is here that basic assumptions about what it means to be alive and to continue with one's life can be made. Linklater then builds upon this by incorporating Geoffrey Warnock's argument of 'limited sympathies'. Warnock argues that man is "predominantly pre-concerned with the satisfaction of his own wants and those of one's group", meaning that there is a "liability to act… harmfully or damagingly... to others outside one's own circle of sympathies", and since everyone will be a non-member to some group there will always be the tendency for an individual to "stand outside the limited scope of ethical concern of many communities, and is vulnerable as a result to their injurious behaviour".[13] As a result of these limited sympathies Linklater argues that "all people have an interest in global rules of forbearance" and recognising the need for conventions against harm as a way of protecting themselves from harm.[14] Finally, Linklater highlights Barry's observation that all societies have developed quite a limited range of punishments, such as the deprivation of money or property, physical confinement, loss of body parts, pain and death, as a way of demonstrating that there are things that all individuals wish to protect regardless of their personal view of the good life. From this it can be judged that even societies with very different ideas about what constitutes

[11] Mackie, J *Ethics: Inventing Right and Wrong* (London: Penguin, 1977)
[12] Linklater, A. *The Problem of Harm* (2011) p.30. Also see Linklater, A. 'The Harm Principle in Global Ethics' *Global Society* Vol.20 No.3 (2006) p.331-332
[13] Warnock, G. J. *The Object of Morality* (London: Methuen, 1971) p.21, 80
[14] Linklater, A. *The Problem of Harm* (2011) p.83. Also see Linklater, A. 'The Harm Principle in Global Ethics' *Global Society* Vol.20 No.3 (2006) p.331-332

the good life possess similar understandings of the most fundamental forms of harm that can befall all human beings.[15]

Therefore, it is possible to isolate those factors that are of central importance in any human life, regardless of what the person chooses as his particular end goal, and develop a universal understanding of what it means to cause harm. Martha Nussbaum argues that through a notion of overlapping consensuses core vital interests held by all individuals can be established "without accepting any particular metaphysical conception of the world, any particular comprehensive ethical or religious view, or even any particular view of the person or human nature".[16] Quite simply, an individual's core interests can be determined by isolating those aspects of the human condition where, if the quality was to fall below a threshold level, the individual would cease to be considered to be living as "truly human, that is, *worthy* of a human being".[17] For example, being creatures of flesh and bone instantly "implies mortality, vulnerability and agency"[18], demonstrating how the need to protect the physical body is one of our most important vital interests. But protecting the physical body is not all. The need for mental integrity, autonomy, liberty, a sense of self-worth and a degree of privacy are each vital in an individual's life and thus need protecting.

Vital Interests

Even though the vital interests may differ in wording, content and structure compared to those argued by Feinberg and Rawls, the list below is similar in that it represents a set of ethical conditions designed to guide vital aspects of the human condition that can be endorsed by people who would otherwise have very different views regarding the aims and means for one's life.

Physical Integrity

Maintaining the integrity of the physical body is one of the most fundamental interests an individual has. The body is the physical home and representation of the *self*. The body represents main mechanism through which an individual experiences the world and carries out his wishes. If the body is damaged it severely hinders the ability to actualise any other aspect of the human experience. As such, there is a first and foremost interest in protecting

[15] Linklater, A. 'The Harm Principle in Global Ethics' *Global Society* Vol.20 No.3 (2006) p.332; Linklater, A. *The Problem of Harm* (2011) p.83; and Barry, B. *Justice as Impartiality* (Oxford: Oxford University Press, 1998) p.88

[16] Nussbaum, M. *Women and Human Development: The Capabilities Approach* (Cambridge: Cambridge University Press, 2000) p.76

[17] Nussbaum, M. *Women and Human Development* (2000) p.73. Emphasis in the original.

[18] Butler, J. *Precarious Lives: The Powers of Mourning and Violence* (London: Verso, 2004) p.26

the body, both as the physical home of the *self* and the main means through which an individual can actualise and interact with the rest of reality. If the physical body is damaged or violated to the extent that its integrity falls below a threshold level, it becomes unable to function properly. So basic is the interest in physical integrity that while people and societies have different and incompatible ideas that jostle with one another about what constitutes the good life, "virtually *any* conception goes better in the absence of physical injury".[19] Maintaining the integrity of the physical body is achieved in two ways: first, by providing the body with what it needs, and second is by protecting the body. The first aspect involves providing the body with its biologically necessary requirements in order to prevent the body from becoming unable to function, die prematurely or make it so that life is reduced to such a level as to not be worth living. Stanley Benn, Richard Peters and Martha Nussbaum each list these requirements as "the need for oxygen, food and drink, elimination... sleep and rest"[20] or equally put, "to be able to have good health, and be adequately nourished".[21] The second aspect to maintaining physical integrity is the importance in 'protecting' the physical body. This means that the individual must not be subjected to "absorbing pain or suffering" or to be inflicted with "grotesque disfigurement".[22] Also, the individual must have his physical sovereign boundaries of the body respected, "being secure against assault, sexual assault or abuse".[23]

Many types of physical violence can come into conflict with an individual's physical integrity, for example striking, cutting, amputating or severely damaging the body, as well as causing the body to experience prolonged periods of pain. Similarly, depriving the body of food, water or sleep can very quickly damage the body on a fundamental level and prevent it from operating properly.

Mental Integrity

If the body is the physical representation or the 'home' of the self and the means through which an individual experiences and actualises the world, then the 'psyche' is the individual's metaphysical home and the *place* where the world is experienced and actualised. The psyche is responsible for one's faculty of reason or the sum of a person's intellectual capabilities, representing the immaterial and actuating part of one's life. Feinberg notes that there must

[19] Barry, B. *Justice as Impartiality* (1998) p.88
[20] Benn, S. I. and Peters, R. S. *Social Principles and the Democratic State* (London: Allen and Unwin, 1959) p.67
[21] Nussbaum, M. *Women and Human Development* (2000) p.78
[22] Feinberg, J. *Harm to Others* (1984) p.37
[23] Nussbaum, M. *Women and Human Development* (2000) p.78

exist a "minimal intellectual acuity, emotional stability, absence of groundless anxieties" if the individual is to continue with his more ultimate interests.[24] To damage an individual's psyche is to prevent him from experiencing, actualising and interacting with the world as he normally would. Martha Nussbaum argues that if an individual's mentality or psyche is severely damaged then "we may judge… that the person is not really a human being at all".[25] Furthermore, much like physical pain, mental distress is harmful in and of itself. Having one's mental integrity blighted by overwhelming fear, anxiety, abuse or neglect is harmful because of the immediate mental pain it causes, aside from any long-lasting psychological damage that may accompany it. Maintaining an individual's mental integrity would therefore prevent any actions which cause great levels of stress or anxiety within the individual or can encourage the individual to have a mental breakdown.

Autonomy

The concept of autonomy is the capacity for self-rule. That is, one must be able to decide for oneself, without external manipulation or interference, what shape one's own life will take. As Nussbaum puts it, autonomy is being able to "form a conception of the good and to engage in critical reflection about the planning of one's life – the protection of the liberty of conscience".[26] Maintaining the integrity of an individual's autonomy requires, first, that the individual's ability to function rationally is protected. This means that the individual has the capacity to plan, choose, and reflect on options in terms of arguments, evidence and potential choices so as to make a decision.[27] Secondly, in order for an individual to be an autonomous agent he must be free to direct his decision-making process, meaning that it should not be excessively influenced or controlled by another force. Autonomy is circumvented if an individual's decision-making process is distorted through some pressure being applied to alter it. If an outside force puts pressure on an individual's decision-making process, the decisions made are not taken in light of the individual's own wishes or beliefs, but are based on the will of the person applying the force. The individual loses self-mastery and becomes a

[24] Feinberg, J. *Harm to Others* (1984) p.37
[25] Nussbaum, M. *Women and Human Development* (2000) p.73
[26] Nussbaum, *Women and Human Development* (2000) p.79. Feinberg calls this the 'Condition of self-government', and Richard Lindley refers to it as 'authorship' and 'self-rule', but it is essentially referring to the same phenomenon. See Feinberg, J. 'The Idea of a Free Man' in *Educational Judgments: Papers in the Philosophy of Education* edited by Doyle, J. F. (London: Routledge, 1973) pp.143-165; Lindley, R. *Autonomy* (Basingstoke: Macmillan, 1986)
[27] Frankfurt, H. 'Freedom of the Will and the Concept of the Person', *Journal of Philosophy* Vol.68 No.1 (1971) p.7

tool of the will of another. Indeed, autonomous agents must be able to act for "reasons all the way down according to their actions and according to their reasons".[28]

Autonomy is vital because respecting autonomy is akin to respecting the individual as a rational, self-determining agent.[29] For Immanuel Kant, the importance of an individual's autonomy is the result of respecting his rational nature, or his humanity: "humanity itself is a dignity…it is just in this that his dignity consists, by which he raises himself above all other beings in the world".[30] To treat an individual as if he were not autonomous is to treat him as if he were not a self-determined being, a non-person, more like a tool than an agent. In the words of Kant it is to treat the individual as a *thing* with only subjective value rather than a *person* with objective value.[31] Failure to respect an individual's autonomy is harmful because it fails to let him guide his own life and decisions.

Liberty

Closely connected to the concept of autonomy is the interest an individual has in liberty. Liberty, as John Stuart Mill notes, is "not the so-called Liberty of the Will… but Civil, or Social Liberty: the nature and limits of the power which can be exercised by society over the individual".[32] Autonomy is the freedom *to* decide one's will, while liberty is the freedom *from* constraints on acting out that will. As such, liberty is often simply defined as the "absence of interference or control"[33], whereby defending an individual's liberty is to set a limit on the extent of intervention by other individuals or society. For example, if an individual is prevented by others from doing what he could otherwise do, he is, to that degree, "unfree".[34] This means that the individual is afforded the right to be free from outside

[28] Herman, B. *The Practice of Moral Judgement* (Harvard University Press, 1996) p.228
[29] Berlin, I. *Four Essays on Liberty* (Oxford: Oxford University Press, 1969) p.137
[30] Kant, I. *Practical Philosophy* translated and edited by Gregor, M. (Cambridge: Cambridge University Press, 1999) p.6
[31] Kant's distinguishes between *things*, which are without reason but still have relative worth, and *persons*, whose nature sets them out as an end itself. If 'things' have any value at all it is only extrinsic, conditional and subjective and value is therefore equal to the price that someone chooses to set upon it. Rational beings, on the contrary, are called *persons*, as their very nature points them out as ends in themselves, as something which cannot be used as merely a means or restricts the freedom of action. Kant, I. *Groundwork of the Metaphysics of Morals* translated and edited by Gregor, M. (Cambridge: Cambridge University Press, 1998) p.37; and Kant, I. *Fundamental Principles of the Metaphysics of Morals* (London: Longmans, 1926) p.35
[32] Mill, J. S. *On Liberty* Edited by Gray, J (Oxford: Oxford University Press, 1991) p.5. For more on the distinction between 'social freedom' (liberty) and 'freedom of will' (autonomy) see Isaiah Berlin who points out that the question 'who governs me?' is logically distinct from the question of 'how far does government interfere with me?'. Berlin, I. *Four Essays on Liberty* (1969) p.130
[33] Feinberg, J. 'The Idea of a Free Man' (1973) p.7
[34] Violation of liberty implies the *deliberate interference* with one's activities. Berlin notes how Helvetius made this point very clearly: "the free man is the man who is not in irons, nor imprisoned in a gaol…it is not lack of freedom not to fly like an eagle or swim like a whale". Berlin, I. *Four Essays on Liberty* (1969) p.122

forces that wish to control, alter or interfere with the actualisation of his plans.[35] For example, external constraints might include physical barriers or coercive threats since, as Joseph Raz argues, acts of coercion directly encroach upon the freedom to act by eliminating options or courses of action otherwise available to an agent.[36]

Protecting an individual's liberty is important because if an individual finds himself with an area of non-interference that is too narrow, or nonexistent, then he becomes unable to continue with his other needs, goals or activities. Restraining individuals from doing what they otherwise could do goes against their interests in being free agents: "Where, not the person's own character, but traditions or customs of other people are the rule of conduct, there is wanting one of the principle ingredients of human happiness".[37] Incarceration or restraining otherwise free actions of the individual, therefore, are classic examples of how liberty can come under threat.

Human Dignity as Amour-Propre: A Sense of One's Own Self-Worth

Confidence in one's self-worth is so fundamental that without it one can become unable to continue or realise endeavours that are needed to fulfil one's aspirations. The requirement of self-worth demands that the individual's own sense of value is left intact. Without self-respect individuals are forced to feel worthless, meaning that "nothing may seem worth doing" and activities become "empty and vain" and they "sink into apathy and cynicism".[38] Damaging an individual's sense of self-worth was thus, for John Rawls, a violation of what perhaps is "the most important primary good of all".[39] Moreover, the experience of having one's self-worth attacked is a negative state in and of itself. That is, being in a state whereby the individual is forced to feel disgust with himself is emotionally harmful.

There are two aspects to an individual's sense of self-worth, first is how he views himself and second is how others view him. The first aspect is based on the argument that one of our most important and intimate relationships we have is with our self. As June Tangney and Ronda Dearing argue, "every time you look in the mirror you are faced with your closest ally and your, potentially, greatest enemy".[40] How an individual views himself, or is forced to view himself, involves accessing one of his most intimate relationships and the ability to attack this relationship means the ability to attack his core and his self-esteem. When an

[35] The term 'plan' is here intended to refer merely to whatever it is that a person broadly wants to do in and with his life.
[36] Raz, J. *The Morality of Freedom* (Oxford: Clarendon, 1986) p.369, 154
[37] Mill, J. S. *On Liberty* (1991) p.63
[38] Rawls, J. *Theory of Justice* (1971) p.440
[39] Rawls, J. *Theory of Justice* (1971) p.440
[40] Tangney, J. P. and Dearing, R. L. *Shame and Guilt* (London: Guilford Press, 2002) p.52

individual evaluates his sense of worth he views himself through a particular set of eyes and judges himself as those eyes would judge him. By viewing himself through these eyes the individual is forced to see the situation in a particular way. To be sure, this external spectator does not have to physically exist but rather exists as a metaphor to represent the new position as compared to the previous "unconscious state he thought or hoped or unthinkingly assumed he was in".[41] This new point of view can be actual or imagined; self- or externally created; a representation of his own personal standards; a particular individual, identity group or even a higher power; or quite simply a set of social constructs and norms that shape interpersonal lives. For example, to create emotions of shame or humiliation in an individual is forced to him to view himself through eyes that regard him as degraded, disgusting or dirty.

The second aspect of an individual's sense of self-worth is related to how he is viewed by those of his identity group. It is not just how the individual views, or is forced to view, himself that is important, but also how he thinks others are viewing him. This means that reputation plays a vital role in an individual's self-worth. The individual, by virtue of being a social animal, becomes a member of one or more identity groups, built on or guided by a specific set of social rules or norms. His life is shaped by these norms as he forms his conception of himself according to whether he follows them or not. By failing to live up to the rules of his social group he loses respect of that group. Firstly, this means that he runs the risk of losing important material benefits that his current position affords him – job, money, security. Secondly, since an individual draws his own conception of himself from how others view him, when they condemn him, his sense of self is externally attacked. Furthermore, since he himself has endorsed those standards he condemns himself when his failings are brought to others (and his own) attention.[42] This is the 'looking glass self' where the "ego thinks of itself as others think of it".[43]

Another side to this notion of self-worth as a social experience is the argument that an individual forms morally worthwhile bonds with other people from which he defines his identity and draws his own value. The breaking or betraying of those bonds can affect how that individual views his value. Concern must be given to relationships between the individual and the associations to which he is a member, and the ethical significance to be

[41] Taylor, G. *Pride, Shame and Guilt* (Oxford: Clarendon Press, 1985) p.66

[42] To say that an individual's actions are brought to 'his own attention' might sound paradoxical given that he should have been aware of it from the start, but this is not necessarily so. Individuals will carry out actions and then either delude themselves or consciously ignore what or why they are doing it. People are not always 'aware' of their actions or the reason for doing them – 'lying to themselves' for example – until an outside power brings the activity to their conscious self.

[43] Mannheim, B. F. 'Reference Groups, Membership Groups and the Self Image' *Sociometry* Vol.29 No.3 (1966) p.266

attributed to these associations. It is possible to argue that one of the most obvious moral bonds an individual might have is between himself and his community, though it is important to understand that one's communities can come in a variety of forms, including political parties, social movements, and labour unions. What is important is that the bonds that an individual makes to various, even overlapping and contradictory groups, are important to the individual in how he defines himself and the strength he draws.

Privacy

Privacy is a concept often used but rarely precisely defined.[44] As such, the 'umbrella' of the privacy concept can include a range of prohibitions and claims. For some, privacy is a psychological state[45]; while others define privacy as the extent to which "information about them is communicated to others";[46] and some see it purely as a physical state of affairs, being separated off from the rest of society.[47] This can mean that privacy is used to protect, among other things, freedom of thought, control over one's body, solitude in one's home, and control over information about one's self.[48] However, regardless of these many definitions, there are two concepts that are particularly relevant to intelligence collection and how it violates the interest in privacy: privacy as *boundaries* and privacy as *control*.

Throughout society there are many established boundaries that mark out areas where outside intrusion is unwelcome. These boundaries separate out what is private on the inside

[44] Arthur Mills declared that privacy is "difficult to define because it is exasperatingly vague and evanescent", and Julie Innes states that the legal and philosophical discourse on privacy is in a "state of chaos", while William Beaney has noted that "even the most strenuous advocate of a right to privacy must confess that there are serious problems in defining the essence and scope of this right". Beaney, W. 'The Right to Privacy and American Law' *Law and Contemporary Problems* Vol.31 (1966) p.253; Innes, J. *Privacy, Intimacy and Isolation* (Oxford: Oxford University Press, 1996) p.3; and Mills, A. *The Assault on Privacy: Computers, Databanks and Dossiers* (Michigan: University of Michigan Press, 1971) p.25

[45] Weinstein, M. A. 'The Uses of Privacy in the Good Life' in *Privacy: Nomos XIII* edited by Pennock, J. R. and Chapman, J. W. (New York: Atherton Press, 1971) p.94

[46] Westin, A. F. *Privacy and Freedom* (London: Bodley Head, 1967) p.7. For 'limited access' theory of privacy see Altman, I. 'Privacy – A Conceptual Analysis' *Environment and Behaviour* Vol.8 No.1 (1976) p.7; Breckenridge, A. C. *The Right to Privacy* (Lincoln: University of Nebraska Press, 1970) p.1; and Reiman, J. 'Privacy, Intimacy, and Personhood' *Philosophy and Public Affairs* Vol.5 No.1 (1976) p.42. For 'selective disclosure' see Fried, C. 'Privacy: A Moral Analysis' *Yale Law Review* Vol.77 No.1 (1968) p.475; Laufer, R. and Wolfe, M. 'Privacy as a Concept and Social Issue' *The Journal of Social Issues* Vol.33 No.3 (1977) p.34; and Miller, A. *The Assault on Privacy* (Ann Arbor: The University of Michigan Press) p.25

[47] Brandeis, L. And Warren, S. 'The Right to Privacy' *The Harvard Law Review* Vol.4 No.5 (1980) pp.193-220. Theorists who define privacy as 'to be let alone' see: Beytagh, F. 'Privacy and the Free Press: A Contemporary Conflict in Values' *New York Law Forum* Vol.20 No.3 (1975) p.455; Bloustein, E. 'Group Privacy: The Right to Huddle' in *Individual and Group Privacy* edited by Bloustein, E. (New Brunswick: Transaction Books, 1978) p.123; Freund, P. 'Privacy: One Concept of Many?' in *Nomos XIII: Privacy* edited by Rennock, J. R. and Chapman, J. W. (New York: Atherton Press, 1971) p.182-198; Konvitz, M. 'Privacy and the Law: A Philosophical Prelude' *Law and Contemporary Problems* Vol.31 No.2 (1966) p.279; and Monagham, H. P. 'Of Liberty and Property' *Cornell Law Review* Vol.62 No.1 (1977) p.414

[48] Benn, S. 'Privacy, Freedom and Respect for Persons' in *Nomos XIII: Privacy* edited by Rennock, J. R. And Chapman, J. W. (New York: Atherton Press, 1971) p.3

from that which is public on the outside. Over-stepping the mark, as it were, and violating an established boundary means violating the privacy of that person. Privacy as an area established by a boundary protects the individual from intrusions upon himself, his family, his home, his relationships and communications with others. This conception views privacy as a type of isolation or seclusion as the individual removes himself from society and sets out a sphere of non-intrusion. These boundaries can be physical – walls, clothes, bags for example – or they can be metaphysical - like 'personal space'. This concept of privacy means that the right 'to be let alone' is a question of what the relevant boundaries are, as the individual retreats to an area where others cannot enter, demarcated by a particular line in the sand.

Privacy as *control* is the right of the individual to control those things pertaining to himself, that is, "the control we have over information about ourselves"[49] or the "control over one's personal affairs".[50] Privacy conceived as thus can often equate to the notion of property rights. Judith Thomson argues that, while "we have fairly stringent rights over our property, we have very much more stringent rights over our own persons".[51] The individual's body is his intrinsically, inherently his without question. This claim includes the self and any extensions of that self. Someone's image, voice or even personal details work in the same way as any other property: an individual can sell the right to them or he may invite someone to use them, but if he decides that he no longer wishes for others to use them then his property right is violated if they continue to do so.[52] According to this notion of ownership, "one's actions and their history 'belong' to the self which generated them and [are] to be shared only with those with whom one wishes to share them".[53] Adam Carlyle Breckenridge argues that this means that "privacy is the claim of the individual to determine the extent to which he wishes to share himself with others".[54]

Privacy is often seen as a vital interest as a result of both its instrumental and its intrinsic worth. Instrumentally, it is vital since having one's privacy violated can result in severe physical, monetary, or social penalties. As long as we live in a society where "individuals are generally intolerant of life styles, habits and ways of thinking, and where

[49] Fried, C. 'Privacy' (1968) p.475
[50] Gross, H. 'Privacy and Autonomy' in *Privacy: Nomos XIII* edited by Pennock, J. R. and Chapman, J. W. (New York: Atherton Press, 1971) p.169
[51] Thomson, J. J. 'The Right to Privacy' *Philosophy and Public Affairs* Vol.4 No.4 (1975) p.303
[52] Extrapolated from the argument of ownership made by Judith Thomson in 'The Right to Privacy' (1975) p.304
[53] Shils, E. 'Privacy: Its Constitution and Vicissitudes' *Law and Contemporary Problems* Vol.31 No.2 (1966) p.290
[54] Breckenridge, A. C. *The Right to Privacy* (1970) p.1

human foibles tend to become the objects of scorn or ridicule", the desire for privacy will continue unabated.[55] Furthermore, protecting one's privacy is also central to maintaining the interest one has in autonomy and one's sense of self-worth since the more information another has about one, the more power this person has over one. For this reason David Solove couches privacy in terms of power, arguing that, "Privacy is an issue of power; it affects how people behave, their choices, and their actions".[56]

Privacy also has intrinsic value regardless of the financial or social damage that any violation might cause. Those who have nothing to hide would still object to other people being able to see or listen to them while they are in their home. Many philosophers argue that there is a need for a sphere of privacy in order for individuals to relax, find emotional release, self-reflection and self-analysis.[57] Individuals cannot survive without a space to call their own, free from the gaze of others. There must be a space where interference is prohibited as violations can cause anxiety, distrust and annoyance. Furthermore, even though the individual might not directly experience his privacy being violated it can be argued that he is still 'harmed' insofar as his vital interests are wronged when this occurs. For example, a camera inside an individual's home constitutes a violation of his interest in privacy and it can be argued that the individual is, as a result, harmed, even though he might not experience the interest violation in a "tangible or material way".[58]

Conclusion

By establishing an ethical framework that is capable of highlighting the 'harm' that intelligence collection can cause it is possible to better understand what it is about intelligence collection that might be considered 'objectionable'. That is, if intelligence comes into conflict with an individual's vital interests as described here, it can be argued that the 'harm' caused, without further qualification, should be prohibited. However, in the next section it will be argued that it is possible in some instances to justify the harm caused by an action by making reference to the surrounding circumstances. By using the just war tradition as a basis, Section Two will argue for a set of Just Intelligence Principles whose job will be to understand if and when the harm caused by the intelligence collection is justified.

[55] Parent, W. A. 'Privacy, Morality and the Law' *Philosophy and Public Affairs* Vol.12 No.4 (1983) p.276
[56] Solove, D. 'Conceptualising Privacy' *California Law Review* Vol.90 No.4 (2002) p.1143
[57] See Westin, A. *Privacy and Freedom* (1967) p.34; Bazelan, D. 'Probing Privacy' *Georgia Law Review* Vol.2 No.1 (1997) p.588; Weinstein 'The Uses of Privacy in the Good Life' (1971) p.99
[58] Feinberg, J. *Harm to Others* (1984) p.35

Section Two: Just War and Just Intelligence

In the previous section it was argued that all individuals posses a set of vital interests that are necessary for carrying out more ultimate aims and aspirations. Violating an individual's vital interests, it was argued, can be said to harm him and should, under normal circumstances, be prevented. Furthermore, it can be argued that intelligence collection activities can come into conflict with an individual's vital interests, causing him harm and should, as a result, be prohibited. However, as it was previously indicated, intelligence does play a vital role in protecting the political community from threats and as such there is a moral argument to make whereby acting to prevent these threats can justify the harm caused. What this section will do is propose an ethical framework that is capable of outlining under what circumstances, if any, the harm caused by the intelligence collection is justified. By examining the principles established in the just war tradition and adhering to the ethical principles on which they are based, it is possible to create a set of intelligence-specific principles, the Just Intelligence Principles. The first part of this section will outline the just war tradition and why it is the most appropriate source to draw from, while the second section will explore the principles of just cause, legitimate authority, right intention, last resort, proportionality and discrimination, discussing how each of these principles can be applied to intelligence collection.

Just War Meets Just Intelligence

It is impossible to think of a single 'just war doctrine', with a single point of linear development from a single idea. Instead, 'just war' is better understood as a set of "recurrent issues and themes in the discussion of warfare… which reflect a general philosophical orientation towards the subject".[59] What can be seen is an organic, evolutionary process that has altered over time in response to the moral issues of the day. It first took shape at a time when the Roman Empire was trying to reconcile the tensions between the pacifist themes of Christian theology and the practical needs of protecting its borders. As an ethical framework the just war tradition was designed to grapple with the notion that there are some acts, such as killing someone, that "in the normal context are gravely wrong", while understanding that in certain circumstances, war for example, these same acts cannot totally be "dismissed by pacifist anathema which insist that the virtuous abstain from it".[60] The state must be able to

[59] Clark, I. *Waging War: A Philosophical Introduction* (Oxford: Clarendon, 1988) p.31
[60] Quinlan, M. 'Just Intelligence' (2007) p.2

act to protect those whose duty it is to care for. However, this does not allow unrestrained action and, as such, there is still a need for limiting the damage that war can cause. As a result, what evolved over the centuries was a set of principles designed to govern and limit the activity of war and the harm it can cause, while maintaining the broader context of the duty of the public authorities to be able to use violence for the protection of one's state or that of international peace and stability.[61]

Given that the just war tradition is well versed in reconciling the tension that is born from balancing the needs of the political community with the damage that these needs can cause, it represents the most appropriate starting-point in designing an ethical intelligence framework. As the previous section noted, intelligence collection includes practices that can cause harm to those it targets and as such is unacceptable in an everyday context. However, by creating an ethical framework based on the just war tradition and establishing a set of Just Intelligence Principles, it is possible to understand when this harm is actually justified given the prevailing circumstances. These Just Intelligence Principles demand both a limitation on the harm that is caused by intelligence collection, while also outlining exactly when that harm is justified. Each of the Just Intelligence Principles is based upon the ethical arguments made by the just war tradition and as such demonstrate a moral argument for the control and use of intelligence collection.

These Just Intelligence Principles include the following:

- Just Cause: There must be a sufficient threat to justify the harm that might be caused by the intelligence collection activity.
- Authority: There must be legitimate authority for engaging in the intelligence collection activity, representing the political community's interests, sanctioning the activity.
- Intention: The activity should be used for the intended purpose and not other (political, economic, social) objectives
- Proportion: The harm that is likely to be caused should be outweighed by the probable gains
- Last Resort: Less harmful acts should be attempted before more harmful ones are chosen.
- Discrimination: There should be discrimination between legitimate and illegitimate targets of intelligence collection.

[61] Orend, B. *Morality of War* (Peterborough: Broadview Press, 2006) p.9; Turner, J. T. *Just War Tradition and the Restraint of War: A Moral and Historical Inquiry* (Princeton: Princeton University Press, 1981) p.xxi

Just Cause

Thomas Aquinas, one of the first just war theorists, argued that for a war to be just there must be some reason or injury to give cause, namely, "that those who are attacked must be attacked because they deserve it on account of some fault".[62] International law currently frames the main justification for going to war as self-defence based on the argument that states have an ethical duty and right to defend themselves when attacked.[63] This justification for killing in the context of a war of self-defence can be extrapolated either from the 'domestic analogy' or from the argument that the state has an ethical duty to protect its people. This first moral argument is based on the ontological justification for wars of self-defence drawn from the 'domestic analogy' whereby the ethical framework designed for everyday activities is extrapolated 'up' in instances such as war. The second moral argument is based on the argument that "allows one to justify courses of action with reference to the good of the political community" and "maintains that acting in the national interest is itself complying with a moral principle".[64] In short, in order to protect the political community, methods which cause varying degrees of harm can be justified.

The just cause equivalent for intelligence collection is that there must be a *sufficient threat* to justify the harm that might be caused by a particular activity. It is the role of intelligence agencies to safeguard and maintain a state's "national security and, in particular, its protection against threats", including threats from "espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means".[65] This is not an effort to universalise British legal statements, but rather this statement reflects the types of threats that states currently perceive as being the main dangers they face. In order to protect the political community from these dangers the intelligence community acts to locate them, assess their probability and then prevent them. The intelligence community is tasked with trying to "evaluate whether or not there is a danger of enemy attack"[66], and by investigating those potential threats the intelligence community is acting out of self-defence as it seeks to maintain national security. It is through the detection and prevention of potential threats that intelligence collection therefore receives its just cause.

---

[62] Aquinas, T. 'From *Summa Theologiae'*, in *International Relations in Political Thought* edited by Brown, C., Nardin, T. and Rengger, N. (Cambridge: Cambridge University Press, 2002) p.214

[63] For example, the United Nations Charter states that nothing "shall impair the inherent right of individual or collective self-defence if an armed attack occurs". UN Charter Article 51.

[64] Erskine, T. 'As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering' *Intelligence and National Security*, Vol. 19, No. 2 (2004) p.364

[65] United Kingdom Security Service Act 1989 Chapter 5 Section 1.

[66] Cohen, R. *Threat Perception in International Crisis* (Madison: University of Wisconsin Press, 1979) p.5

Legitimate Authority

In order for a war to be considered morally permissible according to the just war tradition it must be authorised by the right authority, that is, those who have the right to command by virtue of their position. As Aquinas stated, "the ruler for whom the war is to be fought must have the authority to do so" and "a private person does not have the right to make war".[67] The principle of legitimate authority is based on the argument that those entrusted with the common good are charged with the duty to protect the political community: "since the care of the common weal is committed to those who are in the right authority, it is their business to watch over the common weal".[68] Therefore, it is only that body charged with protecting the common good, holding their interests in mind, which can take them to war justly.

In the same way that there is a need for a legitimate authority to justify war, so to must a legitimate authority be present to sanction the harms caused by intelligence collection. Since intelligence collection involves some form of harm, society needs to rest the authority to act in institutions that represent the wishes and needs of those they are charged with protecting. Furthermore, one might argue that intelligence collection needs to be authorised by a body that is able to ensure that the Just Intelligence Principles are being met fully and without bias. Those planning, performing or even managing operations often have invested interests in getting their job done. There are also huge external pressures on the intelligence community to provide the 'correct' information in a timely fashion to their clients. As such, as David Omand points out, there is a need for "proper oversight from outside the intelligence community and a robust mechanism where any individual issue raised can be done so without fear, yet done in ways that will protect the essential secrecy of the business".[69] Therefore, there must be an objective authority that is able to weigh up the harms caused against the necessity of protecting the political community in an unbiased way.

Consequently, one can argue that in order for intelligence collection to be just there must be, in the words of the just war tradition, a *legitimate authority sanctioning the activity* – "it must be decided on behalf of the community, not simply the act of private individuals".[70] The question must be, however, who or what forms the legitimate authority in the case of intelligence. The answer to this, similar to the instance of war, is that it is in the political community and that community's representatives that legitimate authority is founded. States matter morally only because the people inside them matter morally and the

[67] Aquinas, T. 'From *Summa Theologiae'* p.214
[68] Aquinas, T. 'From *Summa Theologiae'* p.214
[69] Omand, D. 'The Dilemmas of Using Secret Intelligence for Public Security' in *The New Protective State: Government, Intelligence and Terrorism* edited by Hennessy, P. (London: Continuum, 2007) p.165
[70] Norman, R. *Ethics, Killing and War* (Cambridge: Cambridge University Press, 1995) p.118

state's right to self-defence rests on the idea that the people of that state have the right not to suffer attack. Therefore the state draws its legitimacy to authorise the use of intelligence from the argument that it is acting to protect the political community. The state is charged with the duty to act in the best interests of those it governs, with powers being entrusted to the government as agents of the political community. What this means is that in many instances it will be the state that acts as the legitimate authority, with particular institutions whose duty it is to represent the political community's interests and wishes, acting as the authorising power.[71]

Examples of the sort of state institutions that can fulfil this role can be seen in many of those existing oversight mechanisms employed by Western liberal democracies. For example, there are three main oversight mechanisms currently in use whose purpose is to monitor the use of intelligence and determine if the actions carried out are done with the best interests of the political community in mind: the judiciary, the legislative and the executive. Each of these institutions represents the political community in a different way and is tasked with protecting it from a variety of threats. The judiciary is regarded as one of the most unbiased bodies given that it is well versed in making decisions based on available evidence rather than social fluctuations and must represent its results in terms of reason.[72] However, there are often questions of accountability and knowledge in that the judiciary might not fully understand the importance of politically charged information as well as not being easily held accountable to the political community. While the legislative does represents a powerful means through which the wishes of the political community can be more easily articulated it has problems in that it has, on more than one occasion, failed in its role because of political infighting as well as being notoriously public and slow, making it inappropriate for individual operation authorisation. The executive, in comparison, has the benefit of offering brevity in decision-making, though this does raise concerns regarding the issue of politicalization and the problem associated with placing control in a small number of hands. Regardless of the

[71] As it was noted in the Introduction, this is not to say that other entities that are not states cannot carry out 'just intelligence' simply because they are not a state. For example, Evans has argued that "some people have fought wars for statehood and *ipso facto* have not fought them as states... against other states which claim to have sovereignty over them". Therefore, political communities that are not necessarily states can also have intelligence mechanisms which act so as to protect them. These political communities would therefore have to rest the authority to sanction their activities in some 'legitimate authority', as well as fulfilling the other *just intelligence principles*, if they wish their intelligence collection to be just. Some fear that such a definition will provide the possibility for non-state actors, like terrorists, to claim themselves as 'legitimate authorities'. However, to what extent this is actually possible given difficulty for small groups to successfully claim to fight on behalf of those without having any substantial way of proving it. See Evans, M, 'Moral Theory and the Idea of a Just War' in *Just War Theory: A Reappraisal* edited by Evans, M. (Edinburgh: Edinburgh University Press, 2005) p.17

[72] Horowitz, D. L. 'The Courts as Guardians of the Public Interest' *Public Administration Review* Vol.37 No.2 (1977) p.148

mechanism chosen, however, what should be clear is that resting authority in one or more of these bodies represents a means of evaluating and sanctioning intelligence in reference to the needs and concerns of the political community while demonstrating a reduced risk of bias.

Right Intentions

It is thought by just war theorists that it is not enough to have an objective just cause for war, but there must also be a proper subjective right intention. That is, the intention behind an act alters the moral quality of an act and, as such, has become an important part of common ethical discourse, altering how an event is talked about, speculated on, and judged.[73] Leaders must be able to justify their decisions, noting that they had the right intentions: "for those that slip the dogs of war, it is not sufficient that things turn out for the best".[74] The reasoning behind this is that it is very possible for "war to be declared by legitimate authority and have just cause, yet nonetheless be made unlawful through a wicked intention".[75] This means that even when there is just cause for war, this reason cannot then be used to serve as a cover for the pursuit of other aims. The aims of the war must be consistent with the just cause invoked to justify the war. If it is a war of self-defence, for example, then the intention of the war must be to deal with this and not fight a war of greed or lust. These intentions are then reflected in the war itself. How the war is carried out should reflect the intention behind the war. For example, if the just cause is one of self-defence then the intention of the war must flow directly from this and not involve tactics of domination or subjugation.

By drawing on this logic it can be argued that in order for intelligence collection to be morally permissible *the intelligence collection activity should be used for the stated purpose and not other political, economic, or social objectives*. This means that the intention should be to deal with the just cause directly rather than using the just cause as an excuse for other purposes. The intention will be then be reflected in the type of actions carried out and the ends sought. For example, since the just cause for the Just Intelligence Principle is to assess and determine the reality of a threat, the intention, and therefore the means employed, should directly correlate to the threat. The means used, who is targeted, and how much harm is allowed, should all flow from the intended purpose of dealing with the threat. This principle of right intention is designed to prevent the use of intelligence collection for personal, political or economic gain, even though there might be an existing sufficient threat.

---

[73] See Thomson, J. J. *Rights, Restitution and Risk: Essays in Moral Theory* (Cambridge: Harvard University Press, 1986) pp.101-102; Scanlon, T. M. and Daney J. 'Intention and Permissibility' *Supplement to the Proceedings of the Aristotelian Society* Vol.74 No.1 (2000) pp.301-317

[74] Lackey, D. P. *The Ethics of War and Peace* (London : Prentice Hall International, 1989) p.32

[75] Aquinas, T. '*Summa Theologiae'* (2002) p.214

Last Resort

In the just war tradition the principle of last resort is an attempt to allow those relatively benign means of responding to a crisis, like diplomacy or economic pressure, a chance to resolve the issue before the resort to organised violence is permitted. This way, if it is possible, more harmful acts are avoided. Richard Miller argues that, "even if [force] is sometimes necessary and morally justifiable, *but* the just cause could be achieved by non-violence means then the party has a moral duty to prefer these methods".[76] However, Robert Phillips warns that, "it is a mistake to suppose that 'last' necessarily designates the final move in a chronological series of actions".[77] If it did, then force would never be legitimised since one could always continue to negotiate. Instead, what it demands is that actors "carefully evaluate all the different strategies that might bring about the desired end, selecting force as it appears to be the only feasible strategy for securing those ends".[78] If time and circumstances permitted other means short of force then they should be used. But there is not a rigid set of steps that one must follow at all times, beginning with the least harmful and ending in war.

Based on this conception of last resort, one can argue for a similar rationale for the Just Intelligence Principles. In order for an intelligence collection activity to be just, it must only be used once other less harmful means have been exhausted or are redundant. Any attempt to deal with the threat should use the least harmful first and thus give the opportunity for more harmful activities to be avoided. While there is no rigid methodology or steps that must be worked through, it does require that some of the more harmful actions are not resorted to out of ease or expediency.

Proportionality

The idea of proportionality is one of the oldest principles not only of the just war tradition, but also of moral theory and military strategy in general.[79] Leaders and individuals are constantly tasked with weighing up the costs of an action against what can be gained. The principle of proportionality is similar in that it establishes the notion that the violence of war should be proportionate to the threat that it is meant to overcome, placing a limit on the amount of harm allowed for a given action. Kateri Carmola argues that the need for a principle of proportionality is rooted in the human tendency towards disproportionate,

[76] Miller, R. B. *Interpretations of Conflict, Ethics, Pacifism and the Just War Tradition* (Chicago; London: University of Chicago Press, 1991) p.14
[77] Phillips, R. *War and Justice* (Norman: University of Oklahoma Press, 1984) p.14
[78] Bellamy, A. J. *Just Wars: From Cicero to Iraq* (Cambridge; Malden, MA: Polity Press, 2006) p.123
[79] See Coates, A. J. *The Ethics of War* (Manchester: Manchester University Press, 1997); Johnson, J. T. *Morality and Contemporary Warfare* (London: Yale University Press, 2001); Lackey, D. P. *The Ethics of War and Peace* (1989); Norman, R. *Ethics, Killing and War* (1995)

unmeasured, passionate and cruel responses.[80] Clausewitz warns that war by its very nature tends towards the extreme and the utmost use of force: "an act of violence which in its application knows no bounds and in which a proportionate response to another's power is met by an escalating response and so on".[81] Whilst war might be the legitimate answer to right a wrong, not all wrongs a state can suffer are of sufficient magnitude to justify the harm that might be caused: "some wrongs are neither grievous nor widespread enough to legitimate the inevitable evils that war entails".[82] This principle demands that the negative consequences of the war are in proportion to the gains to be achieved.

One can argue that, for intelligence collection to be just, the level of harm that one perceives to be caused by the collection should be outweighed by the perceived gains or avoided harms. In collecting intelligence there is always an objective of acquiring information. In order for the action to be just it must be determined whether the information to be gained is of such value as to outweigh the overall harm caused. For example, as already mentioned in the Introduction, Michael Herman pursues this general assessment for the ethical evaluation of intelligence when he argues that "knowledge and activities can be examined separately, and then can be integrated into an ethical balance sheet".[83] Erskine examines this stance and notes that when looking at intelligence in this way, if "At the bottom of the ledger the benefits of intelligence knowledge are found to be in credit... then the means employed to gather intelligence can be morally justified by the positive impact of knowledge acquired".[84] The principle of proportionality is consequentialist in that it evaluates the relevant harm and damage caused as a consequence and weighs it against the relevant expected gains or the harms avoided.[85] This limits the use of intelligence collection by preventing highly harmful collection means from being used when the benefit is likely to be minimal, even though that there might be a just cause, a right intention and legitimate authority present.

---

[80] Carmola, K. 'The Concept of Proportionality: Old Questions and New Ambiguities' in *Just War Theory: A Reappraisal* edited by Evans, M. (Edinburgh: Edinburgh University Press, 2005) p.97

[81] Clausewitz, C. *On War*, ed. and trans. Howard, M. and Paret, P. (Princeton, N.J.: Princeton University Press, 1989) p.76

[82] Bellamy, A. J. *Just Wars* (2006) p.123

[83] Herman, M. *Intelligence Services in the Information Age* (London: Frank Cass, 2002) p.290

[84] Erskine, T. discussing consequentialist theory in 'Rays of Light' (2004) p.366

[85] Consequentialism is actually a broad umbrella term including 'classical utilitarian', for example, which holds that the property that matters is how far sentient beings enjoy happiness; others would emphasise consequences like human freedom, social solidarity, autonomous development of nature, or a combination of the above See Baron, M. W., Pettit, P. and Slote, M. *Three Methods of Ethics* (Oxford: Blackwell, 1997) p.5; Bentham, J., Burns, J. H. and Hart, H. L. A. editors *An Introduction to the Principles of Morals and Legislation* (Oxford: Clarendon, 1996); Darwall, S. L. 'Introduction' in *Consequentialism* edited by Darwall, S. L. (London; Blackwell Publishers, 2003) pp.1-8; and Mill, J. S. *Utilitarianism* edited by Crisp, R. (Oxford: Oxford University Press, 1998)

Discrimination

The requirement that an attack must discriminate between legitimate and illegitimate targets is one of the most stringently codified just war rules, as reflected in the international laws of war.[86] Traditionally, the distinction between legitimate and illegitimate targets was seen to arise out of the moral prohibition against taking 'innocent life'. Those who were 'innocent' had done nothing to warrant being targeted, whereas those who were 'not innocent' had acted in some way or there had "something about them" so as to justify them being targeted.[87] Although, rather than referring the moral status of the individual and discriminating on the basis of moral guilt, 'innocence' in this sense is based on the negative etymological derivation of the word from the Latin *nocere* (to harm) to mean 'harmless', rather than 'blameless'.[88] The principle of discrimination therefore distinguishes between those who would cause harm, or more typically understood as those who present a threat.[89] The reason why those who represent a threat are highlighted as legitimate targets is based, in the first instance, on the moral right of the individual to act in self-defence, whereby the armed solider who poses a threat can be attacked out of pre-emptive self-defence. The principle of self-defence essentially means that if someone attempts to kill an individual, then that individual's right to life justifies his killing the attacker if necessary – the attacker's right to life is in some way overridden by the defenders right to life. There is a strong ethical and philosophical tradition that argues that the individual has first and foremost the right to protect his own life, even at the expense of another's life.[90] Richard Norman then extends this logic: "what would you do if someone attacked your sister? And the implied answer would be to defend her... and so you ought to also be prepared to defend your country and to kill in her defence".[91] As

---

[86] Geneva 1949; 1977 *Geneva Protocol II Additional to the Geneva Convention of 1949: The Protection to of Victims of Armed Conflicts Section* Chapter 11 'Protection of Civilian Population' Article 51 §2

[87] Nagel argued the idea that it is not fair to target just anyone in war, there must be "something about them" in order to justify it. Nagel, T. *The View From Nowhere* (Oxford: Oxford University Press, 1986) p.162

[88] See Coates, A. J. *Ethics of War* (1997) p.233-235. Also see Norman, R. *Ethics, Killing, War* (1995) p.168; McMahan, J. 'Innocence, Self-Defence and Killing in War' *The Journal of Political Philosophy* Vol.2 No.1 (1994) p.193; and Nagel, T. *Mortal Questions* (Cambridge: Cambridge University Press, 1979) p.70

[89] Ian Clark also argues that it is possible to discriminate between legitimate and illegitimate targets based on other factors such as 'political', 'institutional', 'moral' or 'military' alignment. Political discrimination distinguishes between those who are in support of the government; institutional between those who are a part of the mechanisms of war; moral focuses on 'moral guilt'; and military distinguishes between soldiers and civilians. Clark, I. *Waging* War (1988) pp.88-92

[90] While there is much literature that debates the principle of self-defence the argument that there is a right to defend one's self when threatened is well established. See, Alexander, L. 'Self-Defence and the Killing of Non-Combatants: A Reply to Fullinwider' *Philosophy and Public Affairs* Vol.5 No.4 (1976) pp.408-415; Kasachkoff, T. 'Killing in Self-Defense: An Unquestionable or Problematic Defense?' *Law and Philosophy* Vol.17 No.5/6 (1998) pp.509-531; Montague, P. 'The Morality of Self-Defense: A Reply of Wasserman' *Philosophy and Public Affairs* Vol.18 No.1 (1989) pp.81-89; Otsuka, M. 'Killing the Innocent in Self-Defense' *Philosophy and Public Affairs* Vol.23 No.1 (1994) pp.74-94; and Thomson, J. J. 'Self-Defense' *Philosophy and Public Affairs* Vol.20 No.4 (1991) pp.283-310.

[91] Norman, R. *Ethics, Killing, War* (1995) p.120

such, those who represent a significant threat are legitimate targets because the state is acting out of self-defence. As such, current legal canons translate the distinction as existing between soldiers who bear arms and are legitimate targets because of the threat they pose, and civilians who represent no direct danger and so are illegitimate targets.

A second way of understanding the principle of discrimination is based on Walzer's argument that an individual becomes a legitimate target because he has become a "dangerous man" and has, therefore, acted in such a way as to waive or temporarily suspend those rights that would have otherwise protected him from attack.[92] By taking up arms the soldier has clearly demarcated himself as separate from the ordinary civilian and sacrifices some of his rights in the process, such as, the right not to be attacked.[93] It can be argued, therefore, that combatants are legitimate targets because they acted in such a way as to waive their normal protective rights.

For intelligence, one can argue that in order for the collection of information to be just there must be discrimination between targets. Just as soldiers are legitimate targets because they are a threat and because they give up certain protective rights, arguably any individual can act in a way that makes him a threat or where he forfeits certain protective rights. In this way, civilians and not just soldiers can become legitimate targets if they have acted in such a way as to mark themselves as a threat. Walzer notes that while it can be hard to understand this extension of legitimate status beyond the class of soldiers, through modern warfare this has become common enough. Civilians can become 'partially assimilated' when they are "engaged in activities threatening and harmful to their enemies".[94] This notion of partial assimilation means that when the individual carries out some act – making himself a threat or contributing to the threat for example – there are occasions when the civilian makes himself a legitimate target. The principle of discrimination for the Just Intelligence Principles therefore distinguishes between those individuals who have no involvement in a threat and are protected and those who have made themselves a part of the threat and in doing so have become legitimate targets.

[92] Walzer, M. *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 2000) p.145
[93] McMahan, J. 'On the Moral Equality of Combatants' *Journal of Political Philosophy* Vol.14 No.4 (2006) p.381
[94] Walzer, M. *Just and Unjust Wars* (2000) p.145, 146

Conclusion

This section has argued that activities that cause harm should be, if there are no other intervening considerations, prevented. However, this section has also claimed that there is an ethical argument to be made that this harm can be justified in reference to principles such as those seen in the just war tradition. War is an established case where the actions it entails can cause devastating amounts of harm, but if the circumstances surrounding the war satisfy the just war principles then it is possible to argue that the harm caused is justified. What this section has demonstrated is that by using those principles established by the just war tradition it is possible to transfer the ethical arguments made onto intelligence collection. That is, the harm caused can be justified given the correct circumstances. These principles set limits on the use of intelligence collection in that the activity is to be prohibited if they are not satisfied.

What will be demonstrated in the next section, however, is that intelligence collection involves a variety of activities, each of which can cause a different level of harm. Therefore, there is a need to understand both what alters the level of harm caused and how these different levels can then be related to the Just Intelligence Principles. This will be achieved through the creation of a Ladder of Escalation.

Section Three: Ladders and Levels

Section One of this chapter outlines an ethic against harm as a means of demonstrating what it is about intelligence collection that is ethically unacceptable. The second section then established a set of Just Intelligence Principles designed to outline if and when these harms, in relation to the surrounding circumstances, can be justified. However, the problem for intelligence collection is that it is an umbrella term that covers a vast range of different activities that can be used in a variety of different situations. The harm caused as a result can be equally diverse as each activity has the potential to cause a different amount of harm to the target. What this section will argue is that because different intelligence collection activities can cause different amounts of harm, by determining the level of harm caused by each activity it is possible to spread them up a metaphorical Ladder of Escalation.[95] Furthermore, depending on the level of harm caused by the activity, the circumstances required to justify that harm will change. Therefore, it is necessary to outline how the Just Intelligence Principles can also consist of various levels in order for them to be applied to the different levels of harm caused.

Ladder of Escalation

The metaphor of the 'Ladder of Escalation' is useful because it illustrates how intelligence collection consists of various activities, each of which can cause a different degree of harm. These different collection activities can be placed on a graduated ladder over different levels depending on the harm that is caused. Similarly, the Just Intelligence Principles can be separated out and then placed on a graded ladder alongside the levels of harm. By doing this it is possible to portray the idea that there is a correlation between the two and that in order to justify certain harms you must have the same or higher level of Just Intelligence Principles present. As the level of harm goes up the Ladder of Escalation so should the Just Intelligence Principles.

[95] This metaphor of a 'Ladder of Escalation' is drawn from Herman Kahn's work on the problem of escalation in a thermonuclear age. Kahn probes the dynamics of escalation and demonstrates how the intensification of conflict can be depicted by means of a definite escalation ladder, ascent of which brings opponents closer to all-out war. At each rung of the ladder, before the climb proceeds, decisions must be made based on numerous choices. As such, Kahn's ladder metaphor for understanding the coercive features of international affairs offers a "convenient list of the many options facing the strategist in a two sided confrontation". Kahn, H. *On Escalation: Metaphors and Scenarios* (London: Pall Mall Press, 1965) p.37

Measuring the Levels of Harm

One of the main benefits of the Ladder of Escalation is its ability to outline the different levels of harm that can be caused by various intelligence collection activities. The question, however, must be how to determine and differentiate these different levels of harm. Intuitively, there is already the sense that different activities will cause different amounts of harm. For example, it is natural to experience a longer term of isolation compared to a shorter term as more harmful to oneself. What will be argued here is that depending on the particular vital interest violated, the severity of the violation and the duration of the violation, the level of harm caused is altered.

The first point argues that, *all other things being equal*, some interests such as physical and mental integrity can take precedence over the other interests such as autonomy, liberty, self-worth or privacy.[96] Berlin declared that liberty and autonomy are not necessarily the first need of an individual: "the peasant needs clothing or medicine before, and more than, personal liberty".[97] This is not to say that the other vital interests outlined above are not truly vital, for they are. If an individual is deprived of them then he would be unable to continue his life in any meaningful way. There must be, however, an understanding that if some interests, like and physical and mental integrity, are severely violated then an individual's interest in autonomy, liberty, self-worth or privacy can become redundant. There must be a basic level of physical and mental integrity in order for the other vital interests to be realised. In addition, some of the intelligence collection activities might affect more than one of the vital interests and in some instances one violation of an interest can have repercussions causing even more violations. In general it can be argued that the greater the number of vital interests that are violated the greater the harm.

'Severity' refers to the degree of the violation. The greater the extent to which the individual has his interest(s) violated the greater the harm caused. This is because an individual's vital interests are not binary concepts – whole one minute and destroyed the next – but are made up of degrees. The individual does not have his autonomy one minute and find himself completely subjected the next, for he can come under another's influence in various ways and to various degrees. By altering the severity of the violation one alters the level of harm caused.

[96] Berlin declared that in much the same way that boots were more important than the words of Shakespeare, liberty and autonomy are not necessarily the total first needs of an individual. Berlin, *Four Essays on Liberty* (1969), p. 124

[97] Berlin, I. *Four Essays on Liberty* (1969) p.124

Finally, the degree of harm produced can depend on the temporal quality of the activity. H. E. Baber points out that, "intuitively, duration of a harmed state figures importantly in assessments of its seriousness… being locked in the bathroom for 20 minutes is not a great harm, whereas being imprisoned for 20 years makes an important difference to a person's other interests".[98] This is because many transitory hurts do not harm us. They come, are felt, pass without leaving any mark, and are forgotten quickly. Over time, however, the building up or continuation of a violation can have profound effects on an individual's attempt to fulfil his needs and goals. Those violations which span greater amounts of time and become chronic distractions can begin to impede even those interests that are said to be timeless. Similarly, repetitive small violations can become increasingly harmful. For example, if acts of low severity become "prolonged, recur continuously or occur at strategically untimely moments" they can become chronic distractions.[99]

However, the point of 'other things being equal' demonstrates that the degree of harm caused is dependent on all three aspects brought together. For example, saying that the interest in physical integrity is more important than autonomy is done while the severity and temporal quality of the violation are equal. It would be folly to argue that a prick on the finger is more harmful than being locked away for twenty years simply because it was a physical attack. Furthermore, vital interests make a chain whereby the whole chain is no stronger than its weakest link.[100] This means that there are few tradeoffs between the vital interests: an excess of one good will not necessarily make up for the lacking of another interest. For example, all the self-worth in the world "will not help you if you have a fatal disease and great physical strength will not compensate for destitution or imprisonment". [101] Furthermore it should be noted, as Feinberg does, that "bare minimum invasions of interests just above the threshold of harm are not the appropriate concern".[102] That is, vital interests can be wronged in often quite insignificant ways that would not really constitute harming the individual. The violation must be more than to cause annoyance, inconvenience, hurt or offense.

[98] Baber, H. E. 'How Bad is Rape' *Hypatia* Vol.2 No.2 (1987) p.131
[99] Feinberg, J. *Harm to Others* (1984) p.46
[100] Feinberg, J. *Harm to Others* (1984) p.37; Rescher, N. *Welfare: The Social Issue in Philosophical Perspective* (Pittsburgh: University of Pittsburgh Press, 1972) p.5
[101] Baber, H. E. 'How Bad is Rape' (1987) p.129
[102] Feinberg, J. *Harm to Others* (1984) p.188; Rescher, N. *Welfare:* (1972) p.188

Levels of Just Intelligence

Once the level of harm caused by the intelligence collection activity has been ascertained it is then possible to compare this against the corresponding level of the just intelligence principle to determine if the act is justified or not. By looking at the circumstances surrounding the activity and evaluating if they meet the level of just cause, legitimate authority, right intention, last resort, proportionality and discrimination, it can be determined whether the activity is prohibited or permissible.

Just Cause: Levels of Threat

The Just Intelligence Principles as stated above argued that there must be a 'sufficient level of threat' to provide a just cause for the use of intelligence collection. Political communities face threats to their security in one form or another almost every day and not all threats should be perceived as equally 'threatening'. Michael Quinlan argues that at one end of the spectrum "might be solid warnings of terrorist plans... at the other, finding out what the 'bottom line'... on an impending negotiation about tariffs in trade in cabbages".[103] Given that intelligence collection can cause various levels of harm it can also be argued that the greater the level of harm caused the greater the level of threat needed to justify it. Determining the level of threat is dependent on a variety interweaving factors, including the 'nature' of the threat and the degree to which the threat is backed up by evidence.

Understanding the 'nature' of the threat involves examining the threatening act, what is being threatened, who is making the threat, and how far away the threat is. That is, the political community has a vast range of interests that it must protect and for every one of these interests each can be threatened in a variety of ways. Depending on how the two interact with each other the level of threat can be altered. For example, interests such as the economy, civil order, technological advance, people's safety and diplomatic relations, can each be threatened militarily, politically, financially or through civil disobedience, and by combining the two categories in various ways it is clear that the level of threat alters. Another factor that can alter the level of threat is the type of entity the threat is emanating from. For example, David Singer argues that through "a combination of recent events, historical memory, and identifiable socio-cultural differences" it is possible to provide the "vehicles by which vague out-group suspicion may be readily converted into concrete hostility towards a specific foreign power".[104] Questions regarding the entity's historical experience, the rhetoric

[103] Quinlan, M. 'Just Intelligence' (2007) p.7

[104] Singer, D. J. 'Threat Perception and the Armament Tension Dilemma' *Journal of Conflict Resolution* Vol.2 No.1 (1958) p.93

being used, the social, economic or cultural situation both parties are in, what the antagonists have to gain by carrying out the threat, what their ideological position is, and what their actual capabilities are, can all affect the level of threat. Finally, timescale is also crucial in understanding the level of threat in that those threats that are close pose a greater degree of urgency and can therefore be more threatening in comparison to those that are temporally distant. In some cases, time can very much be of the essence. Walzer, therefore, notes that there is distinction between those threats that are "close but not serious" and others that are "serious but not close".[105] The temporal quality of the threat also refers to a situation where if waiting were to greatly magnify the risk then there is an ethical impetus to deal with the threat sooner rather than later.

The second element in understanding the level of threat is the degree to which it is reasonable to assume the threat is real. It has been argued that in order for intelligence agencies to collect information there first must be some evidence present so as to provide a just cause. However, given that it is the duty of intelligence agencies to provide the very information that is then used to establish the just cause, there is the problem on how to make the initial ethical calculation with no information provided. The answer to this is that for those activities that cause a low level of harm, there only has be a low level of evidence to act as a just cause, whereas for those activities that cause a high level of harm there must be a greater level of evidence. This notion of levels of evidence is itself nothing new. Various legal systems mark out levels of evidence, or 'burdens of proof', which are required when assessing whether certain actions are permissible or not. Legal canons mark a distinction between a *reasonable suspicion*, a *probable cause*, a *balance of probabilities, clear evidence,* and *beyond any reasonable doubt,* whereby depending on the circumstances the level of proof required changes. For example, reasonable suspicion is a low standard of proof often required to determine whether a brief investigative stop or search by a police officer or any government agent is warranted. For anything that is more 'intrusive', to detain someone for example, a higher burden of proof must be provided, for instance a probable cause. These different levels of probability provide, what Polyvious Polyviou calls, the "best compromise" between two often opposing interests, "the intrusions upon the individual and the security of the state".[106] This notion is compatible with intelligence collection. Intelligence is essentially a calculation of probabilities and possibilities about activities that it is not meant to know about. Intelligence by its very nature is engaged with uncertainties: "intelligence rarely tells

[105] Walzer, M. *Just and Unjust Wars* (2000) p.252
[106] Polyviou, P. *Search and Seizure: Constitutional and Common Law* (London: Duckworth, 1982) p.97

you all you want to know. Often difficult decisions need to be made on the basis of intelligence which is fragmentary and difficult to interpret".[107] Often the intelligence operative must engage with the evidence available and determine what action is best given the range of possibilities. Therefore, actions that cause a low level of harm can be used to collect information with only a 'reasonable suspicion' that the threat exists. If the information collected proves fruitful then it can be used as further evidence for the justification of those activities which cause a greater level of harm.

Legitimate Authority: Oversight & Chain of Command

The principle of legitimate authority is based on the argument that only those who are charged with protecting the political community can justify harm caused by intelligence collection. Therefore, in order for an authority to be legitimate there must be some way of illustrating that the authorisation process is both unbiased and that the higher the level of harm caused the higher the level of authority there is sanctioning the action.

Since every political community has its own mechanisms for oversight, it would be too difficult to outline a single and rigid hierarchy of authority. However, what is evident is that the judicial, legislative and executive branches of various political systems possess some notion of a chain of command whereby the higher up one goes the greater the responsibility shouldered. Therefore, it is possible to understand a general notion of levels of authority by arguing for a chain of command where as the level harm caused goes up so should the level of responsibility to the political community. For example, low level harms can be authorised by the internal apparatuses in place in various intelligence systems, from the case officer up to the director of the particular intelligence agency. However, for the middling to higher levels of harm outside authorisation would be needed. By applying to the judiciary, legislative or executive for authorisation and progressing up the various hierarchies it is necessary to climb the chain of command as the harm goes up.

Proportionality: What to Include and Exclude

In order for intelligence collection to be justified it must create more good, or avoid a greater bad, than the damage caused by the collection activity. The question, however, is what should count as the 'good' and the 'bad' in this particular moral calculation. The answer to this is similar to the arguments made when evaluating the benefits and the costs of war. That is, it is only those goods that are related to the aim of the just cause that should be counted as a

[107] Parkinson, J, and Walker, C. *Blackstone's Counter-Terrorism Handbook* (Oxford: Oxford University Press, 2009) p.95

positive while almost all damages caused should be included as a negative. That is, "if war has certain aims, the goods involved in achieving those aims count towards it proportionality but goods incidental to them, such as boosting the economy or science, do not".[108] Thomas Hurka asks to imagine a situation where "our nation has a just cause for war but is also in economic recession, and that fighting the war would lift both our and the world economies out of this recession".[109] Although the economic benefits here are very real, these cannot be counted as towards the proportionality calculation. We cannot justify killing in terms of the economic gains that it might produce. In contrast to this, however, while only certain goods may be counted in favour of acting, *all* damages or harms, must be counted. Returning to Hurka's example, while the boost to the economy cannot be counted as a relevant good, the fact that it might hurt the economy could be counted as a negative.

As such, in order to satisfy the principle of proportionality there must be a calculation of the overall damage, and not the just the 'harm', that an intelligence collection action might cause. That is, harm is a reference to the extent to which the action violates the target's vital interests, but this is not to say that some intelligence collection activities do not have wider repercussions. In much the same way that war might damage an economy and so have this negative aspect counted, if the intelligence collection causes damage to the social cohesion of a society or harms and/or damages another individual then these damages must be accounted for as well.

Discrimination: Who to Target?

Despite the different conceptions of how and where the line between 'legitimate' and 'illegitimate' targets is drawn, there is still an understanding that having a line is important and necessary. In Section Two of this chapter it was argued that the principle of discrimination is the result of the threat the individual poses. That is, by acting in a threatening way he waives his protective rights. The question for this section is how individuals can represent varying levels of 'combatantcy' and on what grounds this evaluation is made.

For intelligence collection the simple dichotomy of civilian-soldier is not precise enough to illustrate the varying degrees that the traditional 'civilian' might represent a legitimate intelligence target. Indeed, Asa Kasher argues that, "if one is interested in a

[108] Hurka, T. 'Proportionality in the Morality of War' *Philosophy and Public Affairs* Vol.33 No.1 (2005) p.40; others who promote a similar view of proportionality and the relevant goods see McKenna, J. C. 'Ethics and War: A Catholic View' *American Political Science* Vol.54 No.3 (1960) p.651; and Regan, R. *Just War: Principles and Cases* (Washington, D.C: Catholic University of America Press, 1996) p.63

[109] Hurka, T. 'Proportionality' (2005) p.40

morally justified delineation that includes those who directly jeopardise others, then the category of 'members of armed forces' should not be used".[110] Beyond the core of the military force of a political community there are numerous men and women that can be considered a threat. For example, the current industrialisation of war means that threats have become increasingly dependent on a combination of military and civilian efforts and support structures. Richard Regan argued that, "in my opinion, those who enable an enemy to march and provides food sustains an enemy army's ability to fight; therefore those who produce shoes or food for an unjust enemy's armed forces may be targeted at their factories and farms".[111] In this instance, munitions workers who make weapons for the army and, as a result, directly contribute to the war effort can be thought of as posing a threat. Walzer argues that while they do not become fully integrated into the category of soldier they should be considered as partially assimilated into the class of soldier, and can therefore be targeted at certain times.[112] They might not be armed and ready to fight but they are to some extent engaged in activities that are "threatening and harmful".[113] Clearly, there are varying degrees, times and circumstances which exist and alter whether an individual can be targeted or not.

For the *just intelligence principle* of discrimination, the line that distinguishes between legitimate and illegitimate targets is dependent on the extent the individual represents a threat or the extent he has acted so as to waive his normal protective rights. The evaluation as to what extent the individual is a 'threat', and therefore to what extent he is a legitimate target, is similar to that discussed in the section on just cause. The just cause section argued that several factors went into determining if a threat existed and what level that threat posed, including the history of the those involved, what they had to gain, and probability of the threat existing. Similarly, like factors go into determining if an individual poses a threat. Questions include what role the individual plays in the chain of events; what the likelihood is of his involvement; what his history is; what his cultural, social or economic background is and how that is likely to affect his role as a threat; what his rhetoric is; what he has to gain or lose; and what his capabilities are and finally to what organisation he is connected to or associated with. Although these are not exhaustive questions, they portray the idea that many intermingling factors go into making composite of his identity and it is from this that his level of threat can be determined. Depending on his level of threat or the extent

[110] Kasher, A. 'The Principle of Distinction' *Journal of Military Ethics* Vol.6 No.2 (2007) p.159-60
[111] Regan, R. *Just War* (1996) p.90
[112] Walzer, M. *Just and Unjust Wars* (2000) p.146
[113] Walzer, M. *Just and Unjust Wars* (2000) p.146. Also see: Coates, A. J. *The Ethics of War* (1997) p.236; Slim, H. *Killing Civilians: Methods, Madness and Morality in War* (Basingstoke: Palgrave, 2002) p.188

to which he contributes to that threat the level of harm that can be used against him changes. That is, the more harmful the activity the greater threat he must represent.

The other factor that alters an individual's status as a legitimate or illegitimate target is the extent that he has forfeited or waived his protective rights. Depending on an individual's actions he can temporarily suspend his own rights. For example, Walzer argues that when someone tries to kill, "he alienates himself from me... and from our common humanity" and as such loses his right not to be killed.[114] Similarly, individuals can alienate their protective rights by either consenting to waiving them or by forfeiting them through untoward activity. Taking Walzer's example, the soldier alienates himself by trying to kill someone and therefore loses the protective rights that prevent him from being targeted.[115] The criminal loses some of his liberty when he breaks the law or the individual loses some of his privacy when he talks loudly in a crowded restaurant. Equally, when individuals take certain jobs or act in a threatening manner they consent to waiving or forfeiting their rights or privileges.

For the purpose of intelligence, the question is to what extent the individual has either acted untowardly so as to lose his protective rights or knowingly consented to waiving them. Again, the answer to this evaluation can depend on several factors, but, for Tony Pfaff and Jeffrey Tiel, the answer is the extent to which the individual has decided to "play the game".[116] That is, "consent to participate in the world of national security on all levels of a country's self-defence structure together with the quality of the information possessed"[117] justifies the individual as a legitimate target. The individual has consented to waiving his normal protective rights. It can be argued, therefore, that the higher up in the state's national security infrastructure an individual is the more of his protective rights he waives or forfeits. Holding a particular job; acting in a threatening manner; being a member of a state's infrastructure, are all examples of how the individual can forfeit or waive his protective rights. Therefore, depending on the type of activity that the individual carries out the sort of protective rights he loses can change. The greater the level of threat he poses the more of his protective rights he loses and therefore the greater the level of harm that can be used against him.

---

[114] Walzer, M. *Just and Unjust Wars* (2000) p.142

[115] For more on the debate regarding the right to life and whether it is an inalienable right see, Feinberg, J. 'Voluntary Euthanasia and the Inalienable Right to Life' *Philosophy and Public Affairs* Vol.7 No.2 (1978) pp.93-123; and Kasachkoff, T. 'Killing in Self-Defense' (1998) pp.509-531.

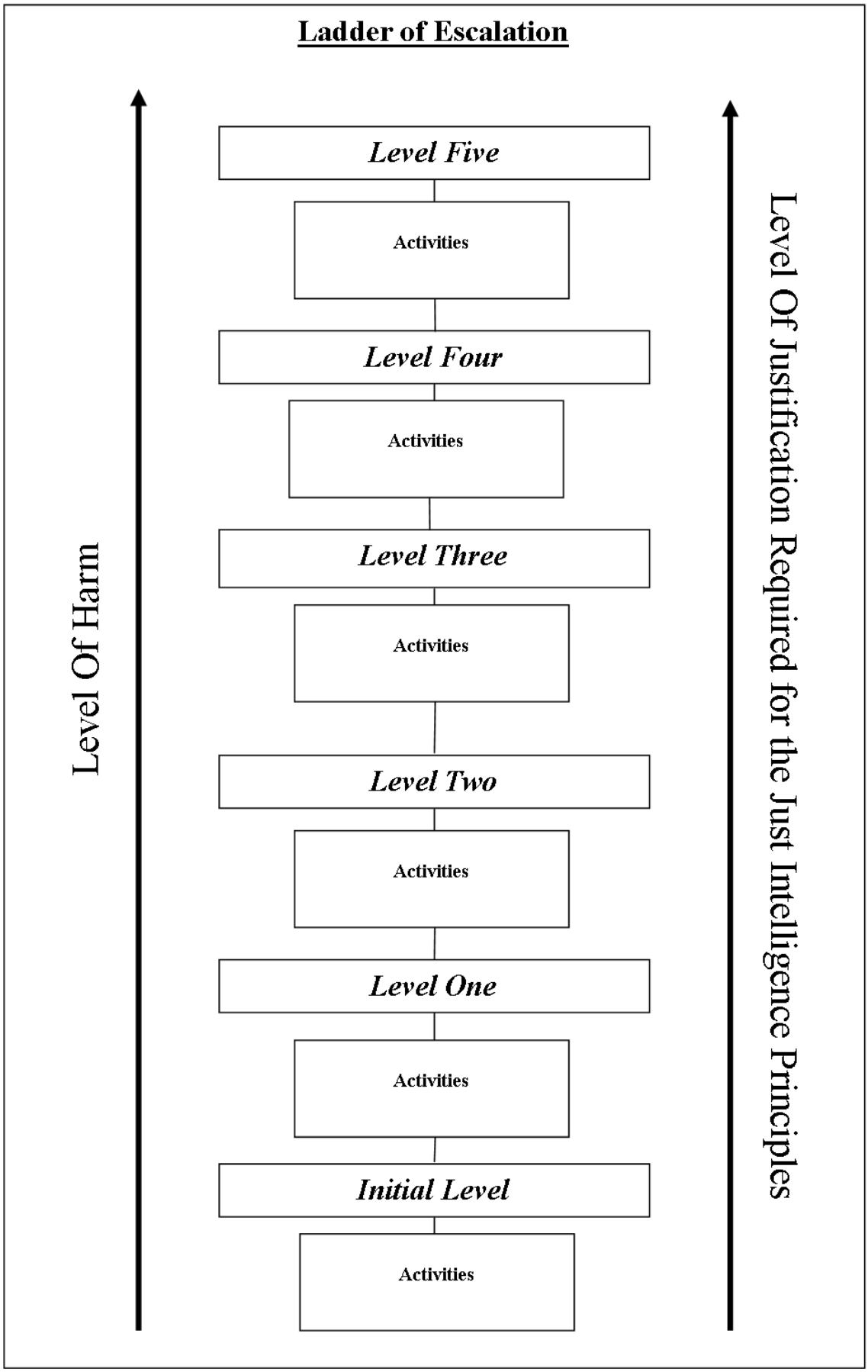
[116] Pfaff, T. R. and Tiel, J. R**.** 'The Ethics of Espionage' *The Journal of Military Ethics* Vol.3 No.1 (2004) p.7

[117] Pfaff, T. R. and Tiel, J. R**.** 'The Ethics of Espionage' (2004) p.6

Ladder of Harm and the Ladder of Just Intelligence

In Figure 1.0 below it is possible to see the general trend of the Ladder of Escalation as it compares the different levels of harm and Just Intelligence Principles. This ladder illustrates that as the level of harm goes up, according to the number, severity and range of vital interests violated, so too must the justification. By using this framework it is now possible to ethically evaluate intelligence collection as used by the political community to protect itself.

Figure 1.0


Ladder of Escalation
Level Of Harm
Level Five
Activities
Level Four
Activities
Level Three
Activities
Level Two
Activities
Level One
Activities
Initial Level
Activities
Level Of Justification Required for the Just Intelligence Principles

Conclusion

This chapter has shown that harm is a fluid notion. Individuals hold a vast variety of interests in their lives that, if they are to be happy, need to be pursued. But many of these interests have the precondition that more fundamental interests are secured. If these base interests are not secured, higher ones cannot be attempted and individuals are therefore said to be harmed. The most serious forms of harm are those that interfere, violate, setback, thwart or disturb the greatest number of our fundamental interests in the most severe way and for the longest time. Moreover, intelligence collection can, to varying degrees and in different ways, violate these vital interests and as such cause harm. Therefore, there is an important argument to be made that intelligence collection should be limited in its use.

However, this section has also argued that intelligence is a vital part of maintaining the political community and should not be dismissed without regard to the circumstances that surround it and the good that can be done. By using the just war tradition as inspiration, this chapter has shown how it is possible to create a set of Just Intelligence Principles that outline when the political community is justified in using intelligence collection. As long as there is a just cause, a legitimate authority, the right intention, a proportional benefit, and discrimination between legitimate and illegitimate targets, then the use of intelligence collection is justified. Finally, what this chapter has outlined is the notion that there are varying degrees of harm caused by the intelligence collection depending on the means used. As such, the Just Intelligence Principles need to be flexible enough to accommodate the varying levels of justification needed. To this end, a Ladder of Escalation has been outlined to illustrate that as the levels of harm caused by the intelligence collection activity goes up, so too must the just cause, the level of authority, the proportional gains, and the level of threat seen in the target. By establishing this ethical framework it is now possible in the remainder of the thesis to ethically evaluate the different intelligence collection activities. By looking at the harm caused and the possible circumstances these means of intelligence collection might be used in, it is possible to evaluate when and if intelligence collection can be justified.

Chapter Two: "The Eyes Have It"
Imagery Intelligence

If 'seeing is believing' and 'a picture can speak a thousand words', then the importance of imagery intelligence as a collection discipline needs little explanation. Advances in technology have meant that imagery intelligence offers the analyst the ability to see, record and evaluate scenes that would otherwise be out of reach. Imagery intelligence provides decision makers with a physical representation of the information, making it a more graphic and compelling form of intelligence since an image is much more easily understood by policymakers than other forms of intelligence.[1]

However, collecting imagery intelligence can come into conflict with an individual's privacy and autonomy and, as a result, cause harm. It is the aim of this chapter to explore both how and to what degree imagery intelligence causes this harm as well as outlining whether or not this harm can be justified in accordance with the Just Intelligence Principles set out in Chapter One. First, this chapter will outline what imagery intelligence is, demonstrating how it is distinguished from the other intelligence collection disciplines as well as from other forms of non-intelligence imagery collection. The second section of this chapter will explore in greater detail the principles of privacy and autonomy so as to better understand the way imagery intelligence might come into conflict with these vital interests. In the third section different illustrative examples of imagery intelligence will be explored so as to highlight the different types and levels of harm they can cause. Finally, this chapter will employ the Just Intelligence Principles of just cause, legitimate authority and discrimination so as to determine if the harm caused can be justified.

[1] Lowenthal, M. *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003) p.62

Section One: The Nature of Imagery Intelligence

Imagery intelligence is often described simply as information that can be seen: maps, drawings, photographs and other representations of the world in image form. However, while imagery intelligence is intelligence seen, not all things seen are intelligence. This section will argue that imagery intelligence has four elements that define its practice and distinguish it from both the other intelligence collection disciplines as well as from other forms of imagery collection that is not intelligence. These factors include the *visual* element; the *intentional observation of a target*; the use of a *security lens*; and finally that it is *technologically captured* in some way.

Visual Images

The first important aspect of imagery intelligence is that it is visual. Imagery intelligence is about which what is seen. That is, the means through which the information is collected involves capturing and representing a visual image through some technological means. For example, video recordings and photographs are two of the most common examples of what imagery intelligence produces and demonstrates how visual information is presented. This visual quality is clearly imagery intelligence's most distinguishable feature and separates it from the other collection disciplines, like human and signals intelligence. However, while this separates it from the other collection disciplines, it tells us little about how imagery intelligence is separate from the other images not necessarily understood as intelligence. It is the other elements that mark imagery intelligence as distinct from ordinary imagery collection.

Intention

The second element of imagery intelligence is that there is a *difference between seeing and observing*. People 'see' things all the time. The majority of the time they are actually unable to stop 'seeing' things. The mind is barraged with an endless stream of visual events, most of which it chooses to ignore. Seeing is often a mindless, constant, passive and unintentional. By contrast, 'observing' has a purpose, it is an intentional act on behalf of the viewer. There is an active hunt, a desire to find, and the aim to look for something. This aspect of imagery intelligence is important as it highlights the fact that it is an activity that is purposefully carried out, something an individual intended on doing after deliberation. Indeed, for imagery intelligence the intention is to collect information through the observation of a specific target.

Highlighting this intention is important for two reasons. First, by highlighting that this is an intended activity it means that those individuals who carry it out are morally culpable for the harm that the activity then causes. The individual is a moral agent, someone who is aware of his activities and the consequences of carrying them out, who is in possession of the capacities for deliberation and action.[2] Therefore, he is morally culpable for those activities that he intentionally carries out. This is important since in order to contemplate moral guidelines by which one can both prescribe and judge appropriate conduct then one must be clear that this is a purposeful act carried out by individuals who are moral agents.[3] As a result, it is possible to hold the intelligence operative, and by extension the organisation that authorises his actions, responsible for the harm caused by his actions.[4] He can be expected to respond to moral guidelines and be held morally accountable for his actions. Second, by noting that this is an intentional act it separates imagery intelligence from the everyday visual stimulus that an individual can receive. For example, there is clearly a difference (both ethical and physical) between passively watching people go by and watching people for the specific purpose of collecting information about them.

Security Lens

The third aspect of imagery intelligence and intelligence more broadly, is that it views the world through a 'security lens'. This security lens is shaped by the threats and risks a community faces and determines what information is intelligence and what is just data. By looking at the world through this security lens, raw information is evaluated in regards to the end goal of protecting the political community. Again this is an important point to make for two reasons. First is that by highlighting this security lens it makes clear how almost any information can be turned into intelligence depending on the circumstances. A report on a weather front, for example, can become intelligence if it is related to a specific operation. By passing the information through the security lens the information can then be transformed into intelligence as the 'who', 'where' and 'what' of a scenario are all perceived differently.

[2] Erskine, T. 'As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering' *Intelligence and National Security*, Vol. 19, No. 2 (2004) p.362
[3] Erskine, T. 'As Rays of Light' (2004) p.361
[4] While claiming that the intelligence organisation itself is a moral agent and is therefore morally culpable for the actions it authorises is a controversial statement, Erskine makes a compelling argument that supports this point. For the argument that intelligence organisations specifically are moral agents see Erskine, T. 'As Rays of Light' (2004). For the more general argument on organisations as moral agents see Erskine, T. 'Assigning Responsibilities to Institutional Moral Agents: The Case of States and Quasi-States' *Ethics & International Affairs* Vol. 15 No.2 (2001) pp.67-85 and Erskine, T. 'Locating Responsibility: The Problem of Moral Agency in International Relations' in *The Oxford Handbook of International Relations* edited by Reus-Smit, C. and Snidal, D. (Oxford: Oxford University Press, 2008) pp.699-707

Second, since this security lens is shaped by the intention to protect the political community it can have important consequences for the ethical evaluation of imagery intelligence. That is, the end goal for an activity can alter the ethical evaluation of that activity. Acting to protect the political community is judged in a different way to an activity carried out by or for a private commercial goal, for example. This also stresses the point that this project is only concerned with actions carried out by or on behalf of the state, and that private companies that carry out intelligence for their own needs are not being considered.

Capturing the Image

The final aspect of imagery intelligence is how the information is 'captured'. Imagery intelligence essentially takes something that can be seen, 'captures' it and presents it in some visual way. This aspect is important because before an item is captured it only exists in the mind of the beholder, an image that comes and goes in an instant. Imagery intelligence takes various 'scenes' in their transient state and turns them into a physical entity that can then be stored, retrieved, analysed and presented. Imagery intelligence represents this information through a medium that can be seen. For example, photographs, pictures, drawings or maps are all physical representations or reflections of what exists in the real world. This is important because it separates imagery intelligence from forms of intelligence that are seen but are transient or subject to interpretation.

Types of Imagery Intelligence

These criteria provide the blueprints for imagery intelligence, illustrating those characteristics that make imagery intelligence what it is. However, the term 'imagery intelligence' houses a variety of highly diverse collection activities. These activities will generally fall into two groups, that is, the use of imagery intelligence to monitor large, state-level events and the use of imagery intelligence on the domestic level, collecting information on individuals and their activities.[5] Imagery intelligence at the international level tends to focus on military activities or activities that can only be witnessed by looking at a wide-angle viewpoint. For example, troop movements, military and industrial installations, weapon test sights, mapping of terrain, regional disturbances, inter-state relationships and other inter-actor events. In comparison,

[5] This divide is not based on any ethical assumptions – that one is more or less harmful than the other. Rather, the purpose is purely to help with understanding the types of activities involved, how they are used and the type of end they are targeted for.

imagery intelligence in the domestic sphere focuses on activities at the societal or individual level.

Imagery Intelligence and the International

Throughout its brief history, imagery intelligence at the state level has been heavily dominated by the United States and, during the Cold War, the Soviet Union. As a result of the constant rivalry between these then superpowers, the Cold War saw a rapid development of imagery intelligence. However, despite this Cold War focus, imagery intelligence had indeed been used for some time before. It was during the First World War that visual and photographic reconnaissance saw its strategic début. At the beginning of the First World War the British Royal Flying Corps conducted aerial surveillance of the German troops advancing through Belgium and aerial surveillance was quickly recognised as an impressive substitute to cavalry patrols offering the ability to survey battle lines from Switzerland to the North Sea.[6] Brigadier General William Mitchell wrote, "one flight over the lines gave me a much clearer impression of how armies were laid out than any amount of travelling on the ground".[7] World War Two saw the importance of military surveillance advance further as the United States remodelled B-17 and B-24 aircraft with cameras in order to give a bird's eye view of the battle below.[8] This meant that by the beginning of the Cold War the potential importance of imagery intelligence had been clearly established. However, it was during the prolonged Cold War that its true importance was demonstrated, not least of all because it was seen by the West as an essential tool for piercing the Iron Curtain.

It is, therefore, during the Cold War years that imagery intelligence sees some of its most important developments: the construction, launch and advancement of spy-planes and satellite based imagery collection. The first spy-plane to be developed, the U-2, was designed with the hope of obtaining reliable data on the 'bomber gap' between the superpowers. These planes would take pictures of the ground in order to provide a visual account of location and development of various systems. A series of 30 U-2 flights were performed over Soviet controlled space providing imagery intelligence "impressive enough to persuade America's leaders that the Soviets had far fewer bombers than initially feared".[9] Currently, the U-2R is the version used which has a range of more than 3,000 miles, a maximum speed of 528 knots

[6] Andrew, C. *Her Majesty's Secret Service: The Making of the British Intelligence Community* (London: Viking Press, 1986) p.133
[7] Quoted in Shulsky, A. *Silent Warfare: Understanding the World of Intelligence* (Washington, D.C.: Brassey's, 2002) p.21
[8] Richelson, J. T. 'Intelligence: The Imagery Dimension' in S*trategic Intelligence: The Intelligence Cycle* Volume 2 edited by Johnson, L. K. (London: Praeger Security International, 2007) p.61
[9] Johnson, L. *Secret Agencies: US Intelligence in a Hostile World* (London: Yale University Press, 1996) p.15

at an altitude of 40,000 feet and can be equipped with a variety of sensors including electro-optical and an all-weather, day or night Aperture Radar System.[10] They can detect both the visible and non-visible parts of the electromagnetic spectrum, transmitting back in real-time and have the added bonus over satellites of being more easily 'directed' to a specific location when urgency is required.

The second major military imagery intelligence advancement during the Cold War was the development and launch of the first imagery based satellite by the Americans, CORONA. This satellite used photographic film to take pictures of the land far below, giving details of industrial buildings, medium-range, intermediate-range and intercontinental ballistic missile launching bases, as well as Soviet construction sites for submarine and surface fleets.[11] Over the years CORONA was replaced by an increasing number of upgrades that gave American military intelligence the ability to see more than ever before. For example, the KH-11 first developed in 1976 represented a quantum leap in imagery technology, providing for the first time the ability to return images in real-time rather than film having to be ejected in canisters and collected. Other advances included an increase in resolution as well as the development of electro-optical cameras that were able to 'see' through cloud cover and even at night.[12] The current ONYX satellite is a system that, rather than employing an electro-optical system, carries a radar imaging systems that offers the ability to monitor foreign weapon storage sites, troop movements and even the tracking of underwater submarines in almost any weather conditions.[13] Finally, satellites equipped with multi-spectral or hyper-spectral imagery (MSI and HSI) derive an 'image' from analysing the individual electromagnetic 'reflections' given off by an object when scanned, often referred to 'measurement and signals intelligence' or MASINT. MASINT can therefore be vital in determining the presence of chemical or biological warfare agents or clandestine nuclear test sites.[14]

As such, spy-planes and satellites illustrate some of the most vital advances in military imagery intelligence, providing the ability to see from a vantage point far beyond the normal capacity of any individual. The building and development of weapons and industry,

[10] Richelson, J. T. *The U.S. Intelligence Community* (Boulder, Colo.: Westview Press, 2008) p.158
[11] Johnson, L. *Secret Agencies* (1996) p.177
[12] Resolution refers to the smallest object that can be distinguished in an imaged. There is often a trade-off of how big the scene is and the resolution – the greater the resolution the smaller the scene viewed. It is often measured in size – inches or meters for example. For a list of American satellites, their launch dates and their optical capabilities see Graham, T. and Hansen, K. *Spy Satellites and Other Intelligence Technologies that Changed History* (London: University of Washington Press, 2007) p.136
[13] Richelson, J. T. *The U.S. Intelligence Community* (2008) p.180
[14] Dupont, A. 'Intelligence for the Twenty-First Century' *Intelligence and National Security* Vol.18 No.4 (2003) p.18

troop movements and even just the lay of the land can all be monitored over a varied amount of time. Satellites and spy-planes, therefore, represent some of the most important tools in a state's effort to know and prepare for military attacks in an uncertain world.

Society and the Individual

Society-based imagery intelligence is generally aimed at monitoring individuals in the hope of stopping or preventing damage at the societal level. Threats to a society are just as likely to come from within its own borders as they are from an outside military incursion. Therefore domestic imagery intelligence can include, "the prevention or detection of serious crime"[15]; maintaining the general peace of society; as well as protecting the state from "espionage, terrorism and sabotage".[16] Unlike military and international imagery intelligence, which is dominated by the global superpowers, domestic or society imagery intelligence is used by many more states, varying in coverage according to costs. Intelligence organisations that specialise in domestic intelligence collection include, for example, the Security Service in the United Kingdom (commonly referred to as MI5), the Federal Bureau of Investigation (FBI) in the United States, the Canadian Security Intelligence Service (CSIS), the Chinese Ministry of State Security (MSS), France's Direction Centrale du Renseignement Intérieur (DCRI) and the Federal Security Service (FSB) of the Russian Federation, to name but a few. These agencies rely on the use of closed circuit television systems, 'intensive surveillance' and 'intrusive surveillance' in order to provide the required imagery intelligence.

Closed circuit televisions, or CCTVs, have become a common landscape feature for a lot of states. Indeed, many have argued that we are living in a 'CCTV culture', where it is "virtually impossible to move through public spaces without being photographed and recorded".[17] These electronic eyes watch, follow and record the daily activities of individuals within a society in order to provide information on problem areas, locate and highlight suspicious elements or follow a specific target. Furthermore, technological advances mean that cameras are able to recognise faces and behaviour in individuals so as to detect problems quickly and allow swift action before they are able to disrupt the peace.[18] 'Intensive surveillance', in comparison, involves the covert monitoring and recording of a target's movements by an intelligence officer with a camera. For example, this can involve a

[15] *Intelligence Service Act 1994* Chapter 1 §1.2 a) and b)
[16] *Security Service Act 1989* Chapter 5, §2.1
[17] Armstrong, G. and Norris, C. *The Maximum Surveillance Society: The Rise of CCTV* (Oxford: Berg, 1999) p.3. On this issue also see Ball, K. and Webster, F. 'The Intensification of Surveillance' in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age edited* by Ball, K. and Webster, F. (London; Sterling, VA: Pluto Press, c2003) pp.1-15 and Lyon, D. *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity Press, 1994).
[18] The system is called 'Neural'. See Gibb, J. *Who's Watching You?* (London: Collins & Brown, 2005) p.26

‘stalking’ method, whereby an individual is followed and photographed as he performs certain activities. Finally, ‘intrusive surveillance’ involves planting an electronic device that covertly records the target while he is in his private property. These three collection means – CCTV cameras, intensive surveillance and intrusive surveillance – are the backbone of the domestic imagery collection system and therefore represent the most relevant set of imagery intelligence activities for this chapter.

Conclusion

Imagery intelligence clearly plays an important role in maintaining the security of the political community. It provides analysts and policymakers with physical, relatively easy to understand and recordable forms of intelligence at both the international and domestic level. On the international level it means one state is able to view another state’s land, defences and military activities, while on the domestic level it can collect intelligence about people and their individual actions. However, as will be explored in the following section, collecting this information has the potential to violate an individual’s privacy and autonomy and as a result cause harm. The next section will examine privacy and autonomy in greater detail so as to highlight the way imagery intelligence these violate an individual’s vital interests and how the level of harm caused can be changed as a result.

Section Two: Harm and Imagery Intelligence

As the previous section illustrated, imagery intelligence represents a powerful tool for the state at both the domestic and international level. Internationally, imagery intelligence views, records and transmits activities relevant to military operations or actions that can only be seen from a distant vantage point. Domestically, imagery intelligence forms a vital part of the surveillance machine that is charged with the watching, recording, tagging, verifying, numbering and monitoring of individuals in order to maintain and protect the peace and security of a society. However, regardless of this international-domestic distinction, there are several overarching issues that need to be understood in order to determine what it is about imagery intelligence that makes it harmful. Chapter One argued that privacy and autonomy are two of an individual's most vital interests and if these interests are violated in a significant way then the target is said to be harmed. This section will build upon Chapter One by illustrating the specific ways imagery intelligence can violate these vital interests. First, the concept of privacy will be examined in greater detail, discussing the different spheres of privacy an individual has and how imagery intelligence can violate them, as well as the extent it is reasonable for an individual to exert control over his image and in doing so prohibit others from utilising it. In addition, this section will explore the ability and tendency of imagery intelligence to violate an individual's autonomy as a result of the Panoptic characteristics often associated with ubiquitous monitoring. Once the relevant issues have been outlined, Section Three will apply the harm ethic to several imagery intelligence illustrative examples so as to outline the specific level of harm caused by each one.

Privacy

In Chapter One it was argued that the interest in privacy can be understood in terms of boundaries constructed "in both thought and in fact" and designed to "provide clear lines of demarcation" that separate the private sphere from the public one.[19] Furthermore, it was argued that an individual's privacy also consists of the right to claim possession of information pertaining to that individual. This section will expand on this initial work by, first, outlining some of the boundaries imagery intelligence can come into conflict with and, second, discussing the types of information connected to the individual that imagery intelligence might attempt to appropriate.

[19] Steinberger, P. J. 'Public and Private' *Political Studies* Vol.47 No.2 (1999) p.292

Of the types of boundaries that will be examined in this chapter the main ones include 'international boundaries' and 'personal boundaries'. 'International boundaries' are those borders that separate states or other international bodies from each other. What was once achieved by mountain ranges or rivers is now done by lines on a map, often recognised in law and internationally agreed. The current conception of the international system is one that involves self-contained state entities, separated and demarcated by specific boundaries and imbued with sovereign power.[20]

While violating a state's territorial integrity by crossing its borders is not necessarily equivalent to violating its privacy, it can be argued that a state can possess some sense of privacy and that these boundaries can act to mark it out. The state can hold information and it can have the right to keep that information to itself if it wishes, and keeping that information within its territorial borders is one way of demonstrating this. The territorial borders simply act to highlight the distinction between the inside and the outside of the state.

'Personal boundaries', in comparison, are those boundaries designed to protect the privacy of an individual or groups of individuals, existing as boundaries created and maintained by socially and legally established norms. Common examples can include an individual's home, property, car, clothing, bags or personal effects. Each of these represents a physical boundary that marks a sphere where the outside world cannot enter without permission or justification.

It was also argued in Chapter One that privacy is related to the ability of the individual to make legitimate claims to control his own information and therefore prevent others from accessing it if he so chooses. It was argued that individuals have the right to control those things connected to them, controlling *who* knows *what* about them. One's body is one's own intrinsically, inherently and without question. That is, "one's actions and their history 'belong' to the self which generated them and [are] to be shared only with those with whom one wishes to share them".[21] Therefore, as an extension of this claim it can be argued that the individual has the right to decide who may look, touch or perceive himself. An individual's image is his property and as a result he can make special claims on it. For instance, by taking a picture of an individual, his image in that picture is still his property and therefore he can make claims equal to that any other of his property claims: he has the right to sell his image or he may invite someone to use his image, but if he decides that he no longer wishes for

[20] For example, the United Nations Charter is based "on the principle of sovereign equality of all its members" under which a state has the right to control its own affairs within its own territory and, under certain circumstances, even has the right to defend their sovereign territory. Charter of the United Nations Article 2; Convention on Rights and Duties of the State Article 1 Sec.49

[21] Shils, E. 'Its Constitution and Vicissitudes' *Law and Contemporary Problems* Vol.31 No.2 (1966) p.290

others to use it then it violates his property right if they do so.[22] The invention of the photographic apparatus means that an individual's visual image can be separated from his real-life subject, allowing for the production, consumption and utilisation of his image. This has resulted in the development of the notion that the individual has the 'Right of Personality' that includes the right of an individual to control the use of his name, image, likeness or other unequivocal aspects of his identity.[23] That is not to say that the individual's claim to his image demands that other people must not even look without permission. Indeed, through the course of everyday activities the individual and his image become part of the public domain. The difference however is that his image is formed as "a transient phenomena in the minds of others", coming and going and barely logged.[24] In comparison, with imagery intelligence, the individual's image is logged, captured and stored without his permission. This is not asserting the right not to be seen but the right not to be watched and to have one's image used without one's permission.

Levels of Privacy

Chapter One made it clear that an individual's vital interests are not binary concepts, whole one minute and destroyed the next. Rather each vital interest can be affected to varying degrees and depending on the extent of the violation the level of harm caused can change. Indeed, an individual has many degrees of privacy as a result of the argument that some spaces are considered more private than others and that some information is considered more private than others. By understanding what the different spheres of privacy are, their importance and how they are formed, for example, and different forms of private information, it is possible to portray the varying levels of harm that can be caused when an individual's privacy is violated.

These levels of privacy are determined, first, by the different types of personal boundaries that exist and, second, the level of 'intimacy' associated with the sphere or the personal information. 'Intimacy' refers to how close the information or private sphere is to the individual's core, a reference to how 'personal' it is to the individual. The greater the intimacy associated with the information or the stronger the socially or legally established

[22] Extrapolated from the argument of ownership made by Judith Thomson. Thomson, J. J. 'The Right to Privacy' *Philosophy and Public Affairs* Vol.4 No.4 (1975) p.304

[23] For example, see the *Civil Code of Quebec* which outlines privacy in article 36 to include the violation of an individual's privacy as involving "using his name, image, likeness or voice". In Germany, the *Basic Law* dictates that "The general right of personality has been recognised. It guarantees against all the world the protection of the personality. Special forms of manifestation of the general right of personality are the right to one's own picture" (§§ 22 ff. of the KUG).

[24] Viera, J. D. 'Images as Property' in *Image Ethics: The Moral Right of Subjects in Photographs, Film and Television* edited by Gross, L., Katz, J. and Ruby, J. (Oxford: Oxford University Press, 1988) p.135

boundary the higher the level of privacy. In response to this privacy can be thought of as consisting of a series of concentric circles around the individual where the closer to the centre one goes the more personal the information and therefore the greater the expectation of privacy. The level closest to the individual's core, the most personal level, concerns the person's most intimate life. Private information at this level can be of a very personal nature including attitudes, conditions or sexual relations. Similarly, spheres of privacy at this level are those where there is a high expectation that the individual is left alone.[25] For example, an individual's own home, private property or clothes all have a long history of being some of the most private spheres as well as being places where an individual is likely to express his most intimate self. A level up, away from the core and becoming less intimate, is information about the individual and his personal life more generally. For example, addresses, telephone numbers, email addresses, credit card information, health, personal opinions, beliefs, views, and interactions with other individuals. At this level Andrew von Hirsch argues that in the social and working world there might be a need for some disclosure given certain social situations, but individuals are not expected to disclose personal details without a justification.[26] Spheres of privacy at this level include those where the individual can expect to be alone, but there is some prospect that there can be some intrusion given a justification. For example, an individual's office, where they are generally expecting to be alone but where, given the working environment, there might be the occasional justified entrance. At the outmost circle there is superficial or general information about the individual.[27] This is the individual's surface information or information he publicly transmits, either willingly or unknowingly, but will often inform little intimate information about the individual other than his immediate facts. Spheres of privacy at this level are the most public, the individual in the street for example. Obviously, these descriptions are not designed to be exhaustive, but rather to demonstrate the concept of varying levels of intimacy and as a result the varying levels of privacy.

[25] Marx, G. 'Some Concepts that May be Useful in Understanding the Myriad Forms and Contexts of Surveillance' *Intelligence and National Security* Vol.19 No.2 (2004) p.234; and Hirsch, A. 'The Ethics of Public Television Surveillance' in *Ethical and Social Perspectives on Situational Crime Prevention* edited by Hirsch, A., Garland, D. and Wakefield, A. (Oxford: Hart Publishing, 2000) pp.59-76
[26] Hirsch, A. 'The Ethics of Television Surveillance' (2000) p.63
[27] Marx, G. 'Some Concepts of Surveillance' (2004) p.234 -236

Social Control

Information, as it is widely quoted, is power. Even the act of simply collecting and collating information is a means of acquiring power over someone, normally at the subject's expense. It is not surprising, therefore, that a number of observers have commented on how the development of the modern state's ability to surveil its people is bound up with the growth of a major mechanism for social control.[28] This section will argue that the use of imagery intelligence exerts a pressure on those it watches and in doing so alters their behaviour, violating their autonomy. George Orwell's *Nineteen Eighty Four* dystopia, with its one-way screens, Thought Police and ever-watching Big Brother, allowed the state to maintain constant vigilance over the intimate lives and relationships of each citizen. In doing so, *Nineteen Eighty Four* highlights the possible power of technology not only to violate an individual's privacy, but also to exert significant control over an individual's autonomy. Although Orwell's dystopia is an extreme representation of a world where those who are able to see all and know all are able to control all, for this project it highlights some important concerns regarding how being watched can alter an individual's actions.

Social control, as James Rule argues, consists of "those mechanisms which discourage or forestall disobedience".[29] These mechanisms are based firstly on 'powers of control', in that those who seek to control "need to be able to apply sanctions or inducements sufficient to discourage the sanctioned person from repeating his disobedient act".[30] These can either be positive- or negative-reinforcement-based, formal or informal, obvious or subtle, symbolic or physical, so long as it provides the impetus for altering the individual's behaviour. The second requirement is that those who are being controlled must be 'aware' that they are being watched and will be punished if they break the rules. This can be achieved through an obvious demonstration of power against infractions or more subtle or even subconscious, general understandings that to break the rules would result in punishment.

It is therefore not surprising that when discussing imagery intelligence analogies of the 'Panopticon' are often made. Proposed in 1787 by Jeremy Bentham, the 'Panopticon' is an architectural system of control and discipline, applicable to prisons, factories, work houses and any space where control was needed.[31] Originally, the Panopticon was a blueprint for a

[28] Foucault, M. *Discipline and Punish: The Birth of the Prison* (Harmondsworth: Penguin, 1979); Giddens, A. *The Nation State and Violence* (Berkeley: California University Press, 1987); Marx, G. *Undercover: Police Surveillance in America* (Berkeley: University of California Press, 1988)
[29] Rule, J. *Private Lives and Public Surveillance* (London: Allen Lane, 1973) p.20
[30] Rule, J. *Private Lives and Public Surveillance* (1973) p.22
[31] Bentham, J. *The Panopticon Writings edited by* Bozovic, M. (London: Verso, 1995) pp. 29-95

semi-circular prison with an 'inspectors lodge' at the centre and cells around the perimeter. Prisoners in their cells would be subject to the gaze of the guards, but not the other way around. This asymmetrical gaze meant that since the prisoners would never know if they were being watched they would be forced to assume that they are *always* being watched. They, therefore, would start to 'self-discipline' their actions and surrender to the wishes of the observers.[32] For Foucault, the Panopticon represented an architecture of power which induces conformity: "he who is subject to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play upon himself; he plays both roles; be becomes the principle of his own subjection".[33]

It can be argued therefore, given the current growth of surveillance, that there are development trends of social transformation similar to those seen in the Panopticon. Many writers believe that the advent of time and space transcending technologies, such as those seen with imagery intelligence, reflect the ability to transfer the dynamic of the Panopticon to non-institutionalised spaces.[34] Even though the Panopticon is a building made out of stone and mortar, it still functions as an ideal, a metaphor and set of practices.

By scrutinising the individual through imagery surveillance power is exercised over him so as to produce high levels of compliance and thus interfere with his autonomy. An individual will act differently if he thinks he is being watched as compared to when he thinks he is alone. Someone being watched will conform to the standards of what is expected by those who are doing the watching. The individual will imagine the watcher is judging him and will alter his behaviour in order to fit in with what the watcher expects. Chapter One argued that autonomy consisted of the individual maintaining the ability to direct his own decision-making process based on his own desires and needs. The decision-making process should be free from undue control or influence as much as possible. The problem in this instance is that those subjected to the Panoptic gaze have their decision-making process influenced as they act to as to comply with the watcher's wishes.

[32] Lyon, D. *The Electronic Eye* (1994) p.65
[33] Foucault, M. *Discipline and Punish* (1979) p.202-203
[34] Foucault, M. *Discipline and Punish* (1979); McCahill, M. 'Beyond Foucault: Towards a Contemporary Theory of Surveillance' in *Surveillance, Closed-Circuit Television and Social Control* edited by Norris, C., Moran, J. and Armstrong, G. (Aldershot: Ashgate, 1998) pp.41-65

Conclusion

This section has explored in greater detail the concept of privacy by looking at both the different types of boundaries used to separate off private spheres as well as looking at different levels of privacy that can exist. It argued that depending on the type of boundary established and the social and legal norms associated with it, it is possible to determine the level of the privacy. It also argued that depending on the degree to which it is reasonable to assume that the information collected is intimate or of a personal quality, the level of privacy can change. Through highlighting these two points it is possible to understand how privacy can exist at varying levels and therefore cause different levels of harm when violated. Furthermore, by examining the Panopticon and the similarities it can have with imagery surveillance technologies, the issue of autonomy has been explored in greater depth by arguing that an individual's autonomy is violated when the Panoptic gaze influences his behaviour. As a result of highlighting these key points it is now possible in the next section to examine the illustrative examples and to outline the harm they can cause.

Section Three: Illustrative Examples

By watching and recording targets through a range of different means, imagery intelligence can provide the 'who', 'what', 'where' and 'when' of a situation. However, depending on the activity used and the way it is used, the level of harm caused can be dramatically altered. By applying the ethical framework set out in Chapter One and further discussed in Section Two of this chapter, to some key illustrative examples it is possible to judge the level of harm caused by imagery intelligence. This section will outline four different examples of imagery intelligence collection as a way of exploring its use and the harm it can cause. It will, first, examine the use of satellites and spy-planes as a means of gathering imagery information in the military and international sphere. Then, second, it will explore the use of CCTV cameras, 'intensive surveillance', and finally 'intrusive surveillance' as examples of imagery intelligence at the domestic level. These examples will then be placed on the Ladder of Escalation according to the level of harm they can each cause. For each activity this section will give a brief overview of what it entails, followed by a discussion of the harm it can cause, making reference to the vital interest(s) violated, the severity of the violation, the temporal quality, and whether there are any mitigating factors that might alter the level of harm.

Satellites & Spy-Planes

The importance of satellites and spy-planes as a means of gathering imagery intelligence is hard to deny. Ever since the first U-2 spy-plane's flight in 1956 and the launch of the first satellite, CORONA, in 1960, the importance of having eyes that could secretly fly over another's territory was undeniable and jealously sought. Satellites and spy-planes can watch facilities ranging from shipyards and missile silos to chemical and biological laboratories and industrial production. For example, by taking photographs of missile test sites intelligence operatives can identify new missile systems and detect changes in operational procedure that can suggest a change in hardware.[35] These eyes in the sky can also provide information on critical aspects of transportation networks, the progress of missile silos, radars or launchers of anti-ballistic missile, and during the Cold War they were considered vital in monitoring any violations of the SALT agreements.[36]

One of the most notable examples of spy-planes being used in detecting an upcoming threat was the Cuban Missile Crisis. The U-2 plane provided the first solid intelligence of

[35] Breckinridge, S. D. *The CIA and the U.S. Intelligence System* (Boulder, Colo.: Westview Press, 1986) p.140
[36] Greenwood, T. 'Reconnaissance and Arms Control' *Scientific American* Vol.228 (1973) p.14-25

Soviet activities when its photographs showed the erection of offensive missiles in Cuba. Such 'hard' indisputable intelligence gave Kennedy the ammunition to rally national and international support to confront the Soviets and force them to withdraw.[37] For satellites systems like CORONA, Harold Brown, Secretary of Defence during Carter's presidency, commented that: "Our national technical means enable us to assemble a detailed picture of Soviet forces, including the characteristics of individual systems… cameras take pictures of launch impact areas; infrared detectors measure heat from engines; and radars track intercontinental ballistic missiles in flight".[38] A Central Intelligence officer commented how when CORONA was first launched it "increased our knowledge 50 per cent… we were seeing things we had never seen before: military and scientific installations, shipyards, and even submarines being built".[39] Furthermore, Christopher Andrew notes how, just before the first Gulf War, the KH-11 satellite reported 30,000 Iraqi troops moving towards Kuwait along with pickup-trucks carrying ammunition, fuel and water. A few days later these images quickly revealed that this was not simply a show of strength by Iraq but an act of planned aggression.[40]

Level of Harm

It can be argued that the use of satellites and spy-planes violates the interest in privacy. It was argued in the previous section that states have established boundaries and can even make claim to owning certain sets of information, and that when an outside force transgresses either of these two things it is possible to consider the state's privacy as violated. Imaging systems like those used by satellites and spy-planes are designed to see behind a state's borders and to collect information on items that the state has created and therefore owns. A state has the right that its scientific advancements should not be stolen by another state. Indeed, a state has the right to "to provide for its conservation of property".[41] In doing so, these 'eyes in the sky' violate the state's sphere of privacy.

However, while it can be argued that the state can possess a notion of privacy this does not mean it is 'harmed' in the same way as intended by the ethical framework established in Chapter One. This is because the state is essentially not synonymous with a human being. The ethical framework created in Chapter One makes reference to the vital interests as a result of the human condition. The individual, by virtue of being human, has a

[37] Colby, W. and Forbath, P. *Honorable Men: My Life in the CIA* (New York: Simon and Schuster, 1978) p.189
[38] Johnson, L. *Secret Agencies* (1996) p.16
[39] Kessler, R. *Inside the CIA: Revealing the Secrets of the Most Powerful Spy Agency* (New York: Pocket Books, 1994) p.101
[40] Andrew, C. *For the Presidents Eyes Only* (New York: Harper Collins Publishers, 1995) p. 518
[41] *Montevideo Convention on the Rights and Duties of States* Article 3;17

set of interests that must be maintained lest he be harmed and unable continue with his life in a truly human way. States, alas, cannot make this same claim. The state is not harmed when its privacy is violated, but rather it is damaged. While acknowledging that there are a number of legal issues associated with violating the sovereignty of another state, which can in themselves raise important ethical questions, when a state's privacy is violated it is not harmed in the way intended by the ethical framework establish in Chapter One.

This point is most clearly understood when satellites scan inanimate targets, such as buildings or topographic features in that the buildings are not harmed. However, when a satellite or spy-plane is used to focus on an individual and collects personal information, then the action is similar to that of a focused CCTV camera scan or even the use of intensive surveillance, depending on the type and duration of the focus. The harm caused is, therefore, similar to that discussed in the sections below. When the target is not necessarily a specific individual but involves looking at a group, such as when a satellite or spy-plan focuses on an army or troop movement, the individual and his personal information is not the focus; rather the troop as a whole is. Given that it is the troop rather than the individual is the object of concern, it can be argued that in these situations it is not necessarily the individual's privacy that is violated but the state's and therefore it is the state that is damaged as compared to the individual being harmed.

Therefore, those scans carried out by spy-planes or satellites that collect information available only on the top-soil normally with optical-electro cameras, known as surface-scans, that do not focus on in an individual or his personal information do not directly cause harm. Even though it can be argued that these surface-scans could include looking at thousands if not millions of individuals, they are not, as it were, the direct target of the scan. Instead, it is the state that is the referent object: what it does, where its resources are, where its military is. While individuals do make up the state, and will obviously be active in the military or its industry, they are not the target of interest and are never really focused upon. In the case of the Cuban Missile Crisis or Iraqi troop movements mentioned above, the individuals that are engaged in these activities are never the focus, but rather the group or activity as a whole is. The individual, it can be argued, is therefore not harmed. Therefore, these surface-scans feature at the very bottom of the Ladder of Escalation at the Initial Level. However, the state's privacy is still violated and it is therefore damaged as a result, a damage which must be accounted for in the proportionality calculation in the Just Intelligence Principles.

Closed Circuit Television Cameras

At the centre of the question, 'are we becoming a surveillance state' rests a concern over how many closed-circuit television (CCTV) cameras exist in any given society, how often they capture an individual's image, and what is done to that image after it has been captured. Sophisticated devices and technological developments have greatly enhanced the capacity of the state to capture, monitor and categorise the daily lives of its citizens. Such observation has become increasingly systematic and embedded in everyday life, particularly as society is forced to deal with ever-increasing bureaucratic, domestic and consumer pressures. However, it can be argued that the fear and anxiety that is expressed at the escalating number of CCTV cameras present in society can be encompassed in the concern they raise regarding the affect they can have on an individual's privacy and autonomy.[42]

As an example of this new wave of 'watched societies' the United Kingdom represents one of the most heavily surveilled nations in the world. In response to the claim that CCTV cameras are the silver-bullet to crime problems[43], during the 1990s approximately 78 percent of the Home Office crime prevention budget was spent on installing CCTV cameras, with a further £500 million of public money being invested from 2000 to 2006.[44] Although it is difficult to state exactly how many cameras exist, recent estimates place the number of cameras on the streets of the United Kingdom at four million, capturing an individual's image as many as 300 times a day.[45] These CCTV cameras can also be augmented by recognition software that can automatically read faces or biometric data and match them to a stored pictorial database.[46] Also, Kingston University, London, is developing a system dubbed 'Comatica' which is able to compare frames and assess the likelihood of problems developing: "detecting unattended bags, people who are loitering or even predict if someone is about to commit suicide by throwing themselves on the track".[47]

CCTV cameras are used in a variety of ways and with the aim of protecting against a number of problems, from deterring and fighting crime, to keeping track of 'suspicious'

---

[42] Fox, R. 'Someone to Watch Over Us: Back to Panopticon?' *Criminology and Criminal Justice* Vol.1 No.3 (2001) p.251

[43] Bannister, J., Fyfe, N. and Kearns, A. 'Closed-Circuit Television and the City' in *Surveillance, Closed-Circuit Televisions and Social Control* edited by Norris, C., Moran, J and Armstrong, G. (Aldershot: Ashgate, 1998) p.22

[44] House of Lords: Select Committee on the Constitution *Surveillance: Citizens and the State* 2nd Report of Session 2008–09 (6th Feb. 2009) §70 p.20 Available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/surveillance_report_final.pdf Accessed 9th July 2009

[45] Gibb, J. *Who's Watching You?* (2005) p.22

[46] Fox, R. 'Someone to Watch Over Us' (2001) p.256

[47] Wakefield, J. 'Surveillance Cameras to Predict Behaviour' BBC News 1st May 2002. Available from http://news.bbc.co.uk/1/hi/sci/tech/1953770.stm Accessed May 20th 2009

characters and even as an early detection of potentially dangerous threats like terrorism. For example, street-level cameras can be used to monitor and track suspicious elements; motorway cameras are designed to prevent cars from breaking the speed limit or catch those who have not paid their tax; cameras inside shopping halls are designed to catch shoplifters or prevent misbehaviour from certain elements; and cameras at cash points are designed to stop fraud. In this way, these cameras are recognised as a vital tool in maintaining the peace and protecting a society. Deputy Chief Constable Graeme Gerrard, Chair of the CCTV Working Group, states that, "when a crime has occurred CCTV is a vital element of the investigative process. It is not an understatement to say now that the first piece of evidence that an investigating officer will go looking for is the CCTV evidence".[48] Furthermore, when London was suffering from a nail bombing campaign, the discovering of the perpetrators was made possible by CCTV evidence in terms of actually detecting that crime, causing many officials to ask, "what value do you put on the price of that detection?"[49]

Level of Harm: Privacy in Public

Generally the resistance to the use of CCTV cameras is framed in the language of privacy. Both Reg Whitaker and Simon Garfinkle claim that the rise of CCTV cameras signals the "death of privacy".[50] As it was argued in Chapter One, privacy is essential for an individual to feel comfortable, find emotional release and to act without feeling like he is being judged. Section Two in this chapter furthered this by outlining the varying levels of privacy an individual has as a result of the type of information or sphere of privacy being targeted. The question for CCTV cameras then is, to what extent an individual can expect his privacy to be maintained when in a public space. Moving about in public spaces is never truly anonymous. An individual can be seen and recognised by those around him. Thus, it can be argued that anyone who wants to remain unobserved and unidentified should stay at home or only go out in disguise. Robert Hallborg argues that this is fundamental to the very nature of what it means to go out in public: "we cannot possess rights not to be watched when we are in public" since such rights cannot exist in public places.[51] However, there is a difference between being seen by other people, whose memory of you comes and goes, and having someone closely observe you and record what you are doing. According to Andrew Hirsch,

[48] House of Lords *Surveillance* (2009) §76 p.21
[49] House of Lords *Surveillance* (2009) §.76 p.21
[50] Whitaker, R. *The End of Privacy: How Total Surveillance Is Becoming a Reality* (New York: The New Press, 2000); Garfinkle, S. *Database Nation: The Death Of Privacy In The 21st Century* (California: O'Reilly & Associates, 2001)
[51] Hallborg, R. 'Principles of Liberty and the Right to Privacy' *Law and Philosophy* Vol.5 No.2 (1986) p.177-178

CCTV surveillance infringes privacy because the scrutiny "is not casual or momentary, but focuses more closely on the activities in public of particular individuals".[52] Essentially, when CCTV cameras watch and record an individual's image and location they violate his privacy in that it is not just about who is 'seeing' him but who gets to 'watch' him. For that reason it can be argued that even though the individual is in a public space he is still afforded some level of privacy, that is, the right not to be scrutinised or closely observed without his permission. The invention of the photographic apparatus and related systems means that an individual's image can be fixed in a material form and then exploited over time without any consent from the owner of that image. Moreover, the fact that the image is then stored also multiplies the effect of the privacy violation. Since the "longer the tapes are archived, the greater potential threat" especially if they are "indexed according to who and what they show" as they can more easily be searched or integrated into personal profiles.[53]

The use of CCTV-type surveillance systems can also have an effect on an individual's autonomy. In the nightmare presented in George Orwell's *Nineteen Eighty Four* it was not just the lack of privacy that was so harrowing, but also the use of surveillance as a major mechanism for social control. Indeed, the loss of privacy was instrumental to social control as the desired end. If everything can be observed, the argument goes, everything can be controlled. If the surveillance is strong enough then it can be used to prevent disturbances from terrorist outrages to economic crises.[54] The presence of a CCTV camera can shape behaviour patterns by simultaneously "intimidating some people while reassuring others".[55] If an individual knows he is being watched by an asymmetrical gaze then he will act in the way he thinks that observer expects. Moreover, he will begin to habitually alter his actions all the time since he is unable to know if he is actually being scrutinised at any given point in time. It is in this way that CCTV systems are often equated with the Panopticon.[56] As Nick Fyfe and Jonathan Bannister note, the power of CCTV, much like the Panopticon, is not vested in surveillance of a particular individual but the "electronic gaze of the camera" which induces a "state of consciousness and permanent visibility that assures the automatic functioning of power".[57] Therefore, the individual's own actions are brought to his mind, he looks at them

[52] Hirsch, A. 'The Ethics of Television Surveillance' (2000) p.64-65
[53] Froomkin, A. M. 'The Death of Privacy?' S*tanford Law Review* Vol.52 No.5 (2000) p.1468
[54] Ball, K. and Webster, F. 'The Intensification of Surveillance' in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age edited* by Ball, K. and Webster, F. (London; Sterling, VA: Pluto Press, c2003) p.4
[55] Patten, J. W. 'Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places' *Ethics and Information Technology* Vol.2 (2000) p.185
[56] Lyon, D. 'The Search for Surveillance Theories' *Theorising Surveillance: The Panopticon and Beyond* edited by Lyon, D. (Devon: Willan, 2006) pp.3-20
[57] Fyfe, N. R. and Bannister, J. 'City Watching: Closed Circuit Television Surveillance in Public Spaces' *Area* Vol.28 No.1 (1996) p.39

through the eyes of those who are watching him and then alters them to comply with what he considers is expected of him. By carrying out this process the individual's autonomy is altered; he acts according to the desire of the watchers rather than as a result of his own will.

However, there is clearly a big difference between the near total watchfulness seen in Orwell's dystopia and what is experienced in the current situation by the average person. Therefore, the question must be to what extent CCTV systems truly reflect the Panopticon and its harmful effects. Does it in fact alter an individual's behaviour? In many ways, the answer to this is related to the affects it can have on groups of people. For example, the "Panoptic sort" describes a system of categorising the population to a hitherto unimagined degree and allows information holders to make predictions about the behaviour of the people on whom the information was collected.[58] Combine this sorting process with the ability to watch different types of people and there is the potential for the discrimination against specific social sub-groups, social exclusion and the lessening of social bonds.[59] A system that decides what is, and what is not, suspicious behaviour, appearance or identity can cause repercussions for society as it gives rise to a prevailing climate of suspicion; adversarial relationships; weakening of society's moral fibre and social cohesion and the potential for abuse from a totalitarian government.[60] By creating this type of atmosphere it can be argued that the individual will begin to feel the Panoptic gaze to a greater extent and will become ever more likely to alter his own autonomy in order to fit in. This means that CCTV scans that focus on a group because of their race, ethnicity, religious orientation or age can cause a greater level of harm. Singling out a specific subsection of society based on appearance encourages the degradation of social cohesion as certain groups become suspects regardless of what it is they might or might not have done; they are watched regardless of any proven guilt.[61]

In general, however, the level of harm caused by many uses of the CCTV camera is relatively low. On the one hand it can be argued that the individual does in fact retain some degree of privacy while out in public and still maintains some control over his image and how it is used. However, moving about in public is never truly anonymous and by entering the

---

[58] Gandy, O. *The Panoptic Sort: A Political Economy of Personal Information* (New York: Westview Publishers, 1993)

[59] Bauman, Z. *Intimation of Postmodernity* (London: Routledge, 1992); Bogard, W. *The Simulation of Surveillance* (Cambridge: Cambridge University Press, 1996); Lyon, D. 'An Electronic Panopticon? A Sociological Critique of Surveillance Theory' *The Sociological Review* Vol.41 No.3 (1993) pp.653-678; Mathiesen, T. 'The Viewer Society: Michelle Foucault's Panopticon Revisited' *Theoretical Criminology* Vol.1 No.2 (1997) pp.215-234

[60] Clarke, R. 'Information Technology and Dataveillance' *Communications of the ACM* Vol.31 No.5 (1988) p.505

[61] Laidler, K. *Surveillance Unlimited: How We've Become the Most Watched People on Earth* (Thriplow: Icon, 2008) p.209

public sphere there is, to some extent at least, an acceptance that one will be seen. An individual's surface image, while being private, is readily exposed to the rest of the world and he must recognise this fact. The body, essentially the most private realm of intimate experiences, is also a public entity, a "spectacle and the medium through which common experience is realised and represented".[62] By entering the public domain there is a tacit consent to waive the control one has over one's immediate image. Furthermore, if the type of personal information collected is only very basic – an individual's image and nothing else – then nothing essential about the individual can be determined. Who the individual 'is' is not gained.

And while the idea of the Panopticon "refuses to go away"[63], it can be argued that given the current mechanisms used, the extent to which any individual's autonomy is directly affected is still minimal. One of the key features of the Panopticon is that if the target transgresses then the target is punished in order to reinforce both that those actions are prohibited as well as underlining the belief the target is being watched. For example, in *Nineteen Eighty Four* when Winston Smith failed to keep up the pace with the centrally controlled exercise programme he was quickly reminded of the watchful eye of Big Brother: "6079 Smith W! Yes *you!* Bend lower! You can do better than that. You are not trying... *That's* better comrade".[64] It can be argued that the power of the Panopticon lies in its ability to induce conformity by a rapid intervention when something suspicious is detected.[65] In many ways, people 'forget' the camera's presence and so the ability to bring their own actions to themselves, and encourage them to alter their behaviour and thus affect their autonomy, is reduced. A national survey of existing and planned CCTV systems conducted in 1999 showed that of the five million cameras previously quoted to exist in the United Kingdom, only approximately 1,300 systems incorporating some 21,000 cameras were run by state authorities.[66] As a result, the CCTV Panoptic prison is one that is not as pervasive as many would think and one where the inmates can leave when they want to - something quite different from Bentham's original Panopticon. Since there is no direct punishment and individuals can willingly move out of the electronic gaze the ability to directly alter or control individuals or society is seemingly limited. As Jeffery Reiman argues, CCTV surveillance

---

[62] Brettle, J. and Rice, S. *Public Bodies, Private States: New Views on Photographic Representation and Gender* (Manchester: Manchester University Press New York, 1994) p.1
[63] Lyon, D. 'Surveillance Theories' (2006) p.4
[64] Orwell, G. *Nineteen Eighty Four* (London: Penguin Books, 1987) p.39
[65] McCahill, M. 'Beyond Foucault: Towards a Contemporary Theory of Surveillance' in *Surveillance, Closed-Circuit Television and Social Control* edited by Norris, C., Moran, J. and Armstrong, G. (Aldershot: Ashgate, 1998) p.44
[66] Webster, W. 'CCTV Policy in the UK: Reconsidering the Evidence Base' *Surveillance and Society* Vol.6 No.1 (2009) p.17

poses a symbolic risk to society by jeopardising peoples' sense of their own activity rather than a physical or direct means of controlling society. As a symbolic messenger, CCTV "insults rather than injures".[67]

There is, however, a difference in degrees to which a CCTV camera can scan the target and as such different degrees to which it can violate an individual's privacy. CCTV cameras can capture the immediate image and location of the individual while not actually taking any more information than this. The target is not identified, has no information about his personal life acquired, nor is he really focused on. This is a passive scan where the individual is seen but not really examined in any way. In this instance the level of information gathered is not very personal and so, in reference to the levels of intimacy outlined in Section Two of this chapter, there is only a minimal violation of privacy. Compared to this, however, are those CCTV scans that not only capture the individual's image but focus and capture his identity or follow him as he goes about his activities. This type of scan is a greater violation of the individual's privacy because the amount of information collected from him is both greater in quality as well as quantity.

Therefore, for those cameras that passively scan, never focusing on or singling out a particular individual and as such literally taking only the surface image, it can be argued that both the affect on the individual's privacy and autonomy is limited and therefore would feature at the Initial Level on the Ladder of Escalation. In comparison, if the CCTV camera focuses, identifies, follows or singles out an individual then the level of harm caused is increased. This means that the level of harm caused features at Level One of the Ladder of Escalation. Furthermore, scans that focus on particular individuals because of their racial, ethnic, religious or other socially-based signifiers cause a higher level of harm because they separate out these individuals, treat them differently and promote the segregation of that particular social group, causing a greater interference with their autonomy as well as promoting social decohesion. Profiling therefore causes a higher level of harm as well as raising concerns regarding the affect it can have on social stability.

Intensive Surveillance

Sometimes referred to as 'covert surveillance'[68], 'light covert intelligence'[69] or more colloquially 'stalking', intensive surveillance involves the covert monitoring of a target's

[67] Reiman, J. 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' *Computer and High Technology Law Journal* Vol.11 (1995) p.39
[68] House of Lords *Surveillance* (2009) Chapter 3 §85 p.23

movements, rendezvous, acquaintances, and any other activity that can be seen and recorded. Intensive surveillance is similar to CCTV cameras in many ways in that it involves visually tracking an individual from a distance. The main difference, however, is that with intensive surveillance the gaze is much more rigorous as it follows the individual to a much greater extent and collects a greater quantity and quality of information. Intensive surveillance is normally very specific over who the target is or what it focuses its attention on and is performed by highly trained individuals who are experts at following a target without being detected.

This intensive surveillance work is normally carried out by small groups of highly skilled specialist operatives who work in vehicles, on foot or from 'static observation posts'. A 'static observation post' is a fixed position from which surveillance of a certain location can be carried out. An agent will sit with recording equipment in order to gather information about a location – a foreign embassy for example – recording who visits it, at what point and with whom. Faces are then checked against a 'mug book' containing thousands of photographs of people of concern. For example, during the Cold War some 250 agents "spent their time sitting in dark drab rooms equipped with binoculars, cameras, a log book and an overflowing ashtray".[70] 'Mobile surveillance', in contrast, is where agents track a moving target. For instance, Tony Geraghty outlines the often used ABC system:

> At least three teams follow the target: A (for Adjacent also known as eyeball) is the nearest; B for Backup is further back, preferably concealed from the quarry. Both usually stick to the same side of the road. C for Control has a wide field of vision on the opposite side of the road, guiding the other two with a concealed throat microphone and discreet hand signals.[71]

Another method is called 'target control', where a number of agents in a number of streets connected by secure communicators keep the target within a web of agents, so that while they might not be able to see the target directly he is still controlled.[72]

During the Cold War this type of surveillance was carried out by domestic intelligence operatives, often following individuals from foreign states while in their own country. For example, John Sawatsky, of Canadian intelligence, tells the story where Soviet

---

[69] See Northcott, C. 'The Role, Organisation and Methods of MI5' *International Journal of Intelligence and Counterintelligence* Vol.20 No.3 (2007) pp.453-479; Morgan, R. E. *Domestic Intelligence: Monitoring Dissent in America* (Austin: University of Texas Press, 1980)

[70] Hollingsworth, M. And Fielding, N. *Defending the Realm: MI5 and the Shayler Affair* (London: André Deutsch, 1999) p.64

[71] Geraghty, T. *The Irish War* (London: HarperCollins Publishers Ltd, 2000) p.144

[72] Hollingsworth, M. And Fielding, N. *Defending the Realm* (1999) p.64

cultural attachés upon leaving the Russian Embassy in Ottawa, would drive around the Canadian countryside for about three hours before going on to meet with contacts and agents.[73] The Canadian intelligence operatives would follow and visually record their actions using cameras in order to provide the physical evidence to help in convictions. This type of intensive surveillance operation was an everyday feature of the Cold War for both sides of the Iron Curtain. However, these targets became very apt at losing the watchers, and in many ways provided the training the intelligence community would need for the current emphasis on terrorists and criminals. For example, in the fight against crime, intensive surveillance is a key weapon for organisations such as the FBI and the British Serious Organised Crime Agency in their fight against organised crime syndicates and drug cartels. Assistant Chief Constable Nick Gargan argues that, "the use of covert surveillance is indispensable... in the fight against all forms of criminality".[74] Furthermore, for British intelligence these 'watchers' proved indispensable in the fight against IRA terrorists in both Northern Ireland and on the British mainland. By the 1990s, T Branch (Irish counterterrorism) was engaged in dozens of operations backed up by the surveillance powers of A Branch. Indeed, "T Branch was prepared to risk watching the bombs being planted, in the hope that the perpetrators would lead them to bigger fish".[75]

Level of Harm: Intensive Surveillance

In much the same way that CCTV cameras violate an individual's privacy by watching him, so too does intensive surveillance. The individual's every activity is recorded and scrutinised. Who the target is, where he is going and with whom he is associating, all becomes the concern of the watching intelligence operative. As the name might suggest, intensive surveillance is indeed more exhaustive than CCTV surveillance and as such involves a greater violation of an individual's privacy. The information it gleans from its target is both of a greater quantity as well as being of a more personal quality. In reference to the levels of intimacy described in Section Two, intensive surveillance goes deeper than CCTV cameras; it seeks to know and identify the person: who he is, where he is going, what he is doing and to track him as he goes along his path. This type of information collected is quite personal, getting to the 'who' of the target to a much greater extent than that seen with CCTV cameras.

The other important difference between CCTV cameras and intensive surveillance is the temporal quality of the surveillance. The longer the individual is being followed or

[73] Sawatsky, J. *Men in the Shadows: The RCMP Security Service* (Toronto: Doubleday, 1980) p.29
[74] House of Lords *Surveillance* (2009) §86 p.23
[75] Urban, M. *UK Eyes Alpha: The Inside Story of British Intelligence* (London: Faber, 1996) p.278

watched the more his privacy is violated. So, while it is possible to escape the watchful eyes of CCTV cameras by going into areas where there are no cameras, shaking off an intensive surveillance team is less easy. Intensive surveillance by its nature is designed to follow the target wherever he goes, and in doing so gives the target even less respite than CCTV cameras; there is no place to be alone when the target is in public. This makes the violation of the interest in privacy greater than CCTV surveillance.

Finally, in comparison to the use of CCTV cameras, there is not the same degree of consent. It can be argued that one mediating point for the use of CCTV cameras is that when the individual enters the public realm he acknowledges the use of CCTV cameras and gives tacit consent to their (briefly) recording his image. He knows the cameras are there, that they are watching him and so he offers a limited consent to them recording his image in exchange for the benefits of security offered. Intensive surveillance, however, does not have this. The individual is unaware that he is being targeted and as a result he has not consented to it. Therefore, hidden observation is problematic because it removes consent, that is, the ability of the person being watched to decide who and how the world sees him.

So, while it can be argued that there is clearly not the same effect on an individual's autonomy because he is unaware that he is being watched, and therefore is not likely to alter his behaviour, the degree to which is privacy is violated is much greater than that seen with CCTV cameras. Even compared to the deep-level CCTV camera scans, the use of intensive surveillance collects both a greater quantity of information because it never leaves the target alone as well as a greater quality given that it collects more intimate details. Furthermore, while there is a feeling with CCTV cameras that they are watching all the time, and it might be true that they are always recording, there is chance of escape. However, with intensive surveillance while the individual is out in the open there is essentially no escape. No matter where the individual goes, so too goes the tracker. However, similar to CCTV cameras, there is still the mediating point that the individual is moving about in a public space and must, even to a limited extent, recognise that when in public spaces his sphere of privacy is reduced and that he is going to be seen. As a result of all these factors intensive surveillance causes a level of harm which means it features at Level Two on the Ladder of Escalation.

Intrusive Surveillance

'Intrusive surveillance' involves placing electronic cameras, or 'bugs', that capture a target's actions when he is within his own house or property in the hope of recording nefarious activity. Moreover, the placement of such devices will often involve 'covert interference'

with that property. Tactics could involve either breaking and entering the property to place the device, or intelligence agencies employing telephone companies to put a fault on a targets line, so when they report the fault an intelligence agent could respond and use the granted access to plant the bug.[76] Reported examples of such a device include the installing of a camera in the target's television: "so that when the occupant sits to watch television, which we have rigged so that the television is watching him".[77] Equally, direct access to the house is not always needed. By renting a neighbouring property, agents can drill a small hole through an adjoining wall and then feed a small fibre optic camera through the hole. One of the greatest benefits for planting the devices inside a target's home is that nefarious activities are more likely to occur in areas where the actor feels he is protected and free from watching eyes.

Levels of Harm: Privacy at Home

The walls that surround a person's home clearly demarcate a sphere of privacy. There is a long history which underlines the understanding that there exists a sphere of privacy that revolves around personal property, such as the home, which constitutes an important limit on outside interference.[78] The home or any similar property represents one of our most sacred and protected realms, and crossing this particular line represents a clear violation of an individual's sphere of privacy. Even if the target is unknowing to the fact that he is being watched, the intrinsic value of having an important space of privacy, where he can find emotional release, means that any violation is still harmful.

Of all the boundaries that individuals put around themselves, the physical walls of their house or home are some of the most obvious, strict and clearly defined indicators of a private sphere. Socially accepted, widely understood and even legally proscribed, there is little chance of interfering with someone's property accidentally or without knowing that this is an important private sphere.[79] Indeed, this boundary represents one of society's most important manifestations of the private sphere. Furthermore, the type of information collected from an individual when he is within his own property is of more private quality than that when he is in public as it will often be of a very intimate and sensitive nature. It can include very personal attitudes, conditions and behaviours that would only be revealed to those that an individual feels close to or can trust. It does not have to be particularly unique, but it is

[76] Hollingsworth, M. and Fielding, N. *Defending the Realm* (1999) p.66
[77] Geraghty, T. *The Irish War* (2000) p.143
[78] Fairfield, P. *Public/Private* (London: Rowman & Littlefield Publishers, 2005) p.101, 107
[79] For example, Article 8 of the European Convention on Human Rights guarantees the right to respect for privacy of one's family life and one's home.

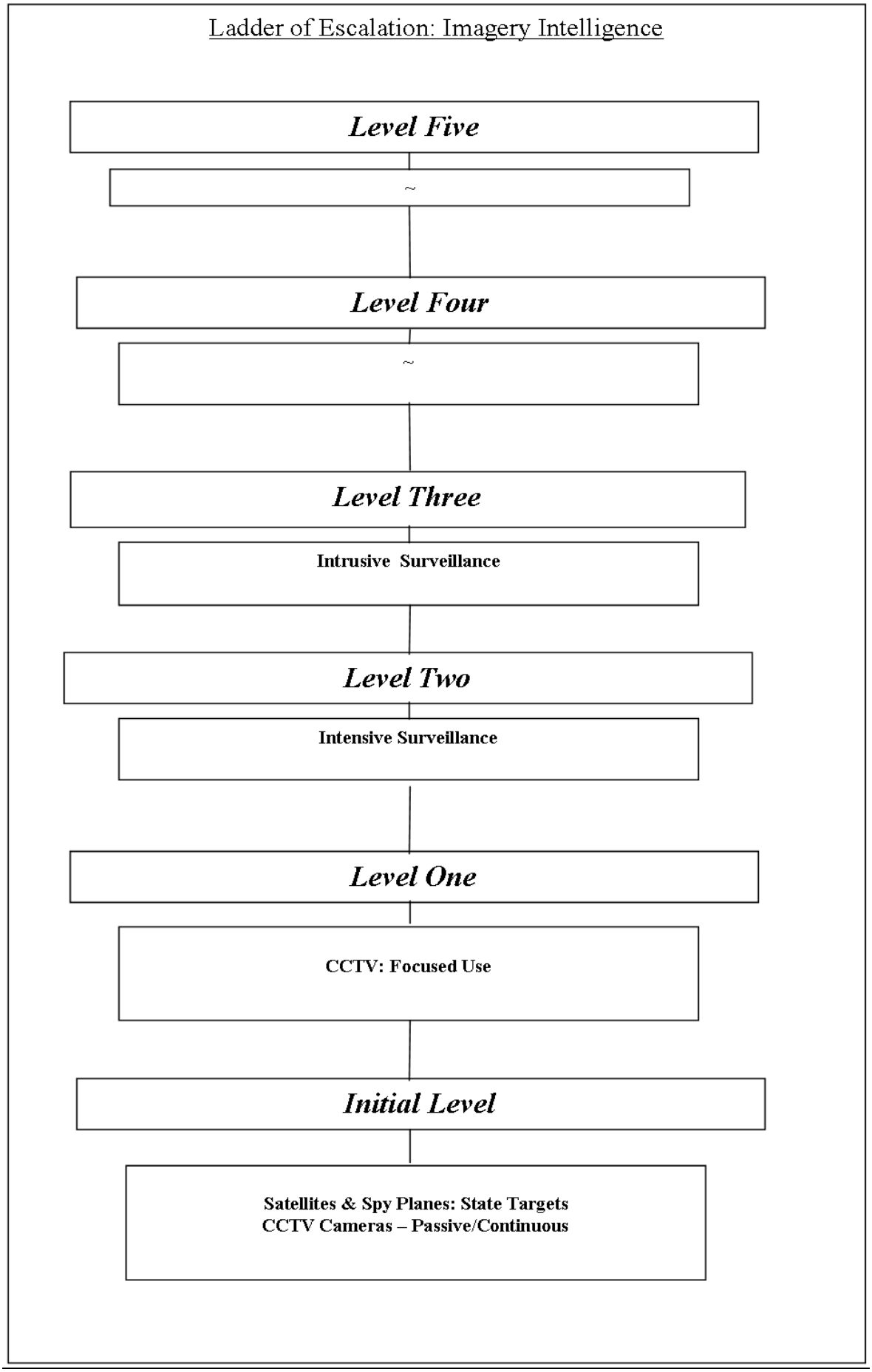
normally of such intimate detail that in general only a few would ever witness it, for example, sexual relations, acquaintances, nudity or personal habits. It can be argued that the intimacy level for this information is one of the closest to the individual's core. As a result, given the social and legal norms that maintain the boundaries of the individual's property as well as the argument that the information kept within the property is likely to be highly intimate, to breach this sphere is one of the most severe violations of an individual's interest in privacy.

In comparison to the use CCTV cameras and intensive surveillance, the individual maintains a higher level of privacy when it comes to his private property, highlighted by both social and legal norms. Therefore it can be argued that interfering with someone's property and placing technical devices designed to record activities from within that property features highest on the Ladder of Escalation of all the imagery intelligence collection activities, at Level Three.

Conclusion

By exploring these four different types of imagery collection activities, this section has demonstrated the level of harm caused by imagery intelligence. It argued that it can vary depending on the sphere of privacy violated, the extent the individual can expect to have control over information pertaining to his self and how 'intimate' or 'personal' this information is. It argued that Satellite and spy-planes feature at the lowest level on the Ladder of Escalation, the Initial Level, as does passive CCTV scans, whereas intensive CCTV scans figure at Level One. Intensive surveillance operations cause a Level Two harm and using an electronic device to see and record inside someone's private property, namely a home, is a Level Three harm. In Figure 2.0 it can be seen how they would appear on the Ladder of Escalation in comparison to each other. In the next section these different activities will be examined in reference to the Just Intelligence Principles so as to determine if and when they are justified.

Figure 2.0


Ladder of Escalation: Imagery Intelligence
Level Five
~
Level Four
~
Level Three
Intrusive Surveillance
Level Two
Intensive Surveillance
Level One
CCTV: Focused Use
Initial Level
Satellites & Spy Planes: State Targets
CCTV Cameras – Passive/Continuous

Section Four: Just Imagery Intelligence

The previous sections in this chapter have outlined the different imagery intelligence collection activities and the different levels of harm that they can cause. In order for each of these imagery intelligence collection activities to be just, however, the level of harm caused must be matched to a corresponding level of just cause, authority, proportionality and discrimination. The principles of right intention and last resort are generally not dependant on the level of harm caused but need to be fulfilled in an appropriate manner. Therefore, they will only be directly discussed if there is something relevant. As such, this section will go through each of the imagery intelligence collection activities and the different levels of harm that they can cause and discusses the extent the principles of just cause, legitimate authority, proportionality and discrimination are fulfilled. Finally, this section will bring these assessments together onto the Ladder of Escalation to illustrate how they compare to each other.

Surface Satellite and Spy-Plane Scans

It was argued in Section Three that using satellites and spy-planes to scan a state's features – such as topographic information, troop movements, buildings or weapons – causes the lowest level of harm because states do not experience harm in the way this thesis sets out, and so features at the Initial Level of the Ladder of Escalation. As a result, the use of satellites and spy-planes will in the majority of cases require little or no level of threat, does not have to discriminate between states as targets (although it might be politically sensible to do so) and even the authority can be very low or non-existent (although again, given the political ramifications states might wish to allocate a higher level of authority so as to ensure that any political fall-out is fully considered by the appropriate individuals). The main consideration is, when the state's privacy is violated, how is it best to incorporate this negative into the principle of proportionality. That is, although the state is not harmed by the violation, it is wronged and this wrong should be taken into account when determining if the operation is proportional.

CCTV

It has been argued that those CCTV scans that are on a passive scan, not focusing on or singling out a particular individual, do not identify who the target is or follow the target from place to place can cause a low level of harm and as such features at the Initial Level. Being

placed at the Initial Level means that passive scans can be used on everyone with no need to authorise or to have a just cause. However, due to issues associated with storage and the use of this information for other, more harmful, practices the level of harm could be increased if the pervasiveness of the data collection is increased or the storage of the data is made easily accessible or held for long periods of time. Also, there should be care not to use CCTV cameras to single out or discriminate particular sections of society since these actions cause a greater degree of harm to the society in the form of social decohesion and the fracturing of society. In comparison, those CCTV cameras that perform more intensive scans – identifying the individual for example – the level of harm features at Level One on the Ladder of Escalation, meaning that there must be some level of threat in order to provide a just cause, an appropriate level of authority to sanction the scan and attempt to discriminate between legitimate and illegitimate targets.

Just Cause

Those CCTV scans that focus on an individual, look at his face or identity, single him out or follow him cause a higher level of harm and therefore require that there be some form of threat, though the threat itself need only be suspected, indistinct, something of low importance or of low impact ability. That is, it is not enough to suspect everyone and anyone; the target must have done 'something' to warrant the attention. Examples of this type of threat include 'suspicious behaviour', 'antisocial behaviour' or other activities that are likely to cause a breach of the peace. Although the detection of 'suspicious' behaviour is not an exact science, there is clearly a difference between someone who is going about his normal business and someone acting suspiciously. Guidelines designed to detect suspicious behaviour state that, "the first and most obvious suspicious person is someone who is doing something unexpected, such as working in an area where work is not generally done, or repeatedly doing the same route or even doing a route which is illogical, or overacting, acting nervous, et cetera". [80] Clearly this not designed to be an exhaustive description, but rather to give an indication of the type(s) of behaviours involved. Other examples of this level of threat include anti-social behaviour and disturbances of the peace, both of which threaten something of low importance to the state and are generally of low-impact. For example, disturbances or breaches of the peace involve an offence constituting a malicious and wilful intrusion upon

[80] Isaacs, R. 'What constitutes Suspicious Behaviour and What to do About it?' *The Lubrinco Group* Available at http://www.lubrinco.com/articles/Informed%20Sources%20November%202003.pdf. Accessed May 1st 2009

the peace and quiet of a community or neighbourhood.[81] Therefore, abusive, rowdy, disruptive, aggressive, lewd or offensive behaviour are examples of the type of activity that represents a just cause for the CCTV cameras focusing in on an individual and even tracking him for a short while.

Authority

Given the low level of harm caused by the CCTV cameras, even when they focus on a particular individual for a short while, the level of authority required can be minimal. That is, for those sitting in the control station operating the devices, as long as they have been sufficiently trained and understand the responsibility they have to not abuse the system, they can make the judgement themselves about whether the target is in fact presenting the level of threat described. They can act as the appropriate authority. However, they are responsible for their own actions and they need to understand the rules and regulations by which their actions are governed. They are not average individuals, but very much workers trained for this type of job.

Proportionality

The principle of proportionality is designed to make sure that the harm caused to the target, the agent and society in general is proportional to the gains or prevents greater damages. This means that preventing minor offences from happening does not create a sufficient level of good to outweigh the overall damage caused by the use of CCTV cameras. For example, in November 2008 the UK Home Secretary stated that "it [CCTV camera] should not be used to snoop on people suspected of minor offences such as dog fouling or putting out the rubbish on the wrong day".[82] That is, it could be argued that these 'offenses' are not sufficient enough to outweigh the level of harm caused by CCTV camera systems that feature at Level One on the Ladder of Escalation. Furthermore, if there were enough CCTV cameras watching all the streets to capture individuals putting out their rubbish on the wrong day, the harm caused to society with such permeating coverage would never be outweighed by the gains of having rubbish bins only out when they should be. Instead, they should be used for more serious offences, like detecting breaches of the peace or anti-social behaviour that might cause damage to people or property.

[81] The UK Court of Appeal defined a breach of the peace as being 'an act done or threatened to be done which either actually harms a person, or in his presence, his property, or is likely to cause such harm being done' – see *R v Howell* [1981] 3 WLR 501 Court of Appeal

[82] BBC News 'Extent of Council Spying Revealed' 26th March 2009 Available at http://news.bbc.co.uk/1/hi/7964411.stm Accessed 1st May 2009 Accessed 9th July 2009

Discrimination

According to the principle of discrimination, in order for the imagery intelligence collection to be just it must discriminate between those who pose no threat at all and those who pose some level of threat. For the use of intensive CCTV scans to be just they must only focus on those who have acted in such a way as to pose some threat. This threat can be demonstrated by the target acting suspiciously or in an anti-social manner, for example, in that these actions have resulted in him forfeiting his privacy rights. Conversely, those who have not acted in a threatening way – literally walking down the street minding their own business – cannot be focused upon directly or 'identified' by the cameras and should have their image destroyed after a reasonable amount of time.

Intensive Surveillance

The level of harm caused by the use of intensive surveillance features at Level Two on the Ladder of Escalation. Intensive surveillance demonstrates a greater violation of the interest in privacy since it collects information that is both more personal and of greater quantity than that seen for CCTV cameras. Therefore, in order to be justified there must be a low-to-medium level of threat, a higher level of authority than that seen for CCTV cameras and discrimination between targets.

Just Cause

In order for intensive surveillance to be just there must be some threat that is clearly understood, though it might still be temporally distant and threatens something of mediocre importance with a medium-low impact ability. One example of this type of threat might be criminal elements like drug or contraband smugglers. They pose a threat to the safety and peace of society since they can cause damage to the lives of many people and cause significant damage to the cohesion and stability of a society while not actually posing a direct or imminent threat. That is, they pose a constant threat to something important, though their impact in the immediate future is dispersed and relatively low. As such, drug operations would offer a just cause for an operation involving intensive surveillance.

Another, quite different, example involves foreign diplomats from states with whom there are unfriendly relations. If there is a history of subterfuge and espionage then there is evidence to support the argument that they might pose a threat, even if it is indistinct or temporally distant. For example, during the Cold War, foreign diplomats from the Eastern bloc were often responsible for carrying out intelligence operations against the West when

they were stationed in another country. Even though there is no direct threat, the history of previous attempts would give just cause, enough to justify the level of harm associated with intensive surveillance. Therefore, in both examples mentioned above where Western intelligence operatives followed Soviet embassy personnel (and vice-versa), given the history between the two sides it can be argued that there is enough evidence to present a legitimate threat and therefore a just cause for the use of intensive surveillance.

Authority

While Level One harms could be authorised by the trained operatives, in order for Level Two harms to be just there must be an even higher authority to sanction it. That is, at Level Two it can still be internal to the intelligence agency but must be higher than those who are directly involved in the operations. That is, departmental heads or deputy-head of the intelligence agency performing the activity can act as suitable authority. For example, for the British Security Services this responsibility would fall to the respective heads of each of the main branches and then that individual would be held responsible for his decisions on a regular basis to either the Director General or the Deputy Director General (or in the case of drugs operations in the UK then it would be the Serious Organised Crime Agency and its Director General).

Proportionality

Sir Christopher Rose, the Chief Surveillance Commissionaire discussing intensive surveillance commented that "the methods have to be proportional to what is sought to be achieved… it must balance the intrusiveness of the activity against the operational need".[83] This means that the threat, as well as the gains from performing this particular operation, must be sufficient enough to outweigh the harm. For example, during the 1960s the American Army carried out its own intelligence collection programme with the aim of being better prepared for social instability and any actions it might have to take. As a result it started the Continental United States Intelligence Programme (CONUS) in the summer of 1965 as an early warning system for social disturbances. At the height of the programme in 1968-69 an estimated 1,000 plain-clothed investigators were photographing those who attended political rallies, even including "mother and church organisations" who were meeting on the need for world peace.[84] While it could be argued that there was a just cause, given the social instability

[83] House of Lords *Surveillance: Citizens and the State* (2009) §.310 p.73
[84] Morgan, R. E. *Domestic Intelligence* (1980) p.61

at the time and the likelihood that the army could be called upon to intervene, the use of such intelligence collection disproportionate to the threat that these rallies posed.

Discrimination

Those targeted must be linked to the threat in some way or have acted in some way to waive or forfeit their right to privacy. In the instance of the drug smugglers or dealers, there is often a large network of individuals who are connected. Those who have become a part of the criminal activity have broken the law and so have acted in such a way as to forfeit their protective rights and are therefore legitimate targets. However, those related to legitimate targets but are not involved in the threat have not directly waived or forfeited their protections to make them legitimate targets for intensive surveillance. In the case of foreign diplomats, by taking the job within the state's infrastructure and even by travelling to a posting abroad they have 'joined the game' to quite a significant degree and so have waived their normal protective rights. They are, therefore, legitimate targets for intensive surveillance. It can be argued, however, that when they return home or retire, if they show no other indication of state activity, they regain their rights and are therefore illegitimate targets. Another group of illegitimate targets are those who happen to be the nationality of a foreign country who are merely visiting another state. Despite travelling they have done nothing to warrant being targeted.

Intrusive Surveillance

Of the imagery intelligence collection illustrative examples provided in this thesis, those technical devices that are placed inside a target's personal property feature highest on the Ladder of Escalation at Level Three. This is because they violate one of the most important privacy boundaries that an individual can erect around himself, and as such the information gleaned from such invasions is generally of the more personal quality. Not only this, but since the individual is unaware that he is being watched there is no consent present as was the case for the use of intensive surveillance and CCTV cameras.

Just Cause

In order for the level of harm caused to be justified, there must be a medium degree of threat. This means that the threat is targeting something of importance or has the ability to cause a reasonable amount of destruction. Furthermore, there must be evidence 'on a balance of probabilities' that demonstrates that the threat exists. For example, during the British

engagements with the IRA, there was a constant underlying tension and a high possibility of destructive aggression. So, if there is evidence that suggests an operation is afoot, although it can still be temporally distant, then this would represent a just cause. For example, British intelligence used concealed monitoring of Hugh Jack, a known IRA activist, to gain information regarding his weapons running. By the summer of 1993, this surveillance lead to the arrest and prosecution of Robert Fryer, a member of the IRA's punishment squad, and Sean McNulty, a culprit of previous bombings of several oil and gas installations in northern England, as they left the property carrying submarine guns and bombs across a London street.[85] Another example of a sufficient drug cause would again involve a drugs case, but at this level of harm there must significant evidence to prove that the targeted property is a storage house, manufacturing or dealing den for the drugs themselves.

An example drawn from the literature which demonstrates a lack of just cause is British intelligence breaking into the house of Ken Gill, a member of the TUC General Council from 1974 to 1988 and the general secretary of TASS, the union that represented white-collar workers in the engineering industry. He was also a long standing Communist Party member and became an integral part of the planned merger between TASS and the manual engineering union, AUEW. During the merger talks "his [Gill's] home was broken into and a bug was placed inside his room to monitor Mr Gill and other trade unionists".[86] In this example, the threat that he represented (the potential to cause social unrest or to cause a swelling in the communist ranks) was temporally distant, of low destructive quality and generally undefined and therefore was not a sufficient just cause. If it was discovered through the use of an activity that caused a lower level of harm that he was planning violent actions or actively promoting violent social unrest then this might provide a just cause for this level of harm, but otherwise the threat in this example is insufficient.

Authority

The level of authority required for this degree of harm should be one that is outside the organisation that carries out these activities and should be authorised by the politico-judicial branches of the state. The assessment regarding whether there was a sufficient threat or not should be done rationally, with relevant facts presented, weighed and judged, with as little bias as possible. As such, it can be argued that the authorisation of such operations should be done by the judicial wing of government, since the courts are often practiced in weighing up evidence and determining if certain acts reach the sufficient criteria required to invade

[85] Urban, M. *UK Eyes Alpha* (1996) p.279
[86] Hollingsworth, M. And Fielding, N. *Defending the Realm* (1999) p.67

someone's privacy. A council of judges would further ensure that the evidence was relatively free from personal bias. This will equally ensure that political trends would not cloud the decision-making process, as it could be argued was seen in the Gill case. An appropriate example might be specialised judges who act to decide if the evidence provided is sufficient enough to violate the targets privacy in this way.

Discrimination

There should be discrimination between targets so that only those individuals involved in the preparation of the threat or the carrying out of the threat are targeted. Furthermore, those who are established members in the threatening organisation can be legitimate targets given that by taking on such a position means that they have forfeited their protective rights. In the example of the IRA, those members who are directly involved in the planning and implementing of the threat, or those who are members of the organisation are legitimate targets since they have acted in a way as to become part of the threat. However, their family or friends are not legitimate targets and every effort should be made to avoid involving them. For example, when there is no legitimate target in the room being monitored, the cameras should be turned off and then turned on at a later date to see if a legitimate target is present.

Conclusion

Those who can see the furthest, the quickest and in the greatest detail have an instant advantage in the struggle to protect the political community from both internal and external threats. The argument for the importance of imagery intelligence is compelling, with its tangible representation of the evidence, the ability to see far beyond what would be available normally, and the option to keep the image stored for later analysis. This chapter has demonstrated how satellites, spy-planes, CCTV cameras, intensive surveillance and intrusive surveillance can all play a vital role in providing physical and tangible information that can be vital in protecting the political community. However, the very act of collecting imagery intelligence raises the possibility of causing harm to those it targets, a harm that cannot go unchecked. This chapter has argued that the collection of imagery intelligence can violate the privacy and autonomy of those it targets and in doing so without justification should be prohibited. By exploring imagery intelligence and outlining the unique level of harm that different examples can each cause and then examining this with respect to a set of Just Intelligence Principles, this chapter has been able to argue under what circumstances these particular acts can be justified. In the next chapter the same process will be used to evaluate the use of signals intelligence and whether it is ever just to intercept another's communications.

Chapter Three: The Information Nation
Information Transmission, Collection and Storage

Life in the modern age is a mass of information being transferred, stored and processed in ever faster and more efficient ways. Communications, data, pictures, music, activities, business deals, and, increasingly personal information, are all collected, digitalised and transferred along information highways. Indeed, technology has revolutionised how people communicate, interact, organise and carry out their lives, as well as turning modern society into an 'information nation' where the drive for ever more efficient and effective governance becomes tied up with technology and the ability to collect and process vast amounts of information. For the intelligence community this technology opens up untold opportunities in new means of protecting the political community. However, the problem for the intelligence community is that new technology also brings with it a host of new threats and dangers.

This chapter will examine the use of signals intelligence by looking at how the intelligence community intercepts, collects and monitors information transmitted in a signal in order to better understand the mind and intentions of the sender or receiver. Furthermore, another issue examined in this chapter is the growth of the 'data intelligence', exploring the role intelligence plays in collecting an individual's personal information as his activities become increasingly being digitalised, collected and stored away.

As a means of ethically evaluating the use of signals and data intelligence, this chapter will start by outlining those activities associated with signals intelligence as it attempts to gain access to the signal in transmission. Then, in Section Two, this chapter will expand the ethical framework established in Chapter One by examining those ethical issues relevant to signals intelligence. By exploring these issues and applying them to different illustrative examples, it is possible in Section Three to outline the different levels of harm signals intelligence can cause. Finally, Section Four will apply the Just Intelligence Principles to better understand if and when these varying levels of harm are justified.

Section One: Signals and Data Intelligence

While signals intelligence is clearly information derived from the use of signals, not all signals are intelligence. Nor is all data related to the individual data intelligence. There is an important distinction between the haystack of everyday signals and data sets that permeate every aspect of the modern world and the needle of intelligence within it. This section will outline those aspects that mark a signal as intelligence and therefore distinguish signals intelligence as a collection discipline as well as outlining some of the activities being employed to collect and store important personal data. This section will argue that signals intelligence has the following four essential elements: the *signal* element; the *intentional act of observing by the operative*; the *security lens that is shaped by the intended goal*; and the feature that it is electronically *captured* in some way. Discussion of the activities employed by signals intelligence will follow. After investigating signals intelligence, this section will examine the growth of data intelligence, highlighting data-mining and dataveillance as two areas of study.

Signals

One of the most distinctive markers of signals intelligence is, unsurprisingly, the fact that it involves the interception, collection, utilisation or analysis of *signals*. In its most basic form, a signal is the transference of information from one point to another. The signal is the medium through which the information is carried. These signals will, in the majority of cases, be in the form of an electromagnetic wave – light, microwaves or radio waves for instance – for the simple reason that information technology has evolved in such a way as to be heavily reliant on this type of transmission. An example of this focus on the electromagnetic spectrum as being central to signals intelligence can be seen from the United States Marine Corps Manuel signals intelligence definition, "intelligence gained by exploiting the adversary's use of the *electromagnetic spectrum*".[1] As such, almost all modes of transferring data from one point to another will involve taking that data, turning it into some code and then transmitting that code via the electromagnetic spectrum. However, this does not mean that other forms of signals do not exist. Quite the opposite. One of the most common, and for intelligence operatives one of the most important, forms of signals that can be intercepted is sound signals. When individuals speak they are transferring information from one point, the

[1] United States Marine Corp 'Signals Intelligence' *Marine Corp War Fighting Publication* 2-15 (1999) p.1 Available at http://www.fas.org/irp/doddir/usmc/mcwp2-15-2.pdf Accessed 16th April 2008 Emphasis added.

speaker, to another point, the listener. The sound waves are the signal and, therefore in this instance, signals intelligence involves accessing and collecting information while it is in this form. A vast majority of modern signals intelligence relies heavily on the ability to intercept sound and electromagnetic waves in order to either analyse the signal itself and draw conclusions from its particular characteristics or to access the information within the signal and be able to determine what is being 'said'.

Intention

The chapter on imagery intelligence took care to mark the difference between passively seeing something and actively observing it, where the latter was distinguished from the former by virtue of the intention of the individual to actively look and collect information. Similarly for signals intelligence, there should be care to understand that there is a difference between hearing and listening when listening is for the explicit purpose of collecting information. Hearing happens all the time. It is, like seeing, almost impossible for an individual to stop hearing the constant audio stimulus of the world around him. However, if he is listening to collect information from those around him then he is intentionally taking in what is being said, paying heed to the actual words and collecting information which is not intended for him. Words are no longer coming and going, barely recognised and never logged, but are being heard, understood, processed and used. Again, what is important about this is that signals intelligence becomes a purposeful activity, engaged in by rational, moral agents. As it was argued in Chapter Two, this means that the harm that is caused by signals intelligence is the responsibility of the intelligence operatives that carry it out and by extension the organisation for which they work. Furthermore, this distinction outlines the difference between the accidental interception of a signal and the intentional monitoring carried out by intelligence agencies.

Security Lens

The third element that marks signals intelligence as something special is the security lens through which the information is viewed. This security lens is shaped by the desire to protect the political community, reacting to threats and risks a community faces, and determines what is intelligence and what is just information. There is something special about the type of information that is sought, how the information is viewed, and whether that information is then defined as intelligence. This is an important aspect of signals intelligence given the sheer

volume of signals that flow through the ether all the time. A select amount of this information is useful, while the majority of it is just 'noise'. For example, even though an intelligence agency might collect all signals traffic from the China Sea, and while it is information and signals in the purest sense, it is not all intelligence since the vast majority will be fishermen reporting on their catch and location. However, what is most important about this security lens is that it highlights the end for which the intelligence collection is intended, that is, the protection of the political community. By having the intended goal of the collection activity as the protection of the political community, it was argued in Chapter One and again in Chapter Two, the action is judged in a different way to those activities carried out by or for private goals because of the ethical good that the political community represents. This is an important distinction as it alters the type of ethical calculation that is made in regards to if and when signals intelligence is justified.

Technology and Capturing the Information

Finally, signals intelligence must be captured and processed through some technological means. Electromagnetic waves travel at the speed of $3x10^8$ m/s, and are literally gone almost as soon as they are sent. Human beings do not have the ability to directly access these fast moving signals. Signals intelligence is, therefore, only made possible by advances in physics and the ingenuity of human beings. The capturing process then turns the information, existing non-physically in the ether, into a tangible item that can be processed, evaluated, manipulated, and analysed in the hope of gaining intelligence from it. For example, pressing one's ear against a wall to hear the conversation of one's neighbours is not signals intelligence; whereas placing a bug on the premises, capturing it and recording is.

Signals Intelligence: Communications

While there are an assortment of different signals that are used in various different ways throughout the modern world, for the purpose of ethically evaluating the practice of signals intelligence this thesis will distinguish three main sub-categories.[2] These sub-categories of signals are: traffic analysis, electronic communication interception, and 'bugging', which involves putting a listening device in the vicinity of a conversation so as to capture it. Depending on the type of the collection, the target, method and aim can vary. This section

[2] These categories themselves are not necessarily exhaustive but represent the broadest and most utilised forms of signals intelligence. Furthermore, the distinctions themselves are not ethically relevant. Rather, the distinction is in order to help make evaluation easier by dividing activities along common lines.

will briefly outline what each of these actions involves and what activities they therefore perform.

Communication interception involves deriving intelligence from the interception and interpretation of a communication by someone other than the intended recipient. The form of the communication and the means of carrying out the communication can vary, including oral, radio, telephone, facsimile, or email. However, regardless of the different formats, the main point remains the same, that something is being communicated and that the intelligence operative is attempting to access the message so as to determine both what is being said and who is saying it.

'Wiretapping' is traditionally the term used as communication interception originally involved breaking into the electronic wire carrying the message and intercepting what was being communicated. Whitfield Diffe notes, however, that the term should not be taken too literally, "it is no longer restricted to communications travelling by wire… and the thing being tapped need no longer be a telephone call in the classic sense; it may be other forms of electronic communication, such as fax or data".[3] For messages travelling a short distance, the signal will often only travel down phone wires or through microwave telephone exchanges. If the telephone to be tapped is serviced by an old fashioned exchange, the engineer has to visit the exchange in person and make the adjustments, but with digital exchanges the telephone can now be intercepted from the telephone headquarters.

For transmissions over slightly larger distances or through mobile equipment, wireless transmissions are the norm. Alistair Harley, a former MI5 technical officer, argues it is actually easier to intercept the communication once it leaves the wires.[4] Microwaves networks are made up of chains of towers relaying message from hilltop to hilltop across the country, and therefore offer a good opportunity for signals interception. By physically standing between the two with an antenna an agent can intercept all messages being transmitted. For instance, electronic experts do not consider it coincidence that one of BT's biggest transmitters, called Hunter's Stone Tower, which relays hundreds of thousands of calls, was built just four miles from Menwith Hill, one of the biggest American-run signals intelligence bases located in the United Kingdom.[5]

---

[3] Diffie, W. and Landau, S. *Privacy On The Line: The Politics Of Wiretapping And Encryption* (Cambridge: MIT Press, 1998) p.151

[4] Keefe, P. R. *Chatter: Dispatches From The Secret World Of Global Eavesdropping* (New York: Random House, 2005) p.50

[5] Parker, J. *Total Surveillance: Investigating the Big Brother World of E-Spies, Eavesdroppers and CCTV* (London: Piatkus, 2000) p.121

For those messages that transverse continents or large distances, communication satellites are the main means of information transference. In 1945, Arthur C. Clarke, a science-fiction writer and inventor, published an article called *Extra-Terrestrial Relays* where he argued that three satellites positioned over each ocean region (Atlantic, Pacific and Indian) in geosynchronous orbit could provide communication for the whole earth.[6] Clarke's dream was realised with *Intelsat*, when in 1964, 1967 and 1969 saw the launch of three satellites into geosynchronous orbit designed to carry communications from each of the four corners of the world. In response to this leap in communication technology, American intelligence launched its own signals intelligence satellites, including geosynchronous satellites initially give the codename RHYOLITE in the early 1970s and JUMPSEAT, first one launched in 1971, which was able to 'hover' over the Soviet Union for eight to nine hours at a time by maintaining a highly elliptical orbit. in 1968 and a series of others called JUMPSEAT and TRUMPET over the next few decades. These satellites were designed to intercept the communication as it was being sent across continents as it detoured via outer space.[7]

The last method used, designed for long-distances or intercontinental communications, is fibre optics. Fibre optics have the benefit of being able to carry a far greater information load compared to satellites and once the initial payout of laying them is covered they are relatively cheap to maintain. The fibre optic system works by laying cables between countries along which information is then relayed.[8] The problem for intelligence agencies is that in order to access the information within the fibre optic cable they must first find the cable and second break into it without the owner noticing.[9] If they are able to achieve this, the amount of information available is great in quantity given that this is increasingly becoming the main means of inter-continental communication.

Traffic analysis, in comparison to wiretapping, does not actually involve accessing the message within the communication, but rather focuses on characteristics of the message itself, like who is talking to whom, how often and for how long. By doing this it is possible to draw conclusions about relationship networks and even any imminent operations. The two main activities that enable traffic analysis are called 'pen registering' and 'track and trace'. The pen register is a detailed list of all the numbers a particular phone has rung. In

[6] Clarke, A. C. 'Extra-Terrestrial Relays: Can Rocket Stations Give World-Wide Radio Coverage' *Wireless World* (October, 1945) pp.305-308
[7] Richelson, J. T. *The US Intelligence Community* (Boulder, Colo.: Westview Press, 1999) p.177, 179. For a list of American satellites, their launch dates and their optical capabilities see Graham, T. and Hansen, K. *Spy Satellites and Other Intelligence Technologies that Changed History* (London: University of Washington Press, 2007) p.136
[8] Richelson, J. T. and Ball, D. *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries* (Boston: Allen & Unwin, 1985) p.176
[9] Keefe, P. R. Chatter (2005) p.73

comparison, a track and trace is the inverse of this, taking note of the phones that called a particular number.[10] Of all the communication intelligence collection activities, traffic analysis is one of the easiest forms of information gathering. This is because the logging of these details is actually built into the telephone system itself. A pen register is that component of the telecommunication system that makes itemised billing possible, as each number called, when the call was made, for how long and to whom, is all recorded for the benefit of the bill payer. Similarly, track and trace was made possible by virtue of the individual's need for 'caller ID', whereby who is calling one is made known before one picks up the receiver.[11]

While bugging is similar to the wiretapping in that it involves capturing a set of conversations, it is different in that it involves recording conversations spoken by people in the immediate room and not technologically confined or enabled. In order to intercept these conversations, a device with a microphone is secreted away where important conversations might occur, the bug then picks any ensuing conversation, record them and transmits the recording back to an intelligence officer. The main challenge for effective bugging is gaining access to the right room where the right people are talking about the right topic and placing the bug somewhere it will not be detected. During the Cold War both sides had hundreds of engineers and craftsmen trying to fit microphones and transmitters in a wide range of items, from "kitchen cutting boards to felt-tip pens, oil filters, video cassettes, tool boxes, toy trains, batteries, cigarette lighters, teddy bears, chess sets, paintings, wallets, statues and toilets".[12] If access to the room is not gained, then a 'constant microphone' can be used, whereby a laser or similar device is trained onto the windows and is sensitive enough to detect the vibrations made by the sounds from within the room.[13]

Data Intelligence: Data-Mining & Dataveillance

Edward Forster, in his short story *The Machine Stops,* describes a world where almost every activity performed is aided in some way by a vast computerised system known simply as The Machine: "The Machine feeds us and clothes us and houses us; through it we speak to one another, through it we see one another, in it we have our being; The Machine is omnipotent, eternal; blessed is The Machine".[14] Over the last two decades, the role and pervasiveness of computers and the Internet has exploded in ways unimagined and has resulted in a world with

[10] Diffie, W. and Landau, S. *Privacy On The Line* (1998) p.117
[11] Diffie, W. and Landau, S. *Privacy On The Line* (1998) p.117
[12] Kessler, R. *The CIA at War: Inside the Secret Campaign Against Terror* (New York: St. Martin's Press, 2003) p.73
[13] Todd, R. W. 'Electronics and the Invasion of Privacy' in *Privacy* edited by Young, J. B. (1978) p.312
[14] Forster, E. M. *The Machine Stops* (DodoPress, 1909) p.26

eerie similarities to that described by Forster. "Over the last 15 years the Internet has developed from a specialist network of academic researchers into a mainstream communications mechanism".[15] The advent of both the modern computer and the Internet has revolutionised how people carry out their lives to such an extent that it is nearly impossible for many to function without coming into contact with a computerised system of some form. However, with every new piece of technology there is also a new set of threats that goes with it. For example, David Wall argues that the growth of the Internet has just facilitated the extension of existing criminal activities: drug dealers can now organise, push and sell their wares via emails, as well as enabling paedophiles the ability to both communicate their undesirable practices as well as target their victims.[16] Other actors, notably terrorist groups like Hezbollah, have taken to using the Internet in order to further their aims: "email and web discussions have been used to plan operations, while websites are commonly used to bypass media editorial controls and communicate directly with groups' supporters and potential recruits".[17] Furthermore, recent scientific developments have provided new sources of intelligence as well as new ways of storing and sharing information. Most notable is the advancement in DNA profiling, where an individual's identity and even previous locations can be determined by the genetic code they leave behind.

The task that faces the intelligence operative is how best to utilise this computer revolution to first help fight existing threats and second to tackle the new computer-based crimes finding ground. This has lead to the development of two important computer-based practices. The first is called 'data-mining', which involves collecting and collating an individual's personal information onto a single data store. This can include a variety of different sets of information that cover almost every aspect of an individual. Data-mining accesses and cross-references these different information stores in the hope of drawing conclusions about the individual. For example, financial accounts, medical records, fingerprints or DNA samples are all types of personal information that are collected, digitalised and stored so that they can be used to draw a profile of an individual when necessary. The second computer-based intelligence development is called 'dataveillance' and involves monitoring the 'electronic footprint' inevitably left behind by the individual when his activities interact with a computerised system. Many actions an individual performs in both the real and cyber-world create a digital footprint, recording time, place and action.

---

[15] Brown, I. and Karff, D. 'Terrorism and the Proportionality of Internet Surveillance' *European Journal of Criminology* Vol.6 No.2 (2009) p.119

[16] Wall, D. 'Policing the Internet: Maintaining Law and Order on the Cyberbeat' in *The Internet, Law and Society* edited by Akdeniz, Y., Walker, C. and Wall, D. (Harlow: Longman, 2000) p.156

[17] Brown, I. and Karff, D. 'Terrorism and the Proportionality' (2009) p.120

Intelligence operatives believe that by collecting all the different bits of personal information and turning them into what David Solove calls a "digital dossier" it is possible to gain an insight into both the individual's past as well future activities. These digital dossiers can be analysed in the hope of "discovering meaningful patterns in the data", the goal of which is the "extraction of meaningful intelligence, or knowledge, from the patterns that emerge within the database".[18] Both these intelligence activities rely heavily on signals to collect and monitor people's information, as well as the ability to store, cross-reference, and process this information. Without the vast storage capacity of computers and the abilities offered by networks and the Internet, such activities would be impossible. For example, if intelligence agencies are to combat threats like online fraud, online sexual offenders, or even online terrorists, they must be able to track people's activities within the digital realm. Furthermore, if they are to locate suspects then they need databases of information so that they can make full identifications from a relatively small original data set.

Conclusion

Forster's *The Machine* depicted a world where every activity is influenced, mediated, aided and even controlled by technology, and for our modern world there are striking similarities. Indeed, technology and science have come to define what it means to live in the modern world. No actor – state, organisation or individual – can avoid becoming increasingly dependent on or even a slave to it. What this means for intelligence is that if it is to be able to both face the new threats that technological revolutions bring as well being capable of facing existing threats as they become scientifically accomplished they too must master this modern medium. This section demonstrates the techniques associated with signals intelligence as a means of collecting and monitoring all information which is transmitted. It also discusses the growth of the information nation and the important role that data intelligence can have as a result of its ability to collect, digitalise, and evaluate raw data and turn it into intelligence. However, while the use of signals and data intelligence can both be vital tools for the intelligence community, they can cause harm by coming into conflict with an individual's privacy and autonomy. The next section will investigate these concerns by furthering the work already done in Chapters One and Two.

[18] Oscar. G. 'Data Mining and Surveillance in the Post 9/11 Environment' in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* edited by Bell, K. and Webster, F. (2003) p.28

Section Two: Privacy and Personal Control

The previous section outlined the types of activity required by signals and data intelligence to intercept, collect and utilise information as it is being transmitted or stored. However, Paul Fairfield argues that "in the present age of science-technology and the dawning of the age of information, the impression is growing that privacy is under threat in ways wholly unlike those in former years".[19] Indeed, it seems that with the advancement of technology there is almost always advancement in the misery that can be caused. Alan Westin argued that even though the invention of the phone and the microphone represented important innovations in how individuals can communicate, they also meant that "now informal and tentative conversations are vulnerable to being overheard and recorded by third parties".[20] As personal information is increasingly digitalised, transmitted and stored via an array of different signals, there is the increased fear that this information will be taken out of one's sight and out of one's control.

In Chapter One it was made clear the importance privacy played in the individual's life. Chapter One argued that privacy can be represented in terms of the ability to maintain varying spheres of privacy as well as the ability to maintain control over personal information. Chapter Two then furthered this understanding by exploring various spheres of privacy associated with imagery intelligence and the degree to which the individual can control who has access to his image. This chapter will build upon this work by outlining other forms that personal information can take and the degree of privacy associated with them. By better understanding the concept of personal information in this way it is possible to comprehend the way and the degree to which signals intelligence can cause harm.

Privacy as Control

Privacy as control is based on the argument that, one's actions and their history 'belong' to the individual that generated them and is to be viewed only with those with whom one wishes to share them.[21] Claim of ownership does not stop at the physical body, but extends to information that is connected to the individual in a significant way. Both Chapter One and Chapter Two explored the argument that an individual's personal information acts in the same way as other property rights. It was argued that the individual can sell the right to his information or he may invite someone to use it, but if he decides that he no longer wishes for

[19] Fairfield, P. *Public/Private* (London: Rowman & Littlefield Publishers, 2005) p.1
[20] Westin, A. *Privacy and Freedom* (New York: Atheneum, 1967) p.338-339
[21] Shils, E. 'Privacy: Its Constitution and Vicissitudes' *Law and Contemporary Problems* Vol.31 No.2 (1966) p.290

others to use it then they violate his right if they continue to do so. Collecting or utilising an individual's personal information without prior consent violates the interest in privacy and therefore causes harm. However, the type of information referred to in Chapter Two related very much to the individual's image. This chapter focuses, in comparison, on information that is connected to the individual either by it being descriptive of him or because he has authored it.

Authorship

Those things which are created by an individual are each, through that individual's innovation and actions, his property. To violate this claim by intercepting or utilising the created information means violating the individual's privacy. This notion of authorship is not unheard of in the wider literature. John Locke asserted that individuals have property rights over those things that are the fruits of their labour: "Whatsoever he removes out of the state that nature hath provided, and left it in, he hath mixed his labour with, and joined it to something that is his own, and thereby makes it his property".[22] By virtue of the efforts of the individual, he has created something out of himself and since it is a part of him, he claims certain rights to it. The individual makes these claims not only to physical items created by him, but to other non-material creations as well, the words out of his mouth for instance. James Boyle calls this the notion of the "romantic author", whereby the individual who mixes his unique personality with ideas, who displays originality and novelty in his creation, and fixes them in some medium, produces something that is automatically and intrinsically his.[23] For example "a telephone conversation, personal diary, love letter, or email"[24] are owned by the individual by virtue of his creating them.

Descriptive Information: Control of Information Pertaining to the Self

Information pertaining to the self is personal information because it is connected to the individual by virtue of it being information *about* the individual, broadly understood as 'descriptive information'. This is essentially information that describes the individual in some way, either as a feature of the individual - who he is, what he is and where he is – or as a description of the individual's transactions. For example, an individual's features can, firstly, refer to characteristics including biological, biographical, and sociological data. Biological

[22] Locke, J. *Second Treatise of Government: and, A Letter Concerning Toleration* by Laslett, P. (Cambridge: Cambridge University Press, 1960) p.306
[23] Boyle, J. *Shamans, Software and Spleens: Law and the Construction of the Information Society* (Cambridge, Mass.; London : Harvard University Press, 1997) p.54
[24] Kang, J. 'Information Privacy in Cyberspace Transactions' *Stanford Law Review* Vol.50 No.4 (1998) p.1207

data might include biometric data, sex, height, weight, blood type, fingerprint, DNA or retina scans; whereas biographical data is someone's date of birth, marital status, sexual orientation, ethnicity or national origin, criminal record or educational status; and finally, social information including relationships, friendships, and religious and political affiliations. Even though the individual did not create this information per se, he owns it because it is an extension of his own body. This is essentially the argument made in Chapter Two, that the individual owns his own image because it is an outward extension of him.

Descriptive information can also include data that is created as the by-product of an individual's actions. When an individual performs an act, it will often create ripples in the world. These ripples can then be intercepted and analysed and by doing so the action that created the ripples can be determined. For example, a by-product of an individual going to the shop and buying items would be the electronic report created outlining what it is he bought and the bank account used to pay for it. This information is owned by the individual because it is both authored by him – through the action of buying food – as well as being descriptive of certain facts about him, his bank account and items bought. While this type of information might not have been of much concern a few decades ago, given the explosion of the Internet, cyberspace and computerised mass collection and processing capabilities, it has become an increasingly important aspect of information ownership. As the information highways overflow with information about an individual's activities, the ability to control this information has become an increasing concern. By collecting this information, cross-referencing it into a searchable database and then comparing it against previously outlined profiles, it is possible to create a veritable "crystal ball" which can be used to both understand the individual and predict his intentions.[25]

Privacy as Boundaries

As previously argued, at the heart of privacy is the belief that there are realms that are separated off from the rest of society, and interference within these realms is prohibited. Chapter One argued that private spaces are those realms erected as the result of some physical or socially constructed barrier, placing the private sphere on one side and the rest of society on the other. Chapter Two explored this notion further by examining those barriers that go into creating some of the most protected spheres. The concern for signals and data intelligence is that these boundaries can now be transcended with increasing ease. Wiretapping, bugging and Internet monitoring can all probe more deeply, widely and softly

[25] Keefe, P. R. *Chatter* (2005) p.99

than traditional methods, transcending barriers that have historically made personal information inaccessible. Gary Marx argues that, "boundaries that have defined and given integrity to social systems, groups and the self are increasingly permeable and prone to outside interference".[26] As such, in addition to the boundaries discussed in the Chapter Two – namely the importance of the home as a protected sphere – it can be argued that for many electronic communications there exists a sphere of privacy around the signal itself that has a strong expectation, both legally and socially[27], which dictates that the individual is 'in' private. This boundary is supported and demarcated by the clear distinction between the 'inside' of the communication where the message exists and the 'outside' where the rest of society exists.[28]

Degrees of Privacy

This is not to argue, however, that all information that describes the individual is his and his alone. Tom Gerety claims that making privacy *all* control over *all* information about oneself, one's group and one's institutions is wrong, for "surely privacy, in law as in life, should come to much less than this".[29] And, indeed, this is true. However, it is possible to understand certain types of information as being connected to the individual in a significant way and as a result demanding a level of protection. Chapter Two argued that there are different levels of privacy associated with information. Similarly, it can also be argued that descriptive and authored information can also be judged to consist of different levels of privacy. Chapter Two noted that this difference was based on the degree the information was perceived as being 'intimate' or 'personal' to the individual. That is, depending on the degree to which the

[26] Marx, G. 'Ethics for the New Surveillance' *The Information Society* Vol.14 No.3 (1998) p.171

[27] For example, in America the *Electronic Communications Privacy Act of 1986* (ECPA) was enacted to extend government restrictions on wiretaps on telephone calls and transmissions of electronic data by computer. Specifically, ECPA was an amendment to Title III of the *Omnibus Crime Control and Safe Streets Act of 1968*, which was primarily designed to prevent unauthorized government access to private electronic communications. Later, the ECPA was amended, and weakened to some extent, by some provisions of the US *Patriot Act 2001*. In addition, Section 2709 of the Act, which allowed the FBI to issue orders to Internet service providers (ISPs) demanding them to disclose records about their customers, was ruled unconstitutional under the First Amendments in ACLU v. Ashcroft (2004). In Europe, the *European Convention on Human Rights* protects these forms of communications under *Article 8 Privacy* providing a right to respect for an individual's "private and family life, his home and his *correspondence*" [Emphasis added]. This is equally reflected in the *United Nations Declaration of Human Rights Article 12 Privacy* which dictates that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence".

[28] This inside/outside distinction is still valid despite the advent of wireless technology and cyberspace communications such as emails since even though there might not be the physical wire to 'cut-into', there is still a data-stream, a signal or some notion of the communication having an inside to which only certain individuals are allowed access and an outside where the rest of the world exists. Furthermore, there is still an established understanding that even though it could be thought that communications are 'in the air' they are still 'private' communications between specific individuals.

[29] Gerety, T. 'Redefining Privacy' *Harvard Civil Rights-Civil Liberties Law Review* Vol.12 (1977) p.263

information reveals the individual's personal identity the level of privacy afforded alters. As a result, those signal collection activities that collect highly personal information are more harmful than those that collect less personal information. Highly personal information is demonstrated by it being either revealing of an individual's intimate core or because it is information the individual has demonstrated in some way that is off limits to others. Similarly, depending on the type of boundary placed around the information, the level of privacy it is afforded can be changed.

Additional Harms: The Panoptic Gaze and Social Cohesion

In Chapter One it was argued that the use of intelligence can cause damage to both society and other individuals not directly targeted quite separately from, and in addition to, the harm done to the target. This additional damage is important because it should then be taken into account by the proportionality calculation carried out in Section Four. These damages might not always accompany the initial harm, but it is because of the initial violation of an individual's vital interest that these additional damages can come about.

As discussed in Chapter Two, one concern associated with surveillance is the effect of the Panoptic Gaze on the individual's autonomy. It was argued that people alter their behaviour when they think they are being watched, often in order to comply with what they think their watchers want from them. Their autonomy is affected as they begin to self-discipline or condition their actions. Moreover, when the surveillance is asymmetric and widespread or ubiquitous people begin to self-discipline their actions even when they are not being watched as they must assume that they are always being watched. Similar to the argument made in Chapter Two in relation to CCTV cameras, people will alter their behaviour if they think their communications, words or personal data is being monitored. In comparison to the use of CCTV cameras, however, it can be argued that the effect of the Panoptic Gaze is likely to be stronger since the greater the level of privacy the individual assumes he is in the greater the affect on his autonomy is likely to be if he thinks it is being violated. Therefore, surveillance through monitoring an individual's communications or by accessing his personal information is likely to have a detrimental effect on his autonomy.

Another concern for signals intelligence is the capacity to collect large amounts of information from an increasing number of people to be stored for long periods of time. Another concern is the effect ubiquitous collection methods can have on the society's cohesion. It was noted in Chapter Two that activities that discriminate on racial, social, ethnic, financial or superficial grounds are likely to cause individuals from that group to feel

excluded from society. This can have repercussions that then cause a breakdown between both the different sectors of society as well as between these groups and the state's own institutions. This can affect the autonomy of those individuals from the discriminated groups as they alter their behaviour so as to be more acceptable to the authority.

This concern becomes acute with respect to the practice of data collection and the use of profiles to highlight various groups as more or less threatening, and thus creating a wedge between them and the rest of society. It can be argued that the development of profiles so as to guide the collection of intelligence can have repercussions on both the individual targeted and the rest of society or his social group. There are those that believe that through the use of facts like race, religion, gender and class it is possible to create predictive models. They argue that because of the relatively high correlation between personal attributes it is a fairly cheap and easy way of predicting an individual's or a group's behaviour.[30] However, profiling bestows the individual and his social subgroups with a particular label. Those that fall under this label are then treated as the label dictates rather than as the individuals they are. Spiros Simitis explains that a profiled individual is "necessarily labelled and henceforth seen as a member of a group, the peculiar features of which are assumed to constitute personal characteristics".[31] Individuals are therefore treated according to a stereotype rather than any actions that they might have done. This label can then close options to the individual that would have otherwise been open. Furthermore, labelling people can cause a tendency to create self-fulfilling prophecies. That is, when individuals are treated in a certain way or feel there are certain expectations of them, there is a pressure placed on them to act accordingly.[32] Such activities can then affect their autonomy because if they feel that they are likely to be marginalised or victimised this then forces them to act differently. For example, Oscar Gandy fears both of these problems have already come to pass for African-Americans where the use of race as a bar to employment has lead to a belief amongst the group that investment in education makes little sense.[33]

---

[30] Hausman, D. and McPhereson, M. *Economic Analysis and Moral Philosophy* (Cambridge: Cambridge University Press, 1996)

[31] Simitis, S. 'Reviewing Privacy in an Information Age' *University of Pennsylvania Law Review* Vol.35 No.3 (1987) p.719

[32] Robert Merton argues that "in the beginning, a *false* definition of the situation evokes a new behaviour which then makes the original false conception come 'true'. This specious validity of the self-fulfilling prophecy perpetuates a reign of error. For the prophet will cite the actual course of events as proof that he was right from the very beginning". That is, people react not only to the situations they are in, but also to the way they perceive the situations and to the meaning they assign to these perceptions. Merton, R. *Social Theory and Social Structure* (New York: Free Press, 1968) p.477

[33] For more on racial profiling and the harms it creates see Harris, D. A. 'Driving While Black and Other Traffic Offences: The Supreme Court and Pretextual Traffic Stops' *The Journal of Criminal Law and Criminology* Vol.87 (1999) pp.544-582; Kennedy, R. *Race Crime and the Law* (New York: Patheon, 1997); Lever, A. 'Why Racial Profiling is Hard to Justify: A Response to Risse and Zeckhauser' *Philosophy and Public Affairs* Vol.33

Conclusion

Privacy, it has been demonstrated, can be affected by signals intelligence in a slightly different way to those discussed in the previous chapter on imagery intelligence. The main concern for imagery intelligence is related to questions regarding the various spheres of privacy and the individual's claim to his image, for signals intelligence the focus is on the different forms in which personal information can exist and the level of control the individual can exercise over it. In this section it was argued that privacy can be understood as the ability to control two different forms of information, that is, information which is authored by the individual and that which is descriptive of the individual and his actions. Furthermore, this section has also highlighted how these types of information can be connected to the individual depending on how personal or intimate they are, and as a result can be afforded different degrees of privacy. By using this information and applying it to a set of illustrative examples, the next section will outline the various ways in which signals intelligence can violate an individual's privacy and autonomy and therefore cause them various levels of harm.

No.1 pp.94-110; and Robinson, M. 'The Construction and Reinforcement of the Myth of Race Crime' *Journal of Contemporary Criminal Justice* Vol.16 (2000) pp.133-156

Section Three: Illustrative Examples

In the first part of this chapter it was demonstrated that there is a range of different formats that information can be transmitted and stored in and that for each of them it is the duty of signals intelligence to find a way of accessing and collecting the information. Furthermore, it was also argued that new technologies have opened up various means of collecting, utilising and storing an individual's personal data. This chapter also noted that by accessing this information, given that it is often the property of someone else, signals and data intelligence can come into conflict with another's privacy. By applying the ethical framework, established in Chapter One and then furthered in Section Two of this chapter, to a series of different signals intelligence illustrative examples this section will examine the varying levels of harm that signals intelligence can cause as a result of this conflict. Once the level of harm is established it will then be possible in the next section to incorporate the Just Intelligence Principles and determine if and when these harms are permissible.

Communications Intelligence: Traffic Analysis

One of the first tools available to communication intelligence is called 'traffic analysis' and is used to "derive useful information from fluctuations in the volume and other external characteristics of the communication, even when the content of the message cannot be understood".[34] Every communication has a 'header' of information designed to inform the system where it is to be sent and who has sent it. From these headers, traffic analysis provides the intelligence officer with a list of who a particular individual is in contact with and who is in contact with said individual. By monitoring a communication signal itself, rather than the message held within, conclusions can be drawn without having to actually decipher or 'break' into the message. For example, if an army headquarters and its subordinate command posts exchange an unusually large number of messages an analyst might conclude that an important operation was about to take place. For example, Peter Wright, a former MI5 official, writes that by analysing the radio activity of British intelligence, Soviet intelligence could know when British counter-intelligence operations were underway and whether one of their own operations might be in jeopardy.[35] Furthermore, analysing communication traffic can provide information on a target's location, relationships and connections, possible upcoming events, and even an organisation's hierarchy. For example, traffic analysis was vital in an British

[34] Shulsky, A. N. *Silent Warfare: Understanding the World of Intelligence* (Washington, D.C.: Brassey's, 2002) p.26
[35] Wright, P. and Greengrass, P. *Spycatcher: The Candid Autobiography Of A Senior Intelligence Officer* (New York: Viking, 1987) p.52-53

operation that led to the discovery of a stash of illegal drugs worth £19 million in a Dutch registered car. By using a mobile phone from a 'low grade' drug dealer, British intelligence was able to analyse who the dealer had been in contact with and from this conclusions about the entire network could be made.[36] As a result of the important role that traffic analysis can play, in 2009 the British government proposed a Bill that would create a database to collect and retain the traffic information for the various forms of electronic communication. The *Communications Data Bill* proposed would track all emails and phone calls, detailing the times, dates, durations and location of the calls, numbers called, and emails sent. Information was to be stored for two years within a centrally searchable database.[37]

Level of Harm: The Privacy of Relationships

By collecting information on whom an individual is in communication with, traffic analysis violates the individual's privacy. In Section Two it was argued that private information was information authored or descriptive of some intimate or personal aspect of the individual. In the case of traffic analysis it can be argued that information regarding who an individual has been in contact with is private since this type of information relates to his relationships, something that falls under the category of 'personal information'.

Given that this type is not superficial information, but refers to a personal aspect of the individual's life, the level of harm caused features at Level Two on the Ladder of Escalation. In reference to the levels of intimacy outlined in Chapter Two it is clear that information regarding who an individual talks to, when he talks to them and for how long is information that features at middle level. There indeed might be more personal types of information but it is still a level above those superficial data sets such as those shown on a regular basis to the outside world. In relation to intensive surveillance, another Level Two harm explored in Chapter Two, the level of harm is similar even though if it is of a slightly different quality. While the privacy of intensive surveillance was mediated by the target moving out in the public realm, it was argued that he still maintained the right not to be stalked or to have his personal relations monitored in this fashion. Similarly, in regards to traffic analysis, the individual maintains the right to not have his personal relations monitored in this way.

---

[36] Home Office *Protecting the Public in a Changing Communications Environment* April 2009 p.9 Available at http://www.parliament.uk/deposits/depositedpapers/2009/DEP2009-2754.pdf. Referred to as the 'Dutch drug case' hereafter.

[37] BBC News 'Giant Database Plan Orwellian' October 15th 2008. Available at http://news.bbc.co.uk/1/hi/uk_politics/7671046.stm Accessed 1st November 2008. Referred to as the 'Communications Data Bill' hereafter.

Wiretapping

Technologically aided communication is and will continue to be a central part of modern day life, whether talking over the phone, writing an email or sending a fax, to people close or people far, chatting idly or outlining important plans. Regardless of the different things that can be said, communication is central to how both individuals and states carry out their lives. For intelligence agencies, however, being able to access what others say can be a vital resource in locating and preventing many threats. Mark Lowenthal argues communication intelligence "gives insight into what is being said, planned and even considered" by one's friends and enemies alike. For Lowenthal, this is as close as one can come, from a distance, to reading another side's mind.[38] Therefore, despite the piety of Secretary Henry Lewis Stimson, who, on becoming Secretary of State for President Hoover in 1929, claimed that 'Gentlemen do no read each other's mail', communications intelligence over the last century has continued ahead full force.

For military operations, being able to intercept a communication is a vital tool. Intercepting communications between command bases and subordinate actors can provide a huge tactical advantage and the chance to scupper any planned attack. For example, during the Second World War, under the rubrics of Ultra and Magic, vast amounts of accurate and timely information were made available to the British and American political and military leaders.[39] In international diplomatic relations, targets can include various state organs and institutions, military officers, ambassadors, bureaucrats or anyone who can give an insight into another state's operations and opinions. For instance, American intelligence focuses on communications between the Chinese Ministry of Defence and subordinate ministries, Russian military units, the President of Egypt and his subordinates, and Israeli officials and representatives on the West Bank.[40] This is just a small snapshot of the extensive communications network employed by a state such as the United States, but it should be clear the type of targets and concerns it can have. Military and diplomatic wiretaps allow for an unparalleled view of the opponents hand and allow an opportunity to prepare for any surprise.

Furthermore, monitoring communications of one's own people is well documented. During the Cold War, both the West and the Soviets would use wiretaps on their own populace as much as they did the other side's diplomats and military. For example, in the United Kingdom in the 1960s and 1970s, constant targets for wiretaps included union members and individuals showing socialist leanings, especially as the fear of Soviet influence

[38] Lowenthal, M. *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003) p.65
[39] Shulsky, A. N. *Silent Warfare* (2002) p.25
[40] Richelson, J. T. *The US Intelligence Community* (1999) p.181

grew stronger: "whenever a major dispute came up – at Ford's, in the mines or the Post Office – immediately it would be a major area for investigation".[41] Similarly, in America the so-called 'Huston Plan' called for various agencies of government, including the NSA, CIA, FBI, and military intelligence agencies, to conduct wide-ranging wiretaps targeted toward dissident groups and individuals. For example, Operation SHAMROCK, effective from August 1945-1975, routinely intercepted international telegrams sent to or from America.[42] One of the most infamous American cases of domestic wiretapping was that of Martin Luther King Jr. For a number of years the FBI had been investigating King's alleged ties to the Communist party. John Edgar Hoover, first Director of the FBI, had made it clear that he saw King as a serious threat to the security of the country and was determined to find evidence of his communist connections. As a result, wiretaps were put on any and all the phones that King might use as he travelled around the country. This activity continued unabated until 1969, during which no evidence of communist connection came to light.

The importance of wiretaps has also continued into the twenty-first century. Regardless of whether the communication is travelling a long or short distance, there are a set number of ways for it to travel. What this means is that all actors – be them state, terrorist or criminal – must use the same information highways. For signals and data intelligence, by gaining access to these highways means that they have access to the communications of those actors. Furthermore, in the current digital age the task of tapping a target's wire has never been easier. For example, the British telephone company, BT, has the capability referred to as System X to tap phones without physically interfering with individual lines or switchboards.[43]; and the MI5 telephone operation, TINKERBELL, employs British Telecom 'secret squirrels' that operate from the 9th floor of the BT Gresham Street headquarters and taps an estimated 35,000 lines.[44]

Level of Harm: The Privacy of Communications

Tapping an individual's lines of communication violates the interest he has in privacy by, first, intercepting and utilising information he has authored and, second, by violating a sphere where there is a strong expectation that he is in private. An individual has the right to control

[41] Cathy Massiter quoted from Hollingsworth, M. And Fielding, N. *Defending the Realm: MI5 and the Shayler Affair* (London: André Deutsch, 1999) p.76
[42] Morgan, R. E. *Domestic Intelligence: Monitoring Dissent in America* (Austin: University of Texas Press, 1980) p.75
[43] Hollingsworth, M. And Fielding, N. *Defending the Realm* (1999) p.74
[44] Dorril, S. *The Silent Conspiracy: Inside the Intelligence Services in the 1990s* (London: Mandarin, 1994) p.151

who has access to his words by virtue of him being the creator of those words.[45] Furthermore, even though the wire or wireless signal used to carry the communication leaves the individual's private property, and therefore leaves the normal expected sphere of privacy, there is still an understanding that the wire itself is a sphere of privacy. Robert Hallborg argues that private spaces are those "constructed in such a way as to prevent the public from being able to observe... quite casually and with little effort, what is transpiring therein".[46] For communications and signals, regardless of whether the medium through which the signal is being carried is wired or wireless, there is still a clear distinction between the 'inside' where the communication exists and the 'outside', where everything else exists. There is a clear boundary the intelligence agencies must physically cross – the act of tapping the wire or breaking into the signal – if they are to gain access to the message inside. There is also an established and long held expectation that one's communications are considered private and therefore should be immune from outside interference.

The importance of the private sphere and the level of personal information associated with a is significantly high. Given that "interactions are invariably governed in one fashion by pre-understandings regarding personal boundaries and personal space",[47] and since communicating by phone calls or email has, in many ways, become central to how individuals act out their private lives, there has developed an expectation that communications between two parties have the potential to be highly private. That is, the sphere of privacy associated with telephone communications has developed in such a way that individuals carry out highly personal parts of their life through them and, as such, expect a high degree of protection to be afforded to this particular realm.

Furthermore, even though wiretapping as an activity is generally localised to a single individual or property, if it were to be used ubiquitously or on a specific social group then the level of harm caused would increase. This is the result of the affect the Panoptic gaze can have on both the individual and society as a whole. As mentioned in the previous chapter, people alter their behaviour when they think they are being monitored so as to conform to what they think their listeners want. George Orwell, in his dystopia *Nineteen Eighty* Four, gave the extreme example:

[45] Obviously this is within reason. If an individual is talking within a public realm and has acted so others overhear, then they are not necessarily responsible for overhearing the words. However, such accidental overhearing is not really an issue in the type of cases being discussed here.
[46] Hallborg, R. 'Principles of Liberty and the Right to Privacy' *Law and Philosophy* Vol.5 No.2 (1986) p.179
[47] Fairfield, P. *Public/Private* (2005) p.15

> How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they would plug into your wire whenever they wanted to. You had to live in the assumption that every sound you made was overheard, and every movement scrutinised.[48]

Even if an individual is not actually being listened to directly, the fear that he might be means that he self-disciplines his actions. That is, he alters his decision-making process so that his actions fit what he perceives are wishes of his watchers and in doing so they violate his autonomy. With ubiquitous monitoring it can be argued that the individual is more likely to believe that he is being monitored at any given moment and is therefore is more likely to alter his behaviour. In comparison to the previous chapter where the Panoptic gaze was discussed in regards to CCTV cameras, it can be argued that ubiquitous monitoring of an individual's private conversations will affect his autonomy to as greater degree. This is because the level of privacy expected with telephone conversations is greater in comparison to CCTV monitoring. The greater the expectation of privacy there is the greater the affect the fear of being monitored will have on an individual's actions and therefore his autonomy. Furthermore, ubiquitous monitoring in this way can cause a breakdown in social cohesion as groups begin to feel victimised against as a result of their social associations. As mentioned in the previous section, a breakdown in social cohesion can cause additional harm as individuals alters their behaviour to become more 'acceptable', or because they fall into self-fulfilling prophecy behaviour, or as a result of the breakdown in trust between them and other social groups or the state in general.

In conclusion, regardless of the many forms of communication that now exist, there is an understanding that they all exert a sphere of privacy. There is a clear boundary demarcating this sphere and the need to physically break into someone's wire is indicative of this. The information transmitted between individuals while communicating in this manner is socially and legally understood to exist within an established sphere of privacy and therefore there is an expectation that they will not be overheard. This means that wire tapping features at Level Three on the Ladder of Escalation. Furthermore, if targeted wiretapping causes a Level Three harm and given that widespread, blanket or ubiquitous use of telephone tapping can cause additional harms as a result of the affect it can have on a society, *en mass* wiretapping will feature at Level Four on the Ladder of Escalation.

[48] Orwell, G. *Nineteen Eighty Four* (Penguin Books, 1987) p.5

Bugging

The last of the three communication collection activities explored in this thesis is the use of electronic listening devices known as 'bugs', which listen, record and transmit the conversation of people as they are talking to each other face to face. In 1952 the American ambassador, George Kennan, ordered a thorough search of his Moscow office when he took the post: "one of the experts suddenly began hacking away at the wall behind a wooden replica of the Great Seal of the United State. Finding nothing in the wall he then attacks the seal itself and triumphantly extracted a pencil shaped listening device".[49] Furthermore, Christopher Andrew notes how one of the greatest counter-intelligence successes by Soviet intelligence was achieved by an agent called Zolushka (CINDERELLA) who was able to successfully plant a listening device in the office of Ambassador Sir Derek Riches as well as another one behind the desk of SIS Chief of Station Peter Lunn in the late 1960s at the station in the Middle East. This bug, RUBIN, was used to identify over 50 British agents in the Middle East and Europe: "of greatest interest is the identification of an SIS group consisting of a courier and two agents in the highest government circles in Iraq".[50]

Domestically, bugs are used by both the security services to detect and prevent terrorists as well as by police forces to combat crimes, especially in the fight against drugs. These operations will often involve breaking into the target's property in order to plant the device or drilling through a neighbouring property's wall. According to former MI5 officers, breaking into a property was "absolutely routine" and it was not just private homes, "they'll do offices; they'll do banks; no holds barred, it didn't matter".[51] The use of bugs has most recently been targeted towards the prevention and capture of terrorists. In February 1999 Dame Stella Rimington, former Director-General of MI5, said that all intelligence agencies should have the legal power to break into people's homes to obtain information on terrorism: "without the power to enter, to eavesdrop and to search, you can't be an effective security service".[52]

The Level of Harm: The Privacy of Conversation

It was argued in the previous chapter on imagery intelligence, that there is a long and well established precedent that one of the most important private spheres is the individual's home

[49] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane, 1999) p.440
[50] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999) p.443
[51] Dorril, S. *The Silent Conspiracy* (1994) p.148
[52] Hollingsworth, M. And Fielding, N. *Defending the Realm* (1999) p.68

and property.[53] Similarly, planting a listening device inside this sphere necessarily violates a boundary that is both highly private and has a clear indication of an 'inside' and an 'outside', marked by a recognisable physical barrier that must be overcome. Furthermore, not only do listening devices violate the boundaries of the target's home, but they also violate the interest that the target has in maintaining control of some of his most intimate words, relations, ideas and activities. As was the case with wiretapping, what the individual says, who it is said to, and what other activities he performs are all created by the individual and therefore it is up to him who gets to access that it.

Given that, as it has been previously argued in Chapter Two, the home is one of the most obvious and important manifestations of an individual's private sphere. Any violation of it is likely to cause a high level of harm. Many see their home as one of their most personal domains, meaning that the type of information likely to be revealed there has the potential to be personal, intimate or secretive in some way. It can include very personal attitudes, conditions and behaviours that would only be revealed to those that an individual feels close to or can trust. Such information is not willingly offered to outsiders. The activities an individual carries out in his home do not have to be particularly unique, but they are normally of such intimate detail and circumstance that, in general, only a few would ever witness them. For instance, the types of information communicated in this sphere might include an individual's sexual relations, acquaintances, nudity, personal habits, or private business dealings. However, even places like work spaces, such as an office, can hold a similar level of privacy given that the individual in many working environments can hold a high expectation that he is alone and that when he discusses things with someone inside his office his words are protected by the surrounding walls.

Therefore, the level of harm caused by using a bug to intercept an individual's communication is similar to both the harm caused by 'bugs that see' from the chapter on imagery intelligence in that they violate spheres that have a high level of privacy and because they both capture information the individual has the right to control. These bugs violate the socially and legally constructed and recognised private sphere. As such, the level of harm caused by these bugs features at Level Three on the Ladder of Escalation.

[53] Fairfield, P. *Public/Private* (2005) p.101, 107

Data Intelligence

The dramatic growth in the size and significance of the Internet and computerised systems in recent years has had some profound effects on society. It has changed the way people interact with each other, how they pass their time and how they pursue their life's desires. It has also had a similar effect on how potential threats, terrorists and criminals, carry out their plans and aims. This means that if intelligence agencies are to face the threats of the digital age then they must be able to engage with this new medium and learn to fight both old threats in new ways as well as fight the new types of threats this technology has given birth to. To this end, it is the job of data intelligence to engage with the digital world, monitor and intercept people's activities, and provide intelligence agents with the resources necessary for tackling the relevant threats. Furthermore, data intelligence can cover the establishment and management of information databases, a phenomenon that is on the increase.

The two examples of data intelligence discussed in this chapter include the interception, collection and utilisation of digital data created as a by-product of interacting with computerised systems – known as dataveillance – and using a computer system to collect, store or analyse information pertaining to an individual or group of individuals – known as data-mining. By collecting these different types of information the aim is to create an dossier on either a specific individual or groups of individuals, from which it is possible to get a better understanding of who the individual is, what they have done and what they might do next.

Data-Mining

David Solove argues that as a result of the computer revolution, never before have governments had the ability to collect information on the individual in such unparalleled ways. For example, information can be collected and collated on where the individual lives, his phone numbers, physical descriptions, age, medical details, legal transgressions, political party affiliation, place of work, property value, financial documents, and then all this information again on his children and spouses.[54] This is mainly the result of a government driven intention to reorient their public bureaucracies in an information dominated society in the hope of delivering a more efficient and fraud proof service. This has led to the creation of many national and local initiatives designed for better co-ordination across a variety of public as well as non-public agencies, including interdepartmental coordination, networking computers and increasing biometric monitoring so that information that was once

[54] Solove, D. *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) p.4

sporadically distributed throughout the system can now be crossed-referenced and pooled with ease.[55] A United Kingdom government White Paper in 1999 outlined this vision arguing for linkages between the government and other public bodies: "Technology will be seen to help make it much easier for different parts of government to work in partnership: central government with local authorities or the volunteer sector; or government with third party delivery channels such as the Post Office or private sector companies".[56] Thanks to developments in information technology intelligence agencies now have a fast, efficient, delocalised, increasingly cheap and omnipresent ability to process an enormous amount of personal data.

As a result of this increased interconnectivity, however, there is the fear that "we are currently confronting the rise of what should be referred to as a digital dossier world".[57] By collecting an individual's various stores of personal information and collating it into a dossier it is believed that it is possible to run the dossier through a programme that can then determine much about the individual. Spiros Simitis notes two examples where data-mining has been used, which should demonstrate how the activity can be applied to intelligence collection. First is what he calls the 'transparent patient', where by taking information from patients, the medical systems are able to identity both sources of additional expenses and patients that are particularly costly. They are then able to treat and charge people according to the risk they pose.[58] The second instance is by the Health Council of Oslo where, by analysing the behavioural patterns of small children, it was thought that it might be possible to indicate psychological problems that could lead to anti-social activities in later life. The project scanned police files for children who exhibited anti-social or delinquent behaviour; those children that turned up then had their school records scanned to identify typical dangerous signals. Once these signals were understood the school records would be rescanned looking for these dangerous signals in other children in the hope of highlighting those children who exhibit similar tendencies and are therefore more likely to exhibit anti-social behaviour in later life.[59]

---

[55] Raab, C. D. 'Joined-Up Surveillance: The Challenge to Privacy' in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* edited by Bell, K. and Webster, F. (London; Sterling, VA: Pluto Press, 2003) p.43

[56] Cabinet Office, *E-Government: A Strategy for Modernising Government* (1999) CM4310 1999 p.4. Available at http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm Accessed May 2008

[57] Solove, D. *The Digital Person* (2004) p.1

[58] Simitis, S. 'Reviewing Privacy in an Information Age' (1987) p.711

[59] Simitis, S. 'Reviewing Privacy in an Information Age' (1987) p.713-714. Other government programs designed to achieve the same goals include the French *Gamin* project in 1973, and even a FBI 'geek test' launched after the Colombine incident.

One important issue that has emerged in response to data-mining in intelligence collection is the collection and use of DNA-profiles. DNA has gained notoriety recently in response to its assumed infallibility in identifying individuals and placing them at a certain scene. By cross-referencing DNA gathered at a scene with profiles stored on a database it is possible to make a direct link between what happened at that scene and that particular individual. The issue that arises for intelligence collection in general, and data-mining more specifically, is under what circumstances DNA can be taken from an individual and put on a database, how long can it be stored on that database and who has access to that database.

Dataveillance

Dataveillance, in comparison, relies less on collecting information that is descriptive of the individual but rather involves tracking that information created as a by-product of the individual moving in an increasingly computerised system. The argument for dataveillance is based on the premise that the planning of almost any activity creates a pattern or 'signature' that can be found in the ocean of transaction data created in the course of everyday life.[60] Serge Gutwirth asks, "what can be deduced from the fact that Mr X uses more gas than he needs for his work, and he fills his car up during working hours in the same locations and buys items from a jewellers, florist and hotel?".[61] Actions on the Internet are easier to track given the nature of the beast. Websites can track a customer's web-surfing secretly when he accesses the web-site, including data about the ISP, computer hardware and software, the website he linked in from and exactly what parts of the website he explored and for how long.[62]

In response to this new form of intelligence the American Defence Advanced Research Projects Agency (DARPA) in the Pentagon began funding a research project called Total Information Awareness (TIA). TIA's aim was to create a programme of "prototypical data collection aimed at discovering and tracking terrorists through the digital paths of their routine transactions".[63] The argument goes that, "if credit card databases were linked with air-line ticket transactions, with immigration databases and lists of suspected terrorists a whole lot of bells would have alarmed when ten thousand dollars was wired to a Florida SunTurst bank account in the name of Mohammed Atta... when Zacarias Moussaoui uses a credit card

[60] Dempsey, J. X. and Flint, L. M. 'Commercial Data and National Security' *The George Washington Law Review* Vol.72 (2004) p.1464
[61] Gutwirth, S. *Privacy and the Information Age* (Oxford: Rowman & Littlefield Publishers, 2002) p.18
[62] Solove, D. *The Digital Person* (2004) p.23
[63] Rubinstein, I., Lee, D. and Schwartz, P. 'Data-Mining and Internet Profiling: Emerging Regulatory and Technological Approaches' *The University of Chicago Law Review* Vol.75 No.1 (2008) p.271;

to pay for his flight, and when a dozen suspected terrorists buy one way tickets to America".[64] By their own accounting, the TIA programme would intercept, collect and collate information about the transactions people carry out as well as education, financial activities, travel and immigration data.[65]

Data Searches

For both data-mining and dataveillance there are a few different types of searches which can be performed. These different searches trawl the electronic highways and byways in different manners, looking for different things and providing different types of data sets. One search type is 'targeted searching', whereby databases are searched in order to obtain information about a subject who is already known, gaining a greater insight on an individual.[66] Another type of search is called 'event-driven', whereby a programme surveys the information stores in the hope of discovering the perpetrator of a particular past event. A common example is searching sex offender registers, cross-referencing it with addresses after a rape in a particular area.[67] Finally, there is 'pattern-based' information processing, where a model of assumptions is created, a search of the various information formats is searched and people who fulfil this model are highlighted.[68] This type of search can include accessing both different databases so as to look for both patterns and individuals who fulfil those patters, as well as monitoring the internet looking for activity patterns. Finally, another type of search would include searching internet activity logs. Every individual who accesses the internet leaves fingerprints as they move through cyberspace, fingerprints that are logged by the servers, internet providers and are associated to the individual through the often unique Internet Protocol (IP) number. By examining a particular IP numbers (that is, the individual's computer) it is possible to catch people carrying out untoward activities.

Levels of Harm: Personal Information

As everyone's life becomes ever more digitalised, the ability to record and monitor the individual and his actions has become increasingly easy. Lawrence Lessig and David Lyon are both concerned that as a result of the rise of activities such as data-mining and dataveillance, the threat to privacy will become all too pervasive: "not only are people subject

[64] Keefe, P. R. Chatter (2005) p.100
[65] Safire, W. 'You are a Target' *The New York Times* November 12th November 2002 p.A35.
[66] Slobogin, C. 'Government Data-Mining and the Fourth Amendment' *The University of Chicago Law Review* Vol.75 No.1 (2008) p.322
[67] Slobogin, C. 'Government Data-Mining' (2008) p.323
[68] Rubinstein, I., Lee, D. and Schwartz, P. 'Data-Mining and Internet Profiling' (2008) p.262

to surveillance as they walk down the street, but increasingly in their homes as they transverses the information highways".[69] Given that data-mining involves collecting information that describes various parts of the individual and his life, by collecting this information without justification or permission it violates his ability to control personal information and as such infringes his interest in privacy. Similarly, dataveillance necessarily involves collecting information that is both authored by the individual as he carries out his activities as well as describing his personal and even intimate activities. This means collecting this type of information violates the individual's privacy in that he has his personal data accessed as well as being watched while he carries out his activities.

The severity of violating an individual's privacy in either of these two ways can vary depending on the information collected. It has been previously argued that the more personal or intimate the information, the greater the claim to privacy there is. If the information contains intimate details about the individual's life or information he wishes to keep secret then the level of harm caused is going to be quite high. In comparison, if the information reveals little about the individual's personal life or the individual has not acted in a way so as to mark the information as private then the level of harm caused is going to be much lower. For example, databases storing information such as gender, age, height, weight, hair colour, and other superficial information is less private than an individual's fingerprint; but fingerprint information is less private than DNA or medical records.[70]

It can be argued that collecting, digitalising and storing an individual's superficial data such as height, sex and clothing only minimally violates his privacy and therefore causes a Level One harm. Collecting an individual's fingerprints is a greater violation of the individual's private information as it is connected to the individual to a greater extent and in a more intimate way. It causes a Level Two harm. It can then be argued, in comparison, that collecting an individual's DNA causes a Level Three harm. That is, an individual's DNA is not the same as many of the other mundane pieces of information about the individual, but rather represents "an individual's very genetic soul... the essence of that individual".[71] The

[69] Lessig, L. *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); Lyon, D. *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001)

[70] This level of privacy is reflected in national law: officials such as police have access to fingerprint databases but if officials want to access medical records they must apply for a court warrant. In the UK the fingerprint database is called the National Fingerprint Database (IDENT1) accessible by police and in American it is the Integrated Automated Fingerprint Identification System (IAFIS) accessible by the FBI. In comparison, access to medical records is restricted in the UK under the *Data Protection Act 1998* and in America by the *Health Insurance Portability and Accountability Act of 1996*, both requiring court orders before allowing access.

[71] Human Genetics Commission 'Nothing to Hide, Nothing to Fear? Balancing Individual Rights and the Public Interest in the Governance and Use of a National DNA Database' *A Report by the Human Genetics Commission* November 2009 Available at

law reform organisation JUSTICE referred to the information contained in a sample of DNA as "the most intimate medical data an individual may possess",[72] and the human rights organisation Liberty repeatedly referred to the "essential intimacy" of DNA information.[73] Furthermore, there is the concern that DNA databases, such as the British National DNA Database (NDNAD), over-represents certain ethnic backgrounds and people from vulnerable groups, and in doing so can have severe social consequences. While it may not have been the intention, there has been a disproportionate representation of certain sub-groups. For example, a report of the Equalities and Human Right Commission (EHRC) notes that "by our own calculation... in excess of 30% of all black males are on the NDNAD, compared with only 10% white males and 10% Asian males".[74] This overrepresentation of certain groups can then have negative social consequences. The implications of a database that over-represents particular groups can include stigmatisation and a breakdown in trust and cooperation in a society. The fear of stigmatisation is that the taint of suspicion lingers in relation to individuals in virtue of the retention of their DNA profiles that can then lead to either inappropriate treatment later in life or can even spread like a stain across their associated, and overrepresented, group. The EHRC commented, "We are concerned that the high proportion of black males recorded on the database is creating an impression that a single racial group represents an 'alien wedge' of criminality".[75] Furthermore, overrepresentation of a particular group can come with a loss of trust and confidence in the state apparatus that can lead to a decrease in the willingness of people in communities perceived as victimised to cooperate.

In a similar way, depending on the intimacy of the information, dataveillance can vary in the level of harm it can cause. Those activities an individual does in public, for example, would be considered less private than those he carried out in the privacy of his home. Buying groceries and petrol are seen as less private than business dealings done behind closed doors. Depending on where the individual carries out his activities and the intimate nature of those activities the level of harm caused is altered. Therefore, similar to intensive surveillance discussed in Chapter Two, monitoring an individual's personal actions carried out in public would constitute a Level Two harm. By contrast, actions done behind closed doors in a

---

http://www.hgc.gov.uk/UploadDocs/DocPub/Document/Nothing%20to%20hide,%20nothing%20to%20fear%20-%20online%20version.pdf Accessed 4th April 2010

[72] JUSTICE *Keeping the Right People on the DNA Database: Science and Public Protection* July 2009 p.2 Available at http://www.justice.org.uk/data/files/resources/188/DNA_databse_HO_consultation_JUSTICE_response_21jul09.pdf Accessed 4th April 2010

[73] Liberty *DNA Retention* Available at http://www.liberty-human-rights.org.uk/human-rights/privacy/dna-retention/index.php Accessed 4th April 2010

[74] Bennetto, J. *Police and Racism: What Has Been Achieved 10 Years After the Stephen Lawrence Inquiry Report?* (London: Equality and Human Rights Commission, 2009) p.5

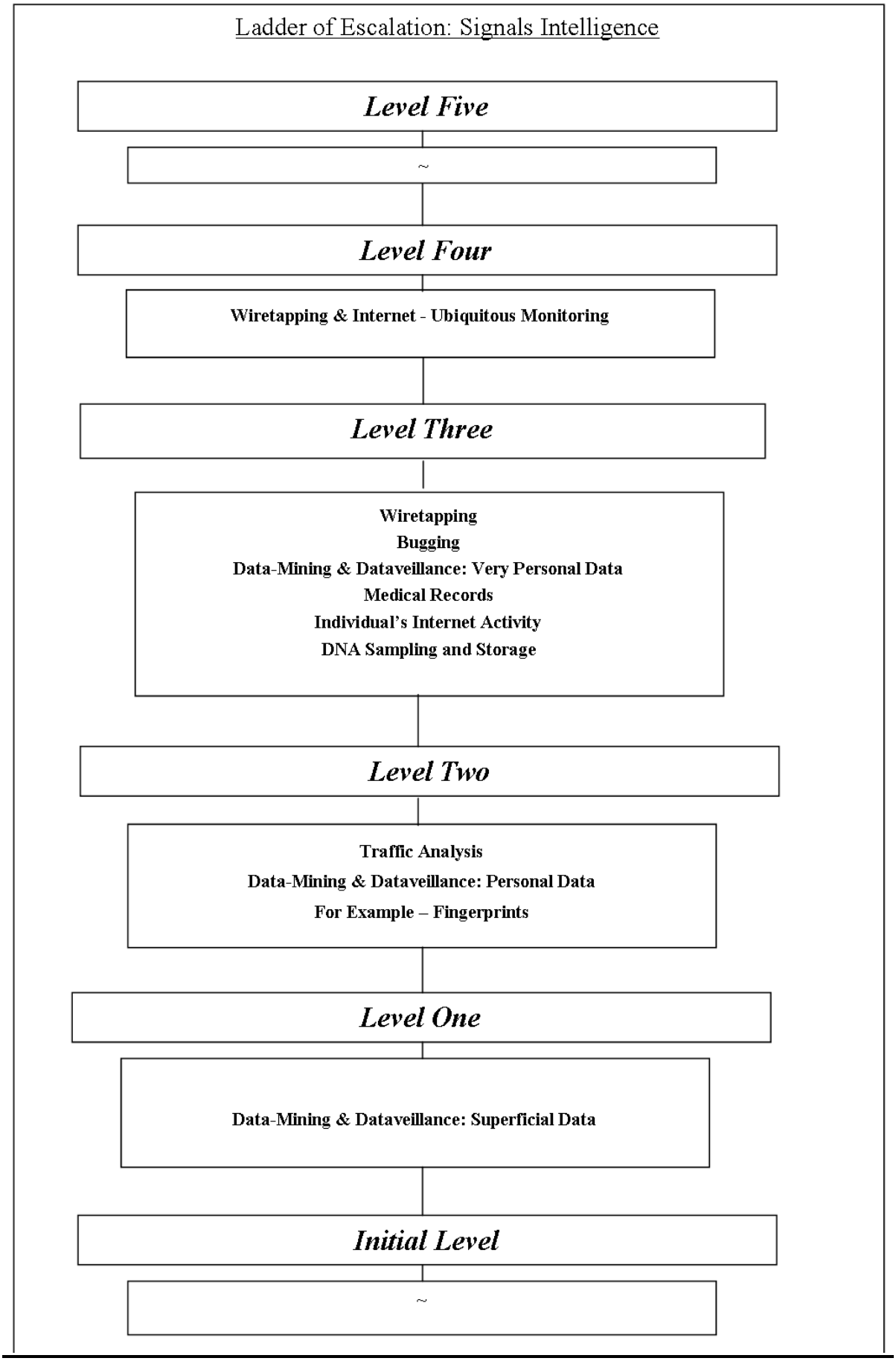
[75] Bennetto, J. *Police and Racism* (2009) p.39-40

sphere that maintains a greater level of privacy, such as business dealings or internet activities[76], would therefore be more private and would cause a Level Three harm.

Furthermore, by making the collection of personal information easier, quicker and more efficient, now more than ever a single actor can collect vast amounts of information on an increasingly larger number of people. What this means is that, similar to ubiquitous telephone monitoring, when dataveillance and data-mining are used *en masse* there are additional harms that need to be included. That is, individuals within a society that monitors all data must assume, because they can never know otherwise, that all their actions are being watched and judged, meaning that they alter their actions to accord with what they think their watchers want from them, affecting their autonomy. Again, similar to the case of communication interception, the effect large-scale monitoring has on an individual's autonomy is greater in comparison to that seen with CCTV cameras because the degree of privacy expected in these areas is greater. That is, the greater the expectation of privacy there is the greater the extent to which an individual will discipline his own actions if he fears he is being monitored. Moreover, the more pervasive the monitoring being carried out the greater the fear that is experienced by the individual that his actions are being monitored, meaning there is a greater chance of the individual altering his actions. Finally, *en masse* monitoring of private information can cause detrimental effects on social cohesion, causing additional harms. For example, the use of profiling can have negative effects on the wider social group that is being targeted. Profiling can label the individual and either cause him to be treated as the label demands or encourages the individual himself to act in the way he thinks he should act according to that label. Therefore, depending on the level of harm caused by the targeted use of dataveillance or data-mining the level of harm caused for the ubiquitous use of that action is greater. For example, focused use of monitoring an individual's internet activity features at Level Three on the Ladder of Escalation, meaning that ubiquitous monitoring in this way will feature at Level Four. What Figure 3.0 below shows is how the different activities involved in signals and data intelligence relate to each other in terms of the harm they cause the individual.

[76] Even though the technology associated with the Internet means that in many instances the server on which the activity being carried out is 'outside' the individual's house, it is similar to telephone calls in that it is still expected that the individual is carrying out the activity 'inside' his house and the communication itself is protected.

Figure 3.0


Ladder of Escalation: Signals Intelligence
Level Five
~
Level Four
Wiretapping & Internet - Ubiquitous Monitoring
Level Three
Wiretapping
Bugging
Data-Mining & Dataveillance: Very Personal Data
Medical Records
Individual's Internet Activity
DNA Sampling and Storage
Level Two
Traffic Analysis
Data-Mining & Dataveillance: Personal Data
For Example – Fingerprints
Level One
Data-Mining & Dataveillance: Superficial Data
Initial Level
~

Section Four: Just Signals Intelligence

The previous sections of this chapter have outlined the type of activities employed in signals and data intelligence, examining key features as well as the main concerns raised by their use. Section Three used explorative examples of both signals and data intelligence to illustrate the types and levels of harm these activities can cause. This section will combine the conclusions made in Section Three with the Just Intelligence Principles outlined in Chapter One in order to illustrate if and when the harm caused can be justified and therefore under what circumstances signals and data intelligence are just.

Traffic Analysis

The use of traffic analysis is an important tool in protecting the state against threats from criminal and terrorist elements, as well as being useful for understanding upcoming military and intelligence operations. Knowing who is talking to whom allows agents to establish important relationship links between different actors both internationally and domestically. However, given that those subjected to such monitoring techniques have an interest in keeping their relationships private if they wish, collecting this type of information can violate this interest and cause a level of harm that features at Level Two on the Ladder of Escalation.

Just Cause

Given that the level of harm caused by traffic analysis is a Level Two on the Ladder of Escalation, the threat required must be more than just a reasonable suspicion. In fact, there must be a probable cause that the threat exists, though the threat itself threatens something of mediocre importance with medium-low impact ability. One example of this type of threat, also outlined in Chapter Two for the use of intensive surveillance, can include criminal elements such as drug or contraband smuggling. This type of activity poses a threat to the safety and peace of society in a mediocre way since it can cause damage to the lives of many people and cause significant damage to the cohesion and stability of a society while not actually posing a direct or imminent threat. This type of activity represents a constant threat to something important, though its impact in the immediate future is dispersed and relatively low. As such, drug operations would offer a just cause for using traffic analysis. This means that the above ‘Dutch drug’ example given has a sufficient level of threat in the form of a drug ring, supported by the drugs found in the car, to act as a just cause. In comparison, the communications database proposed by the British government fails to have a sufficient level

of threat to act as a just cause. Its ubiquitous nature means that when it collects the information there is no expectation that the targets represent a threat in any way. Furthermore, using background threats such as 'terrorism' and or the 'War on Terror' are too broad to act as a just cause for the level of harm caused.

Authority

While Level One harms would require departmental heads to authorise its use, in order for Level Two harms to be just there must be an even higher authority to sanction it. That is, at Level Two it can still be internal to the agency but must be higher than those who are directly involved in the operations. For example, departmental heads or deputy-head of the intelligence agency performing the activity. In the Dutch drug case, while the police represent the correct force to request the information, the authorisation cannot come from a figure directly connected to the case but rather someone in charge of the department or of the whole force. In the proposal to establish a communications database that collected and stored all communication data there is little demonstration of a sufficient authority. Currently, police and intelligence agencies can ask telecommunication providers for information on telephone calls made. The provider can then query the request and then refer it to the Interception Commissioner and an appropriate watchdog. Under the proposed Bill, however, this check would be removed. The information would be centrally stored and accessible to the agents as they needed it, with no authorisation procedure required.[77] This means that there is no oversight for this type of intelligence collection.

Proportionality

In the Dutch drugs case, the gains are clear – establishing further relationships within the drug trade – and the harms caused are also localised and inflicted upon only those who are legitimate targets. Therefore, the violation of a few selected individuals' privacy is outweighed by the conceivable gains. In comparison, the Communications Bill proposed would not fulfil the proportional calculation. The gains are indistinct and relatively unknown, other than the wide reaching "saving lives and tackling crime"[78], while the costs are widespread. Concerns over storing such personal information over long periods of time, the effect it might have on social cohesion and the indirect harm it might cause to an individual's

[77] BBC News 'Warning over Phone Calls Database' 15th July 2008. Available at http://news.bbc.co.uk/1/hi/uk_politics/7507627.stm Accessed 1st November 2008

[78] Smith, J. Former Home Secretary quoted in BBC News 'Plan to Monitor all Internet Use' Monday 27th April 2009. Available at http://news.bbc.co.uk/1/hi/8020039.stm Accessed 29th April 2009.

autonomy each act as a cost and would need to be reconciled if it was to be proportional. On balance, therefore, the cost of having everyone's privacy violated is not outweighed by the general claim of crime prevention.

Discrimination

In order for the principle of discrimination to be satisfied it must be shown that those who have their privacy violated have acted in some way to justify it. In the Dutch drug case, those individuals have a clear connection to the drug world, given that they were found with contraband on their persons. These individuals had acted in a way that demonstrated the threat they posed and therefore waived the right to their privacy. For those connected to the drug cartel, while they might not pose a direct threat, their membership in the organisation demonstrated their consent to the waiving of their protective rights. In comparison, the communications database fails to fulfil the principle of discrimination. By collecting information on all communications it is collecting information which, in the vast majority of the time, will be from people who are wholly innocent. It is unable to discriminate between those who are guilty and those who are innocent, and therefore is unjust.

Wiretapping and Bugging

The potential value to be gained from using wiretaps and bugs in the military, diplomatic, counter-terrorist and even the domestic sphere is clear. Both give a view of what is happening and what is thought inside a world normally out of reach. However, they can cause quite severe levels of harm since they both violate a target's interest in privacy by violating an established private realm and intercepting highly personal or important information. This means that they both feature at Level Three on the Ladder of Escalation and therefore will require similar justifications in order for them to be just actions.

Just Cause

In order to justify the harm caused by a Level Three activity there must be evidence proving that 'on a balance of probabilities' that there is a threat targeting something of importance or has the ability to cause a reasonable amount of destruction. In the battle against other intelligence agencies or military operations the threat is normally clear and present, especially in cases where there has been a long history of antagonism. During the Cold War the most obvious example for the West and the Soviets would be each other. For example, the tapping the phone of Alexei Kosygin, the Soviet Premier, in 1967 during a visit to the United

Kingdom, had a just cause given the hostility between the countries. Many years of intelligence and military antagonism has meant that it is more than reasonable to expect an intelligence or military threat from the other. In the case of tapping or bugging diplomatic communication it is often useful to know the true intentions of foreign powers, both allied and hostile. In instances where there is a clear demonstration of antagonism or a history of clashing interests, then the threat that another state can pose to the security of one's own is cause enough to justify the tapping of the wires. This means that 'neutral' and 'allied' states, will generally be, though not always, off-limits. States, even overtly friendly ones, will at times come to clash over certain issues, and when that state represents a threat to the interests of one's own state, then in those areas there is a just cause. However, there should be some evidence to suggest that the target state is presenting a threat in some way. For example, evidence suggesting that Pakistan was developing nuclear weapons would present a significant threat, enough to act as a just cause for the tapping of the Pakistan Atomic Energy Commissioner and Pakistan nuclear facilities; the tapping of Israeli representatives in the West Bank is justified given the current tensions; and finally it can be argued that even friendly states might clash over certain issues, such as the British and American over weapon deals, which can act as a just cause in these areas, though intercepting communications on other issues would be prohibited.

Domestically, a distinction should be made between those domestic targets that are actual threats, those who are just possible threats and even those are just an annoyance to the political elites. It will be demonstrated in the below examples that in some instances the use of wiretaps in the domestic sphere can be legitimate while in others it is not. For instance, terrorist or criminal organisations who have demonstrated a history of aggressive and/or destructive capabilities and intentions demonstrate that they can, at any moment or even in the future, cause a significant amount of damage and as such provide a just cause for the use of wiretapping or bugging. For British intelligence, there is a just cause for tapping the telephone or bugging the house of known IRA terrorists given the recent violent history between the two sides. One example is that of Sean McNulty, a member of the IRA Active Service Unit (ASU) that had previously bombed two oil and gas installations and was a target for surveillance.[79] However, tapping the wires of protest groups and trade unions, as became customary for British intelligence during the 1960s and 1970s[80], does not have the same just cause because while they might have been politically inconvenient or even might disturb the peace, there was very little evidence that they posed a direct, destructive threat to the state

[79] Hollingsworth, M. And Fielding, N. *Defending the Realm* (1999) p.135
[80] Hollingsworth, M. And Fielding, N. *Defending the Realm* (1999) p.76

and its people. Even though fear of Soviet subversion was prevalent, there was often no evidence of any direct plan at the time to act as a just cause. For example, during the 1978 pay dispute at Ford car manufacturer, MI5 worked on behalf of the government to undermine the Union's position. MI5 permanently tapped the telephone of Syd Harraway, a key shop steward at the Ford plant at Dagenham.[81] In this instance, the legally constituted union demonstrated no direct, destructive intention and as such it did not present a sufficient level of just cause for this type of intelligence collection. Another important case of wiretapping where there is no just cause is that of Martin Luther King Jr. For decades the FBI investigated King for alleged Soviet connections since Hoover was convinced he was a tool of the Soviets and desperately wanted to prove a connection between him and the Soviet bloc.[82] When no connection turned up, however, the use of the wiretaps should have been stopped; the initial just cause of King being friends with known communist sympathisers was a limited just cause to begin with and when no more evidence turned up then the just cause was not sufficient. Without a concrete link between King and the Soviets there was no just cause for the level of harm caused by the use of wiretaps.

Authority

Given that the use of wiretaps or bugs causes a Level Three harm, in order for them to be sanctioned authorisation must come from outside the intelligence organisation. The assessment of whether there is a sufficient threat or not should be done rationally, with relevant facts presented, weighed, judged and with as little bias as possible. As was argued in the example of 'bugs that see' discussed in Chapter Two, it can be argued that the judiciary is most suited to this evaluation given that the courts are often practiced in weighing up evidence and determining if certain acts fulfil the appropriate criteria. By having a council of judges it would further ensure that the evidence was relatively free from personal bias. Furthermore, given that there is the fear that the politics of the day might sway what is a legitimate case, by placing the authority in the judicial wing it removes the opportunity for the operations to be politically biased. This criterion might have proved beneficial for both the King and trade union cases given that it in the former it was the personal bias of Hoover that swayed the case against him and in the latter the political fears held by the British government. William Turner, FBI special agent 1951-1961, noted that the King case was a

[81] Hollingsworth, M. And Fielding, N. *Defending the Realm* (1999) p.76
[82] Sullivan, W. C. *The Bureau: My Thirty Years in Hoover's FBI* (New York: Norton, 1979) p.135

"frightening example of how political police can misuse their powers" for political or personal ends.[83]

Discrimination

The legitimacy of targeting diplomats, military personal or intelligence agents for wiretaps is quite straightforward; each of these targets has, to this level at least, agreed to take part in the national defence apparatus and understands that their positions are likely to mean that they will be regular targets for information collection of this type. They know and accept the harms when they take on their positions and are therefore legitimate targets for wiretapping. For example, when American Ambassador George Kennan first took up his post in 1952 one of the first things he did was to order a thorough search of both the embassy and his own residence, clear in the knowledge that both would be heavily bugged.[84] However, family or friends of those within the defence apparatus are illegitimate targets given that they themselves have not taken on a position or acted in a way as to represent a threat, but are merely related to people who are. This means their conversations should not be tapped and any conversations they have should be marked 'non-pertinent' and the interception should be stopped. Domestic cases, however, are less clear cut. Members of the IRA are legitimate targets since they have acted threateningly and have forfeited their protective rights as a result. Again, family members and friends, where there is no evidence to indicate that they are involved, are illegitimate targets and should not have their wires tapped. In the case of the unions and other politically active groups, even though these groups have acted in a way to become politically active and have 'joined the game' in some way, they are not threatening enough in themselves to represent a legitimate target. For example, politically active individuals like King may have acted in a way as to pose enough threat for traffic analysis, but without further evidence there is no threat sufficient enough to justify the use of wiretapping. However, since using blanket wiretaps that ubiquitously listens to a large number of people's communications features at a Level Four on the Ladder of Escalation, there is a need to discriminate between those individuals who have demonstrated a significant degree of harm and those who have not. Therefore, given that by its very nature *en masse* communication monitoring is unable to discriminate, in that for the vast majority of the time it will be targeting individuals who have not acted in any way so as to make themselves a threat, it is prohibited.

[83] Turner, W. *Hoover's FBI: The Men and Myth* (New York: Dell Publishing, 1971) p.288
[84] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999) p.440

Data Mining and Dataveillance

The activities of data mining and dataveillance are similar in that they both involve accessing personal information about people and doing so without consent of the owner, violating their privacy. Section Three argued that depending on the type of information that was accessed, collected, utilised or stored, when done without the consent of the individual the level of harm caused can vary from Level One through to Level Four.

Just Cause

Those data collection activities that cause a Level One harm, namely collecting information on an individual's superficial features, would, similar to other Level One harms, require that there be 'suspicion' of some threat, even though the threat itself is only suspected, indistinct, towards something of low importance or of low impact ability. It is not enough to suspect everyone and anyone. As it was argued in the previous chapter, threats at this level can include general disturbances to the peace, such as anti-social behaviour.

For Level Two harms, the just cause involves a threat that is both relatively clear and understood and threatens something of mediocre importance with medium-low impact ability, though it might still be relatively temporally distant. There must also be a *probable cause* to believe that the threat exists. For a targeted search looking into a specific individual then that individual must be suspected of being a threat sufficient to justify a Level Two harm. Targeted searches can also be used to investigate a specific website as well, with the site itself being the target. This would involve logging those particular individuals who look at a website that is acting as the just cause. For targeted-searches, therefore, given that the target is already known, it can, if severe enough, act as a just cause for collecting further information. With 'event-driven' matches the event acts as the just cause to justify the use of data-mining or dataveillance. For example, in a rape case it is the rape itself that is the just cause for the use of data-mining to aid investigations. Most commonly a search of a DNA database will be carried out based on any collected hair, blood or semen deposits obtained.[85]

[85] The type of databases in question will often include those individuals who have previously committed crimes, especially if sexually motivated, and will have their information stored for a particular amount of time. This, however, raises concerns for how long the information can be held and whether the initial DNA collection was justified. If, for example, the DNA was initially collected in regards to a previous sexual offense then there is just cause for collecting and storing the information. If, however, the information was collected and the individual proven is not convicted then there is no just cause to keep the information for any particularly lengthy period of time. There is currently significant controversy regarding this issue. Under the legislation currently in force, the police in England and Wales may retain fingerprint and DNA data taken from individuals arrested for a recordable offence for an indefinite period, irrespective of whether such individuals are actually convicted. However, in December 2008 the European Court of Human Rights held that the indefinite retention of such data violated Article 8 of the *European Convention on Human Rights* (right to respect for private and family life) due

However, pattern-based searches like those seen with Total Information Awareness (TIA) programs or the case of the prevention of anti-social activity in children do not possess a just cause. With TIA, the searches are carried out regardless of any particular threat present and as such there is no just cause. Randomly searching information stores with the hope of finding a threat, means that for the majority of the time no threat exists. This means that searching an individual's personal data in the hope of finding markers which demarcate him as dangerous will have no just cause for while the search may eventually find something, for much of the search the threat is unknown.

Finally, in order to collect information on an individual's internet activities, given that it involves accessing personal internet information the just cause must be sufficient to justify a Level Three Harm.[86] This means that there is a threat that is targeting something of importance or has the ability to cause a reasonable amount of destruction. At this level the threat must have evidence that 'on a balance of probabilities' demonstrates that the threat exists. For example, suspected terrorist activity, drug operations, and sexual offences are all sufficient just causes. For example, a 10-month international police investigation into an online peer-to-peer network was coordinated by the Child Exploitation and Online Protection Centre (CEOP) in the UK. The investigation centred on a network used by paedophiles to request, trade and create hundreds of child abuse images.[87]

Authority

Similar to other Level Two harms, in order for the data search to be justified it can still be internal to the agency but must be higher than those who are directly involved in the operations. For example, departmental heads or deputy-head of the intelligence agency performing the activity are appropriate sanctioning authorities for Level Two harms. For Level Three harms, warrants authorised by a council of judges, as outlined in the previous chapters, must be obtained. So, for many targeted searches or event-driven searches, the evidence should be presented to either the departmental head or the courts depending on the information involved, which can then authorise the search. This can essentially be done on a

---

to the "blanket and indiscriminate" nature of the police powers. In order to comply with this decision, the British Government therefore introduced a new retention framework as set out in the *Crime and Security Act 2010*. The key change was that fingerprint and DNA data from adults arrested but not convicted would be deleted after six years, rather than retained indefinitely. Note that the relevant provisions of the 2010 Act have not yet been brought into force; the indefinite retention regime therefore continues to apply at present. Furthermore, this 6 year retention fails to comply with the European Court of Human Rights' decision given that it originally recommended a 24 month retention period.

[86] Note that there is a difference between looking at 'who has visited a particular website' and 'what websites an individual is looking at'.

[87] Home Office Report *Protecting the Public* (2009) p.9

case by case basis. However, with pattern-based searches, such as proposed by the TIA project, the wide collection methods used means that the affects are spread through society, and therefore no case-by-case authorisation can be given.

Proportionality

In the case of targeted and event-driven searches, the use of data searches to combat specific issues like fraud or sexual abuse on the internet, it can be argued that the localised privacy violations and the harm caused can be outweighed in relation to the gains. In comparison, with respect to large data-sweeps like those seen with TIA-type operations, the costs can include not only the violation to an increased number of people's privacy but also the effect it can have on the general population or even social-subgroups, such as damages to their autonomy, liberty and degradation to social cohesion. Individuals and subgroups of society become victim to a data-based or internet-based Panoptic gaze. They alter their activities so as to fit in with what they think their watchers expect of them. Furthermore, certain groups might feel that they are being victimised and this can lead to social decohesion, similar to those instances discussed in previous examples.

Discrimination

For targeted searches, the ability to discriminate between targets is clear; those who are presented as sufficiently threatening are legitimate targets. For event-driven searches however, care must be taken to only target those who have some direct connection to the event. However, with TIA and other pattern-based investigations, since the level of harm caused features at Level Four on the Ladder of Escalation as a result of the effect they can have on an individual's autonomy and social cohesion, they must only target those who represent a clear threat or are connected to a clear threat in some way. Given that by their very nature these types of searches are unable to discriminate in this way, their use is prohibited.

Conclusion

This chapter has demonstrated how signals and data intelligence can play a vital role in determining, locating and preventing a variety of threats that face the political community. However it argued that that these actions can cause various levels of harm since their use can come into conflict with an individual's privacy and autonomy as well having the potential to affect the cohesion of the political community. By outlining various types of information, how that information is connected to the individual and how as a result the individual can make claims to restricting others seeing or using that information, this chapter deepened the understanding of privacy. As a result of this deeper understanding it is possible to better comprehend the ways that signals and data intelligence can violate an individual's vital interests and therefore cause harm. This chapter argued that individuals maintain a right to privacy in regards to their relationships, their communications and even their physical activities, and that depending on the how intimate these are the level of harm caused is changed. However, by making reference to the Just Intelligence Principles outlined in Chapter One this chapter examined those instances where there is sufficient reason to justify the harm caused by these collection activities. It was also shown, however, that collection activities that cause a level of harm at Level Two or above and collect information *en masse* cannot be justified given that they are unable to discriminate between legitimate and illegitimate targets.

Chapter Four: The Dark Arts
Human Intelligence

While a large amount of important information can be collected through signals and imagery intelligence, there are certain types of information that are impervious to these technical means of collection and, instead, rely on humans as the means of collecting the information. For example, some of the most valuable information – plans, intentions, and beliefs for example – might only exist within the heads of those in power or be stored out of reach of technical collection mechanisms. Only human agents, with their ability to engage with other people, create relationships and physically access certain areas, offer a way of collecting this information. For example, Jeffery Richelson observes that technical systems "cannot photograph planning or policy documents locked in a vault" and that some of the most important types of information for state officials include being able "to understand the decision process involved in foreign, military and economic policymaking in both hostile and friendly nations".[1]

The reason why human intelligence has proved itself so successful is that almost all targets – states, groups, organisations or individuals – have a 'human factor' associated with them that intelligence operatives can engage with and exploit. The problem, however, is that the type of activities employed by intelligence operatives can come into conflict with an individual's vital interests and, as a result, can cause him harm. In comparison to the chapters on imagery and signals intelligence, human intelligence encompasses a wider range of collection activities. For this reason, the review of human intelligence will be divided between two chapters. The division is based on a distinction between those human intelligence collection activities that are 'indirectly coercive', to be discussed in this chapter, and those that are 'directly coercive', which will be discussed in the next chapter. First, this chapter will outline why human intelligence is a separate and important intelligence collection discipline as well as outlining in greater detail the basis for the division mentioned. Section Two will expand on the ethical framework established in Chapter One by exploring some of the ethical issues associated with human intelligence so that in Section Three it is possible to apply the ethical framework to a series of illustrative examples. In Section four, the Just Intelligence Principles will be incorporated to determine if the harm caused is justified.

[1] Richelson, J. T. *The U.S. Intelligence Community* (Boulder, Colo: Westview Press, 1995) p.244

Section One: Nature of Human Intelligence

Human intelligence is very simply the use of human operatives to collect information of intelligence value. By using humans as a means of collection it is possible to access and collect information that might not physically exist, but can be extracted from the feelings, opinions, plans, intentions, inter-personal relationships, nuances or general personalities of an individual, group or state. Clearly, human intelligence represents a form of collection quite unlike the two technical forms previously discussed. What this section will outline is what goes into making human intelligence separate from the other intelligence collection disciplines, as well as what it is about human intelligence that makes it distinct from similar information-related actions human beings carry out. Furthermore, this section will also mark a distinction within human intelligence between those actions which are directly coercive and those which are indirectly coercive, as a means of dividing human intelligence collection activities between this and the next chapter. This division is a means of separating out the different human collection activities in order to make the task of ethically evaluating them more manageable.

The Human Aspect

The first, and most obvious, characteristic of human intelligence is the fact that it uses human beings – their senses, skills, intuitions and relationships – to find, collect and then communicate the intelligence. This is because the information is either stored or exists in such a way that it can only be accessed by a human agent. That is, in many instances the information will be in the head of some individual or kept locked away in a repository where it can only be accessed by human hands. This means that the information cannot be 'captured' by some piece of technology, but rather relies on another individual divulging the information or the intelligence officer accessing the information directly.

One of the greatest strengths of human intelligence is its ability to capitalise on the natural tendency and necessity of human beings to form relationships with each other and the power found within those relationships. These relationships are varied and can include ones of trust, threats, coercion, physical pleasure or pain, manipulation, deceit or mutual cooperation. It is through the exploitation of these relationships that human intelligence is made possible. For example, torture, interrogation, gaining access to a group, persuading an individual to divulge state secrets and even securing a defector all rely on the ability to form

and use relationships between two or more individuals. Only humans are able to form these relationships and therefore only humans can access this type of information.

In comparison to signals and imagery intelligence there is noticeable difference in how the information is 'captured'. In previous chapters, technology was essential in actually taking the information from its raw state and then representing it in some way, whereas with human intelligence, the operative collects or even absorbs the information, stores it within him and then transmits it back to his master. Although this information can then be represented, transmitted or relayed through a variety of technical means – phone, email, or even Morse code – the act of capturing information is achieved by the individual.

Intention

In both previous chapters on imagery and signals intelligence, it was noted that there is an important difference between the casual observation and the intentional hunt for information that was vital to the definition of intelligence. This separated out those actions that collect information without realising it, and those purposeful actions performed by intelligence actors designed to collect information. It was argued in Chapters Two and Three that because of this intention the individual carrying out the activity and the organisation he represents are moral agents and are morally culpable for the harm they cause. Similarly, human intelligence involves a series of actions that are carried out intentionally by an agent aware of his activities, and therefore is morally culpable for any harm caused. As a result, it is possible to draw a distinction between the relationships individuals make with each other on a regular basis, and the intention behind those relationships made by the intelligence officer.

Security Lens

Again, similar to those issues discussed in previous chapters, one of the most important aspects of what makes intelligence separate from other activities is the security lens it uses. This security lens distinguishes the information individuals and corporate organisations collect and dispense every day and the security lens filters the information and turns it from simple data into intelligence. More importantly, however, is that this security lens highlights the point that the information which is important is that intended for the protection of the political community. The security lens is shaped by the relevant threats that face the political community and the intelligence operatives act in response to those threats. Therefore, this security lens stresses the end to which human intelligence is being carried out, as the

protection of the political community and in doing so alters the ethical calculation made. As it was argued in previous chapters, by having the intended goal of the collection activity as the protection of the political community the action is judged in a different way to those activities carried out by or for private goals. That is, actions for the protection of the political community are judged in a fundamentally different way in comparison to the actions carried out by a private firm or individual because of the ethical good that the political community represents.

A Human Intelligence Divide: Indirectly Coercive and Directly Coercive Acts

Since much of human intelligence involves getting a target to carry out an activity they would otherwise not wish to do, human intelligence necessarily has a coercive element to it. The concept of coercion signifies, in a most general sense, the exercise of power over an individual in order to get him to do something that he might otherwise not have done. This broad understanding can refer to obvious threats and/or violence as a means of forcing someone to do something as well as less obvious acts of coercion such as subtle pressures designed to guide another's actions.[2] For human intelligence it is no different; a pressure of some form is applied in order to get the target to cooperate. Furthermore, this pressure can be both direct, compelling the individual to do something, or indirect, guiding or encouraging a specific response. As such, in this thesis a distinction will be made between those human intelligence activities that are 'directly coercive' and those that are 'indirectly coercive'.

The former 'direct' coercive form of human intelligence involves power being applied to an individual in order to alter his behaviour as a direct consequence of the coercion. The target is directly aware of the coercion and acts because of it. There is a threat that is presented to the individual and he is aware of the ultimatum that is being presented. In comparison, indirect coercion involves pressure being applied to alter the individual's behaviour without a direct confrontation. The pressure attempts to guide rather than force the individual's choices and, as such, he might not be aware of the controlling pressure that is being applied. For example, direct coercion can involve activities that involve threats, violence or ultimatums, where the target is told in no uncertain terms that he is to capitulate or he will suffer the consequences. The threat or use of physical force, for example, is directly coercive. The "force is directly applied to cause a behaviour in another person" and

[2] Pennock, J. R. 'Coercion: An Overview' in *Nomos XIV: Coercion* edited by Pennock, J. R. (Chicago: Aldine, 1972) p.4

the individual is directly aware of the coercion.[3] Conversely, indirect coercion can involve actions like bribing someone and manipulating or deceiving him, where the pressure is applied to guide or influence the individual's actions and the ultimatum is not so starkly presented.

Indirect Coercive Human Intelligence: The Dark Arts

The cloak and dagger of the intelligence world is what most people think of when human intelligence, and even intelligence in general, is mentioned. It is what is most often portrayed in popular culture with intelligence officers running double lives and engaging in romantic affairs. This is not without good reason. Loch Johnson notes that "virtually every nation resorts to the 'dark arts' of espionage to protect its government, economy and citizens".[4] Throughout the Cold War intelligence agencies on both sides used methods of deception, manipulation and bribery as fundamental tools of the trade. This chapter will focus on these so-called dark-arts, including the use of 'official' and 'unofficial covers', to infiltrate and penetrate various targets, as well as those tactics used to persuade a specific target into cooperating.

Covers, Recruitment and Broken Hearts

Although there are many different activities, tactics or tools at the disposal of the intelligence operative, this chapter will look at two broad categories of human intelligence activities. The discussion will first focus on penetration and infiltration tactics where false identities are used to gain access to areas that would otherwise be off-limits. Second, it will discuss those activities and tactics used to encourage a target into cooperating with an intelligence officer. This second group of activities will explore three important types of recruitment: the defector, 'pitch' recruitments and seduction.

Covers: The Masks We Wear

In many ways, an individual's identity as perceived by the outside world is just a mask he chooses to wear each day, constructed from various facts that people know about him: his accent, records, what he tells others about himself and anything that physically marks him as who he is. These expressions of an individual's identity are merely outward representations

[3] Bayles, M. D. 'A Concept of Coercion' in *Nomos XIV: Coercion* edited by Pennock, J. R. (Chicago: Aldine, 1972) p.19
[4] Johnson, L. 'Spies' *Foreign Policy* no.120 (2000) p.18

of the person that exists beneath. However, one of the benefits of masks is that they can, quite easily in fact, be changed. By altering the operative's name, job and credentials, and by training him in different languages and anything else that is required, he can be provided with a new identity. This cover must provide the intelligence officer with a "plausible reason for being in a particular country" including "visible means of financial support, and a pretext for meeting people with access to secretive information".[5] By doing this, an individual who would otherwise be unwelcome in a certain group or country can turn into a welcomed member and, as a result, become privy to information, resources and individuals that would be inaccessible to outsiders. From here the intelligence operative can carry out several different collection activities. These new identities allow access to areas from which the operative can collect information as well as providing an opening to establish contact with people so as to carry out recruitment operations. In both cases, a cover is necessary since the officer's true identity would prevent any such activity.

There are essentially two different types of cover and, depending on how and to what end the cover is employed, the type of new identity assigned can vary. In the American parlance the distinction is between 'official cover' and 'non-official cover' and in Soviet terminology the division was between 'legal' and 'illegal' officers, though the distinction amounts to the same thing. 'Official' or 'legal' covers are where the assumed identity hides the officer's intelligence role but not his state affiliation. For example, a cover as a diplomat, attaché, military serviceman, or embassy employee makes clear who the officer works for but not his job as an intelligence operative. This type of cover provides the officer with several advantages. The first is that the official position that is assumed often comes with diplomatic immunity so that should the officer's true identity be discovered then the most a state would do is expel him as a *persona non grata.*[6] In addition, posing as a diplomat improves access to information and individuals of importance as the officer has a genuine reason for meeting with host-government officials as well as other diplomats. However, there are obvious drawbacks to this type of cover, namely that given the connection to the home country the officer is a clear target in the eyes of other intelligence agencies and while his position might give him access to some individuals it can also block access to others. Furthermore, for those operations designed to infiltrate a group, any affiliation with the state is an automatic disqualifier. In order to solve these problems intelligence officers can also have 'non-official' or 'illegal' covers. These covers involve creating an entirely new identity designed to detach

[5] Shulsky, A. N. *Silent Warfare: Understanding the World of Intelligence* (Oxford: Brassey's, 1991) p.12
[6] Shulsky, A. N. *Silent Warfare* (1991) p.12

the officer from both his home allegiance as well as his intelligence role. This will include an extensive, elaborate and verifiable synthetic life, called a 'legend', which acts as a justifiable reason as to why the individual should be where he is with as much distance from his home allegiances as possible.[7]

The Pitch: Turning the Individual

One of the main sources of information on any organisation is most naturally going to be from someone who is part of that organisation, someone who is entrusted with secrets, someone who is knowledgeable on the inner workings of the organisation and someone who has a genuine reason for being on the inside. Therefore, it is only natural that an intelligence agency is going to try and establish contact with individuals from within a particular organisation and try to convince them to provide information. Indeed, it is the job of intelligence officers to locate, assess and turn such individuals. In order to achieve this, the intelligence officer must locate those he thinks will prove to be a fertile source and then offer a 'pitch' designed to persuade the target into becoming an agent. Although in some instances this can be quick and simple, it more often involves a lengthy process of locating the individual, collecting information on him, making an approach, forming a bond with him and then using that bond to create the right mental state so as to encourage the final recruitment.[8]

Romeo Agents and Honey Traps

A part of intelligence that has often received a disproportionate amount of attention from the media and general public is that of 'Romeo agents' and 'honey traps', whereby the human need for companionship and love is used as a means of gaining information and cooperation from other individuals. Marcus Wolf, former head of the East German intelligence agency Hauptverwaltung Aufklärung (HVA), stated that, "Romeo spies gained notoriety across the world by winning women's hearts in order to obtain the state and political secrets to which their targets had access".[9] Moreover, as women took on "formerly male jobs as secretaries to

---

[7] Andrew, C. and Gordievsky, O. *Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975-1985* (London: Sceptre, Hodder & Stoughton, 1993) p.94

[8] For more detail on what is involved in each of these recruitment steps see; Dzhirkvelov, I. *Secret Servant: My Life with the KGB and the Soviet Elite* (New York: Simon & Schuster, 1989) p.177; Epstein, E. *Deception: The Invisible War Between the KGB and CIA* (New York: Simon and Schuster, 1989) p.182; and Kessler, R. *Inside the CIA: Revealing the Secrets of the World's Most Powerful Spy Agency* (New York: Pocket Books, c1994) p.34

[9] Wolf, M. and McElvoy, A. *Memoirs of a Spymaster: The Man Who Waged a Secret War Against the West* (London: Pimlico, 1998) p.123

important figures" it is not surprising that they represented an important intelligence target.[10] Both Romeo agents and honey traps depend on finding individuals who have access to valuable information but are emotionally vulnerable or lonely. By offering to fill the emotional vacuum, Romeo agents and honey traps incorporate themselves within an individual's life, using charm and seduction as the snare. Once the agent has gained the trust and affection of the target, he is then able to use this as a means of extracting information or ensuring cooperation.

Defections and Walk-Ins

One important distinction in human intelligence that is often made is that between recruited sources like those mentioned above, where the intelligence officer 'persuades' someone to become a source, and defections, where someone approaches a foreign intelligence agency, often by physically walking into the building, and offering his services. This is quite different from the methods mentioned above because it does not require intelligence officers going out and hunting or looking for sources, but rather involves the defector making himself available. Why the individual might choose to offer up this information can vary from case to case, but can often stem from desires for money, disgruntlement with his position, ideological beliefs, the need to find sanctuary for some wrong done, or because of a host of other unhappinesses. What the intelligence agency must do is ensure that it has the appropriate mechanisms ready when a defector decides to make the jump so as to be there to catch them.

Conclusion

Human intelligence provides for the world of intelligence something that the two other technical collection disciplines cannot achieve, the 'man on the ground'. Humans form a fundamental part of any organisation and as such it would be difficult to ignore them as a possible avenue for intelligence. The two main tasks for human intelligence are being able to gain access to areas that are normally off-limits and to carry out either a recruitment exercise or collect information the new-found access provides. This section has outlined some of the main tactics used by human intelligence operatives in order to achieve these two main goals. The next section will look at the main ethical issues these tactics then bring-up, expanding on the work done in Chapter One.

[10] Wolf, M with McElvoy, A. *Memoirs of a Spymaster* (1998) p.124

Section 2: The Harm of Human Intelligence

As the previous section outlined, an intelligence operative's main aim involves either gaining access to important information or gaining access to someone who has the information and who can provide it. However, in order to achieve these aims the tactics employed by the intelligence operative can come into conflict with the individual's vital interests. This section will explore these tactics in greater detail in reference to the ethical framework established in Chapter One and highlight how they can cause harm. It will explore the use of deception, manipulation, seduction, and bribery.

Deception and Lying

Deception has never been a stranger to military strategy or intelligence. Feigning, misleading and providing misinformation is at the heart of espionage. The question, however, is to what extent these deceptions and lies are harmful to those subjected to the untruths. While it is arguable that deceiving and lying are natural human activities, with many interpersonal encounters involving some form of deception, these are recognised and accepted as normal means of greasing the wheels of everyday social life.[11] They are, it is quite clear, very different from those deceptions carried out by intelligence operatives.

'Deception' can be understood quite broadly as any action or activity that is knowingly designed and intended to encourage an audience of some sort to believe in something which is untrue. This definition is broad in the sense that it includes a variety of different actions designed to mislead people about the truth. For example 'deception' can cover the more specific act of lying, hyperbole, pretence, equivocation, distortion, disingenuous statements and omissions, each referring to a particular type of untruthful (in)action. A direct lie, for example, is a message that is communicated with the intention of deceiving others and convincing them of something the liar himself knows to be untrue.[12] In comparison, the 'continuous lie' is where, as Roderick Chrisholm and Thomas Feehan point out, the liar "contributes to D's [the target's] continuing belief in P [the lie]", though the liar

[11] For example, acts of tact, politeness, excuse, reticence, avoidance, or evasion are ways of protecting and promoting social harmony. See Adler, J. E. 'Lying, Deceiving, or Falsely Implicating' *The Journal of Philosophy* Vol.94 No.9 (1997) p.435. Also see Baier, A. 'Why Honesty is a Hard Virtue' in *Identity, Character and Morality* edited by Flanagan, O. J. and Rorty, A. O. (Cambridge: MIT, 1990) pp.259-281

[12] Bok, S. *Lying: Moral Choice in Public and Private Life* (New York: Vintage Books, 1979) p.14. This means that when an individual is communicating something that he believes to be truthful, but in fact it turns out to be false, he is not lying but acting in error. Furthermore, given that the liar has a direct intention to deceive and have the victim believe in the untruth, then joking falsehoods or even flattering statements are not lies as there is no intention for the recipient to believe the literal words.

is not the original source of the lie.[13] In both the direct lie and the continuous lie, there is the communication of some known untruth with the intention to deceive. However, an individual can also lie by withholding information, known as 'lying by omission'. This is where the liar has "failed to do something with respect to D [the target] and the belief in P [the lie]" which he could have prevented.[14] Lying by omission involves an individual either allowing or contributing to a falsehood by omitting certain facts while having the ability to prevent the falsehood from being believed and with intent for a deception to occur.

In Chapter One it was argued that an individual has a vital interest in maintaining his autonomy and that when his autonomy is violated he is harmed. Lying and acts of deception are harmful inasmuch as they violate the individual's autonomy as they cause him to become a tool of another's will. In order to be autonomous, as it was argued in Chapter One, the individual must able to make decisions based on his own motivations and needs, towards his own end, rather than that of another. That is, people must be able to act for "reasons all the way down according to their actions and according to their reasons".[15] However, when people are lied to, their reality is distorted:

> Lies may eliminate or obscure relevant alternatives... at times, lies may foster the belief that there are no more alternatives than is really the case; at others, a lie may lead to the unnecessary loss of confidence in the best alternative. Similarly, estimates of loss and benefits of any action can be varied through successful deception.[16]

This means that decisions are then made on a distorted view of the world, or, more precisely, on the will of the deceiver for he is the one who has created this false view. The victim will act in response to this distorted world view and as a result the deceiver brings the victim under his casual control. The victim of a deception becomes the tool of the deceiver because his decision-making process is based on the deceiver's will rather than his own. Given that an individual's autonomy is not a binary characteristic, whole one minute and completely subjected the next, depending on the nature of the lie or deception the affect on an individual's autonomy can vary. That is, depending on the degree to which it is reasonable to expect the lie will alter the individual's decision-making process the level of harm is altered. The greater the impact of the deception on the individual's view of reality, or the more

[13] Chisholm, R. M. and Feehan T. D. 'The Intent to Deceive' *The Journal of Philosophy* Vol.74 No.3 (1997) p.144
[14] Chisholm, R. M. and Feehan T. D. 'The Intent to Deceive' (1997) p.144
[15] Herman, B. *The Practice of Moral Judgement* (Harvard University Press, 1996) p.228
[16] Bok, S. *Lying* (1979) p.20

intimate the area the deception, the greater the affect it has on his decision-making process. For example, those lies that are related to superficial, non-important, or non-intimate areas are likely to affect the individual's autonomy less than those lies which are on an important, personal issue or something which is going to dramatically alter the individual's decision-making process.

Furthermore, lying can damage society as it "chips away at, and could destroy the social bonds of trust" and as a result breaks down the moral and social relationships that hold a society together.[17] Barbra Misztal argues that for society the notion of trust is "essential for stable relationships, vital for the maintenance of cooperation, fundamental for any exchange and necessary for even the most routine of everyday interactions".[18] Both society and the individual need trust as a fundamental principle for maintaining social cohesion and ensuring everyday fluid co-operation. For the individual, "trust affects our understanding of other people, our sense of who they are and what they are doing"[19] and without this trust "only very simple forms of human co-operation which can be transacted on the spot are possible" as "individual action is much too sensitive to disruption to be capable of being planned without trust".[20] Lying and deception are a poison to trust as they breakdown social-interpersonal bonds. When the lie is between an individual and his political community or the state's representatives then the loss of trust is often extrapolated to the whole system or community. Sissela Bok argues that trust is a social good and that when this trust is damaged "the community as a whole suffers; and when it is destroyed, societies falter and collapse".[21]

Manipulation and Seduction

Closely connected in many ways to some of the issues discussed in the section on deception, manipulation has both a long history within intelligence collection and also poses a problem for an individual's autonomy. Manipulation is that act whereby an individual attempts to direct, control or guide the actions, thoughts or beliefs of another through the application of various pressures on his decision-making process. The first point is that, obviously,

[17] Ikuenobe, P. 'The Meta-Ethical Issue of the Nature of Lying: Implications for Moral Education' *Studies in Philosophy and Education* Vol.21 (2002) p.40

[18] Misztal, B. A. *Trust in Modern Societies: The Search for the Bases of Social Order* (Cambridge: Blackwell Publishers, Inc., 1996) p.12. For more discussion on types of trust see Hardin, R. *Trust and Trustworthiness* (New York: Russell Sage Foundation, 2002) p.3; Hertzberg, L. 'On The Attitude of Trust' *Inquiry* Vol.31 (1988) pp.307-322; and Mollering, G. 'Inviting or Avoiding Deception through Trust? Conceptual Exploration of an Ambivalent Relationship' in *Deception* edited by Harrington, B. (Palo Alto: Stanford University Press)

[19] Govier, T. *Dilemmas of Trust* (London: McGill University Press, 1998) p.6

[20] Luhmann, N. *Trust and Power: Two Works by Niklas Luhmann* translated by Davis, H., Raffan, J. and Rooney, K with introduction by Poggi, G. (Chichester: Wiley, 1979) p.88

[21] Bok, S. *Lying* (1979) p.28

manipulation will have some end in sight; the manipulator will be attempting to either get someone to think something, believe in something or act in some way. The second point is that pressure is essential to manipulation since it is as a result of this pressure that the individual acts in the desired way, as compared to how he might have acted otherwise. This pressure can either be in the form of incentives or as the result of deceptive acts. Using incentives involves "controlling signals about rewards and deprivations or by controlling rewards and deprivations, or both".[22] That is, offering the target something positive if he carries out the desired action or even punishing him if he fails to capitulate.[23] Using incentives will often involve exploiting an individual's weaknesses or his personality since knowing how to 'push someone's buttons' or 'pull someone's leavers' is essential in tailoring the incentives and assuring the correct response.

Another type of pressure that can be applied in order to control the actions of an individual is, again, the use of deception. As noted previously, lying will often involve making someone believe in options, activities, avenues or realities which the individual would have not have believed in before. By altering the target's view of reality, the manipulator is using the deception to guide the target's actions. Obviously not all lies are manipulative, but it can be argued that those lies that are used to control an individual's actions can be manipulative.

The reason why manipulating an individual is harmful is because of the affect it has on his autonomy. Given that the autonomous agent is one that decides his own actions based on his own reasons, when an outside force deliberately applies pressure on his decision-making process it is essentially forcing him to make his decisions based on the will of another. Joel Rudinow notes that by looking at manipulation through the lens of autonomy "finally, we can understand.... that the attempt to manipulate someone is to elicit behaviour without regard for – and with a will to interfere with – his operative goals".[24] The individual becomes the subject of the manipulator's will, a means to the manipulators end, rather than an end in himself.

[22] Green, R. K. and Pawlak, E. J. 'Ethics and Manipulation in Organisations' *The Social Service Review* Vol.57 No.1 (1983) p.35
[23] Rudinow, J. 'Manipulation' *Ethics* Vol.88 No.4 (1978) p.340-1
[24] Rudinow, J. 'Manipulation' (1978) p.347

Seduction

Seduction is not inherently harmful in and of itself. Indeed, individuals can seduce each other with the best of intentions, resulting in no harm. What is harmful about seduction, however, are the methods used and the intent behind them. That is, seducing someone through deception or manipulation is harmful because of the intent behind the seduction itself. Indeed, seduction, as practiced by intelligence operatives, is a special type of manipulation, whereby a manipulative pressure is applied to an individual in order to direct a particular response. This seduction involves exploiting the most intimate feelings an individual has, preying on core emotions in order to provoke the correct response. Seduction attempts to manipulate the individual through targeting his feelings of love, affection and adoration. By utilising these core emotions it is possible to create a situation where the individual will carry out activities that he would have otherwise not done. The person does not simply act weakly because he finds the new prospect overwhelmingly tempting but is brought to this weakness by the influence of someone else.

As a form of manipulation, seduction is harmful because it violates the target's autonomy. The seducer provides the target with false information, distorting the normal view of reality and causing decisions to be based on the will of the seducer. Then, by using the power gained through the seduction, what should be a blight-free activity – that is, deciding whether or not they should perform a particular action – is distorted by intimate emotions based on lies and deception. Furthermore, given that seduction involves exploiting the individual's feelings in an area that is of great intimacy – an exploitation of an individual's most intimate sense of self, his sex and love life – there is the additional harm caused by the affect it can have on his sense of self-worth and mental integrity. It is therefore important to reflect this special quality in the level of harm that is caused when applied to the varying case studies.

Bribery

Bribery, although akin to manipulation in that it involves getting someone to do something they would otherwise not do, is something quite distinct and carries with it a separate ethical status. Bribery occurs when "property or personal advantage is offered... with the intent of ... [to encourage the target to] acting favourably to the offer in contradiction to moral or legal

norms".[25] What is first notable about bribery is that it necessarily involves a payment, either in the form of material goods – money, drugs, food – or as some other non-material benefit – expressed gratitude, favours, or an undeserved promotion – in order to secure or encourage the desired end. However, given that payment of money or other goods in order to obtain a particular service is not itself unethical, since this would render all commerce and employment immoral, it is necessary to note the intention behind the bribe, that is, the wish to control the target's behaviour in some way. Moreover, this desired behaviour will often run contrary to some legal or moral norm, such as those borne from a duty, responsibility or trust that an individual has as a result of his position or role.[26]

What this standard model of bribery demonstrates is that behind a bribe is the intent on behalf of the briber to control and direct the actions of another, that is, "the person bribed would not have acted as he did without the inducement of the bribe".[27] The briber exploits the weaknesses of the bribee in order to alter his decision-making process and get him to carry out an act he might not have previously considered. Even in cases where the individual would have carried out the desired act anyway, as in the case where a bribed judge would have given the same verdict regardless of the bribe, the fact that the briber had the intent of controlling the decision-making process of the target means that there is the intent to circumvent the individual's autonomy.

Moreover, by bribing someone to carry out an act that breaches his responsibilities or duties, any further harm that results from the breach is the responsibility of both the briber and the bribee. Without the influence of the bribe the breach would not have occurred and therefore culpability must be accredited to the briber as well as the individual who actually carried out the act and who still had a degree of choice. Borrowing from legal terminology, "we may view the person offering a bribe as an accessory to the improper act committed by the person accepting that bribe – he is an accessory before the fact and therefore the briber is at least as culpable as his hired agent".[28]

---

[25] Turow, S. 'What's Wrong with Bribery' *Journal of Business Ethics* Vol.4 No.4 (1985) p.249; similar definition is offered by Phillips, M. 'Bribery' *Ethics* Vol.94 No.4 (1984) p.622

[26] Nevertheless, these moral or legal norms can be quite broadly defined: "it is tempting to define a bribe as a payment made to a member of an organisation in exchange for the violation of some positional duty or responsibility" but we can also be bribed to violate a duty we have to non-organisations but where we still have a duty or responsibility to maintain. Phillips, M. 'Bribery' *Ethics* (1984) p.622

[27] D'Andrade, K. 'Bribery' *Journal of Business Ethics* Vol.4 No.4 (1985) p.239

[28] D'Andrade, K. 'Bribery' (1985) p.239

The Bonds that Tie: Breaking Morally Worthwhile Relationships

Forming relationships with people, organisations and groups is an important human characteristic. Out of the multitude of bonds an individual will create in his life, the importance may vary, but the significance to the individual of having bonds does not. "To say that humans are social animals is to say that they depend on others for psychological sustenance, including the formation of their personalities."[29]

As was argued in Chapter One, individuals define their sense of self-worth as a result of how they (think) their identity group sees them. The individual draws his identity from that group of people he identifies with, forming bonds which are morally worthwhile inasmuch as they define who he is. To lose these relationships means the individual is harmed as a result of the damage to his identity and sense of self. Concern must be given to relationships between the individual and the associations he is a member of, and the ethical significance to be attributed to these associations. Furthermore, Toni Erskine argues that it is important to understand that one's morally defining communities can "come in a variety of forms, including political parties, social movements, and labour unions". Moreover, given that relationships are two-way streets, it can be argued that not only is the individual who is forced to betray his friends or colleagues harmed by his losing these bonds, but those people with whom he is bonded are also harmed. In addition, when he betrays or is forced to betray the group, such betrayal can break down trust between and within that social group and can lead to degradation of social cohesion. However, the nature of these bonds can vary between people as "there is a host of allegiances and associations to which individuals are strongly committed"[30], meaning that some betrayals can be more or less harmful than others depending on the individual, the organisation and the types of bonds involved.

Conclusion

These various ethical concerns demonstrate how the use of human intelligence can come into conflict with the vital interests that have been outlined in Chapter One. By examining the issues of deception, manipulation, seduction and the importance of morally constituted interpersonal bonds, this section has expanded on the ethical framework already established. Therefore, in the next section a Ladder of Escalation can be outlined by applying these concepts to a variety of human intelligence examples.

---

[29] Selznick, P. 'The Idea of a Communitarian Morality' *Californian Law Review* Vol.75 No.1 (1987) p.447

[30] Erskine, T. *Embedded Cosmopolitanism: Duties to Strangers and Enemies in a World of 'Dislocated Communities'* (Oxford: Oxford University Press/British Academy, 2008) p.173

Section Three: Illustrative Examples

The previous two sections have demonstrated briefly the sort of activities being carried out by human intelligence operatives as well as highlighting the relevant ethical concerns likely to be raised by them. By combining the work done in these two sections with some illustrative examples, this section will demonstrate the varying levels of harm that human intelligence can cause.

Infiltration and Penetration

One of the most important jobs for an intelligence agency is gaining an insight into the activities, mentalities and personalities of their adversary. Only by gaining access to the adversary's home ground can the intelligence officer collect information or carry out other essential intelligence collection activities, such as recruitment, maintaining an agent or information transmission. In order to infiltrate or penetrate a target, intelligence officers are supplied with 'covers', a full or partial identity that hides offending parts of the operative's identity. In this section three types of cover will be discussed, that is, the use of 'official covers', 'unofficial covers' used against a state or society, and 'unofficial covers' used against a specific organisation or group. By outlining what each type of cover involves, providing illustrative examples and then applying the ethical framework established in Chapter One, it is possible to demonstrate the different levels of harm caused.

Official Cover

As Section One discusses, official covers have the benefit of giving the intelligence operative access to valuable sources of information through the normal diplomatic mechanisms associated with an official posting along with a genuine reason for being in a target country, while also maintaining a level of separation from any intelligence affiliations. During the Cold War, an essential core to U.S. human intelligence involved using official cover operations. For example, "in the late 1970s, the CIA station in London, the agency's largest liaison station, was staffed by some forty CIA officers who worked out of five offices – the Political Liaison Section; the Area Telecommunications Office... the Joint Reports and Research Unit.. the Foreign Broadcast Information Service; and the Office of Special U.S. Liaison Officer".[31] These officers had a variety of tasks including maintaining the intelligence network in the area, monitoring and facilitating the infiltration of illegal cover officers, the

[31] Richelson, J. T. *The U.S. Intelligence Community* (1995) p.245

recruitment of potential agents, working as the liaison between the embassy and the home intelligence team, as well as going on visits around the country in order to collect information from a variety of public sources.

Level of Harm

One of the necessary aspects of an official cover is that the intelligence officer deceives other people about his role as an intelligence operative. In doing so he misleads people in regard to the true intentions behind his activities and interactions. That is, the intelligence officer is intentionally creating a reality where he is not actually an intelligence officer in order that they treat him differently. In this sense, he controls other people's will in regards to himself.

The main victim of his lies, that is those who have their reality distorted the most, will be those individuals he intentionally interacts with and directly aims to influence. For the official cover officer this will most likely be either state officials or any one the operative decides to approach. For everyone else, however, although their view of him is the same as those he directly engages with, the officer's lies do not affect their view of reality in an important area. Therefore, their autonomy is not greatly affected. This demonstrates something important that was mentioned in the previous section in that there are different ways and degrees to which the view of reality can be distorted, and that depending on how and to what extent the target is deceived, the degree to which the autonomy is affected can change. Therefore, in most cases, the degree that this deception affects other people's autonomy is relatively limited. With official cover the officer's citizenship is clear and therefore his intentions are more apparent. This means that people interacting with the intelligence officer have a reasonable ability to make rational decisions in regards to some important information about the officer. Therefore the level of harm caused by official covers features at Level One on the Ladder of Escalation.

Unofficial Cover: Crossing Boundaries

Official cover, however, comes with some inherent obstacles. By expressing state affiliation the intelligence officer automatically sets alarm bells ringing for both other intelligence organisations and individuals with whom he might want to interact. Unofficial cover on the other hand completely removes the officer's true identity and replaces it with one that would make it impossible to know any part of his previous life or allegiances. As such, unofficial covers have the added benefit that they allow access to areas hitherto unavailable, including organisations and other states that would be wary of his home state association. Moreover, a

distinction can be made between two different instances where these unofficial covers are used, between gaining access to a target state or society and gaining access to a particular group or organisation. The former, gaining access to a state, involves getting through the border controls of a state, being able to gain residency, finding a job (quite often running a small business) and assuming the life of the average citizen. The individual is free to move about within the target state, often making no move to be 'noticed' by any particular party. In many examples, it is truly the agent's unobtrusiveness that becomes his strength. By contrast, those covers that are designed to gain access to a particular organisation, group or job require the officer to be noticed by this group, and for him to gain acceptance and trust from its members. While the fundamental principle of unofficial cover is similar for state and organisation infiltration, the methods, targets and actions may vary. As a result, the harm caused can also vary.

Level of Harm

There are a few different techniques for gaining access to another state. One of the most commonly used tactics during the Cold War was to send an officer through a third-party country, gaining residency there first so as to develop his legend before moving on to the main target. There are many examples of this type of infiltration throughout the Cold War. One of the first was a Soviet agent codenamed KONOV, a muscovite Greek who took the identity of Gerhard Max Kohler, a Sudeten-German born in 1917. As a war veteran and radio specialist he was sent to East Germany for four years to work as an engineer and establish his German cover while studying American and German cultures and language. The KGB then had him marry EMMA, a Stasi officer who took the name of Erna Helga Maria Decker. Posing as East German refugees, they crossed to the Federal Republic of Germany with the aim of moving on to America. After visiting America as a tourist, KONOV was able to secure a job under his assumed German identity and gain an immigrant visas. He worked the science and technology circuit and after seven years he and his wife were able to take the oath of allegiance and become American citizens.[32] A similar example is that of Reino Hayhanen who spent three years in Finland developing his identity as Eugene Maki before securing U.S. citizenship.[33]

[32] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999) p.248-9

[33] Andrew, C. and Gordievsky, O. *Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975-1985* (London: Sceptre, Hodder & Stoughton, 1993) p.94. Another means of developing a legend in order to gain access to a target country is to adopt the identity of someone who has passed away. Although this is often used in conjunction with entering the target state via a third-party neutral, this tactic has the benefit that

However, in some instances in order to gain access to certain places the intelligence officer must first secure the support of the target country's communities who are living in third-party states. For example, in order for Israeli intelligence to secure an agent within Syria it sent Eliaha Den Shaul Cohen, a Jew born in Alexandria in 1928 to Syrian parents, to Argentina first in order to make contact with the Syrian community there. Once in Argentina Cohen spent almost a year building himself up as a successful businessman, Syrian patriot and making as many Syrian connections as possible: "in addition to professing his patriotism, he became a well-known supporter of the local Arab newspaper and its editor; he established friendly relations with the Syrian diplomats and military attaché working out of the embassy and in particular Colonel Amin el-Hafaz".[34] When he announced that he had plans to make his move to Syria he was not short of having the right type of support to make his transfer as smooth and natural as possible.

As was the case with official cover, the vital interest violated when an officer assumes an unofficial cover is that of autonomy. Similarly, those individuals who come in contact with the officer under the unofficial cover are subjected to a series of lies and deceptions. They are interacting with the intelligence officer as the assumed persona and, as such, their view of reality in regards to him is distorted. By lying to other people the intelligence operative is controlling how others view him and therefore making them a tool of his will. What this means is that any decisions they make in regards to him are controlled by his lies and deception; he is encouraging them to act differently to how they would have otherwise acted.

For the Lonsdale, KONOV and Hayhanen cases, all of whom spent several years deceiving people so as to build up their 'legend', the harm caused is greater than official covers because anyone who interacted with them was interacting with the adopted identities, having no idea about their state affiliation. This means that the decisions of those who the

---

the legend is already more developed given the existing paper work and records that attest to the new identity's validity. For example, Gordon Arnold Lonsdale was the name of the dead double assumed by Konon T. Molody. After travelling to Canada to solidify his identity, Lonsdale then travelled to London and enrolled as a student on a Chinese course at the School of Oriental and African Studies. By using the identity of someone who was dead, Lonsdale was able to move with greater freedom than his true identity would ever have allowed him. Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999) pp.532-538. For other examples of how the agent develops his legend see: Nikolai Nikolayevich Bitnov who arrived in Canada in 1961 as Leopold Lambert Delbruck in Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999) pp.249-250. Dalibar Valoushok, a 33-year old Czechoslovakian border guard recruited by the KGB and the Czechoslavakian counterpart, the StB, took the identity of a Sudeten-German, Rudolf Albert Herrmann, who had died during the Second World War. See Allen, T. B. and Polmer, N. *Merchants of Treason: America's Secrets for Sale* (New York: Delacorte Press, c1988) p.90

[34] Richelson, J. T. *A Century of Spies: Intelligence in the Twentieth Century* (New York: Oxford University Press, 1995) p.283

intelligence officer interacts with are affected to a much greater extent. For example, people are likely to act differently in regards to someone who is from a friendly nation and who does not work for an intelligence agency than the reverse. However, a difference can be marked between those unofficial cover cases where the operative lies on a superficial level and those cases where deeper lies, designed to control or manipulate, are used. That is, it can be argued that for KONOV and Hayhanen the main targets of their lies were state border officials, whose autonomy was affected relatively significantly because their reality was distorted to a great effect in an area of importance. In comparison, even though they directly lied to their neighbours and friends, it can be argued that their lies were not designed to alter their autonomy to any great effect. The aim was to have the identity believed and to live an unassuming life, rather than to 'pump' anyone directly for information. In comparison, however, in the Cohen case, where he actively engaged and used the Syrian community, the deceptions used were designed to affect other people's autonomy to a much greater extent. Cohen actively went out and discovered the Syrian community, actively lied about who he was and his intentions behind the friendships he made, all in order to gain the community's trust and support.[35] He used his lies, his charm and the relationships he formed with people to influence their decision-making processes and encourage them to give him something they would not have otherwise given. Finally, by forming bonds with those who were members of the Syrian community through deception and manipulation, he betrayed their trust. By breaking these bonds of trust not only did he harm those individuals with which he was bonded, but also risked causing the whole community to lose trust in each other. The argument is that once a mole is found amongst one's own, suspicion and distrust are likely to be felt between all other members of that group.

Therefore, in the case of Lonsdale and Hayhanen, the level of harm caused features at Level Two on the Ladder of Escalation. In the Cohen case, on the other hand, as a result of the type of lie, the attempt to manipulate others and the effect that such actions can have on other individuals and social cohesion as a whole, the action features at Level Three on the Ladder of Escalation.

Unofficial Cover: Joining an Group and Becoming a Member

It can be argued that there is a distinction between using unofficial covers to gain access to another state and using unofficial covers to gain access to a specific group or organisation. The difference comes from the degree of deception and manipulation required to secure the

[35] Richelson, J. T. *A Century of Spies* (1995) p.283

membership. In order to become a member of a specific group or organisation the intelligence officer must use his false identity with the intent of creating interpersonal bonds and then use these bonds to his own advantage. By doing this the intelligence officer is able to gain access to the group, control its members and access information he would not be privy to otherwise.

For example, in 1956 Gunter Guillaume and his wife Christel, both HVA officers, had staged a carefully orchestrated escape from east Germany and set up a small business in Frankfurt to act as a cover for their intelligence activities. Once established they quickly became active anti-communists and members of the Socialist Democratic Party (SPD) and by 1968 Gunter Guillaume had been made chairman of Frankfurt SPD and an elected member of the Frankfurt city council. In November 1969 Guillaume gained a post in the Chancellor's office, initially as an assistant in dealing with trade unions and political organisations and then 1972 he was promoted to become the Chancellor's aid for SPD relations and to arrange the chancellor's travel arrangements.[36] Guillaume had been able to infiltrate the state's governmental infrastructure and gain acceptance.

During the Cold War communist subversion from within was one of the West's biggest fears. This meant that groups with socialist leanings, including political parties or trade unions, were targeted for intelligence infiltration. For example, British intelligence became significantly concerned with the activities, plans and personnel of the Communist Party of Great Britain (CPGB) and so issued officers to penetrate their inner walls. One of the most successful penetration officers for MI5 was Miss Olga Grey. Miss Grey was recruited by Maxwell Knight as a long term penetration agent. On Knight's instructions, Miss Grey started to attend CPGB meetings and was quickly employed as a secretary. Through this role she got to know both Harry Pollitt, the CPGB's general secretary, and Percy Glading, an officer who was later found guilty of espionage.[37] This was a tactic repeated by Knight, again with great success, with another of his female agents joining the CPGB as a secretary and who proceeded to pass records and documents to British intelligence for over a decade. In the end this second agent had managed to fill 32 volumes on internal activities.[38] MI5 operatives were also put inside trade unions, most notably the National Union of Mineworkers during the 1984-85 strikes: "these people were working within, sometimes actually employed by

[36] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane, 1999) p.578
[37] Twigge, S., Hampshire, E. and Macklin, G. *British Intelligence: Secrets, Spies and Sources* (Kew: National Archives, 2008) p.33; Andrew, C. *Defence of the Realm* (2010) pp.179-181
[38] Andrew, C. *Defence of the Realm* (2010) p.401

legitimate organisations, working for the good of their members in the trade union movement... and yet they had the dual role of reporting back to the Security Service certain aspects of what goes on within the union".[39]

Another penetration operation that is vital for any intelligence agency is the infiltration of the opposing state's own intelligence community. An example of this rare achievement was attained by the Czechoslovakian StB when in 1965 two StB illegals, Karl and Hanan Koecher, arrived in New York claiming to be refugees fleeing from persecution in the Czechoslovakia. Fluent in Russian, English, French as well as Czech, they were able to find a job easily working as a consultant for Radio Free Europe. By 1971 Karl succeeded in becoming a naturalised American citizen, his wife a year later. In 1973 Karl moved to Washington and obtained a job inside the CIA as a translator in the Agency's Soviet division with top-security clearance. Not long after he was asked to write intelligence reports based on material from the Soviet bloc.[40]

Level of Harm

Using an unofficial cover in order to infiltrate a group or organisation relies on the extensive use of deception, manipulation and exploitation of other people. Indeed, the difference between state and group penetration is the level and type of deceptions and manipulations that are often used. That is, state-unofficial cover mainly used passive deception, while with penetrating an organisation the intelligence officer must manipulate other people's perceptions of himself to a greater extent and put pressure on them in order to gain acceptance and information. The deceptions carried out are designed to distort the perceptions of those within the group in regards to who the intelligence officer is and what he wants from them. The autonomy of those within the group is violated as they are forced to make decisions based on the reality created by the operative. The reason why these deceptions are more harmful than those used for state infiltrations is the increased amount of lying and manipulation involved. Individuals are having more of their reality distorted and are being manipulated to a much greater extent in increasingly important areas of personal concern.

Additional harm is also caused because when the intelligence operative lies about his intentions for joining the group he not only betrays the trust they have in him but also the

[39] Hollinsworth, M. and Fielding, N. *Defending the Realm: MI5 and the Shayler Affair* (London: André Deutsch, 1999) p.62
[40] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999) pp.261-262

trust they have between each other. When deceit and betrayal is carried out within a closed organisation there is a greater impact on the bonds of trust that bind the organisation together. Moreover, the more close-knit the group, the more profoundly the betrayal is felt.

In the Olga Grey, Karl and Guillaume cases, they each lied about their intentions for joining the group as well as using people to get the access they needed. Miss Grey lied about why she wanted to join the CPGB and then manipulated people by feigning interest in communist ideals; Guillaume lied about why he wanted to join the SPD and manipulated his co-members; and Karl lied about to whom he held allegiance to in order to become an intelligence officer. Furthermore, not only did they deceive other people, but they also betrayed the trust the group had placed in them. This subsequent betrayal adds a further harm to the deceptions mentioned. However, since the degree of harm caused by breaking these bonds of trust is dependent on the characteristics of the group, it can be argued that there is a greater level of harm caused by Karl's infiltration and betrayal of an intelligence agency than the examples of trade unions or Grey's and Guillaume's party infiltration. This is because the level of trust seen within an intelligence agency is special. Very few organisations demonstrate a reliance on bonds of trust and interpersonal dependence to the same extent. The often 'life-or-death' scenarios officers face requires high levels of trust. Indeed, despite the ease intelligence officers show at deceiving, manipulating and betraying those in the outside world, within the group there is a high degree of reliance on comradeships and trust. Wolf, former head of the HVA, wrote on the special type of betrayal felt by intelligence agencies:

> Some people assume that a willingness to betray colleagues might make those who work in the intelligence immune to disillusion when betrayal happens among their own ranks. That is wrong. Betrayal is poison for every intelligence service.[41]

The poison of betrayal can then cause distrust, suspicion and increased monitoring of individuals, which can quickly cause a breakdown of the social cohesion felt within the organisation.

Therefore, with respect to Grey's penetration of the CPGB and Guillaume's penetration of the SPD, given that each lied and manipulated their way into a group, using the feelings and trust of others to their own ends, their actions feature at Level Four of the Ladder of Escalation. In the case of Karl and the infiltration of the close-knit community that is an intelligence organisation, given the wider harms to the organisation and the betrayal felt as

[41] Wolf, M with McElvoy, A. *Memoirs of a Spymaster* (1998) p.174

well as the increased degree of deceptive and manipulative acts, it features at Level Five on the Ladder of Escalation.

Recruitment: Gaining People

While being able to get one's own agents inside an adversary can open up many doors, such tactics are not the only way of getting this information. Indeed, instead of using their own operatives to infiltrate an adversary, intelligence agencies can also recruit those already on the inside. The actual recruitment process is somewhat of an art form, and the tactics used to create the right mental state required for a recruitment can be quite varied. What this section will do is to go through some of the main tactics and 'pitches' used and outline different levels of harm that can be caused.

The Direct Pitch

The first, and often the simplest and shortest recruitment tactic, is the 'direct pitch' whereby the intelligence operative approaches the target offering him something in exchange for his cooperation. Although this is a basic interpretation of the tactic, it demonstrates the principle of offering something in exchange for cooperation. To help ensure success, this tactic can be augmented by running a check on the target in the hope of discovering that he "has committed a minor legal transgression, has financial problems or needs a job", information that can be used as a means of initiating or influencing contact. However, if the target has no problems the intelligence agency can exploit then it is possible to manufacture one: "the position is created for a man so that MI5 can come along and help him out – a bit like breaking a man's leg so that you can offer him a crutch".[42] Obviously, one of the most common examples of this type of pitch is to offer money, but the offer could essentially be for anything, including "loans to relatives, consulting fees, gambling tips, inside information on a stock, or participation in a profitable business venture".[43] For example, in the instance of William Bell, the offer was made by looking into his personal history and discovering he had debts and then using this information as a means of getting him to co-operate. After he was arrested Bell was asked if he supported or had any political sympathies toward his recruiters,

[42] Hollinsworth, M. and Fielding, N. *Defending the Realm* (1999) p.59-60
[43] Epstein, E. *Deception* (1989) p.182

the Polish intelligence. "No", he replied, "Mr Zacharseci (his Polish handler) had found a fool who needed money. I had a weak spot. He took advantage of me".[44]

Level of Harm

When a direct pitch is made the target is approached and offered some benefit in return for his cooperation. This is essentially a bribe. The intelligence agency is using payment with the intent of altering the target's previously conceived will. As a result the interest that is violated is the target's autonomy. The bribe is used to indirectly influence or guide the target's decision-making process, steering him down a path he might not have otherwise travelled. The less opportunity there is to refuse the bribe the more harmful the action is because the degree his will is controlled is greater. However, the degree to which the bribe affects the individual's autonomy is generally, it can be argued, minimal. It is, after all, still a bribe and not extortion or blackmail; the individual will most often have room to decline. Therefore, if there is a reasonable option to turn down the bribe then it can be argued that the target's decision-making process is not hijacked but merely guided. This is, after all, not a discussion on the use of extortion, where the individual is threatened with "some harm in order to obtain" cooperation.[45] If it were, it could be argued that the individual has less room to resist (because of the fear of harm) and so his autonomy would be violated to a greater degree. Bribery, on the other hand, leaves the option (albeit sometimes slim) to resist and so the effect on the target's autonomy is less.[46]

In the case of William Bell, the money given was used as a form of pressure on his normal decision-making process; his will was directed down an avenue which, without the bribe, he would not have necessarily gone. However, given that what was being offered was something he could refuse, his autonomy was not fully usurped. He had a reasonable degree of control over his own will and it can be argued that he was reasonably able to resist the pressures placed on his decision-making process. In this instance, the direct pitch features at Level One on the Ladder of Escalation.

---

[44] Quote in Taylor, S. A. and Snow, D. 'Cold War Spies: Why they Spied and How they got Caught' *Intelligence and National Security* Vol.12 No.2 (1997) p.104

[45] See Black, H. C. *Black's Law Dictionary* 8th Edition (St. Paul MN: West Publishing Company, 1999) p.623

[46] For work on the difference between bribery and extortion see Carson, T. L. 'Bribery, Extortion, and "The Foreign Corrupt Practices Act"' *Philosophy and Public Affairs* Vol.14 No.1 (1985) pp.66-90; Khalil, F., Lawarree, J. and Yun, S. 'Bribery Versus Extortion: Allowing the Lesser of Two Evils' *The RAND Journal of Economics* Vol.41 No.1 (2010) pp.179-198; and Mayer, R. 'What's Wrong With Exploitation' *Journal of Applied Philosophy* Vol.24 No.2 (2007) pp.137-150

Emotional Manipulation

Other recruitment tactics involve creating the right mind-set in the target so that come the final pitch the target believes that cooperation is the correct course of action. The intelligence officer can employ a range of tactics to achieve this, though often it will involve exploiting the emotions or natural inclinations of an individual. Feelings created as the result of a bond of friendship, a sense of obligation resulting from a debt, or some existing resentment, anger, or other strong emotion can all be used by the intelligence officer to influence the target. For example, creating a friendship with the target means that he is less likely to see the final pitch as threatening, with the months leading up to the pitch being used to 'soften up' the target and gradually alter his opinions. This has the added benefit of the 'familiarity factor' whereby "eventually even the most cautious person drops his guard and forgets that the person he is talking to represents a foreign state".[47] Valuable intelligence can often be picked up from casual talk between friends. If the friendship is not enough to achieve the final conversion, however, the intelligence operative can build on it by carrying out some 'favour' so as to create a situation where the target becomes indebted to him. The sense of obligation to fulfil this debt can then be used as a lever on the individual's decision-making process.

Each of these tactics can be seen in the recruitment of 'Mr G': Mr G was a young diplomat who arrived in Moscow in 1953 to work in one of the Near Eastern Embassies. When he first arrived he found it very difficult to secure an apartment due to the bureaucratic processes being overly drawn-out. Soviet intelligence made the initial approach, having the operative establish a 'chance' friendship with Mr G. Once the friendship was established, Mr G commented on "how he was amazed at the slow civil service and how for three months they had not found him a flat"; feigning surprise the recruiter stated that he had some friends that might be able to help him out. A few days later the recruiter called him up and said that his friends had found him a flat. Due to this, the target was now indebted to the recruiter and their friendship had been deepened as a result. In this example, the intelligence officer was also able to use the familiarity factor:

> The conversations moved gradually on to political topics and I began to ask G. about his government's policy towards the Soviet Union... G answered my questions in a relaxed manner and talked more openly every time we met... he told me about the diplomats he knew who were working in the British, American and French embassies, about the matters they discussed, and so on.[48]

[47] Dzhirkvelov, I. *Secret Servant* (1989) pp.186-187
[48] Dzhirkvelov, I. *Secret Servant* (1989) pp.187

By establishing these bonds of friendship and then creating a situation where the target was indebted to the recruiter, the move towards converting him would be increasingly sweetened. Finally, the intelligence officer was then able to capitalise on the 'favour' he had created when, in 1954, a Soviet defector jumped over the wall into Mr G's embassy. The recruiter pointed out that those friends that had helped Mr G before were asking for something in return and that if Mr G was unable to help now then his friends would be in no position to help in the future; Mr G told the recruiter who the defector was and was even able to encourage the embassy to return him.[49]

Another case that involves the manipulation of an individual's emotional state is the recruitment of Abdoolcader, who was approached and recruited in 1967 while working in the Greater London Council motor licensing department. Born into a well-to-do Malaysian family, Abdoolcader had arrived in London ten years earlier to study at Lincoln's Inn. As a result of his repeated failure to pass his law exams and dissatisfaction with his social life he became steadily more bitter and resentful. In 1967, Aleksandr Savin, the recruitment officer, struck up an apparently chance conversation with Abdoolcader in a bar introducing himself as a Pole named Vlad who had lived in England for many years. After several more convivial pub evenings, with Vlad buying most of the drinks, he revealed himself as a Russian. Feeding off Abdoolcader's bitterness and the friendship he had built with him, Savin was able to get him to search the records at his work and provide the details of the individuals who drove cars of certain registration numbers, a number of which belonged to British intelligence, meaning that the KGB were able to identify who these officers were.[50] By exploiting an individual's "sense of personal dissatisfaction that stems from feelings or being overlooked, overworked and under-appreciated", the intelligence officer was able to create the right mindset needed for the final recruitment.[51]

Level of Harm

Using the emotions of someone can often prove to be a valuable lever for intelligence agencies. Exploiting an individual's bonds of friendship, feelings of obligation or even feelings of resentment or bitterness, the recruiter essentially interferes with the individual's normal decision-making process. For example, people will naturally lower their defences if they think they are dealing with a friend, or will become more willing to believe or help out a

[49] Dzhirkvelov, I. *Secret Servant* (1989) p.189-190
[50] Andrew, C. *Defence of the Realm* (2010) p.571
[51] Taylor, S. A. and Snow, D. 'Cold War Spies' (1997) p.107

friend as compared to a stranger. In the illustrative examples mentioned, the intelligence officer forms a relationship with the target and over time is either able to collect information through conversations or to capitalise on the feelings of friendship. Creating this friendship, however, relies on an extensive use of deception and manipulation by the intelligence officer. Not only is the intelligence officer lying about his identity, but also about the intention behind why he wishes to establish the friendship. Furthermore, the intelligence officer is then using the friendship and the associated feelings as a form of pressure to be applied to the target's decision-making process. Had the target known what the intelligence officer was really after when he started the relationship then the target might have acted very differently. Feelings of obligation can also act as a form of pressure on the decision-making process. The individual is made to feel indebted to the intelligence officer for some reason, and either the intelligence officer then explicitly uses this debt to get the individual to act in a certain way or lets the feeling of obligation influence the target's decisions. Furthermore, additional harms can be caused as a result of betraying those bonds the target creates with the intelligence officer. As already noted, individuals form morally worthwhile bonds with each other in order to define themselves, and in doing so they draw strength from these bonds. When these bonds are then manipulated or based on lies there is a great sense of betrayal.

This method of manipulating the emotional bonds of a target figured centrally in the case of Mr G. In this case, the intelligence officer struck up a friendship with Mr G based on a false identity and under false intentions. The intelligence officer's intentions behind this chance friendship were not as Mr G understood them – a genuine interest in Mr G for example – but rather were based in the intelligence officer's desire to use Mr G for his own ends. Mr G's ability to make decisions in regards to the intelligence officer was based on the lies he was told and, as such, his decision-making capacity, and therefore his autonomy, was altered. Furthermore, feelings of obligation and indebtedness were used as a lever on Mr G's decision-making process, pressuring him to return the favour: "Mr G did not know what to do. It was awkward for him to refuse to give me the information, but by providing it he would be breaking the law".[52]

Likewise, Abdoolcader had both his feelings of bitterness and resentment and any feelings of friendship exploited so as to guide his decision-making process. However, in comparison to the Abdoolcader case, it can be argued that the recruitment of Mr G caused a greater level of harm because Mr G's remained ignorant of his 'friend's' true identity,

[52] Dzhirkvelov, I. *Secret Servant* (1989) p.189

meaning that more of his reality was distorted resulting in a greater control over his will. So, while Abdoolcader eventually knew his recruiter's true identity before the final pitch, and was therefore able to make a more informed decision, Mr G. was not afforded this luxury. Therefore, with respect to the activities involved in the case of Abdoolcader the harm is Level Two on the Ladder of Escalation, whereas in the case of Mr G who was not aware of who he was dealing with, though still aware of the connection to an opposing state, the harm is on Level Three of the Ladder of Escalation.

Seduction

The use of seduction, love and even sex has long been an important tool in intelligence. This is because of the influence that affection towards someone can have on the individual. Most individuals are more likely to trust, think favourably of, or be open to those individuals they have fond feelings for, even if that individual is not treating them well. For intelligence, this bond of affection makes the target more malleable to the recruitment process. In comparison to the other pitches discussed, seduction involves targeting and exploiting an individual's core emotions, those most intimate to him, and therefore can cause a different type of harm than previously discussed.

The most infamous type of seduction is that of the 'Romeo agent', where an attractive male agent targets women who were lonely and use their loneliness to create feelings of love and affection. Once the target is enthralled with the Romeo agent these feelings can be used as a lever to influence the target's decisions. In the first illustrative example, the Romeo agent was able to exploit feelings of affection so as to ensure a successful direct pitch. Dagmar Kahlig-Scheffler was a divorced 27 year old western secretary who was hooked by a slender, young, blond East German calling himself Herbert Richter while on holiday in Bulgaria. They were quickly married in a ceremony that was orchestrated by East German intelligence. As a result of the boundless affection that she felt for him, Richter was able to make a direct pitch, telling her who he was, who he worked for and then persuaded her to carry out espionage for him. At his direction, she applied for jobs in the West German Foreign Ministry and at the Federal Chancellery in 1975, and then using a Minox camera she photocopied everything of interest that crossed her desk. As a result of the information she provided, East German intelligence was treated to highly confidential communications between Chancellor Helmut Schmidt and President Carter.[53] The second case is that of

[53] Colitt, L. *Spymaster: The Real Life Karla, His Moles and the East German Secret Police* (London: Robson, 1996) pp. 120-121

Lorraine DeVries, a lonely woman of fifty, who had long given up on any hope of marriage. But while working as a secretary at the Netherlands embassy in Moscow, she met a dashing Russian some ten years her junior, Boris Sergevich Kudinkin. After he had seduced DeVries he rang her in panic, informing her that the KGB had interrogated him about their relationship and claimed that they said they would ruin his career. DeVries agreed to help the KGB if they promised to keep the relationship a secret and leave Boris alone.[54]

The final example involves a 'false flag' case where the intelligence officer says he is working for a different country so as to encourage cooperation. In the example discussed here, Wolf sent Peter Krause to Bonn to seek out a lonely secretary who worked for the Foreign Ministry. Krause soon located Helge Berger, a newly arrived and lonesome individual. After winning her affections, he suggested that they go on holiday and once there he informed her that he was British Intelligence, SIS. She was relieved to hear he was an SIS agent and not East German or Russian intelligence. As a result of using this false flag coupled with the affections she had for him, she was willing to slip him secure documents. Until the very end she believed that she was working for British rather than East German intelligence.[55] It can be argued that her willingness to hand over the secure documents was heavily influenced by the emotional bonds that were created and exploited between her and Peter Krause, feelings built on a false identity and false intentions. In a similar case Roland G. targeted Margarete, a good Catholic who had spent her time working diligently at NATO and living the quiet life until Roland came along and spent considerable time and effort sweeping her off her feet. Roland took her on extravagant trips, evenings at the theatre and lavished attention on her in ways she had never before experienced. After the first night of sexual relations Roland "emptied his heart" to her, telling her that he was Danish intelligence and how Denmark felt left out of NATO and needed its own intelligence. She quickly agreed to help him by supplying NATO secrets, disclosing preparations and evaluations of the Alliances' military manoeuvres as well as any strengths and weaknesses.[56]

Level of Harm

As previously noted, there is something special about the harm caused in seduction cases. This is because, first, seduction cases require a greater degree of deception in the initial stages to secure the seduction and, second, seduction requires manipulating and exploiting

[54] Barron, J. *KGB: The Secret Work of Soviet Secret Agents* (New York: Bantam Books, 1974) pp.162-163
[55] Colitt, L. *The Real Life Karla* (1996) p.122, 126
[56] Wolf, M. with McElvoy, A. *Memoirs of a Spymaster* (1998) p.136

more deeply-felt emotions than in the other tactics. As such, seduction cases can cause a greater level of harm. An individual's 'love life', it can be argued, features at his most intimate level in that who he loves and trusts resides at the root of his sense of self. If a comparison is made to the type of bond made between chance friends, the level of intimacy made with a loved one and the emotions felt, it can be argued, are much closer to the individual's personal core, and are therefore more sorely felt when violated.

In Dagmar Kahlig-Scheffler's case, where the seduction was designed to encourage the success of a direct pitch, the target was willing to provide the information because of the pressure her affection was having on her decision-making process. She was harmed inasmuch as some of her most intimate feelings were used as a lever to influence her decision-making process for another's benefit. Dagmar did, however, know that the person making the pitch was an intelligence officer, meaning that she was afforded some measure of control over her decision-making process. In comparison, DeVries had no knowledge that her Romeo, Boris, was an intelligence officer. While her feelings of affection drove her to act as an agent, she did it while still believing Boris's cover. Therefore, her autonomy was affected to a greater extent because not only was she having her decision-making process influenced through the manipulation of her core emotions, but she also had her view of Boris distorted. However, she was still aware that the information she was passing on was going to the KGB so in this way she was aware of who was using the information and so there was still some ability to control the cost-gains analysis she had to make. In the cases of Helge Berger and Margarete, on the other hand, given that they were both unaware of whom it was they were working for and were actually encouraged to believe that they were working for someone else, their ability to control their own decision-making process was affected to a much greater extent. That is, they were unable to make a fully informed decision in regards to where their information was going and the damage it could cause. Therefore the level of harm caused was greater. In summary then, the harm in the Dagmar case is Level Three, whereas in the case of DeVries the harm caused is Level Four and the harm caused by the activities involved in the cases of Helge Berger and Margarete are at Level Five of the Ladder of Escalation.

Defections

The 'walk-in' or the 'defection' offers the intelligence agency one of the most lucrative opportunities for intelligence collection. A defection is simply where an individual comes to the intelligence agency, quite often by physically walking into an embassy or intelligence building, and offering either himself or information. During the Cold War examples of

defections from both sides of the Iron Curtain exhibited some of the most lucrative sources of intelligence. Unfortunately for intelligence collectors, however, these defections are hard to predict and there is significant pressure to ensure that when they do happen the intelligence agency is able to secure both the individual and the information. There are two types of defections, those who fully defect, leave the job and physically cross the boundary – 'defectors-in-fact' – and those who defect but remain in their job – defectors-in-place – passing information until they choose to fully and physically defect (at which point they become defectors-in-fact).[57] In some instances, the walk-in might demand a price for the information they possess – be it in money, sanctuary or other goods – but this is not always so.[58]

Some of the most note worthy, and also most famous, defections during the Cold War include – defecting from the Soviet bloc to the West – that of Oleg Gordievsky, Vasili Nikitich Mitrokhin and Oleg Penkovsky.[59] Each of these individuals was a defector-in-place for long periods of time until each of them fully defected some years later. For example, Colonel Oleg Penkovsky was deputy-head of the foreign section of the GRU and proved one of the most important defections for the British SIS during the Cold War. Even though his first few attempts to indicate his wish to defect were unsuccessful, since he held such a high position within Soviet intelligence and British intelligence feared that he was a KGB provocation, Penkovsky persisted until they believed his offer in 1961.[60] Analyses of the documents provided by Penkovsky over the years concluded that he delivered "unique information concerning the Soviet intelligence structure, new information on staff responsible for sabotage, subversion, and assassination... the identity of more than 300 soviet intelligence officers and over a dozen agents active in the West".[61]

---

[57] This distinction is made by Marbles, W. 'Psychology of Treason' in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal 1955-1992* edited by Westerfield, H. B. (New Haven; London: Yale University Press, 1995) p.74

[58] One study of reasons why defectors choose to take the plunge demonstrated that while money and financial gain featured as the main reason, 55.4% of the time, it is not ponderously so. Other reasons for defection include dissatisfaction with ones lot, the thrill of the life of a double agent, need to ingratiate or to feel wanted, or for political and ideological reasons. Ideology featured 23.7% of the time, ingratiation, 2.9%, disgruntlement 2.9% and 'other factors' include ego and need for excitement 12.2%. Taylor, S. A. and Snow, D. 'Cold War Spies' (1997) p.102-110.

[59] See Gordievsky, O. *Next Stop Execution: The Autobiography of Oleg Gordievsky* (London: Macmillan, 1995). The fruits of Mitrokhin's defection are illustrated through his publications: Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999).

[60] The Penkovsky case is told in numerous intelligence history books, including: Schechter, J. L. and Deriabin, P. S. *The Spy Who Saved the World: How a Soviet Colonel Changed the Course of the Cold War* (London: Brassey's, 1992); Andrew, C. *Defence of the Realm* (2010) p.493-494; and Richelson, J. T. *A Century of Spies* (1995) p.274-278.

[61] Schechter, J. L. and Deriabin, P. S. *The Spy Who Saved the World* (1992) p.195

In the other direction, defections from West to East, one of the most famous cases is that of Aldrich Ames. In March 1984 Aldrich Ames told his boss, Rod Carlson, that he wanted to see some action; he offered to start meetings with Soviets in Washington in the hope that it might perhaps lead to recruitment or two. According to a CIA investigation Ames stated that his primary motivation for his decision to commit espionage was his "desperation regarding his financial indebtedness he incurred at the time of his separation from his wife, his divorce settlement and his cohabitation with Rosario (his new wife)".[62] In April 1985 Ames made the decision to sell agency secrets to Moscow: "In exchange for $50,000 I provided the KGB with the identities of several Soviet citizens who appeared to be cooperating with the CIA inside the Soviet Union".[63] This was the beginning of what was to be long-term exchange of information for money and proved to be one the most beneficial defections for the Soviet bloc and one of the most costly for the Americans.

Level of Harm

With the walk-ins and defections the onus of acting is on the individual and not the intelligence agency. It is the decision of the defector to offer his services to the intelligence agency. The decision to make the approach is, therefore, that of the defector and is not the result of manipulation, deceit, encouragement or interference. The ability to make decisions is kept intact and the decision-making process is free from interference. The individual's autonomy is therefore left unaffected. He acts and therefore consents to the consequences of his actions.

Furthermore, while there might be some form of payment involved in the exchange of information – money, goods, paper-work – this payment is different from a bribe seen in previous cases. A bribe is used with the intent to alter an individual's choices, to interfere with the normal decision-making process. In the case of a defector the decision to defect has already been made; there is no outside force directly trying to encourage or interfere with the choice to defect. The defector has free rein to defect or not and the decision process is left free from interference. Where the harm can be caused is the betrayal felt by the group that the defecting individual has left. Depending on the type of group he belonged to and the importance of the bonds he had, by defecting he can both harm those individuals who relied on him as well as damaging the cohesion of that group as suspicion fills its ranks. However,

[62] Wise, D. *Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million* (New York: HarperCollins Publishers, 1995) p.113
[63] Wise, D. *Nightmover* (1995) p.115

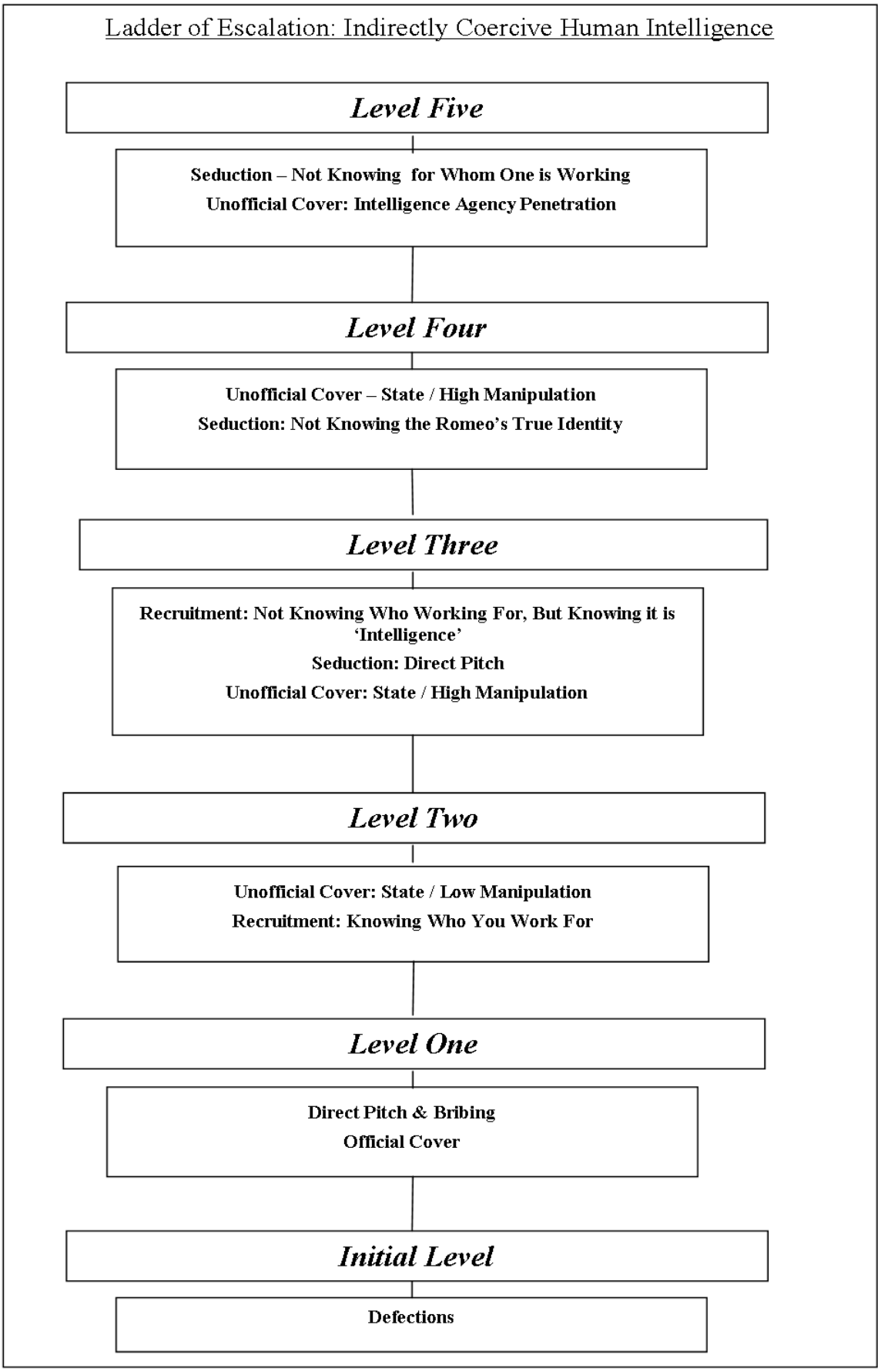
the harm that he causes by his defection is not the fault of the intelligence agency, but rather the defector. It was the defectors choice to change sides and betray his social group, rather than it being the result of some intelligence operation. Therefore, the harm caused remains with him rather than the agency. Therefore, accepting a defection features at the pre-level on the Ladder of Escalation, known as the Initial Level. However, this does not mean that by defecting the walk-in surrenders to all the harm that could befall him. By accepting the defector the intelligence agency is then responsible for those operations that they task for him. He becomes one of their own and therefore, even though he has defected, if they ask him to carry out some act which will cause harm then they are the source of that harm. Furthermore, by accepting the defection they become responsible for his safety as they would any other officer. This is most important for defectors-in-place who are risking themselves for the intelligence agency.

Conclusion

This section demonstrated the various levels of harm that indirectly coercive human intelligence can cause. Defections feature at the Initial Level since they do not affect the individual's autonomy; defections are essentially self-motivated. Using an official cover or a direct pitch are positioned at Level One on the Ladder of Escalation. Even though they each affect an individual's autonomy through different means – the former using a distorted view of reality to encourage the target to act in a particular way while the latter using incentives to influence the decision-making process – both have low impact on the individual's autonomy as he is still the main guide on his will. At Level Two, the use of unofficial state infiltration, where the agents become unassuming members of society, the degree and types of deception used are much greater. This is because, compared to official cover, the ability to control one's own will is circumvented to a greater extent as a result of the greater degree to which the individual's view of options are distorted. Also at Level Two is the case of Abdoolcader: he had his decision-making process interfered with by exploiting his feelings of bitterness and resentment, which means the level of harm is greater than that of a direct pitch, but in the end he is still aware of who he was working for. Therefore, compared to the recruitment of Mr G, the level of harm caused is less and Mr G features at Level Three on the Ladder of Escalation. With the use of seduction it can be argued that in the case of Dagmar that even though she was aware for who she was working, this was after a period lying and manipulation that was targeted at a more intimate part of her life. This is why Dagmar's case

features at Level Three on the Ladder of Escalation. Also at Level Three is the case of Cohen and his infiltration of the Syrian state through the manipulation and exploitation of the Syrian community of Argentina. Cohen manipulated and controlled the decision-making process of other people to a larger extent and in more important ways. The harm involved in cases of unofficial cover used to infiltrate a group is located at Level Four. This is because, in comparison to the unofficial cover of states seen at Level Three in the Cohen case, the degree and type of lying and manipulation used is much greater. Also at Level Four is the seduction of DeVries because she had an intimate part of her life exploited while also never knowing the true identity of her Romeo. She was therefore never really able to act in relation to a truthful version of reality and was always under the control of his lies. This means that she was harmed more in comparison to the Dagmar given that Dagmar was aware of who she was dealing with. However, if the DeVries case is compared the that of Helge Berger and Margarete, DeVires knew that ultimately she was passing information onto the KGB and so could understand the consequences of that action, whereas Helge and Margarete were never aware of who they were working for and therefore were harmed to a greater degree, and therefore feature at Level Five. Finally, also at Level Five is the infiltration of another's intelligence agency. In this case the degree of manipulation, deception and degradation of the bonds of trust as well as the wider effect these actions have on a group as close-knit as this one, means that the level of harm is one of the highest. What Figure 4.0 below shows is how the different activities involved in the so-called dark arts of human intelligence relate to each other in terms of the harm they cause the individual.

Figure 4.0


Ladder of Escalation: Indirectly Coercive Human Intelligence
Level Five
Seduction – Not Knowing for Whom One is Working
Unofficial Cover: Intelligence Agency Penetration
Level Four
Unofficial Cover – State / High Manipulation
Seduction: Not Knowing the Romeo's True Identity
Level Three
Recruitment: Not Knowing Who Working For, But Knowing it is 'Intelligence'
Seduction: Direct Pitch
Unofficial Cover: State / High Manipulation
Level Two
Unofficial Cover: State / Low Manipulation
Recruitment: Knowing Who You Work For
Level One
Direct Pitch & Bribing
Official Cover
Initial Level
Defections

Section Four: Just Human Intelligence

The previous sections of this chapter discussed those indirectly coercive activities human intelligence entails, outlining key features as well as some of the main concerns raised by its use and the various levels of harm that can be caused. In this section, the Just Intelligence Principles will be used to determine if these human intelligence activities can be justified. For each of the different human intelligence collection activities there will be a discussion of the required just cause, authority, proportionality and discrimination. Finally, this section will bring each of these assessments together on the Ladder of Escalation to illustrate how they compare to each other.

Infiltration and Penetration

Official Cover

As previously outlined, an intelligence agency will often send its officers into another country in the guise of state officials so as to gain access to both information stores and important individuals. It has been argued that, as a result, even though the intelligence officer is lying about his true occupation, individuals who come in contact with him are able to make a decision in regards to his state affiliation and, so, their decision-making process is only slightly affected. Therefore, official covers can be placed at Level One on the Ladder of Escalation.

Just Cause

For those activities which cause a degree of harm seen at Level One, there must be a *reasonable suspicion* of a low level of threat in order for there to be a just cause. In the international sphere this low level is often reached. This is because, as Klaus Knorr argues, "while international systems have been systems of cooperation, they have also been threat systems... the choice of conflict has been frequent over the millennia".[64] Therefore, invariably all states will pose at least a minimum level of threat. Even though this threat might be a limited in some instances, given the low level of harm official cover cause, this is a sufficient level of threat to justify its use.

[64] Knorr, K. 'Threat Perception' in *Historical Dimensions of National Security Problems* edited by Knorr, K. (Lawrence: University Press of Kansas, 1976) p.78

Authority

As with other Level One harms, the level of authority required to authorise the use of official covers is relatively low. That is, it can come from within the intelligence agency itself, for example officers who have responsibility for a particular operation. However, there should also be some form of oversight mechanism that exists to make sure that these individuals are acting in accordance with the Just Intelligence Principles.

Proportionality

The principle of proportionality maintained in this thesis takes into account the wider damages caused by intelligence collection. The harm caused by the deception must be outweighed by the good provided by the official cover. Moreover, it must also be determined if there are any additional damages caused by official covers that need to be included in the ethical calculation. For example, it can be argued that for official covers, the effect that discovering an agent can have on international diplomacy should be taken into account. That is, even though official covers have almost become an accepted part of international relations, finding an intelligence officer can always lead to strained relations between states even if the response is most often to export the individual as a *persona non grata* with little real fallout. However, if it is likely that discovering the agent will lead to severe and/or harmful consequences for the agent or the state then the calculation is altered.

Discrimination

Given that in the majority of cases, those who are under official covers will generally target those who are a part of the state infrastructure, the principle of discrimination can be satisfied. Those who are working in an official capacity for their government are legitimate targets because they have waived their protective rights by taking on a job within the state's infrastructure. Care, however, must be taken not to use or influence those who have not done anything to waive or forfeit their protective rights, for example the average citizen.

Unofficial Cover – State

In the previous section it was argued that there is a distinction between those unofficial covers that take up unassuming lives within a social group and those that directly interact and exploit people for their aims. The former, as a result of the degree and type of lies propagated and low level of manipulation, in comparison to the latter, cause a lower level of harm. This means that in many cases where unofficial cover is used to gain entrance to a state the harm

caused is Level Two. However in those instances where the intelligence officer is encouraged to interact, manipulate and gain the trust of people, then the level of harm caused is higher, a Level Three.

Just Cause

When discussing state penetration operations, the level of threat is determined by the threat that the targeted state represents. That is, the state being penetrated must represent a sufficient enough threat to justify the level of harm caused by acts of deception and manipulation. For Level Two harms the target state must represent a greater level of threat as compared to official cover. This means that there must be some reason for why that state is to be deemed a threat in some way, that is, to be neutral or hostile to the needs and concerns of one's own state. This means that 'friendly states', unless they have acted in some way as to promote a probable threat, are not likely to present a just cause for this type of infiltration. The cases discussed in this chapter are mainly drawn from the Cold War period, during which there was more than enough history of hostility between the West and the Soviet bloc to act as a just cause for a Level Two harm. Therefore, for the cases of Kohler and Hayhanen there was a sufficient just cause. For the case of Cohen, which caused a Level Three harm, clearly the threat required should be higher than in the other two cases, necessitating a hostile or potentially hostile state for a just cause. For Israel, Syria was a country which was increasingly becoming one of the most radical Arab states: "its politics, geographic proximity and large arsenal made it a major concern for the Israeli leaders"[65]; thus it represented a sufficient level of threat to act as a just cause. In comparison, however, if any of the cases had been between American and the United Kingdom, then the years of cooperation, openly friendly relations and lack of any immediate threat or issue would have meant that there was no just cause for the use of unofficial cover in this way.

Proportionality

Again, the principle of proportionality takes into account damages caused by the operation in addition to the harm caused to the target and argues that the good of the operation must outweigh these accompanying costs. Additional concerns for unofficial covers can include those problems that arise as a result of the intelligence operative being discovered, for example the damage it might cause to diplomatic relations. Given that unofficial covers often

[65] Richelson, J. T. *A Century of Spies* (1995) p.282

involve a much higher degree of fraudulent activities by the intelligence officer and the fear of having an illegal within one's own borders means that if discovered the repercussions could be much greater than that of official cover.

Discrimination

When an officer uses unofficial cover to become an unassuming member of a society, blending as much as possible into the background and attempting to become as unnoticeable as possible, the officer's lies are superficial inasmuch as they do not alter people's view of reality to any great extent in a vital area. Since the victims of those lies have their autonomy only partially affected, the need to be discriminating is reduced. Therefore they can be used against most people. In the case of the more direct lies which are designed to affect the target's view of reality to a greater extent or in an important field, the individual's autonomy is violated to a greater extent. This means that the officer should therefore only directly target those who are a part of the political system or similar.

In the Level Two cases of Kohler and Hayhanen, the main targets are state officials as they attempt to gain residency. Those officials are legitimate targets given their role within the state's infrastructure. In the Level Three Cohen case, he targets both illegitimate and legitimate targets as he spent considerable time making friends with and manipulating people of a particular community, many of which had done nothing to waive any of their protective rights and so were therefore illegitimate targets. However, some of the individuals with whom he was liaising were part of the political system, including Colonel Amin el-Hafez who was a Syrian politician, military officer and a member of the Ba'th Party. These individuals are clearly part of a military or political infrastructure which means they had tacitly waived their protective rights and were therefore legitimate targets.

Unofficial Cover – Organisation

The use of unofficial cover in order to gain access to a group or organisation will face many of the same issues discussed in the section on unofficial cover for state penetration. The difference, however, is that the level of lies and manipulation required is much higher and will therefore generally feature at a higher level on the Ladder of Escalation. In the Olga Grey and Guillaume cases and the other trade union penetration operations, the harm caused was Level Four as a result of the deceit and manipulation used. In comparison, in the Karl case, where the individual infiltrated an intelligence agency, the level of harm caused featured at Level Five on the Ladder of Escalation.

Just Cause

The level of threat a particular group poses can act as a just cause for investigating that group. For example, those groups that are more 'threatening' – advocating or practicing violence for example – provide a stronger just cause than those groups which are passive – carrying out peaceful protest for instance. By evaluating the group it is therefore possible to determine the level of just cause present. For those cases at Level Four, there must be a significant degree of threat from the group in order to act as a just cause. The level of proof required is such that the officer must bear the onus to prove to an objective third party that the threat is "more likely than not".[66] In the case of Olga Grey, who penetrated the CPGB, there was a sufficient just cause. This is because at that point in time, there was sufficient evidence to argue that this was an organisation that was politically and financially supported by the Comintern as well as propagating policies that would overthrow the government.[67] In comparison, in the case of Guillaume who infiltrated the SPD as well as instances where the British intelligence infiltrated trade unions, there is no sufficient just cause. In the Guillaume case, the SPD was a political party that posed no direct or violent threat. It had stayed within the legal limits of its role. Furthermore, even though trade unions were fielding some support from the Soviet bloc, there was no evidence to prove that they planned any violent action or proposed overthrowing the government. Being an annoyance to the British government is not a sufficient threat. However, had there been sufficient evidence that indicated that the group was planning violent activities then there would be a just cause.

In the case of Karl, who infiltrated another state's intelligence organisation and caused a Level Five harm, it can be argued that intelligence agencies are bodies which pose a significant level of threat by virtue of what they are and their mandate. However, given that an intelligence agency is part of a state, the level of threat it poses can be seen as a reflection of its parent state. Therefore, for states that have a history of antagonism, especially those whose intelligence agencies specifically also have a history of antagonism, the threat of the state as well as the organisation itself represents the just cause. During the Cold War, for example, relations between the Soviet bloc and the West, especially between their respective intelligence agencies, were such that an expressed degree of hostility was present. However,

---

[66] Kiralfy, A. *The Burden of Proof* (Abingdon: Professional, 1987) p.15-16

[67] The Communist International, or the Comintern, intended to fight "by all available means, including armed force, for the overthrow of the international bourgeoisie and for the creation of an international Soviet republic as a transition stage to the complete abolition of the State". From the Minutes of the Second Congress of the Communist International, *Evening Session* 4th August 1920. Available at http://www.marxists.org/history/international/comintern/2nd-congress/ch10a.htm Accessed August 2010

in an America-United Kingdom example, the long-term friendly relations would mean that there is no just cause for this type of infiltration.

Proportionality

Activities that violate different groups or organisations can often have wider repercussions on the domestic society or the system the organisation belongs to. If the group is a social movement or represents certain parts of society, for example, by infiltrating them the state runs the risk of alienating that particular group from the rest of society, which can have a negative impact on the coherence of the society as a whole. Similar to previous chapters where the importance of maintaining social coherence was highlighted, degradation of these social bonds can have a detrimental effect on the relationship between the state and its community, giving rise to fears of marginalisation, exclusion and aggressive tactics by the state towards different social groups.

Discrimination

When discussing penetrating a group or organisation, the principle of discrimination is determined by the character of the group or organisation itself. Those individuals who have joined the group have accepted the character of that group and in doing so opened themselves up to those dangers that the group represents. If, therefore, the group is one that has demonstrated that it is involved in activities that are threatening, then by being a member of that group they have waived their normal protective rights as well as becoming a contributing factor to that threat. Therefore, in the CPGB example, given that their activities were threatening, those who joined the group forfeited their protective rights and become legitimate targets. In the case involving infiltrating trade unions or legitimate political parties, given that the organisations themselves were not threatening, those who joined the group were not legitimate targets as they posed little or no threat.

Finally, those cases that involve infiltrating an intelligence agency, given that intelligence officers are groups of individuals who have ‘entered the game’ to the greatest extent as compared to any other group or individual, they are legitimate targets, even for Level Five harms. Therefore, in the case of Karl, those individuals who were members of the intelligence agency were legitimate targets.

Recruitment

The recruitment of individuals by intelligence agencies relies on an array of different activities and tactics, including the direct pitch, a range of manipulative tactics and preying on an individual's emotional weaknesses. The levels of harm caused can vary according to the type and degree of deception and manipulation used.

Making the Pitch

Just Cause

The use of a 'direct pitch', since it involves the intelligence officer going up to a target and asking him to cooperate, normally in exchange for money or some other favour or goods, features at Level One on the Ladder of Escalation. For Level One harms, the individual approached should represent some level of threat to act as a just cause, however this threat might be relatively low and there only needs to be a *reasonable suspicion* of its veracity. This level of threat might be a reflection of the individual himself or the organisation/state to which the target is directly connected. For example, in the international system, given that most states represent even at a minimum some level of threat, there is reason for direct pitches to those directly connected to the organisation/state.

Those activities that rely on manipulating an individual's emotional weaknesses – manipulating bonds of friendship or pushing emotional levers – the level of harm caused is much greater, ranging from Level Two to Level Five depending on the circumstances. In the case of Abdoolcader, who had his bitterness towards the his circumstances, and therefore the British system, as well as his feelings of friendship manipulated, the harm caused was Level Two since he was eventually told the truth and so was able to make a more informed decision. Therefore, the individual or associated state/organisation, must represent a more substantial threat than that seen with the direct pitch. For Abdoolcader, even though the organisation he works for is not central to the state's infrastructure, given the history of hostility between the East and the West and the relatively low level of harm, it could be argued that there is a just cause. For the case of Mr. G, which was a Level Three case, it can be argued that the level of harm was not justified. The threat for a Level Three harm has to be something of importance or has the ability to cause a reasonable amount of destruction. The state/organisation for which Mr G worked, however, did not necessarily represent this level of threat. If there was a belief of an upcoming operation, or there were significant tensions between the two countries or the organisation for which he worked represented a particular

threat, then there would have been a just cause. But given that Mr G worked for an embassy – which posed no direct threat – of a country with which there was passable relations means there was no reason to fear a threat and therefore no just cause.

Discrimination

In order to determine to what extent those targeted for recruitment are legitimate targets or not, the character of the organisation they belong to or the role they play in a state's infrastructure should be considered. In the case of Abdoolcader, given that the harm caused was relatively low at Level Two and that he had placed himself in the political infrastructure meant that he was a legitimate target in this instance. However, if the case had been that the level of harm were any higher than Level Two and if the organisation he worked for were on the periphery of the state infrastructure, he would have been an illegitimate target. In comparison, Mr G worked for his state's embassy and so was aware of his role in the state's infrastructure, as demonstrated by the type of information he was able to convey when he was asked. As such, even for the higher Level Three harm caused, Mr G's role in the embassy meant that he was a legitimate target. However, given that he was still a junior member of his Embassy, had the level of harm been any higher, he would have been an illegitimate target.

Seduction

The use of seduction is a special case where very intimate, core feelings are manipulated by the intelligence officer in order to gain information. In this way, the level of harm is greater and is reflected in the distribution of activities up the Ladder of Escalation.

Just Cause

For those direct pitches that rely on the use of seduction to influence the target the harm caused is Level Three. This means that there must be a medium level of threat, that is, the threat is targeting something of importance or has the ability to cause a reasonable amount of destruction. At this level there must be evidence that 'on a balance of probabilities' a threat exists. In the case of the Dagmar Kahlig-Scheffler, the climate between the Soviet bloc and the West was one of overt hostility and therefore a sufficient level of threat for a Level Three harm. In comparison, in the DeVries case at Level Four there is no just cause for the activity. This is because the state she was associated with was not directly or overtly hostile. Working for the Norwegian embassy, there lacked the same institutional and political tension. Had she

belonged to a state which represented more of a threat or the tactics used caused a low level of harm then there would have been a sufficient level of threat present.

In the last two cases, that of Margarete and Helge Berger, the harm caused is a Level Five. In both cases the targets worked for states or organisations that were overtly hostile or represented a threat to state interests and therefore represented a sufficient just cause. For example, Margarete worked for the military organisation NATO and Helge Berger worked for the West German Foreign Ministry, both of which, it can be argued, represented an actual threat for Soviet interests. Furthermore, the organisations or departments, both military based, were central to the role of the threat.

Discrimination

In order to satisfy the principle of discrimination, the target must have done something to waive the normal protective rights. In the case of Dagmar Kahlig-Scheffler, she was unemployed when the Romeo agent seduced her and made the direct pitch. She, therefore, was not a part of any state infrastructure, meaning there is no evidence that she had acted in a way that indicated that she had voluntarily given up her protective rights or that she was a particular threat. Therefore, at Level Three she was an illegitimate target. In order for her to be a legitimate target for an operation that caused a Level Three harm she would have had to be have worked for an organisation belonging to a state or group which represented a direct threat.

For those activities where the harm caused is Level Four, the target must be both from a state that is threatening in some substantial way as well as part of the state's infrastructure. In the case of DeVries, therefore, she is a legitimate target. This is because she worked for her state's Embassy and so was well aware of her position in the state's infrastructure and what was expected of her in her position of responsibility.

In the case of Margarete and Helge Berger, the type of organisations or departments for which they worked meant that they had both taken on jobs that were central to the state or belonged to a military organisation and in doing so had taken on positions of responsibility and had thus waived their normal protective rights. However, it can be argued that they were not sufficiently far enough up the ladder to be targeted for such an operation. Therefore, at a Level Five harm they represent illegitimate targets.

Defections

Of the human intelligence collection cases discussed in this chapter, defections represent the lowest level of harm caused. Receiving a defector should be placed at the Initial Level on the Ladder of Escalation. Therefore, there is no need for a just cause, authority or discrimination.

Conclusion

Human beings naturally form relationships with each other and often these relationships play a huge role in their lives. What is important for intelligence collection is being able to exploit these relationships to the advantage of the operative. What this chapter has demonstrated is that through various deceptions and manipulations it is indeed possible, for the talented intelligence operative, to get people to do and believe almost anything. However, exploiting one's fellow man does not, unsurprisingly, come without a price. Coercing people, even indirectly, comes into conflict with their vital interests, namely that interest in autonomy. The manipulations and deceptions outlined in this chapter by necessity guide, encourage or influence the decision-making process of the target in a direction he would not have otherwise gone and to the benefit of the intelligence operative. It was also shown that depending on the degree that the individual's normal decision-making process is hijacked, the level of harm caused can vary. As a result, limitations on the exploitative nature of human intelligence have been established. The Just Intelligence Principles provide these limitations while also making it clear when the actions are justified. Clearly, indirectly coercive human intelligence has its place in the world of intelligence collection, and this chapter has given an idea of what this place can look like. In the next chapter human intelligence collection activities that are directly coercive will be examined. It will explore those actions carried out by human intelligence operatives which directly force another individual into complying with their needs, outlining both the harm this can cause to the individual and discussing whether this harm can be justified or not.

Chapter Five: Coercive Human Intelligence

The previous chapter on human intelligence made it clear that there were several sources and forms of information only accessible to human beings, either by using the intelligence operative to access a particular area, group or individual or by using certain tactics to encourage others to divulge the information. However, the previous chapter also noted a distinction between human intelligence that is 'indirectly' coercive – where the target is indirectly influenced and guided – and human intelligence that is 'directly' coercive – relying on direct force and ultimatums. While the previous chapter focused on the indirectly coercive activities in human intelligence, this chapter will examine directly coercive methods, mainly the use of blackmail and torture. Similar to previous chapters, Section One will outline some definitions and parameters for blackmail and torture, followed by a discussion of how these activities might cause harm in Section Two. In Section Three, illustrative examples will be outlined in order to show how these activities are used in greater detail and the particular level of harm caused by each example. Finally, in Section Four, the Just Intelligence Principles will be applied as a means of showing if and when these particular intelligence collection activities are justifiable.

Section One: Coercive Human Intelligence

Throughout history torture has been used as a tool of the state. It has been used as a means of securing a confession or gaining information, to punish those who transgressed or as a means of deterring and intimidating those who might resist the authority of the state.[1] Similarly, blackmail has proven itself to be a potent instrument for both states and individuals as a means of controlling people for some gain. Indeed, torture and blackmail both have the potential to be powerful means of encouraging even the most reticent to comply. It is therefore not surprising that many powers have put a lot of effort into perfecting these as tools. In this first section blackmail and torture will be examined in order to outline what actions are employed under these two type of activities so as to give a better understanding of what is happening to those targeted.

Blackmail

Throughout history various legal authorities and canons have spent considerable time examining and discussing what blackmail entails and why society should prohibit its use.[2] As it currently stands, the legal definition of blackmail highlights four key points. First, the blackmailer makes an unwarranted demand; second, the demand is made with menace; third, the blackmailer acts with a view to gain for himself or another with the intent to cause a loss to the target; and finally, the blackmailer does not believe that he has reasonable grounds for making the demand or that the use of menaces is a proper means of enforcing the demand.[3] In breaking down this definition it can be seen that there is a clear threat or demand being made

[1] See Langbein, J. H. *Torture and the Law of Proof: Europe and England in the Ancien Régime* (Chicago; London: University of Chicago Press, 1977); Parry, L. A. The History of Torture in England (Montclair, N.J: Patterson Smith, 1975); and Scott, R. *History of Torture Throughout the Ages* (Montana: Kessinger Publishing, 2003)

[2] Prior to the nineteenth century, the crime of blackmail was considered to fall under the banner of robbery and theft, whereby an individual had his property taken from him without his consent through threats – the classic 'your money or your life' case. Over the years, however, the understanding of blackmail has grown in both depth and breadth. No longer does blackmail necessarily involve an illegal threat and the theft of another's property. Rather, blackmail can involve supplicating oneself to another's will in order to prevent the disclosure of embarrassing or damaging information. The case of, 'do as I say or I shall tell your wife about your affair'. See Allridge, P. 'Attempted Murder of the Soul: Blackmail, Privacy and Secrets' *Oxford Journal of Legal Studies* Vol.13 No.3 (1993) pp.368-387; Coase, R. H. 'Blackmail' *Virginia Law Review* Vol.74 No.4 (1988) pp.655-676; Helmholz, R. H. 'The Roman Law of Blackmail' *Journal of Legal Studies* Vol.30 No.1 (2001) pp.33-52; Herring, J. *Criminal Law: Texts, Cases and Materials* (Basingstoke; New York: Palgrave Macmillan, 2009) p.630; Isenbergh, J. 'Blackmail from A to C' *University of Pennsylvania Law Review* Vol.141 No.5 (1993) pp.1905-1933; and Winder, W. 'The Development of Blackmail' *The Modern Law Review* Vol.5 No.1 (1941) pp.21-50

[3] For example most people would think that the threat that 'unless you return the item I lent you I will come round and take it' is reasonable. The application of the menaces (the taking of the object) in this case is therefore reasonable.

by the blackmailer; it is the 'give me or else' part of the act, though how the demand is made can vary.[4] The second point about blackmail is that it involves a gain to the blackmailer or a third party and a loss to the victim. That is, blackmail will involve something being given, whether it is money, services or information. Finally, the demand must be made with 'menaces', a threat of an action detrimental or unpleasant to the person being addressed, although the menace itself does not have to be illegal. Furthermore, these menaces of a threat should be not be minor, in that "the mind of an ordinary person of normal stability and courage might be influenced or made apprehensive so as to accede unwillingly to the demand".[5]

There are, however, several different formats these criteria can take. For example, emotional blackmail, physical blackmail, information blackmail, entrapment blackmail, economic blackmail, et cetera are all different forms of blackmail, changing in response to the threat made or the gain requested.[6] For this thesis the main focus will be on information and entrapment blackmail. Information blackmail is where the "sale of silence by someone who is otherwise free to disclose what he knows" is used in order to get the target to capitulate in some way. Entrapment blackmail involves the target being manipulated and ensnared within a trap designed to provide the information that then forms the basis for the blackmail.

Torture

From its birthplace in the ancient Greek and Roman legal systems, through medieval times and up to the eighteenth century, torture was used in continental European legal proceedings as a means of securing confessions from people, known in the hierarchy of proofs to be the "queen of proofs" as its results were considered beyond reproach.[7] Torture has also been employed as a tool of intimidation and punishment by some regimes so as to instil fear, exert domination, and to punish those who pose a threat to the authority. The study of torture is therefore often broken down into terms of whether it is being used to intimidate, secure a

[4] For example, if Oliver stopped Archie in a dark street, pointed a knife and said 'would you like to give some money to a good cause', this could be regarded as much as a demands as a request. But if an individual offers the money voluntarily, then it is not blackmail: for example, Wendy sees Peter commit a crime and Peter offers money to Wendy to keep quiet is not blackmail. Herring, J. *Criminal Law* (2009) p.630
[5] Herring, J. *Criminal Law* (2009) p.631
[6] Hepworth, M. *Blackmail: Publicity and Secrecy in Everyday Life* (London: Routledge, 1975) p.8
[7] Peters, E. *Torture* (New York: Basil Blackwell, 1985) p.41

confession, carry out punishment or interrogate.[8] While each of these forms of torture are worthy of investigation, they are not all the direct concern of this thesis. Only torture as an interrogation tool, with the specific goal of collecting intelligence information, is the focus. While it can be argued that all forms of torture are politically motivated, and therefore it is impossible to escape some intimidation, for simplicity this thesis will focus on its interrogational aspect, though some consideration will be given to the side-effects when appropriate.

Definitions of torture through the ages have changed little. From Roman jurists of the second and third century to modern day philosophers and lawyers, those who have taken the most trouble to consider the question of what torture is have come up with remarkably similar answers. Third century jurist Ulpian declared: "By *quaestio* [torture] we are to understand the torment and suffering of the body in order to elicit the truth. Neither interrogation itself, nor lightly inspired fear correctly pertains to this edict. Since, therefore, *quaestio* is to be understood as force and torment".[9] Contemporarily, the most prominent definition is that set down in the Geneva Convention Against the Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, stating torture as

> Any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person.[10]

In addition, this convention also binds its signatories to "prevent other acts of cruel, inhuman or degrading treatment or punishment that do not amount to torture".[11] What can be understood from these definitions is that there is a level of suffering inflicted on the individual that is above and beyond that seen in almost any other activity. Furthermore, it is clear that torture is not just about physically attacking someone's body, but also about the psychological or emotional attacks one can suffer.

---

[8] Guiora, A. N. and Page, E. M. 'The Unholy Trinity: Intelligence, Interrogation and Torture' *Case Western Research Journal of International Law* Vol.37 (2006) p.249. For example, David Sussman only explores 'interrogation' torture in his article making it clear the end objective as special. Sussman, D. 'What's Wrong with Torture?' *Philosophy and Public Affairs*, Vol.33 No.1 (2005) p.4; and Wisnewski, J. J. *Understanding Torture:* (Edinburgh: Edinburgh University Press, 2010)

[9] Peters, E. *Torture* (1985) p.1

[10] *Geneva Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, United Nations, 10 December (1984) Part 1 Art. 1 § 1

[11] *Geneva Convention Against Torture* (1984) Part 1 Art. 16 § 1

However, while these definitions give the broad understanding that torture involves severe torment of an individual, what they fail to elucidate is what exactly torture involves, how it works or what makes it 'torturous'. By highlighting some of the underlying principles and mechanisms of torture, not only can the act of torture itself be better understood, but also the affects it can have on the individual and the types of activities employed.

Torture: Mechanisms of Conditioning

The first point for understanding how torture works is recognising it as a specialised form of operant conditioning.[12] After the Korean War a psychologist called Albert Biderman worked to challenge the myth about the ability of Chinese officers to use mystical means to break detainees, and, along with I. Farber, Harry Harlow and Louis West, outlined a system called DDD – Debility, Dependency and Dread – that explained detainee compliance.[13] Using conditioning theory as the basis of their analysis, they argued that the physical, social and emotional conditions created by the three Ds, can be used to, first, break down any resolve or resistance the individual might have, while, second, conditioning his responses. Although torture is rarely as scientific as this, understanding how the mechanisms work upon the human psyche is essential to understanding the main characteristics of torture. *Debility* is designed to attack the body so as to deliberately induce physical and mental weakness in the target. This can be caused, for example, through the use of "noxious stimulation, injury, disease, malnutrition, deprivation, sleeplessness, fatigue... and chronic physical pain".[14] Through the use of physical, psychological and emotional attacks the torturer breaks down any resolve of the target. Furthermore, these attacks act in order to condition the individual into associating resistance with highly negative results.

[12] Operant conditioning is a method of learning that occurs through rewards and punishments for behaviour. Through operant conditioning, an association is made between behaviour and a consequence for that behaviour. 'Reinforcement' and 'Punishment', the core tools of operant conditioning, are either positive (delivered following a response), or negative (withdrawn following a response). This creates a total of four basic consequences: *Positive reinforcement* occurs when a response is followed by a stimulus that is appetitive or rewarding, increasing the frequency of that behaviour; *Negative reinforcement* occurs when the response is followed by the removal of an aversive stimulus, thereby increasing that behaviour's frequency; *Positive punishment* occurs when a response is followed by a stimulus, such as introducing a shock or loud noise, resulting in a decrease in that behaviour; *Negative punishment* occurs when a response is followed by the removal of a stimulus, such as taking away a child's toy following an undesired behaviour, resulting in a decrease in that behaviour. Through selected application of these tools the individual can be conditioned to respond in the correct way. See Skinner, B. F. *The Behavior of Organisms: An Experimental Analysis* (Appleton-Century-Crofts Inc, 1938) p.61

[13] Biderman, A. D. "Communist Techniques of Coercive Interrogation" Air Force Personnel and Training Research Center Development Report Vol.132 (Lackland Air Force Base, Texas, 1956); Farber, I., Harlow, H. and West, L. 'Brainwashing, Conditioning and DDD' *Sociometry* Vol.20 No. 4 (1957) pp.271-285

[14] Farber, I et al 'DDD' (1957) p.272, 273

Prolonged deprivation of life's essential factors is then made more poignant by periods of occasional and unpredictable respite, reminding the victim that the torturer is able to alleviate the pain if he so wishes. This creates a paradoxical *dependency* upon the torturer; the victim is brought to believe that his fate is entirely within the hands of the torturer.[15] This demonstrates another essential characteristic of torture, that it involves a special, asymmetric relationship between victim and torturer. The victim must realise that he is completely at the mercy of the torturer.[16] The victim is completely defenceless and open to constant attack.[17] As a result of this asymmetric relationship, the victim starts to feel obliged to the torturer both as his punisher and saviour. This acts as a positive reinforcement to encourage cooperation. Essentially, favourable responses are met with favourable repercussions, and unfavourable responses are met with unfavourable repercussions. Through punishment both physical and psychological, coupled with select moments of relief and constant variation in the treatment in order to stop the victim from seeing through the ordeal, statements like "you can go sleep now, we'll start again tomorrow", provide positive motivation for compliance.[18]

The final element, *dread*, is not applied directly during the sessions, but is the fear that is experienced between the sessions. As Farber notes, dread is the most expressive term to indicate the chronic fear that they feel: "fear of death, fear of pain... fear of deformity or permanent disability... and even the fear of one's own inability to satisfy the demands of insatiable interrogators".[19] Even in the down-time, when the torturer is not around, the individual is not given respite; the torture continues and therefore the individual is unable to build himself back-up, to offer renewed resistance come the next session.

By combining each of these factors through selective reinforcement of certain responses and the punishment of others, the use of torture is designed to break any resolve the target has while conditioning him to cooperate. The conditions created by DDD provide the means for selectively reinforcing certain modes of response.

Mechanisms for Compliance: Every Man Has His Breaking Point?

Since torture aims to break down an individual's resistance and resolve, while both negatively and positively reinforcing certain responses, it is possible to indicate the sort of

[15] Suedfeld, P. *Psychology and Torture* (New York; London: Hemisphere Publishing Corporation, 1990) p.3
[16] Sussman, D. 'What's Wrong with Torture?' (2005) p.6
[17] This distinguishes torture from many other forms of violence, since most relationships involve the ability to retreat, defend or attack back.
[18] Amnesty International, *Amnesty International: Report on Torture* (London: Duckworth, 1973) p.51
[19] Farber, I. et al 'DDD' (1957) p.273

activities that might be employed by the torturer. What this section will examine is the arsenal of the torturer in respect to the physical and psychological limits of the human body.

Given that the human brain is both the repository for the individual's knowledge as well as the organ that controls all human functioning, it is in many ways the main target for the torturer. As an organ the brain can only operate "optimally within the same narrow range of physical and chemical conditions" and as such "any circumstance that impairs the function of the brain potentially affects the ability to give and withhold information".[20] Therefore attacks that affect the brain or its environment are crucial to torture.

Homeostasis

The brain, like any organ, exists and relies on an internal milieu maintained by and dependant on a complex variety of chemical and environmental factors. Homeostasis refers to the body's ability to regulate the inner environment so as to ensure stability in its normal operations in response to any fluctuations in its environment. Any disturbance in the consistency of this milieu can bring homeostatic imbalance that can severely impact the body and normal brain function.[21]

One of the most important factors in maintaining this equilibrium is body temperature. The temperature of the human internal environment is maintained as near to 37.5°c as possible; an elevation to 41°c or below 31°c will nearly always impair normal brain function.[22] This internal equilibrium is also dependent on the level of both organic and inorganic compounds in the blood stream, and any disturbance in the concentration of the level of either of these can have a direct impact on the brain's normal ability to function. For example, excessive sweating, deprivation of water, diets high or low salt, ingestion of excessive amounts of water, inducing vomiting, diarrhoea, burns, shock caused by injuries, haemorrhages or damage to the kidneys, can all cause the levels in the body's internal chemistry to alter dramatically. Changing the body's chemistry in this way can result in what is referred to as 'brain syndrome', an impairment of the brain's functions across the board.[23] In the first stages the individual might experience "pain, fatigue, thirst, hunger, drowsiness...

[20] Hinkle, L. E. 'The Physiological State of the Interrogation Subject as it Affects Brain Function' in *The Manipulation of Human Behaviour* edited by Biderman, A. D. and Zimmer, H. (New York; London: John Wiley & Sons Inc, 1961) p.20

[21] The awkward term 'brain function' is used because no other word denotes all the complex activities that the higher centres of the brain makes possible.

[22] Hinkle, L. E. 'The Physiological State' (1961) p.20

[23] Brain syndrome is also referred to as 'organic reaction syndrome ', 'symptomatic psychoses, 'toxic infectious exhaustative state' or 'psychosis with somatic disease'.

he may lose the capacity to carry out complex responsibilities accurately, speedily, effectively and plan his activities... he is likely to become emotionally liable, irritable, depressed, jumpy and tense". As the brain syndrome develops the subject's stress levels increase rapidly and, as a result, the subject is likely to suffer sensory experiences, illusions, delusions, hallucinations, or paranoid thinking.[24]

Affecting the Brain as an Information Processor

The brain as an organ is one that deals with information, and as such has become dependent on and sensitive to the types of information it receives. The accumulation and transmission of information through the highly developed nervous and sensory systems found in all human beings is fundamental. Indeed, depriving or overpowering these sensory systems can have severe effects on the brain's normal functions: "deprive the brain of information and it does not function normally... it must have a certain quantity of patterned, meaningful, sensory input from the external environment".[25] For example, isolation, sleep deprivation and fatigue are three factors that can have adverse affects on the brain's normal functioning. An isolation experiment carried out by Donald Hebb between 1951 and 1954, for example, involved putting a 22-year old male in a cubical for twenty-four hours without any sensory stimuli – muted light diffused by translucent goggles, auditory stimulation limited by soundproofing and constant low noise and tactile perception blocked by thick gloves and a U-shaped foam pillow about the head. After just two days Hebb found that the subject's very identity had begun to disintegrate and he suffered eerie hallucinations akin to the drug mescaline as well as deterioration in his capacity to think systematically.[26] Similarly, sleep deprivation has proven itself to be a powerful means of affecting an individual's ability to think properly. The brain, for reasons not yet fully known, cannot function properly without occasional periods of sleep. Indeed, most people deteriorate after about seventy two hours without sleep and the higher functions are the first to go: speech, behaviour, delusions, hallucinations, emotional liability, disorientation and intellectual functions.[27]

---

[24] Hinkle, L. E. 'The Physiological State' (1961) p.25

[25] Hinkle, L. E. 'The Physiological State' (1961) p.27

[26] Hebb, D. O. 'Experimental Deafness' *Canadian Journal of Psychology* Vol.8 No.3 (1954) p.152-56. Also see, Bexton, W. H. Heron, W. and Scott, T. 'Effects of Decreased Variation in Sensory Environment' *Canadian Journal of Psychology* Vol.8 No.2 (1954) pp.70-76. For more information on mescaline and its affects see Hoch, P. H., Cattell, J. P. and Pennes, H. H. **'**Effects of Mescaline and Lysergic Acid (d-LSD-25)' *The American Journal of Psychiatry* Vol.108 (1952) pp.579-584

[27] Edwards, A. S. 'Effects of Loss of 100 Hours' Sleep' *American Journal of Psychology* Vol.54 (1941) pp.80-91; Laslett, H. R. 'An Experiment on the Effects of Loss of Sleep' *Journal of Experimental Psychology* (1924) Vol.7 pp.45-58

Finally, the use of hunger and physical pain are powerful mechanisms for attacking the brain. Inflicting pain is probably one of the first things people think of when torture is mentioned, and this is for good reason. Inflicting pain on an individual involves attacking him on a fundamental level. Pain is one of those sensations that is so aversive to the body that it completely encompasses an individual's entire world view; he is brought to his physical limits as the body cries out to stop whatever is causing the pain.

As for using hunger as a means of attack, it has been seen in starved populations,[28] among inmates in concentration camps[29], prisoners of war[30] and reproduced experimentally[31] that people deprived of food very soon develop persistent hunger that can directly affect their behaviour. As starvation progresses and the threat of death comes closer, the behaviour of the individual starts to be governed by the desire for nutrition and almost all other personal restraints - honour, pride, honesty – drop away. In the advanced stages, defects of memory, confusion, hallucinations, delusions and intellectual deficits become evident.[32]

Humiliation

Clearly, one of the most powerful tools available to any torturer is the ability to attack the physical body. The individual's body, and the brain more specifically, is directly tied to who he is, and attacking the physical body will have direct repercussions on how he thinks. However, this is not the only way of attacking the individual. Indeed, attacking an individual's emotional and psychological self can be equally powerful. There are techniques that rely on the "the disintegration of an individual's personality, the shattering of his mental and psychological equilibrium and crushing of his will".[33] As discussed in previous chapters, both the mental integrity and the sense of self of the individual are directly connected to who the individual is. Like any other physical limb, attacking an individual on a psychological or emotional level can have direct and negative repercussions. Moreover, many of the physical attacks mentioned above can have mirrored affects on the individual's mental stability and sense of worth due to the distress these physical attacks cause to the individual's brain. For

[28] Aginger, J and Hemmager, E. 'Unusual Neural Conditions Following Hunger Period of 1945-46' *Archive of Psychiatry* Vol.186 (1951) pp.483-495
[29] Helweg-Larsen, P., Hoffmeyer, H. and Kiefer, J. *Famine Disease in German Concentration Camps: Complications and Sequels* (Scandinavia: Med Scan, 1952) p.351
[30] Gottschick, J. 'Neuropsychiatric Disease Among German Prisoners of War in the United States' *Archive of Psychiatry* Vol.185 (1950) pp.491-510; Hulgren, H. P. 'Prisoners of War: Clinical and Laboratory Observations in Severe Starvation' *Stanford Medical Bulletin* Vol.9 (1951) pp.175-191
[31] Keys, A. *The Biology of Human Starving* (Minneapolis: University of Minneapolis Press, 1950)
[32] Helweg-Larsen, P. et al *Famine Disease in German Concentration Camps* (1952) p.351
[33] *Ireland v. The United Kingdom* Dissenting Opinion of Judge Evrigenis

example, the use of hooding, sleep deprivation and stress positions can all directly impact the individual's mental integrity.

What has therefore proven to be an incredibly powerful tool for torture is the use of humiliation and degradation of the victim's sense of self worth. Indeed, Richard Arneson argues that "shame, humiliation, and disgust are negative states of mind that can be deployed as tools to induce desired behaviour".[34] How an individual views himself, or is forced to view himself, involves accessing one of his most intimate relationships and attacking it can damage his sense of worth and therefore cause harm.

Conclusion

Blackmail and torture as mechanisms are powerful tools when it comes to forcing a target to capitulate. The stark contrast they highlight to the individual between what he has and what he has to lose if he fails to cooperate means that for intelligence agencies both activities are tempting avenues. In the next section both blackmail and torture will be examined in terms of the vital interests they can come into conflict with in order to outline the harm they can each cause.

[34] Arneson, R. 'Shame, Stigma and Disgust in the Decent Society' *The Journal of Ethics* Vol.11 No.1 (2007) p.32

Section Two: Direct Harms

What is Harmful about Blackmail?

As Section One detailed, blackmail involves an individual who has the view to "gain or cause loss" to someone by making an "unwarranted demand with menaces".[35] But this description does little to outline what it is about blackmail that is harmful.[36] Intuitively there is the sense that there is something noticeably untoward about blackmail and as a crime in society it has been remarked as one of the foulest: "far crueller than most murders because of its cold-blooded premeditation and repeated distress of the victim; incompatibly more offensive to the public conscience than the vast majority of other offences we seek to punish".[37] What this section will do, therefore, is to discuss which of the vital interests blackmail comes into conflict with and how it, as a result, causes harm.

As noted throughout this thesis, autonomy is the individual's ability to act as an end in himself; to be able to choose his own will, free from outside control. Blackmail, however, directly circumvents this vital interest by forcing the individual to base his decisions on the direct wishes of the blackmailer and not himself. Blackmail is essentially about the power the blackmailer has over the victim and the blackmailer using that power to get the victim to do what he wants. This is demonstrated by the fact that blackmail necessarily involves a loss for the victim and a gain for the blackmailer. As Grant Lamond argues, the wrong of blackmail does not simply rest with the fact that the threatening act is impermissible but rather that it "relates to the way action is used to dominate against the victim".[38]

The level of harm caused by blackmail is the result of the type of threat the blackmailer wields over the target as this indicates the extent to which the target's autonomy is affected. It can be argued that if the blackmailer holds a minor threat over the victim then the power influencing the individual's will is minimal and thus the target is only harmed slightly as he has room to resist. In comparison, if the blackmailer has a strong threat over the victim then it can be argued that the victim has less room to resist and therefore has less control over his decision-making ability. The harm is, therefore, greater.

---

[35] Allridge, P. 'Attempted Murder of the Soul' (1993) p.371

[36] See Clark, M. 'There is No Paradox of Blackmail' *Analysis* Vol.54 No.1 (1994) pp.54-61; Gorr, M. 'Liberalism and the Paradox of Blackmail' *Philosophy and Public Affairs* Vol.21 No.1 (1992) pp.43-66; and Lindgren, J. 'Unravelling the Paradox of Blackmail' *Columbia Law Review* Vol.84 No.3 (1984) pp.670-717

[37] The barrister C. E. Bechhofer Roberts in his forward to 'The Mr A Case' quoted in Hepworth, M. *Blackmail* (1975) p.1

[38] Lamond, G. 'Coercion, Threats and the Puzzle of Blackmail' in *Harm and Culpability* edited by Smith, A. and Simester A. (Oxford: Oxford University Press, 1996) p.231

There are then additional harms the individual can suffer caused by the "loss" associated with blackmail. This is the result of the constant draining of a person's resources (both physical and emotional) that blackmail can cause. It can in many instances be literally 'too much' for the individual to handle. Mike Hepworth argues that the "ennervating [sic] and relentless pressure" can "produce a state of suicidal despair in response".[39] The never ending and often increasing demands made, coupled with the constant fear of being 'found out' creates a situation where the individual is constantly anxious, fearful, and unable to be at ease. Depending on the threat used this can cause severe mental anguish and even encourage self-harm. This distress is experienced as a result of the fear the individual has that the threat will be carried out and that as a result he will suffer damage to his reputation and his sense of self-worth. That is, given that the individual's sense of self worth is in a large part the result of the attitude of others – Cooley's "looking-glass self" where the ego thinks of itself as others think of it[40] – to fear the loss of respect from one's identity group can cause stress, anxiety and depression in the individual.

Another concern for the use of blackmail revolves around how the information that forms the basis of the blackmail is collected. Since blackmail in many instances involves the threat of revealing something private, how that information was obtained becomes important. If it was collected by violating someone's privacy then this is an additional harm that needs to be incorporated. For example, tapping an individual's telephone wires to gain the relevant information causes additional harm as a result of the privacy violation. Or, if the information were collected through an entrapment exercise, then the use of manipulation and deception required to set up the scenario creates additional harm, as demonstrated in the previous chapter.

Torture and the Harm Caused

Discussing what is harmful about torture almost seems to be stating a given. The word 'torturous' indicates something that is inherently severely damaging to the individual. However, what this section will seek to unpack is how those methods used can come into

[39] Hepworth, M. *Blackmail* (1975) p.22

[40] Cooley, C. H. *Human Nature and the Social Order* (Charles Scriber and Sons, 1902) p.152. The 'looking glass self' is obviously not the only means through which the individual develops their sense of self or self-worth. Bilha Mannheim argues that there is also the 'real-self image' which is how the ego defines himself, and the 'ideal self' which is what the ego would like to be. These three aspects all interact and play an important part in how an individual develops, through interactions with himself and others, his sense of self. See Mannheim, B. 'Reference Groups, Membership Groups and Self Image' *Sociometry* Vol.29 No.3 (1966) pp.265-279

conflict with an individual's vital interests and thereby outline exactly what it is about torture that is 'harmful'.

Pain: Of Body and Mind

As already noted, pain is often the first thing thought of when torture is mentioned. Pain as a tool attacks the body in a fundamental way, creating a state where the individual's own body is crying out to him, begging him to act in any way to bring it to an end, pushing the physical and mental aspects of the individual to such a limit that it depletes all resolve.

Physical pain is experienced through the body's nervous system and implies a neural perturbation. The amount of pain felt by the individual is directly related to the level of force applied to the body and the degree of sensitivity of the area attacked. Although it is not always the case, often the level of pain experienced will indicate the level of damage being caused to the body.[41] This is because the body produces pain in order to draw the individual's attention to those parts of the body under threat. As such, the levels and degrees of pain can vary, "from momentary seemingly painless to excruciating agonies lasting [or seeming to last] indefinitely".[42]

It can be argued, as it was in Chapter One, pain is a harmful state to exist in and when the individual is suffering from physical pain he is unable to conceive of pretty much anything else. When the body is in extreme pain it is completely debilitated, unable to conceive of anything else as it "forcibly severs our concentration on anything outside of us; it collapses our horizon to our own body and the damage we feel in it... the world of man or woman in great pain is a world without relationships or engagements, a world without exterior".[43]

Mental pain, in many ways, is quite similar. As noted in the previous section there are certain attacks on the body that, while they are felt physically, also attack the individual's mental state or psyche. Sensory deprivation and overload, sleep deprivation, alteration of the body's homeostatic balance, can each affect the individual's mental state. For example, they can cause delusions, hallucinations, or paranoid thinking, emotional liability, disorientation, intellectual dysfunctions, defects of memory, confusion, and intellectual deficits, all a painful

[41] Some parts of the body are blessed with more nerve endings than others as a course of greater operative efficiency for the average individual. These areas are likely to be more vulnerable to pain infliction in some senses, but do not yet promise to be as threatening to the individual's essential welfare when damaged.
[42] Spiller, G. *The 'Sense' of Pain (and Pleasure)* (London: Farleigh Press, 1938) p.4
[43] Luban, D. 'Liberalism, Torture and the Ticking Bomb' *Virginia Law Review* Vol.9 No.6 (2005) p.1430

or debilitating state to experience. The mental pain created, much like physical pain, is one that is inherently harmful to the individual, designed to erode any resolve he might have.

Moreover, mental pain can be created within a target without attacking the brain on a physical level, but by attacking it psychologically. For example, fear, anxiety and dread are purposefully created by the torturer through the use of threats or frightening experiences (mock executions for example), and the manipulation of natural phobias and weaknesses. These mental states inflicted on an individual are 'painful' and can create the same reactions and sensations as discussed with physical pain: the individual's view of reality is eclipsed by the event, he is in pain, his psyche cries out for attention and it inflicts on him the extreme urge to bring the situation to an end.

These attacks can also cause damage to the individual that can then be felt long after the torture has finished.[44] Beatings, stress positions, subjection to harsh environmental conditions are all painful in the immediate sense and in the sense that the damage caused to the body can still be experienced many years later. For example, hand cuffing with flexi-cuffs can cause nerve damage in the hand so that it will never properly work again or will continue to feel pain long after; stress positions force the muscles to their breaking point and beyond resulting in "ankles doubling in size, skin becoming tense and intensely painful, blisters erupt oozing watery serum, heart rates soar, kidneys shut down, and delusions deepen"; and burns caused by exposure to both flames and the sun leave the skin ravaged and sore.[45]

The long-term effects of the mental damage caused can in many ways be harder to see yet the traumatic effects can be even more debilitating to the individual. A study in 1967 of seventy-nine subjects who had been in sensory deprivation and manipulation experiments in a Canadian hospital showed that 60% continued to suffer from "persistent amnesia" and 23% from "serious physical complications". Some participants were still suffering from prosopagnosia (a brain disorder resulting in an inability to identify faces) nearly twenty years

[44] It is important to note the difference between the 'experience' of pain and then the long-term damage the actions themselves will cause because they can in fact harm the individual in two separate ways. Some arguments made to justify the use of torture will make the claim that the pain is experienced but leaves no marks and so, therefore, the act can be used as it will be forgotten or the scars will heal. This distinction notes that there is a harm in the instance of applying pain to an individual, even if the body physically heals afterwards. A body which suffers long term pains or damage is then forced to experience additional pains over a long period. This is relevant when discussing definitions of torture like that put forward by the Bybee Memos, which argue that severe physical pain is only that which is is "serious physical injury, such as organ failure, impairment of bodily function, or even death," and that prolonged mental harm is harm that must last for "months or even years". This definition seems to ignore the experience of mental and physical pain in the immediate sense and only looks to the those damaging effects which would be long lasting.

[45] McCoy, A. W. *A Question of Torture: CIA Interrogation, from the Cold War to the War on Terror* (New York: Henry Holt and Company, 2006) p.46

later.[46] Other studies have shown similar results, outlining that the most common reported psychological problems of torture include long-term anxiety, depression, irritability, aggressiveness, emotional instability, self-isolation and social withdrawal; and further cognitive or neuro-vegitative problems such as confusion, disorientation, impaired memory and concentration, insomnia, nightmares and sexual dysfunction.[47]

Humiliation, Degradation and Self-Esteem

While torture most definitely involves and relies on inflicting mental and physical pain in extreme quantities, there is another important aspect to torture quite separate from these pains but of equal importance; that is, the use of degrading treatment. Degrading treatment is designed to attack an individual's sense of self-worth, causing him to suffer pain in a place beyond the flesh, a place most central to who he is.

Chapter One argues that the individual constructs his 'self-view' as a result of many intertwined factors.[48] One important factor includes how the individual is forced to view himself in relation to his own standards. When he is subjected to degrading treatment he is forced to feel shame, humiliation or disgust with himself.[49] Each of these emotions are

[46] McCoy, A. W. *A Question of Torture* (2006) p.45

[47] The results from both controlled and uncontrolled studies have shown substantial evidence that for some individuals, torture has serious and long-lasting psychological effects. See Basoglu, M., Jaranson, J. M., Mollica, R., and Kastrup, M. 'Torture and Mental Health: A Research Overview' in *The Mental Health Consequences of Torture* edited by Gerrity, E. Keane, T. M. and Tuma F. (New York: Kluwer, 2001) pp. 35–62; Basoglu, M., Livanou, M. and Crnobaric, C. 'Torture vs Other Cruel, Inhuman, and Degrading Treatment: Is the Distinction Real or Apparent?' *Archives of General Psychiatry* Vol.64 (2007) p.284; Costanzo, M., Gerrity, E. and Lykes, M. B. 'Psychologists and the Use of Torture in Interrogations' *Analyses of Social Issues and Public Policy* Vol.7 No.1 (2007) p.7-20; De Jong, J. T., Komproe, I. H., Van Ommeren, M., El Masri, M., Araya, M., Khaled, N., Van de Put, W. A. C. M., and Somasundaram, D. J. 'Lifetime Events and Posttraumatic Stress Disorder in Four Post-Conflict Settings' *Journal of the American Medical Association* Vol.286 (2001) pp.555–562; Priebe, S. and Bauer, M. 'Inclusion of Psychological Torture in PTSD Criterion' *American Journal of Psychiatry* Vol.152 (1995), pp.1691–1692; and Silove, D. M., Steel, Z., McGorry, P. D., Miles, V., and Drobny, J. 'The Impact of Torture on Posttraumatic Stress Symptoms in War-Affected Tamil Refugees and Immigrants' *Comprehensive Psychiatry* Vol.43 (2002) pp.49–55.

[48] Words like 'self-esteem', 'self-worth', 'self-respect' are used in some of the literature interchangeably, or can be used to denote specific aspects at play. In this project they are used to refer to the same general concept of how the individual evaluates his sense of 'self'. See Cast, A. D. and Burke, P. J. 'A Theory of Self-Esteem' *Social Forces* Vol.80 No.3 (2002) pp.1041-1068; Gecas, V. 'The Self-Concept' *Annual Review of Sociology* Vol.8 (1982) pp.1-33; Rosenberg, M. 'The Self-Concept: Social Product and Social Force' in *Social Psychology: Sociological Perspectives* edited by Rosenberg, M. and Turner, R. H. Transaction (New York: Basic Books, 1990) pp.593-624; Rosenberg, M., Schooler, C., Schoenbach, C. and Rosenberg, F. 'Global Self-Esteem and Specific Self-Esteem' *American Sociological Review* Vol.60 (1995) pp.141-56

[49] Martha Nussbaum argues that while the terms shame, humiliation, disgust and embarrassment are related, there are some differences. Shame is typically connected with ideal norms and is connected to society; humiliation is the active, public face of shame, where the individual suffers a severe blow in regards to his public image; embarrassment is a much milder version of humiliation and not as harmful; and disgust is when the individual sees himself as the embodiment of some contamination of some form. Nussbaum, M. *Hiding from Humanity: Disgust, Shame and the Law* (Princeton: Princeton University Press, 2004) p.203-207. However, for the purpose of this thesis, the main point is that the individual evaluates himself as judges himself as less than he is and is harmed as a result.

particularly powerful forms of self-reflection, with contemporary psychological and philosophical theories arguing that they are the distress caused by the individual defining himself as no good or not good enough.[50] The individual views himself through the eyes of his social group. For example, these might include the eyes of his friends and family, himself as an impartial viewer, a higher power or even the torturer. He views himself through these 'eyes' and judges himself as those eyes would. To inflict shame or disgust on an individual is to place him in a particular state or circumstance where he looks at himself through these eyes and sees himself as something less than he is. The feelings created as a result of being made to feel shame, disgust or humiliations are "painful emotions responding to a sense of failure to attain some ideal state".[51]

Torture utilises degrading and humiliating treatment as a form of assault, attacking that which is core to the individual. For example, by making an individual stand in his own wastes for long periods of time, the individual feels dirty, he recoils, feeling disgust at the state he is in and therefore himself. He starts to view himself as an object of disgust. When an individual is forced to carry out homosexual acts that go against his religious belief he sees himself through the eyes of that religion and judges himself degraded or dirty. When an individual is paraded around a room naked on a dog chain, he is being paraded for all to jeer at, he views himself as an object of humiliation with on-lookers judging him, and through them he judges himself and loses value as they laugh at him.

Harm to the Torturer

When discussing the issue of torture there is a large (and albeit right) focus on the impact the torture has on the victim. However, this can mean that the torturer and the harm that he suffers is not taken into account. This is folly given that there are several important studies that have been undertaken, drawing on interviews with former torturers in Greece,[52] Argentina, Brazil, Chile, Uruguay,[53] Nicaragua[54], and Israel[55], which have demonstrated that

[50] Miller, S. B. *The Shame Experience* (Hillsdale: Analytic, 1985) p.32
[51] Nussbaum, M. *Hiding from Humanity* (2004) p.184
[52] Haritos-Fatouros, M. 'The Official Torturer: A Learning Model for Obedience to the Authority of Violence' in *The Politics of Pain Torturers and their Masters* edited Crelinsten, F. D. and Schmid, A. P. (Leiden: Center for the Study of Social Conflicts, 1993), pp.141–160
[53] Heinz, W. S 'The Military, Torture and Human Rights: Experiences from Argentina, Brazil, Chile and Uruguay', in *The Politics of Pain Torturers and their Masters* edited Crelinsten, F. D. and Schmid, A. P. (Leiden: Center for the Study of Social Conflicts, 1993), pp.73–108.
[54] Allodi, F. 'Somoza's National Guard: A Study of Human Rights Abuses, Psychological Health and Moral Development', in *The Politics of Pain Torturers and their Masters* edited Crelinsten, F. D. and Schmid, A. P. (Leiden: Center for the Study of Social Conflicts, 1993), pp.125–140.

the process of training a torturer can cause harms akin to those that the torturer then inflicts on his targets. It has been demonstrated through these projects that in order to train a torturer, he must have those barriers, which would have previously prevented him from carrying out these brutal acts, eroded. This, it is argued, involves subjecting the trainee to a program of considerable abuse and radical dehumanisation that often has deleterious effects on his sense of self, his family, and his community.[56] In their research, psychologists Mika Haritos-Fatouros and Janice Gibson noted that the cruelty of the training programs that the men were put through were so extreme that only a very select few were ever able to make it through to the end and be chosen to torture.[57] The aim was to break down the normal social and personal boundaries that prevent individuals from performing these actions. It would seem that in order to get an individual to inflict inhumane acts on another, it is necessary to remove the humanity in the torturers first.

Harm to Society

The above sections have outlined how the use of torture can have profound effects on both the victim and the torturer. Finally, it can be argued that acts of torture can detrimentally affect society as a whole. Firstly, it can be argued that allowing torture, even in only the most extreme situations, is to bring it in as a legitimate tool of the state. This can have a detrimental effect on the social and legal norms as a result of the normalising effect that any use of torture can have. That is, it is feared that any case of authorised torture will open the flood gates for it to be used in the future and that each time it is used its use becomes more 'normal' and the limits on its use become reduced. This is only going to directly affect the cohesion between a society and its sub-groups as they become, or feel they become, marginalised and targeted. Finally, the use of torture, even for intelligence collection purposes, is necessarily going to cause an intimidating effect. Henry Shue argues that "Almost all torture is 'political' in the sense that it is inflicted by the government in power upon people who are, seem to be, or might be opposed to the government".[58] Individuals will naturally become fearful and less likely to act as freely as they would otherwise.

---

[55] Cohen, S. and Golan, D. *The Interrogation of Palestinians during the Intifada: Ill-treatment, 'Moderate Physical Pressure' or Torture?* (Jerusalem: Israeli Information Center for Human Rights in the Occupied Territories, 1991)

[56] See Waller, J. *Becoming Evil: How Ordinary People Commit Genocide and Mass Killing* (Oxford: Oxford University Press, 2002)

[57] Gibson, J. 'Training People to Inflict Pain: State Terror and Social Learning' *Journal of Humanistic Psychology* Vol.31 No.2 (1991) pp.72-78

[58] Shue, H. 'Torture' *Philosophy and Public Affairs* Vol.7 No.2 (1978) p.134

Conclusion

Blackmail and torture come into direct conflict with an individual's vital interests and in doing so cause that individual harm. Blackmail forcibly affects people's autonomy by directing them to cooperate or let themselves suffer quite severe repercussions, as well as causing varying levels of stress within the individual as they are forced to (continually) suffer a loss of some form. Torture, on the other hand, comes into conflict with all of an individual's vital interests. Detaining the individual and subjecting him to severe physical, psychological and emotional attacks means that he if forced to experience the most extreme form of harm. What the next section will explore is in what ways the tools of blackmail and torture are used and what levels of harm are caused as a result.

Section Three: Illustrative Examples

Both blackmail and torture are seemingly powerful tools for getting someone to cooperate. Section one outlined the mechanics of both of these activities and Section Two highlighted in what ways they can cause harm. Blackmail was seen to come into direct conflict with an individual's autonomy as well as causing various degrees of anxiety and stress. Torture violates almost all the vital interests an individual has as it seeks to push him to his limits and break down any resolve he might have. In this section, by applying various illustrative examples regarding these two activities it is possible to explore both how they are actually used as well as the levels of harm they can cause. The blackmail cases will explore, first, the use of 'information blackmail', where the intelligence agency has information about the individual that is then used as a lever on the individual and, second, the use of an 'entrapment operation' where the individual is enticed to act untowardly so as to provide the blackmail information. The torture examples will include the use of 'The Five Techniques' used during the Troubles in Northern Ireland, the treatment experienced at detention centres such as Abu Ghraib and Guantanamo Bay, and finally the extraordinary rendition programs where individuals are transported to countries known for torture in order to secure information.

Information Blackmail

The use of blackmail often relies on gaining compromising information on an individual. What this information is exactly can vary from case to case depending on the target's social situation. Markus Wolf, former head of the East German intelligence agency HVA, outlined how, "the past was a powerful weapon among the spy services... we sought to bring down politicians or senior figures hostile to us by revealing their Nazi complicity".[59] Or another often-exploited piece of information for blackmailers would be any personal or sexual failing. Being unfaithful is an activity that people will go to great lengths to hide. People in the diplomatic or intelligence services, because of the nature of their work, are expected to live almost impeccable lives: "if you have been unfaithful to your wife, you are probably less afraid of her than your supervisor. You live in fear that he is going to find out about it".[60] It is this common failing that forms the basis of the first case discussed. This case involves a Western European diplomat, known simply as Mr B, who at the time was a functionary of his

[59] Wolf, M with McElvoy, *A. Memoirs of a Spymaster: The Man Who Waged a Secret War Against the West* (London: Pimlico, 1998) p.50
[60] X, Mr. with Henderson, B. E. and Cyr, C. C. *Double Eagle: The Autobiography of a Polish Spy who Defected to the West* (New York: Ballantine Books, 1983) p.87

country's embassy in Warsaw. While there he met and married a young Polish girl, Miss C. Soon they both left Poland to work in Paris. Polish intelligence followed Miss C and intercepted almost all of her mail in the hope of gaining information to be used against her: "we had a file as big as a table on them, with photocopies of every letter from her to her family, to her friends, to her relatives and from them to her".[61] After several years of intercepting her mail, Polish intelligence finally discovered that there was an old flame with whom she had renewed contact. When she informed him that she would be returning to Poland for a visit, Polish intelligence acted quickly so that any encounter could be monitored and recorded. When the Polish wife and her old flame went on a camping trip Polish intelligence was there, ready to capture any indiscretion: "we had more than ten operatives hidden in the area with cameras, tape recorders and other equipment... our photographers took pictures of the couple swimming naked in the lake, we even planted microphones in their tent so that at night when the journalist and young wife were screwing each other we could capture every word".[62] Upon her return, the wife was confronted by a Polish intelligence officer who presented her with the incriminating information and an ultimatum: "I told her, 'you can imagine the situation if your husband knew. He is really a very intelligent man, noble person, from a good family. He isn't going to accept it. He is going to divorce you for sure. You are killing some kind of happiness in your own home. No Poland, no parents, no husband."[63] The Polish wife felt she had no alternative and cooperated with Polish intelligence in every way they asked.

A second example follows the same pattern but focuses on using an individual's homosexuality as the basis for the blackmail. The power for cases based on homosexuality comes from the negative social stigma, and in some cases the illegality, still attached to it. As an ex-intelligence blackmailer notes, "homosexuality, depending on the country within which you are operating, was the classic 'crime against nature'", and therefore knowledge about an individual's sexual inclinations could very often prove to be a potentially powerful lever.[64] Obviously, this type of blackmail can vary greatly from society to society and from person to person: "in Great Britain, knowing someone's homosexuality is not going to be important unless the individual is a member of the British Foreign Service or intelligence service[65]...

[61] X, Mr. *Double Eagle* (1983) p.89
[62] X, Mr. *Double Eagle* (1983) p.90
[63] X, Mr. *Double Eagle* (1983) p.92
[64] X, Mr. *Double Eagle* (1983) p.87
[65] At the time of publication in 1983 homosexuals were banned from working in sensitive government positions such as the Foreign Office or any of the intelligence services from fear of blackmail. Since the early 1990s,

however, if the individual is stationed in a country where homosexuality is classified as a crime, he could get into trouble very easily".[66] This case involves that of Tom Driberg, Labour MP, journalist, member of Labour's National Executive and party chairman. Unfortunately for Driberg, in 1956 his less than discreet activities made him a perfect target for Soviet intelligence.[67] Mitrokhin maintains that the KGB were able to gain evidence of his homosexuality while he visited Moscow and used it to blackmail him for over twelve years: "he was used as both a source of inside information from the Labour National Executive and to promote active measures... wonderfully placed to report to his controller on both the evolution of the Labour Party and the rivalries within the leadership" as well as being useful in influencing "the campaign within the Labour Party for unilateral nuclear disarmament".[68]

Entrapment Blackmail

This first set of examples demonstrates how an individual can easily become victim to blackmail as a result of their own actions. However, if the individual does not act so as to put himself into a compromising position then the intelligence officer is ready to help the situation along. Indeed, the Soviets excelled at using sexual entrapment operations in order to get compromising information on specific targets. As Allen Dulles notes, "the Soviets cannot eliminate love and sex and greed from the scene... so they use them to ensnare people".[69] People working, travelling or visiting the Soviet bloc would start the gears moving automatically the minute they applied for a visa. The visa application, possibly accompanied with a report from the KGB Residency from the home country of the visitor, would be submitted for evaluation; all information on the applicant would be correlated and then the decision would be made as to whether the target was worth the effort. If he was, the visitor would be photographed and followed from his point of entry and they would have his hotel room covered in microphones and cameras. The next stage was then to expose him to desirable women (or men if the first few advances did not seem appropriate), all highly trained and capable in sexual seduction.

---

however, the ban was lifted and there has been a positive drive to recruit more homosexuals in order to be as inclusive as possible while removing the stigma and therefore eliminate the threat of blackmail.

[66] X, Mr. *Double Eagle* (1983) p.87

[67] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane, 1999) p.522-524

[68] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999) p.523, 524, 525

[69] Dulles, A. *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering in a Free World* (Guilford: The Lyons Press, 2006) p.190

The first example involves Phillippe Latour, a forty-two year old electronics engineer who visited Russia in the late 1960s. He worked for a company engaged in developing missile guidance systems for the French government and when he submitted his visa for entry, as an authority in his field, he proved a prime target. In the subsequent file that was developed on him, it was noted that he was a careful, conscientious and very ambitious man, with a taste for fine wine and young women.[70] This, for the KGB, was perfect. One night while out, a slender, well dressed, attractive blonde female came into the restaurant; she was a language teacher and informed Latour that she enjoyed talking to foreigners and so asked if he would like her to act as his guide while in the area. Within two days she was joining him in his hotel room. The following afternoon he was asked to see the manager and found two KGB officers. They gave him an envelope containing photographs revealing the previous night's sexual encounter. The KGB wanted information on the air-to-air missiles that his company was developing and informed him that the woman he had met was actually the wife of an important military leader and that as such this encounter could be construed as an attempt to gain military secrets from her, for which he would be imprisoned for many years.[71] Within three days he provided the information. This betrayal was then used as a further hold over him and he was blackmailed again and again for the secrets he had access to. Other entrapment cases can involve the KGB acting as jealous boyfriends who catch the affair and sympathetic Soviet authorities who offer to help the target out. The offer of help never comes, alas, without strings attached. Such a strategy was used against French Ambassador Maurice Dejean. After using a young actress employed by the KGB to entrap the ambassador, during sexual relations another KGB officer burst into the room claiming to be the jealous husband and, after beating the ambassador up for effect, exclaimed that he would take this to the authorities. Suitable 'friends' were already in place by this point to offer help in exchange for future favours; he became indebted and over time would be "gently asked for the favour to be returned. One favour would lead to another until Dejean crossed the threshold of treason from which there could be no return".[72]

[70] Lewis, D. *Sexpionage: The Exploitation of Sex by Soviet Intelligence* (London: H. Hanau Publications, 1976) p.10-11. As was discussed in the introduction, the cases outlined are done in order to explore the ethical issues that might be caused by these types of intelligence activities. The discussion is not designed to make any statement as to the veracity of the case itself nor the reliability of this particular book as a reflection of historical events. The cases should be assumed to be purely hypothetical and used as such. Therefore, while the facts of the case are open to critique, the ethical calculations made are done so as the case is presented.
[71] Lewis, D. *Sexpionage* (1976) p.14
[72] Barron, J. *KGB: The Secret Work of Soviet Secret Agents* (New York: Bantam Books, 1974) p.187

The final case is similar in that it involves an entrapment exercise but again has the added twist of focusing on an individual's homosexuality. John Vassall, who had worked as a naval intelligence clerk, was posted to the British Embassy, Moscow in 1955. An introverted and vain individual, Vassall found himself isolated and lonely. A month after his arrival, the young clerk was invited to a restaurant and introduced to an attractive female KGB, a 'Swallow', charged with ensnaring Vassall. However, when she failed to gain his attention, they replaced her with a male operative, a 'Raven'. This proved more successful. This Raven agent invited Vassall to a party with some of his closest 'friends', a party which quickly turned into a gay sex orgy, all of which was secretly photographed by the KGB. To seal the deal, the KGB then arranged for Vassall to be caught within a second entrapment operation, having a military officer invite Vassall back to his apartment with the KGB on-hand to burst into the scene mid-event. It was at this point that the KGB officers showed Vassall the photographs of his activities, warning him that he had committed a serious offence under Soviet law. This was the moment he became a Soviet spy. Over the years Vassall handed the KGB copies of secret signals that passed across his desk and when he returned to Britain to take his job as Director of Naval Intelligence, Vassall's value only grew.[73]

Level of Harm: Information and Entrapment Blackmail

As discussed in Section Two, the use of blackmail can cause harm as a result of the impact it has on the target's autonomy as well as causing additional harms in the form of stress and anxiety. For the 'information blackmail' cases, the blackmailer uses the information he has over the individual as a pressure to directly influence his decision-making process. The individual is no longer the author of his own will, but rather the tool of another's will. In comparison to the use of bribery, lying and manipulation discussed in the previous chapter, each of which can come into conflict with an individual's autonomy, it can be argued that the pressure being applied in regards to blackmail is much greater. Bribery, deception and manipulation only influence or guide the individual's will, whereas blackmail is a more direct force, interjecting into the individual's decision-making process and attempting to force a specific response. Therefore, blackmail has the potential to cause a higher level of harm. The exact level of harm caused, however, is the result of what pressure, or in this case what information, is being used. The more severe the repercussions of revealing the victim's secrets the greater the power the blackmailer has and therefore the greater the affect on his

[73] Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive* (1999) p.523

autonomy. In the Polish wife example, therefore, it can be argued that the intelligence operative presented her with quite a dramatic cost. In the words of the Polish intelligence officer, she would be left with "No Poland, no parents, no husband".[74] Being presented with such a level of loss the pressure on her autonomy is quite significant. This point is demonstrated again in the case of homosexual-information blackmail that given the social stigma and the likely backlash that the target would suffer (depending on the social situation) means that there was a significant degree of pressure on the target to comply and therefore his autonomy was significantly affected.

In comparison to those operations where the individual was entrapped it can be argued that there was the additional use of manipulation and deception and therefore a greater level of harm caused. Entrapment operations rely on deceiving the target about who he is sleeping with and the intentions behind the encounter. The Swallow or Raven is manipulating the individual in a very significant way and in an area that is very intimate to the target. Therefore, in the entrapment cases, since the intelligence officer purposefully manipulated the targets in order to encourage the act, the level of harm is greater. Again, in those cases involving homosexuality, if the social situation means that the target is likely to suffer severe repercussions then there is a great influence on his autonomy.

In the Polish wife and Tom Driberg cases, where there was blackmail but with no entrapment, the level of harm caused features at Level Four on the Ladder of Escalation given the pressure placed on their decision-making process. However, in the entrapment cases, such as that of Ambassador Maurice Dejean, Phillippe Latour and John Vassall, given the affect that deception and manipulation have on the target's autonomy in addition to that of the pressure of the blackmail, there is a greater level of harm caused and so features at Level Five on the Ladder of Escalation.

Torture

In recent history, as a result of the Geneva Convention against Torture, the systematic use of torture by Western intelligence agencies has been prohibited. However, this does not mean it does not occur and, indeed, in recent years it has been brought back into debate regarding the possible role it could have in collecting intelligence. After the September 11, 2001 and July 7, 2005 terrorist attacks in the US and UK respectively, many were left with the feeling that they had been let down by their intelligence community. For the intelligence operative,

[74] X, Mr. *Double Eagle* (1983) p.92

"public expectations of intelligence have never being greater"[75] and many blamed the ability of the hijackers to carry out their plan as a failure of the intelligence community to provide timely information that would have stopped it. There is now significant pressure on the intelligence services to look like they are doing more to provide protection. FBI officials have expressed their own frustration at being restrained in their interrogation techniques: "It could get to that spot where we go to pressure – where we will have no choice".[76] Cofer Black, State Department Coordinator for Counterterrorism, noted that "there was a before 9/11 and there was an after 9/11… and after 9/11 the gloves come off".[77] Indeed, shortly after the attack President Bush gave broad powers against terrorists suspects: on November 13th, 2001 he issued orders that allowed for the detention of all Al-Qaeda suspects, denying them access to any civilian court and relegating them to military tribunals; and in January 2002 President Bush acted to 'suspend' the Geneva Conventions by claiming that those detained did not qualify for 'prisoner of war' status and the protection normally accorded by the Conventions.[78] Alan Dershowitz, a criminal law professor at Harvard Law School, argues that given extreme enough circumstances, law enforcement officials would most probably torture; when the costs are massively outweighed by the benefits torture becomes tenable.[79] Torture, it would seem, is back on the table for debate.

In the three cases discussed below, the first examines the use of torture by the British government during the Troubles in Northern Ireland, called 'The Five Techniques', the second explores the treatment received at American-run detention centres designed to 'prepare' its inmates for interrogation, namely Guantanamo Bay and Abu Ghraib, and finally

[75] Jackson, P. and Scott, L. 'The Study of Intelligence in Theory and Practice' *Intelligence and National Security* Vol.19 No.2 (2004) p.139

[76] Pincus, W. 'Silence of 4 Terror Probe Suspects Poses Dilemma' *Washington Post* October 21st (2001) A06

[77] Gellman, B. and Priest, D. 'U.S. Decries Abuse but Defends Interrogation' *Washington Post* December 26th (2002)

[78] Bush, G. W. 'Notice: Detention, Treatment and Trial of Certain Non-Citizens in the War Against Terrorism' *White House*, November 13 2001, Federal Register Vol.22 No.2 p. 57833 [pp.57831-57836] available in *The Torture Papers: The Road to Abu Ghraib* edited Greenberg, K. J. And Dratel, J. L. (Cambridge: Cambridge University Press, 2005) pp.25-28. Administrative lawyers quickly translated the president's directives into policy. On January 9th 2002, John Yoo of the Justice Department's Office of Legal Counsel wrote a forty-two page memorandum asserting that the Geneva Conventions did not apply as those involved fell into a category beyond soldier and civilian called 'illegal enemy combatants' thus placing them outside the Geneva Conventions. See Department of Justice, Office of Legal Counsel, Memorandum for William J. Haynes, General Counsel, Department of Defence, From: John Yoo, Deputy Assistant Attorney General, 'Application of Treaties and Laws to Detainees', available in *The Torture Papers: The Road to Abu Ghraib* edited Greenberg, K. J. And Dratel, J. L. (Cambridge: Cambridge University Press, 2005) pp.38-39, 43-44, 47, 57, 79.

[79] Dershowitz, A. *Why Terrorism Works: Understanding the Threat, Responding to the Challenge* (London: Yale University Press, 2002) p.143

the third involves the rendition of individuals by Western intelligence agencies to countries known for torture as a means of interrogation, referred to as extraordinary rendition.[80]

The Five Techniques

In April 1971 there was a secret meeting in Belfast between senior British intelligence officers and members of the Royal Ulster Constabulary's (RUC) Special Branch. The purpose of this meeting was to discuss the most effective way of gaining intelligence in the battle against the IRA, something the RUC had previously failed in doing.[81] The interrogation methods that were to be used on those arrested by the RUC were to become known as 'The Five Techniques' and would, between 1972 and 1976, occupy the European Commission of Human Rights and the European Court of Human Rights as the Republic of Ireland government sought to have these techniques classified as amounting to torture.[82] The Five Techniques included:

a) wall standing: forcing the detainees to remain for periods of some hours in a 'stress position', described by those who underwent it as being 'spread-eagled against the wall, with their fingers put high above the head against the wall, the legs spread apart and the feet back, causing them to stand on their toes with the weight of the body mainly on the fingers';
b) hooding: putting a black or navy coloured bag over the detainees' head and, at least initially, keeping it there all the time except during interrogation;
c) subjection to noise: pending their interrogations, holding the detainees in a room where there was a continuous loud and hissing noise;
d) deprivation of sleep: pending their interrogations, depriving the detainees of sleep;
e) deprivation of food and drink: subjecting the detainees to a reduced diet during their stay at the centre and during pending interrogations.[83]

[80] These case studies have been chosen for several reasons. The first is that they each provide a different aspect of torture. The Irish case, although it involves acts of humiliation, it was the physical and psychological attacks that feature heavily; and for the Guantanamo Bay and Abu Ghraib cases, the reverse, in that why they both included extreme physical and psychological abuses, the humiliation and sexual abuses featured and were reported on significantly. The case of extraordinary rendition is important for it highlights the question regarding the extent that other states can become complicit in the harm caused. Furthermore, all three represent good examples of interrogational torture by Western states, whereby it is argued that there is the direct and practiced aim of getting intelligence information from the suspects. Finally, they have each received significant attention and feature centrally to the literature and to ignore them as cases would ignore important current debates on the use of torture in intelligence.

[81] Taylor, P. *Beating the Terrorists? Interrogation in Omagh, Gough and Castlereach* (London: Penguin, 1980) p.19

[82] For more on the court case and the commission's report see Rodley, N. S. *The Treatment of Prisoners Under International Law* (Oxford; New York: Oxford University Press, 2009) p.90-92

[83] *Ireland v. United Kingdom*, European Court of Human Rights, Series A, No.25, 41, para.96

The unanimous conclusion of the Commission was that the combination of these techniques amounted to torture.[84] What this section will examine is how these techniques can cause harm to the individual and the level of harm experienced.

Those arrested and subjected to The Five Techniques included Paddy Joe McClean, a remedial school teacher from Bergagh, Tyrone; Jim Auld, a twenty year old unemployed dental technician; Patrick Shivers, a civil rights activist from Toomebridge; Francis McGuigan from Belfast; and Kevin Hannaway who was also from Belfast.[85] By exploring Auld's recollection it is possible to see how The Five Techniques were used and how they affected his physical, mental and emotional state. Auld was taken from his home in the middle of the night to Gindwood Barracks where he recalls receiving some fairly serious physical damage: "they beat with batons, they kicked me around the place. They were aiming towards my privates and my head and they were making me keep my hands at my sides".[86] Without warning or explanation a hood was placed over Auld's head, he was handcuffed and made to run into a post: "straight into my head, flying in full force in it, I just went down". From here they took him inside, stripped him, put him in a boiler suit and then started the next phase. With the hood still on, designed to increase his sense of isolation, he was put in a room filled with an increasingly intense noise, "sounding like an airplane engine or the sound of compressed air escaping". For a solid week the sound was absolute and unceasing and many who experienced it recalled it as the "worst part of the ordeal".[87] Then Auld was forced to stand in a stress position for a long period of time without a break:

> My hands were put up against the wall, after ten or fifteen minutes they started to get numb, so I dropped them down to my side, and as soon as I lifted them off the wall I got beaten with the batons, just beaten solid. You very quickly get the message you weren't suppose to move your hands. But you can only keep your hands up for so long. And so what they did was to set upon me again. I was knocked unconscious. And when I woke up they threw me back up again. It just went on for days. I know I wet myself.[88]

During all this time the men were deprived of food, water and sleep; Auld remembers being kept awake for six days straight.

---

[84] *Ireland v. United Kingdom*, 1976 Y.B. Eur. Conv. on Hum. Rts. 512, 748, 788-94 (Eur. Comm'n of Hum. Rts.) para.794
[85] Conroy, J. *Unspeakable Acts, Ordinary People: The Dynamics of Torture* (New York: Knopf, 2000) p.8
[86] Conroy, J. *Unspeakable Acts* (2000) p.4-5
[87] Conroy, J. *Unspeakable Acts* (2000) p.6
[88] Conroy, J. *Unspeakable Acts* (2000) p.6

Guantanamo Bay and Abu Ghraib

In any discussion on torture, there are two images that dominate the scene: one is the photograph published in various media showing hooded and handcuffed detainees in orange overalls kneeling in wired cages, depicting the detainees at Guantanamo Bay, while the other shows a young female American soldier with a naked man on the floor to her right wearing a dog leash, portraying the treatment of prisoners at Abu Ghraib. These pictures show prisoners being subjected to cruel and humiliating treatment at the hands of U.S. troops. In other photographs naked prisoners are being forced to lie on top of each other in a pile or to simulate sexual acts; several pictures showed naked, hooded inmates, handcuffed in painful positions or tied to beds and cell doors; some detainees had bleeding wounds, and others appeared to have wires attached to their bodies. In response, on September 15th, 2004, the Taguba Report was released testifying that terrorist suspects were being actively tortured in American run prisons in the hope of gaining information. The Taguba Report stated that between October and December of 2003 there were numerous instances of "sadistic, blatant and wanton criminal abuses" at Abu Ghraib prison by the 372nd Military Police Company and the American intelligence community.[89] What is more, Taguba reported that these undertakings were not the work of high-spirited or revenge-driven individuals, but were the result of an ordered effort to break detainees, to make them more malleable to questioning by intelligence operatives. Taguba concluded that, "personnel assigned to the 372nd Military Police Company, 800th MP Brigade, were directed to change facility procedures to 'set conditions' for MI [military intelligence] interrogations". Army intelligence officers, CIA agents, and private contractors had "actively requested that MP [Military Police] guards set physical and mental conditions for favourable interrogation of witnesses".[90]

Those methods used to 'prepare' the detainees are reported in the Taguba Report as:

a. Punching, slapping, and kicking detainees; jumping on their naked feet;
b. Videotaping and photographing naked male and female detainees;
c. Forcibly arranging detainees in various sexually explicit positions for photographing;
d. Forcing detainees to remove their clothing and keeping them naked for several days at a time;
e. Forcing naked male detainees to wear women's underwear;
f. Forcing groups of male detainees to masturbate themselves while being photographed and videotaped;

[89] Tagbua, A. *Article 15-6 Investigation of the 800th Military Police Brigade [The Taguba Report]* (2004) p.16 §5 Retrieved from http://www.npr.org/iraq/2004/prison_abuse_report.pdf on 1st May 2007
[90] Tagbua, A. *The Taguba Report* (2004) p.18 §10

g. Arranging naked male detainees in a pile and then jumping on them;
h. Positioning a naked detainee on a MRE Box, with a sandbag on his head, and
attaching wires to his fingers, toes, and penis to simulate electric torture;
i. Writing "I am a Rapest" (sic) on the leg of a detainee alleged to have forcibly raped a 15-year old fellow detainee, and then photographing him naked;
j. Placing a dog chain or strap around a naked detainee's neck and having a female Soldier pose for a picture;
k. A male MP guard having sex with a female detainee;
l. Using military working dogs (without muzzles) to intimidate and frighten detainees, and in at least one case biting and severely injuring a detainee;
m. Taking photographs of dead Iraqi detainees.[91]

In addition to these actions several detainees also described the following acts of abuse, which under the circumstances Tagbua claims to find credible, given the clarity of the statements made and supporting evidence provided by other witnesses. These include:

i. Breaking chemical lights and pouring the phosphoric liquid on detainees;
ii. Threatening detainees with a charged 9mm pistol;
iii. Pouring cold water on naked detainees;
iv. Beating detainees with a broom handle and a chair;
v. Threatening male detainees with rape;
vi. Allowing a military police guard to stitch the wound of a detainee who was injured after being slammed against the wall in his cell;
vii. Sodomizing a detainee with a chemical light and perhaps a broom stick
viii. Using military working dogs to frighten and intimidate detainees with threats of attack, and in one instance actually biting a detainee.[92]

Extraordinary Rendition

The final case to be discussed involves the rendition of an individual from one state to another for the purpose of torture, which, while it has none of the same powerful imagery that has become associated with the cases of Abu Ghraib or Guantanamo Bay, has still received significant attention from the international community. This is not least of all because it has

[91] Tagbua, A. *The Taguba Report* (2004) p.16 §6
[92] Tagbua, A. *The Taguba Report* (2004) p.17 §8

highlighted important and significant questions regarding the role other states have in facilitating the use of torture. The practice of rendition is itself nothing new. Prior to the terrorist attacks of September 2001, rendition operations were carried out to bring individuals subject to arrest warrants to justice. In recent years, however, what has been alleged is that these rendition programs are being used with the intention of interrogating and torturing individuals outside the normal legal system. Most notably, flying individuals to countries known for torture in order to collect intelligence while distancing oneself from the act. The allegations as they currently stand are that the American CIA flew individuals to other states, including Egypt, Jordon and Syria, with the knowledge and even the intent that they were to be interrogated in ways far too extreme to have been allowed under any American jurisdiction. Furthermore, claims have been made against several European states, stating that they have aided these rendition programs in various ways.

Extraordinary rendition operations in the context of the CIA's counter-terrorism activities are comprised of three steps or elements, namely the apprehension, transfer and end point.[93] All three stages are interconnected and have to be taken into account for a full analysis of the harm caused and the role other states play. Each of the elements, however, can take several forms. The apprehension might, or might not, include a legal process, be ad hoc or planned long ahead of schedule. For example, Monica Hakimi describes that one method involves unlawfully detaining, through kidnapping for example, the target before he is secretly transported.[94] The transfer itself can then occur by various means, the common method involving CIA operated aircraft, although the flights themselves will often either have to refuel or stop in other countries *en route*. Finally, the end point might either be an American military detention centre, a detention centre belonging to a third party state or possibly a joint detention centre.[95] It is here that the individual is tortured for intelligence collection purposes.

One case that has found itself at the fore of the debate on the use of extraordinary rendition is that of a British national Binyam Mohamed al-Habashi, who was rendered from Pakistan to Morocco in July 2002. When Binyam tried to return to the United Kingdom in April 2002 after leaving over a year earlier, he was arrested by Pakistan officials for travelling under a false passport. Binyam claims that he was held by Pakistan officials for a

[93] Reprieve 'Enforced Disappearance, Illegal Interstate Transfer, and Other Human Rights Abuses involving the UK Overseas Territories' (2007). Online Access: http://www.statewatch.org/news/2008/feb/uk-usa-reprieve-submission-FASC.pdf. p.4
[94] Hakimi, M. 'The Council of Europe Addresses CIA Rendition and Detention Program' *The American Journal of International Law* Vol.101 No.2 (2007) p.444
[95] Reprieve 'Enforced Disappearance' (2007) p.4

period of three months during which time he was mistreated and interviewed by CIA officers who threatened to send him to Jordon for torture.[96] Then in July 2002 Binyam claims that he was subject to a CIA-ran extraordinary rendition program from Pakistan to Morocco. It is then in Morocco that Binyam claims to have been tortured.[97] Binyam reports that he was subjected to physical, mental and emotional torture: "Three men came in with black masks. One stood on each of my shoulders, and a third punched me in the stomach... I was made to stand but I was in so much pain I'd fall to my knees. They'd pull me back up and hit me again".[98] Then came what Binyam claimed was the worst part of the torture: "'Strip him' they shouted. They cut off my clothes... I was naked... I thought I was going to be raped. Maybe they'd electrocute me. Maybe castrate me. One of them took my penis in their hands and began to make cuts with a scalpel. They cut all over my private parts".[99] During September and October 2002 Binyam was taken by car to another place where they played excruciatingly loud music constantly: "I think I came to several emotional breakdowns in this time... I never saw the sun, not even once".[100] Binyam was then transferred to Guantanamo Bay. Similar examples of rendition programs include that of Hassan Mustafa Osama Nasr who was kidnapped by CIA officials in Milan before being rendered, via the American base in Avaino, Italy, to Egypt; or, the report of Murat Kurnaz, a German resident rendered from Pakistan to American custody in Kandahar, Afghanistan before finally being transferred to Guantanamo Bay in January 2002 and finally being released in August 2006.[101]

The Harm of Torture

The Five Techniques

It can be argued that each of The Five Techniques used in the Irish case is for the purpose of causing direct harm to the individual. Using stress positions, physical violence and the denial of life's essentials, such as food and sleep, all attack and violate the individual's physical and

[96] Grey, S. *Ghost Plane: The True Story of the CIA Torture Program* (New York: St. Martin's Press, 2006) p.53
[97] Intelligence and Security Committee '*Rendition*' chaired by Murphy, P. (July, 2007) cm.7171 p.33. Online Access: http://www.fas.org/irp/world/uk/rendition.pdf.
[98] Grey, S. *Ghost Plane* (2006) p.57
[99] Grey, S. *Ghost Plane* (2006) p.58
[100] Grey, S. *Ghost Plane* (2006) p.59
[101] Grey, S. and Natta, D. 'Thirteen with the C.I.A. Sought by Italy in a Kidnapping' *New York Times* 25th June 2005. Online access http://www.nytimes.com/2005/06/25/international/europe/25milan.html; Dempsey, J. 'German Foreign Minister Under Fire On Human Rights - Europe - International Herald Tribune' *The New York Times* 31st January 2007. Copy available at http://www.nytimes.com/2007/01/31/world/europe/31iht-berlin.4421471.html?scp=1&sq=German%20Foreign%20Minister%20Under%20Fire%20over%20Guantanamo%20Bay%20Detainee&st=cse Accessed 6th November 2010

mental integrity. Stress positions quite literally push the body to its limit. The arms, legs, muscles, tendons, all scream for the individual to give up, drop the arms and stop. However, when the individual follows this wish, he is set upon by a different type of physical pain in the form of beatings. Furthermore, it is not just the physical damage inflicted, but also the mental pain experienced. As was discussed in the Section Two, a lot of the physical attacks on the body can have psychological repercussions. These pains are then exacerbated by the lack of food and sleep, again directly impacting on the mental state of the individual. Menachem Begin, Prime Minister of Israel from 1977 to 1983 who was tortured as a young man in the Soviet Union, tells in his book, *White Nights: The Story of a Prisoner in Russia*, of how his fellow prisoners who had endured extreme tortures under other regimes and had not cracked, lost the will to resist with sleep deprivation: "in the head of the interrogated prisoner, a haze begins to form. His spirit is wearied to death, his legs unsteady, and he has one sole desire: to sleep, to sleep just a little, not to get up, to lie, to rest, to forget".[102] The individual is physically and mentally harmed as the body is attacked and damaged in a most fundamental way.

Use of 'hooding' and the 'noise room' can then harm the individual by attacking his sensory system and, as a result, his psyche. In Section Two it was outlined how through the use of sensory deprivation and overload the individual's brain is attacked, directly affecting his mental state. With hooding, the individual is forced to experience constant anxiety, never knowing what is going on around him, fearing what is happening, where the next blow might come from and never knowing how to defend himself. This can result in extreme anxiety, stress and can lead to hyperventilation, which, while inside the hood, can cause asphyxiation. Furthermore, constant bombardment of the aural centre can have extremely traumatic effects. The sensory overload attacks the brain and can induce ''a state of psychosis, a temporary madness with long-lasting after-effects.''[103]

The result of these five techniques upon the individual is, understandably, severely detrimental. Of those individuals mentioned, Paddy Joe McClean was deprived of water to such an extent that his tongue swelled up and he almost choked on it; Patrick Shivers hallucinated visions of his dead son; Francis McGuigan hallucinated that he was among his friends but could not realise why they refused to remove his handcuffs and by the end of his

[102] Begin, M. *White Nights: The Story of a Prisoner in Russia* (Harper and Row, 1977) p.107
[103] Conroy, J. *Unspeakable Acts* (2000) p.6

ordeal could no longer even spell his own name or count to ten; and Kevin Hannaway said how he lost the power to talk and would just sit and wait for death.[104]

Although there is no direct documented evidence for the long-term effects of these techniques, conclusions can be drawn from various studies. For example, Doctors Finn Somnier and Inge Genefke examined twenty-four torture survivors 10 years after their torture and found that 71% had nightmares, 79% complained of headaches, 79% impaired memory, 75% impaired concentration, 75% experienced fatigue, 50% suffered persistent fear and anxiety, 38% had impaired hearing, 38% became socially withdrawn, 33% experienced vertigo, 21% reported sexual problems and 12% had constant tremors and shaking.[105]

Guantanamo Bay and Abu Ghraib

Again, as was seen in the Irish case, there is extensive use of physical attacks on the individual. In the Taguba Report, those points lettered a), h), and numbered i) iii), iv), vi) and vii) each outlined a different physical attack that resulted in a physical pain or physical damage of some sort. However, what is important about the activities discussed in this report as compared to those of the Irish case is the increased use of humiliation, degradation and sexual attacks.

As was argued in Chapter One, the individual holds a vital relationship with himself. How he views himself is directly tied to his sense of self-worth. As a result of this, in Section Two of this chapter it was argued that forcing degrading treatment on an individual by making him feel shame or humiliation harms him. Shame is "a *painful* emotion responding to the sense of failure" to attain some ideal state.[106] And this is exactly what those actions listed in the Taguba Report were designed to do. Forcing the individual to feel disgust in regards to himself attacks his emotional core and causes him to lose the will to resist. In the same way that beating and starving an individual is an attack on the individual's physical body, these humiliating acts are an attack on his emotional and psychological self.

For example, Tarek Dergoul who was held in Guantanamo Bay, said that they tied him to a chair so that, "inevitably I'd soil myself. It was humiliating". However, the humiliation was then purposefully driven home: "they were watching through a one-way mirror and as soon as I wet myself a woman MP would come in yelling 'Look at what you've

[104] Conroy, J. *Unspeakable Acts* (2000) p.8
[105] Somnier, F. and Genefke, I. 'Psychotherapy for Victims of Torture' *British Journal of Psychiatry* Vol.149 (1986) p.325
[106] Nussbaum, M. *Hiding from Humanity* (2004) p.184. Emphasis added.

done. You're disgusting'".[107] The point was to emphasise the humiliation felt by Dergoul. His cultural background meant that the use of a female interrogator was even more humiliating, and to be ridiculed in this way would only emphasise the disgust he already felt in himself.

Furthermore, the use of rape and other sexual related abuses attack the individual in an extremely damaging and often violent way. It can hardly be argued that sexual abuse does not have a dramatic and debilitating effect on the individual: "sexual abuse is an extremely damaging form of torture; for tormentors to penetrate this most private realm produces deep feelings of despair and self-loathing".[108] Sexual abuses, and other forms of humiliation, can leave the victim feeling emotionally destroyed, powerless, with severe post-traumatic stress disorders and suicidal tendencies. Furthermore, to force an individual into performing homosexual acts pushes the degradation even further for those whose cultural background emphasises it as an abhorrent way of life. For many it turns what should be an intimate and loving act into a humiliating and painful experience.

Extraordinary Rendition: The Question of Complicity

Given that the two previous illustrative examples on torture outlined the various activities employed and the harm these can cause, the purpose of this section is not to examine the harm caused by extraordinary rendition, but rather to question who is culpable in the harm caused. This is to be done, first, in regards to the actions of the CIA as the main propagators of the extraordinary programs and then, second, in regards to those states who allowed their airspace or equipment to be used in the rendition process.

Whether people are to be morally culpable for the actions of others is the result of the role that they play in "assisting others in their wrong doing, or encouraging them to engage in wrong doing" since it is "through our acts we participate in their wrongs, and so become liable for them".[109] This sentiment is reflected in Anglo-American law whereby one can become liable for a crime by playing a complicit role in another's commission of a crime: "Whosoever shall aid, abet, counsel or procure the communication of any indictable offence... shall be liable to be tried, indicted and punished as a principle offender".[110] John Gardner points out, however, that there can be both strong and weak causal links between the

[107] Rose, D. 'They Tied Me Up Like a Beast and Began Kicking Me' *The Guardian* 16th May 2004. Available at http://www.guardian.co.uk/world/2004/may/16/terrorism.guantanamo. Accessed 4th November 2010

[108] Amnesty International *Cruel. Inhuman. Degrades Us All: Stop Torture and Ill-Treatment in the "War on Terror"* 31st July 2005 Available at http://www.amnesty.org/en/library/asset/ACT40/010/2005/en/69c95ca2-d4c6-11dd-8a23-d58a49c0d652/act400102005en.pdf Accessed 4th November 2010 p.11

[109] Kutz, C. 'Causeless Complicity' *Criminal Law and Philosophy* Vol.1 No.3 (2007) p.289

[110] *Accessories and Abettors Act* 1861 §8

principle and the accomplice, and that depending on the type of causal link, the degree of liability is altered.[111] By examining the extent to which the event would have (not) occurred without the accomplice it is possible to understand if the individual has a strong or weak causal link to the event.

In the instance of the CIA, by looking at the three stages associated with the extraordinary rendition programs, in almost all stages the CIA are directly linked. In some cases, like the case of Hassan Mustafa Osama Nasr who was kidnapped by CIA officials in Milan,[112] the CIA had a direct role in the first 'apprehension' stage of the process. For the 'transfer' stage the CIA also played a central role by physically transferring individuals to states known for their harsh interrogation methods through the use of airplanes chartered and manned by CIA officers. Finally, although the CIA officers themselves might not be in the room while the individual was tortured, they knew both what would happen to the individual once they handed him over and that they actively encouraged the torture by asking for intelligence gained from the torture. Therefore, they are aware, directly facilitate and even benefit from the use of torture by these other countries. This means they are directly involved in the harm caused.

The involvement of European countries on the other hand is less clear cut. The most detailed investigation into this issue so far has been carried out by the Council of Europe Rapporteur Dick Marty.[113] He maintained in two reports that between 2001 and 2006, European airspace had been used for flights operated by the CIA, and at least some of them for the purpose of extraordinary rendition. On September 12th, 2005 the *Guardian* newspaper reported that it had compiled a database of flight records from the U.S. Federal Aviation Administration that demonstrated British logistical and refuelling support for CIA extraordinary rendition operations.[114] In particular, the article referred to the case of Mohammed Saad Iqbal Madni, where it is alleged that the CIA rendered him from Indonesia

---

[111] Gardner, J. 'Complicity and Causality' *Criminal Law and Philosophy* Vol.1 No.2 (2007) p.135

[112] Grey, S. and Natta, D. 'Thirteen with the C.I.A. Sought by Italy in a Kidnapping' *The New York Times* (2005) Available at http://www.nytimes.com/2005/06/25/international/europe/25milan.html Accessed 4th November 2010

[113] Council of Europe, Parliamentary Assembly: 'Alleged Secret Detention and Unlawful Inter-State Transfers of Detainees Involving Council of Europe Member States' Report by Rapporteur Dick Marty, Doc 10957, 12th June (First Report, 2006). Available at http://assembly.coe.int/Documents/WorkingDocs/doc06/edoc10957.pdf Accessed 4th November 2010; and Council of Europe, Parliamentary Assembly: 'Secret Detentions and Illegal Transfer of Detainees Involving Council of Europe Member States' Report by Rapporteur Dick Marty, Doc.11302rev, 11th June 2007. Available at http://assembly.coe.int/Documents/WorkingDocs/Doc07/edoc11302.pdf Accessed 4th November 2010.

[114] Cobain, I., Grey, S. and Norton-Taylor, R. 'Destination Cairo: Human Rights Fears Over CIA Flights' *The Guardian* 12 September 2005. Online access: www.guardian.co.uk/print/0,,5283268-105744,00.html Accessed 6th November 2010

to Egypt, and then flew on to Prestwick airport in Scotland to refuel before returning to Washington. Since September 2005 a number of other reports have referred to the use of UK airspace by CIA-operated aircraft and their possible use in rendition.[115]

In comparison to the involvement of the CIA, while it can be argued that allowing the use of one's airspace is a far cry from the role they played, this does not mean that the other countries which facilitated the rendition, such as the UK, are not complicit in some way. The important question that must be asked is whether the relevant authorities were aware of the CIA flights using their airspace for extraordinary rendition operations. If they were then it can be argued that they are culpable for the harm caused. Becoming aware of how one's airspace is being used and allowing the action to continue does place that particular state in the chain of events. Furthermore, those states which then use the collected information are also increasing their involvement by implicitly sanctioning the collection technique. This was clearly the concern of the British Ambassador to Uzbekistan, Craig Murray, who in July 2004 sent a telegram to both London and British Missions around the world saying: "we receive intelligence obtained under torture from the Uzbek intelligence via the U.S. We should stop... we are selling our souls".[116]

The Maximum Harm

The activity of torture, as explored throughout this chapter, is clearly very harmful. Torture by its very definition is designed to push the body to its absolute limit; to break down any resistance the individual has and to force him to go against his will. Torture is actually designed to be harmful, and what is more, to be harmful in the extreme. As a result, torture will often come into conflict with not just one or even two of an individual's vital interests but virtually all of them simultaneously. Moreover, when it violates these vital interests it does so in the most severe, extreme way. Some of the other activities previously examined – blackmail, manipulation, seduction – it was argued that they violate the individual's vital interests to varying degrees and so various levels of harm are caused. Torture, however, is an utter attack of *all* the individual's vital interests and to an extreme degree, and in doing so

[115] Amnesty International alleged more than 200 CIA flights through the UK, including three flights stopping over in the UK having been involved in rendition operations abroad. European Parliament Temporary Committee, *Alleged 170 CIA flights Through the UK*, including one stopping over in the UK having been involved in rendition operations abroad, 16 November 2006. See Amnesty International, 'UK: Human Rights: A Broken Promise' Report released 23 February 2006. Available at http://www.amnesty.org/en/library/asset/EUR45/004/2006/en/cc167867-d45b-11dd-8743-d305bea2b2c7/eur450042006en.pdf. Accessed 7th November 2010

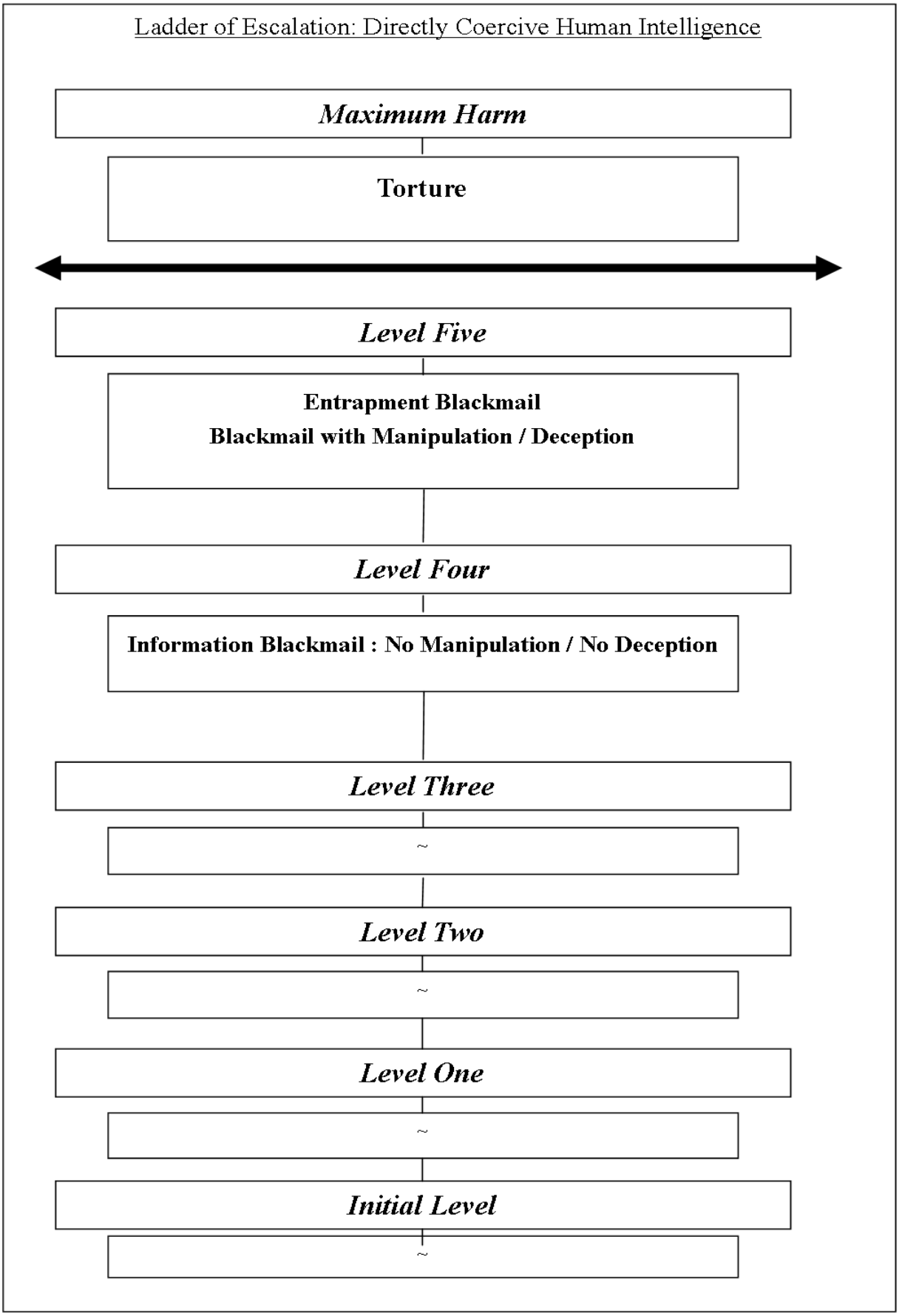
[116] Grey, S. *Ghost Plane* (2006) p.171

causes a level of harm unlike that previously seen. In addition, torture not only significantly harms the individual targeted, but also harms society and even the torturer. Torture is, therefore, one of the most harmful acts that an individual can suffer. This means that torture would always sit at the top of the Ladder of Escalation, above all the other actions discussed in this thesis. Indeed, in order to incorporate this extreme level of harm caused by torture, a separate level of harm on the Ladder of Escalation must be established, called *Maximum Harm*, where actions that cause the most severe harms are placed. This *Maximum Harm* level is not just one more increment on the Ladder of Escalation, but a whole separate category significantly different from any of the other levels, meaning that the activities placed at this level are going to be fundamentally different to those placed at other levels.

Conclusion

Clearly blackmail is one of the more harmful activities explored in this thesis with many of the illustrative examples featuring at either Level Four or Level Five on the Ladder of Escalation. By forcing an individual to cooperate through the use of menaces, that individual not only has his ability to control his own life severely impinged but is also put under quite severe levels of stress and anxiety. Therefore, the use of blackmail, which involves the individual being forced to do something they would have otherwise not done, will always feature at the higher levels on the Ladder of Escalation. In comparison, torture not only features at the higher levels on the Ladder of escalation, but at the highest. So severe in fact is the level of harm caused by torture that a separate level is established, called Maximum Harm, to represent the uniquely extreme type of harm caused. Figure 5.0 below demonstrates both how this new Maximum Harm is positioned in comparison to the other levels as well as how the different forms of blackmail relate to each other in terms of the harm they cause the individual.

Figure 5.0


Ladder of Escalation: Directly Coercive Human Intelligence
Maximum Harm
Torture
Level Five
Entrapment Blackmail
Blackmail with Manipulation / Deception
Level Four
Information Blackmail : No Manipulation / No Deception
Level Three
~
Level Two
~
Level One
~
Initial Level
~

Section Four: Just Human Intelligence

Just Intelligence and Blackmail

The ethical framework that has been established in Chapter One argued that intelligence collection must be limited as a result of the harm it can cause. In the instance of blackmail and torture, this need to limit intelligence is not only clear but also, given the extreme degree to which they affect the individual's interests, they both belong at the top echelons on the Ladder of Escalation. By making reference to the Just Intelligence Principles it is possible to determine if these higher levels of harm can be justified and if so under what circumstances.

Just Cause

It has been argued in previous sections that blackmail can cause a level of harm to the individual that features at either Level Four or Level Five on the Ladder of Escalation. Blackmail in order to be justified would therefore need quite a serious just cause. That is, it should only be used when there is a direct threat present. The threat should be known to the level of 'clear evidence' and should represent a serious threat to the nation's security. In understanding this, it can be argued that the use of blackmail in all the above cases are not justified. In each of the cases, the use of blackmail was almost standard practice; anyone who was of slight interest was targeted and blackmailed in order to put them in the agency's pocket. There was no direct, serious threat to act as the just cause. The only case where there might have been a sufficient degree of threat is the case of Phillippe Latour who worked for a company engaged in developing missile guidance systems. If he was working on a piece of weapon technology where there was clear evidence that it would or could pose a serious threat, then this would be a just cause to investigate the weapon. However, from the case presented there seems to be no direct threat but more a general fact gathering mission, an insufficient threat.

Legitimate Authority

While it is possible for an organisation of sufficient authority to be established to authorise blackmail, in the cases mentioned none of them seemed to have achieved this. For the level of harm caused it would need to be an authority that was external to the agency's own hierarchy and preferably authorised by a senior body of multiple individuals. None of the cases discussed demonstrated this level of authorisation. Instead, it would seem that in each of the cases discussed blackmail was routine and so no authorisation from outside was sought.

Proportionality

In order for the use of blackmail to be proportional, the information gained must outweigh all the negative results of blackmail. That is, those blackmail cases where there are additional harms – for example stress and anxiety caused by the pressure placed on the target – the information gained must be of increasing value.

Discrimination

In order to be a legitimate target it must be demonstrated that the individual is either a threat or has placed himself within the defence infrastructure at a sufficiently high level so as to warrant being targeted. Therefore, in the case of the Polish wife, she would be an illegitimate target since she had done nothing to justify being targeted, except marrying a French diplomat and this is insufficient given the level of harm caused. In comparison, in the case where the French Ambassador, Maurice Dejean, who slept with the KGB actress, it can be argued that not only was he a part of the state infrastructure but maintained a high and prominent position and was thus a legitimate target. John Vassall, the intelligence clerk, and Tom Driberg, an MP in the house of Commons, could also be thought of as legitimate targets given that Vassall was within the intelligence structure and so had waived his rights, as did Driberg given his official position.

Just Intelligence and Torture

Throughout this chapter the use of torture has been explored by examining the various methods employed, highlighting how these methods violate an individual's vital interests in a most extreme, acute and chronic way. By applying these understandings to some examples, including the 'Irish Case', treatment at the Abu Ghraib and Guantanamo Bay detention centres and the practice of extraordinary rendition, the level of harm caused by torture was established. It was concluded in the previous section that torture as an activity should be situated at the very top of the Ladder of Escalation featuring at a separate stage called *Maximum Level.* It was argued that since torture involved the most severe violation of almost all the vital interests an individual has, coupled with the harm caused to the torturer and society as a whole, that torture was an extreme form of harm, above and beyond anything discussed before.

Just Cause

The question now, however, is whether or not it is possible for there ever to be a sufficient enough threat to act as a just cause for this level of harm. This is a difficult question and one that has received much attention recently. There has been a significant amount of work regarding the possible range of the threats that a state might face in the current climate and whether these threats are sufficient to justify torture.[117] By adhering to the ethical framework established in Chapter One and then examined in greater detail throughout the thesis, however, it can be argued that the answer to the question whether there is ever a sufficient level of threat to justify torture is no. By employing the harm ethic it is clear that torture is one of the most extreme forms of harm, causing physical, emotional and psychological obliteration unlike any of the other collection activities, while producing additional harms to the torturer and to society as a whole. As a result of the level of harm caused, it can be argued that torture represents one of those activities that is so inhumane that no threat can exist to justify its use.[118]

This argument – that there are certain activities that cause such high level of harm so as to be absolutely prohibited even in times of war or when facing extreme threat – is not new. It can be argued that there are activities that cause such intense levels of harm and result in the degradation of the human condition to such a degree that it is not possible for the action to be justified. International law, as a reflection of this position, outlines that there are certain actions that are 'crimes against humanity' as a result of their inhumane nature and are

[117] For those that argue to justify torture see: Allhoff, F. 'A Defence of Torture: Separation of Cases, Ticking-Time Bombs, and Moral Justification' *International Journal of Applied Philosophy* Vol.19 No.2 (2005) pp.243-264; Dershowitz, A. *Why Terrorism Works* (2002) pp.131-164 for the discussion of a 'torture warrant'; Lukes, S. 'Liberal Democratic Torture' *British Journal of Political Science* Vol.36 (2006) pp.1-16; Parry, J. 'Escalation and Necessity: Defining Torture at Home and Abroad' in *Torture: A Collection* edited by Levinson, S. (Oxford; New York: Oxford University Press, 2004) pp.145-164; Parry, J. 'Interrogating Suspected Terrorists: Should Torture be an Option?' *University of Pittsburgh Law Review* Vol.63 No.1 (2001) pp.743-766; and Steinhoff, U. 'Torture – The Case for Dirty Harry and against Alan Dershowitz' *Journal of Applied Philosophy* Vol.23 No.3 (2006) pp.337-353. For those who argue that no such just cause can exist Bellamy, A. J. 'No Pain No Gain? Torture and Ethics in the War on Terror' International Affairs Vol.82 No.1 (2006) pp.121-148; Blakeley, R. 'Why Torture?' *Review of International Studies* Vol.33 No.3 (2007) pp.373-394; González Castresana, C. 'Torture as a Greater Evil' *South Central Review* Vol.24 No.1 (2007) pp.119-130; Hunsinger, G. 'Torture Is the Ticking Time-Bomb: Why the Necessity Defense Fails' *A Journal of Theology* Vol.47 No.3 (2008) pp.228-239; Luban, D. 'Liberalism, Torture, and the Ticking Bomb' (2005) pp.1425-1461; McCready, D. 'When is Torture Right?' *Studies in Christian Ethics* Vol.20 No.3 (2007) pp.383-398; Scarry, E. 'Five Errors in the Reasoning of Alan Dershowitz', in *Torture: A Collection* edited by Levinson, S. (Oxford; New York: Oxford University Press, 2004) pp.281-290; Waldron, J. 'Torture and Positive Law: Jurisprudence for the White House' *California Law Review* Vol.106 No.6 (2005) pp.1681-1750.

[118] Another aspect to the criterion of just cause is that the more harmful an activity the more evidence is required to prove that the threat is real, and therefore in the instance of torture the level of evidence required would be 'beyond all reasonable doubt'. It should be noted therefore, that as a marker this is quite demanding in that intelligence often works on partial evidence and probabilities and so it would be quite hard to fulfil this criterion. It is, however, not impossible and more refers to the practical application of torture and intelligence rather than its ethical nature.

absolutely prohibited as a result. That is, those acts which are "particularly odious offences in that they constitute a serious attack on human dignity or grave humiliation or a degradation of one or more human beings".[119] Even in times of extreme threat it is recognised that these actions are still not allowed. What this highlights is that there is an established understanding that certain types of actions are prohibited because of the extreme level and type of harm they cause. What this thesis argues is that torture, with its utter destruction of almost all of an individual's most vital interests, is akin to this idea of crimes against humanity and therefore there is no just cause possible that can justify its use.[120]

Proportionality

Even though it has been argued that using torture would never fulfil the principle of just cause, it is important to understand how the level of harm torture causes relates to the other Just Intelligence Principles. The principle of proportionality stipulates that the cost associated with carrying out the act must be outweighed by the benefits of the information. Indeed, one consequentialist argument for the use of torture would be that when the costs number in the thousands or millions of lives, sticking to one's principles is a grave error. The cost of one life cannot surely outweigh that of hundreds, thousands or millions of others, it is argued. However, the problem with this argument is that it fails to recognise that quite often the intelligence operative is not presented with such a stark contrast between quantifiable high gains in comparison to costs. Much of intelligence comprises of gathering bits of information from many different sources; often intelligence information is as "sparse as a telephone number or an address to check".[121] It is not the situation where one bit of information will provide an instant and quantifiably high amount of gain. For example, the information that was 'produced' in the Irish Five Techniques case demonstrates that while this information might be useful, it is still a long way from those consequentialist arguments that claim that

[119] As defined by the *Rome Statute of the International Criminal Court Explanatory Memorandum*.

[120] Indeed, international law recognises crimes against humanity to include: "For the purpose of this Statute, 'crime against humanity' means any of the following acts when committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: Murder; Extermination; Enslavement; Deportation or forcible transfer of population; Imprisonment or other severe deprivation of physical liberty in violation of fundamental rules of international law; Torture; Rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity; Persecution against any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender as defined in paragraph three, or other grounds that are universally recognized as impermissible under international law, in connection with any act referred to in this paragraph or any crime within the jurisdiction of the Court; Enforced disappearance of persons; The crime of apartheid; Other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health." Rome statute of the International Criminal Court *Article 7: Crimes Against Humanity*

[121] Omand, D. 'The Dilemmas of Using Secret Intelligence for Public Security' in *New Protective State: Government, Intelligence and Terrorism* edited by Hennessy, P (London: Continuum, 2007) p.155

intelligence can save hundreds, thousands or even millions of lives. Lord Parker, who headed a committee that looked in The Five Techniques, noted that:

> As a result [of the internment and interrogation of individuals] the following information was obtained: identification of a further seven hundred members of both IRA factions and their positions in the organisations; over forty sheets giving details of the organisation and structure of the IRA units and sub-units; details of possible IRA arm caches; safe houses; communication and supply routes; details of morale, operation directives, propaganda techniques; the discovery of individual responsibility for about eighty-five incidents recorded on police files which had previously remained unexplained.[122]

Even with these so-called gains it should be clear that they are not sufficient enough to outweigh the costs of torture, including the harm to the target as well as the additional harms caused to the torturer and society as a whole.

Discrimination

The principle of discrimination is used to distinguish between legitimate and illegitimate targets, affording the illegitimate targets protection from the harm that intelligence collection can cause. In Chapter One it was argued that individuals can waive or forfeit their normal protective rights as a result of the actions they carry out, making them legitimate targets. The higher the level of harm caused by the intelligence collection the greater the threat they must pose. However, this does not mean that an individual can forfeit all of his protective rights. Indeed, in times of war even when a combatant is classified as a legitimate target and has waived his right not to be killed, this does not mean that he has waived the right not to be treated humanely. Ian Clark makes the point by asking, "Which is the greater evil, the humane killing of non-combatants or the burning of combatants to death by flamethrowers?"[123] Thomas Nagel argues that flamethrowers as a weapon are an "atrocity" for "burns are extremely painful and extremely disfiguring – far more than any other category of wound" and, therefore, because of the type of suffering caused the use of the flamethrowers is prohibited.[124] Clearly there is this notion that some actions are prohibited because of the inhumane nature of the weapons, meaning that no target, no matter the level of

[122] Parker, 'Report of The Committee of Privy Counsellors Appointed to Consider Authorised Procedures for the Interrogation of Persons Suspected of Terrorism' (1972) Cmd 4901. Held at *Conflict Archive on the Internet* in collaboration with University of Ulster. Available at http://cain.ulst.ac.uk/hmso/parker.htm#2 Accessed November 2010

[123] Clark, I. *Waging War: A Philosophical Introduction* (Oxford: Clarendon, 1988) p.93

[124] Nagel, T. *Mortal Questions* (Cambridge: Cambridge University Press, 1979) p.72

threat, is a legitimate target. It is thus possible to categorise weapons as more or less humane depending on the nature of the weapon, and that some weapons are prohibited as a result. Nagel argues that, "one can justify prohibitions against certain particularly cruel weapons: starvation, poisoning, infectious diseases, weapons designed to main or disfigure or torture" according to the claim "that such weapons attack the men, not the soldiers".[125] Clark notes that this indeed might sound slightly paradoxical idea to some in that the soldier should "lose his right to life (arguably the most important right of all) and yet retain some rights over the manner of his death (arguably a right of the second order)".[126] However, it can be argued that there are instances where being treated inhumanely or being killed in an inhumane manner is worse than a humane death. Indeed, codes of war reflect this understanding and are uniquely concerned with the drawing of lines between different weapons of war. These lines are often drawn either prohibiting the use of weapons because they cannot discriminate between legitimate and illegitimate targets or because they are considered inhumane as a result of the type or level of harm they cause and therefore are prohibited regardless of the target. Accordingly, the St. Petersburg Declaration of 1868, *Renouncing the Use, in Time of War, of Explosive Projectiles,* the 1899 *Declaration on the Use of Bullets Which Expand or Flatten Easily in the Human Body*, the 1980 *Protocol II on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices* (amended in 1996) each renounce the use of certain weapons established on the argument that the weapons should not be employed given that they are "designed or of a nature to cause superfluous injury or unnecessary suffering".[127] If we follow the premise that even fully assimilated combatants are still illegitimate targets for certain weapons because of their inhumane nature, then it is clear that torture, as the epitome of inhumane treatment, will never be able to find a legitimate target.

Torture represents an activity that is inhumane in the extreme. It encompasses a set of activities that violate all of an individual's most vital interests, inflicting the highest level of physical, psychological and emotional pain. Even though it does not kill it is more inhumane in its treatment and therefore should be prohibited absolutely. As Henry Shue argues, "Torture is usually humiliating and degrading – the pain is normally experienced naked and amidst filth. But while killing destroys life, it need not destroy dignity."[128] It can be argued therefore, that in the case of torture there is no act that the individual could perform that

[125] Nagel, T. *Mortal Questions* (1979) p.71
[126] Clark, I. *Waging War* (1988) p.93
[127] *Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices* as amended on 3 May 1996, Article 3 §3.
[128] Shue, H. 'Torture' (1978) p.126

would result in him waiving the right that protects him from being tortured. Essentially, when it comes to torture, everyone, even combatants, are illegitimate targets.

Conclusion

Blackmail and torture are two topics for intelligence collection that have received much attention from academic, professional, and popular communities. In recent years there has been increased pressure on the intelligence community to assume an aggressive stance on intelligence collection; to be seen to be going out and producing intelligence so as to prevent such catastrophes from happening again. This chapter has explored these activities, outlining the tactics used as well as the types of harms they can each cause. What this chapter has demonstrated is, first, that blackmail causes a high level of harm and so its use should be strictly limited and, second, that the level of harm caused by torture is of such a special quality that its use is absolutely prohibited as there is no possible case that could fulfil the Just Intelligence Principles of just cause and discrimination. By combining the work done in this chapter with the work from previous chapters it is possible to now establish an overall Ladder of Escalation.

Conclusion

This thesis started with the proposition that the field of intelligence lacked any coherent, rigorous or systematic ethical review. That is, intelligence has never developed an ethical framework that offered a means of determining if and when intelligence is ethically justified. The Introduction argued that this is unacceptable. Intelligence can claim no *a priori* entitlement to be excluded from the realm of ethics and as such requires an ethical framework specifically designed for intelligence that outlines if and when its activities are justified.

After reviewing well established ethical frameworks such as realism, consequentialism and deontology, it was argued that none are an appropriate means for ethically evaluating intelligence. It was argued that realism is unsuitable since it places too much emphasis on what the state might deem expedient and, as such, ignores some important limits that should be put on intelligence usage.[1] Consequentialism, such as Michael Herman's "ethical balance sheet",[2] presented the problem of being too permissive for some of the more damaging intelligence collection activities as well as presenting several difficulties resulting from the "highly complex computations of goods and harms required".[3] Finally, deontology would be too restrictive and unable to take into account the important ethical role intelligence plays. The Introduction therefore concluded that the most appropriate ethical framework for intelligence collection would be one that takes into account both the ethical role that intelligence plays in protecting the political community as well as the harm that intelligence can cause.

Chapter One, therefore, developed an ethical framework that was able to achieve this aim. It argued that intelligence collection as an activity can cause harm by coming into conflict with an individual's 'vital interests', or those preconditions that every individual needs maintained in order to achieve his version of the good life. Chapter One argued that these vital interests include maintaining an individual's physical and mental integrity, autonomy, liberty, sense of self-worth and privacy. Moreover, it was argued that since these vital interests can be violated to varying degrees, it is possible to have varying levels of harm. The level of harm caused is dependent on which of the vital interests are violated, the severity of the violation and the duration or repetition of the violation. This means that different

[1] Erskine, T. 'As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering' *Intelligence and National Security*, Vol. 19, No. 2 (2004) p.365-266
[2] Herman, M. *Intelligence Services in the Information Age* (London: Frank Cass ,2001) p.203
[3] Gill, P. 'Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'?' *Intelligence and National Security* Vol.24 No.1 (2009) p.90

intelligence collection activities can cause different levels of harm, which can then be spread along a metaphorical Ladder of Escalation according to the specific harm they cause to the individual. Once the level of harm is understood, the intelligence activity can be examined in the context of the Just Intelligence Principles to determine if the harm caused is justified or not. These principles are based on the just war tradition and are designed to reflect the ethical good that intelligence can do while limiting the harm intelligence can cause.

By applying this ethical framework to a series of intelligence collection activities, divided into four chapters according to the different collection disciplines, this thesis explored the ethical framework in greater detail while illustrating how it can work in practice. The collection disciplines explored are imagery intelligence, signals intelligence, indirectly coercive human intelligence and directly coercive human intelligence.

In Chapter Two, the ethical framework was applied to imagery intelligence. By discussing what imagery intelligence entails the chapter outlined four illustrative examples: satellites and spy-planes, CCTV cameras, intensive surveillance and intrusive surveillance. These illustrative examples are designed to explore in greater depth the way that imagery intelligence comes into conflict with an individual's vital interests, namely the interest in privacy and autonomy. It first argued that individuals maintain a degrees of control over their image as well as arguing that there is a difference in the degree of privacy that can be expected depending on where individual is. Secondly, it was argued that if an individual feels he is being watched he is likely to alter his behaviour so as to coincide with the will of the watcher, thus affecting his autonomy. It was concluded that CCTV cameras on passive scan feature at the lowest level on the Ladder of Escalation, the Initial Level, because they only minimally violate the individual's interest in privacy and autonomy. However, focusing or tracking a specific individual represented a greater violation of privacy and, as such, caused a slightly higher level of harm, that is Level One. However, by making reference to the power of the Panoptic Gaze, it was also argued that pervasive monitoring of individuals will likely cause an unwarranted effect on social cohesion as well as affecting the autonomy of those individuals not directly targeted. Therefore, *en masse* or pervasive monitoring through CCTV cameras can cause an increased level of harm.

Intensive surveillance was a greater violation of an individual's privacy given its ability to monitor the individual in both greater quantity and quality, causing a Level Two harm. Finally, it was argued that intrusive surveillance is the highest privacy violation out of the imagery intelligence activities. This is because it violates a sphere of privacy that is established both socially and legally as one of the most intimate and therefore maintains a

greater degree of privacy. Monitoring an individual in his house therefore causes a Level Three harm.

Once the particular level of harm was established, the activities were put in context of the Just Intelligence Principles so as to determine if their use is justified or not. It was shown that CCTV cameras on passive scan can almost always be justified as long as their usage is controlled so as to not cause the detrimental effect of the Panoptic Gaze that was mentioned. Intensive CCTV scans can also be justified providing that the operator is careful to distinguish between the average citizen and those who cause a breach of the peace. Intensive surveillance, it was demonstrated, should be restricted to operations where there is at least a probable threat and should only target those who are connected to the threat in some way. Finally, it was concluded that intrusive surveillance can only be done when it is demonstrated to a third party that there is a significant threat and when the intelligence operatives only target those who are directly related to the threat.

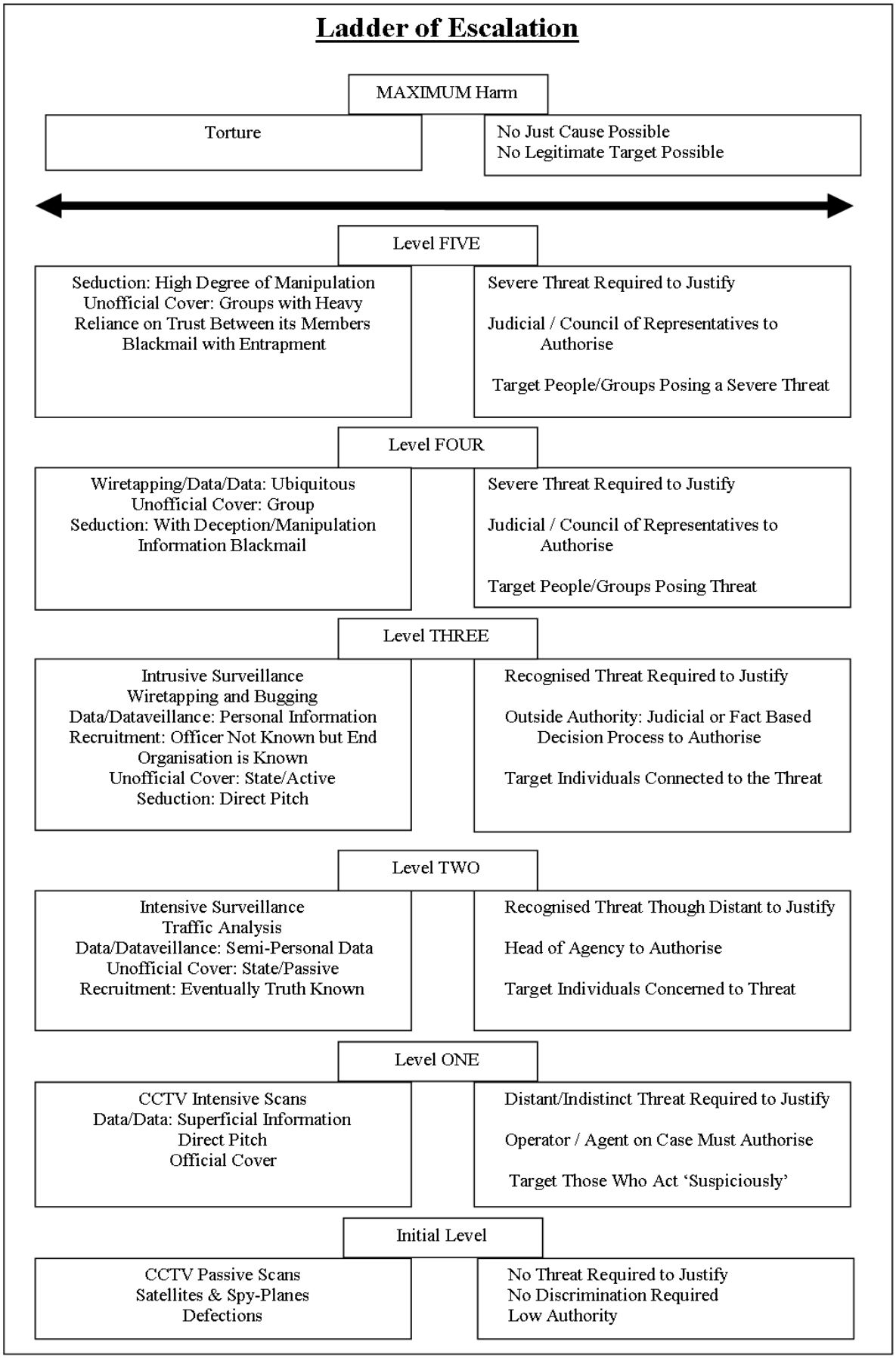
Chapter Three focused on the use of signals intelligence and the growing emphasis on the information nation. This chapter discussed the use of signals intelligence to gather information on an individual's communication network, interception of electronic communications and the ability to listen-in on private conversations. It also discussed the new and growing use of databases and the ability to collect, manipulate and store a whole gamut of private information through data-mining and dataveillance. This chapter furthered the work done on privacy by arguing that the level of privacy associated with an individual's information is the result of how intimate or personal it is. As a result, collecting superficial data through either dataveillance or data-mining featured at Level One, while collecting information on something more intimate – relationship networks through traffic analysis for example – would cause a Level Two Harm. It was also argued that there exists an important and well established sphere of privacy around an individual's communications, even if the signal carrying the communication leaves the individual's private property. Therefore, using devices to listen-in on an individual's conversation or to intercept an electronic communication causes a Level Three Harm. Finally, it was argued that ubiquitous electronic monitoring can have detrimental effects on society as well as on the autonomy of individuals not directly targeted, which causes an increase in the level of harm. One of the important conclusions in this chapter was that for those activities that cause harms at Level Three or Level Four, could not be used *en masse* given their inability to discriminate between legitimate and illegitimate targets.

In Chapters Four and Five the use of human intelligence was discussed, with the cases divided between the two chapters according to whether the actions are directly or indirectly coercive. Chapter Four focused on the use of deception, manipulation and seduction as the main means of recruiting intelligence agents and securing access to information. As a result this chapter examined the various relationships that an intelligence operative can establish with a target and outlined the various levels of harm caused when the tactics used come into conflict with the target's autonomy or sense of self-worth. It argued that those actions that use a limited degree of manipulation – bribery and official covers for example – are the least harmful and are at Level One on the Ladder of Escalation; general unofficial covers and recruitments that involve a slightly higher level of manipulation but where the individual is aware of who he works for causes a Level Two harm; whereas manipulation cases where the individual does not know who he works for are Level Three. The use of seduction as the means for ensuring cooperation then causes Level Four and Five harms as a result of the increase in manipulation and the violation of a more intimate sphere.

Chapter Five discussed the use of more directly coercive methods such as blackmail and torture. It examined the harm that blackmail causes the individual as a result of the effect it has on the individual's autonomy as well as the emotional distress it can cause. It concluded that as a result of the significant degree to which it affects the individual's sense of self-worth and autonomy it can cause a Level Five harm. It also examined the use of torture, outlining the various methods employed by a torturer and detailing the impact these can have on the human body. It argued that, as an activity, torture is one of the most extreme forms of attack the body can suffer, representing the utter destruction of all an individual's most vital interests. As such, the harm torture causes features at a separate level on the Ladder of Escalation above all the others, called a Maximum Level, where only the most severe activities exist. At this special level the use of torture is absolutely prohibited. There can be no just cause nor can any individual ever act in such a way as to waive or forfeit his right to not be tortured.

What the Figure 6.0 of the Ladder of Escalation below demonstrates is how the various activities presented in this thesis relate to each other according to the level of harm they can cause and what standards, if any, must be met in order for their use to be justified.

Figure 6.0


Ladder of Escalation
MAXIMUM Harm
Torture
No Just Cause Possible
No Legitimate Target Possible
Level FIVE
Seduction: High Degree of Manipulation
Unofficial Cover: Groups with Heavy Reliance on Trust Between its Members
Blackmail with Entrapment
Severe Threat Required to Justify
Judicial / Council of Representatives to Authorise
Target People/Groups Posing a Severe Threat
Level FOUR
Wiretapping/Data/Data: Ubiquitous
Unofficial Cover: Group
Seduction: With Deception/Manipulation
Information Blackmail
Severe Threat Required to Justify
Judicial / Council of Representatives to Authorise
Target People/Groups Posing Threat
Level THREE
Intrusive Surveillance
Wiretapping and Bugging
Data/Dataveillance: Personal Information
Recruitment: Officer Not Known but End Organisation is Known
Unofficial Cover: State/Active
Seduction: Direct Pitch
Recognised Threat Required to Justify
Outside Authority: Judicial or Fact Based Decision Process to Authorise
Target Individuals Connected to the Threat
Level TWO
Intensive Surveillance
Traffic Analysis
Data/Dataveillance: Semi-Personal Data
Unofficial Cover: State/Passive
Recruitment: Eventually Truth Known
Recognised Threat Though Distant to Justify
Head of Agency to Authorise
Target Individuals Concerned to Threat
Level ONE
CCTV Intensive Scans
Data/Data: Superficial Information
Direct Pitch
Official Cover
Distant/Indistinct Threat Required to Justify
Operator / Agent on Case Must Authorise
Target Those Who Act 'Suspiciously'
Initial Level
CCTV Passive Scans
Satellites & Spy-Planes
Defections
No Threat Required to Justify
No Discrimination Required
Low Authority

What can be seen from this Ladder of Escalation is that the activities are indeed comparable and can be separated into various levels. Defections from Chapter Four are comparable to the use of passive CCTV scans, satellites and spy-planes discussed in Chapter Two as they all cause the minimal level of harm, and therefore require the lowest level of the Just Intelligence Principles. Offering a direct pitch, using official cover, and intensive use of CCTV cameras cause a similar degree of harm to each other at Level One, even though it can be argued that they affect the individual in quite different ways. Level Two activities include the use of low-level manipulation, traffic analysis and intensive surveillance and therefore require a ranking officer with a reasonable just cause to authorise their use. Level Three includes the most activities, such as the more severe violation of an individual's privacy, some quite severe manipulation tactics and the lower levels of seduction. This level sees the first instance where the authorisation must come from outside the intelligence agency and begins to limit the range of appropriate just causes. Level Four and Level Five feature some of the strongest manipulation and seduction cases, demanding a significant level of authorisation and a clear and present threat to act as a just cause. Finally, at the very top of the ladder is torture, demonstrating how it is above and beyond any other activity discussed and is absolutely prohibited.

Contributions

The Introduction took great effort to argue that intelligence as a field of study and as a practice is one that is starved of an appropriate ethical theory. Given the tendency of the intelligence community to act out of sight and its relatively young official history, there has been little work done on creating an appropriate ethical framework. While there is work that examines some of the more prominent ethical schools of thought and how they would interpret intelligence activities, most notably Toni Erskine's article *Rays of Light to Human Soul*, there has been no attempt to create an ethical theory specifically designed for intelligence.[4] It can be argued, therefore, that a significant contribution of this thesis is the fact that it provides an appropriate ethical framework designed specifically for intelligence. This thesis seeks to further establish the relatively new and increasingly important sub-field of 'intelligence ethics', and in doing so contributes greatly to the separate fields of intelligence studies and ethical theory. By highlighting the ethical good that intelligence collection represents and balancing it against the harm that it can cause to individuals, the

[4] Erskine, T. 'As Rays of Light' (2004) pp.359-81

ethical framework advanced in this thesis offers the criteria for determining when particular intelligence activities are prohibited and when they are permissible.

It was argued in the Introduction that any ethical framework for intelligence must be able to recognise that each intelligence collection activity will differ from its siblings and so a broad justification for the use of intelligence collection would be insufficient. As a result, one of the main benefits of the ethical framework advanced in this thesis is its flexibility, that it can be applied to a range of very different intelligence collection activities, evaluating them according to a common measure and deciding whether each action is justified or not. Therefore, the ethical framework itself is one of the greatest contributions of this thesis as there has previously been no work that offers a common standard against which to judge intelligence collection activities nor has there been a systemic framework for deciding when, if ever, its use is justified. Furthermore, the use of varying levels makes explicit how the different intelligence activities relate to each other, offering a deeper understanding of the field of intelligence as a whole. One of the main contributions of this thesis is, therefore, that it seeks to apply the ethical framework developed to a range of intelligence activities and offer ethical statements or conclusions in light of the cases as presented. However, the thesis does not seek to make any statement on the veracity of the cases or the sources from which they came. As noted in the introduction, the cases are used as a basis for the discussion of the principles of harm and are not meant to strengthen scholars' knowledge of a particular range of information.

Carrying out the intellectual process required to develop the main arguments of the thesis has also resulted in several additional contributions that this thesis can offer. One such contribution is the result of the interrogation of the ethical literature that was carried out in order to create the ethical framework. The Introduction noted that realism, consequentialism and deontology each had something interesting and important to say about intelligence, but that none alone could offer an appropriate ethical framework for intelligence for various reasons. Furthermore, it was demonstrated how these ethical schools often came into conflict with each other, presenting a mutually exclusive relationship. The methodology stated that it would pursue a pluralistic investigation of these different ethical positions in order to create a framework that was capable of incorporating the most important factors from each school. As a result, the ethical framework established is one that is capable of balancing the ethical importance of the political community highlighted by the realist school, the ethical good that intelligence could cause as a consequence, as argued for by consequentialism, the ethical equality of all individuals as required by both consequentialism and deontology, and finally

the need to stress limits and absolute prohibitions when necessary, an important feature of the deontological school. By advancing the notion of harm and developing the Just Intelligence Principles as the most appropriate basis for the ethical framework, this thesis was able to effectively incorporate key lessons from the three ethical schools of thought. In doing so it contributes greatly to the field of ethical theory. Furthermore, the creation of this ethical framework also contributes to the so-called cosmopolitan-communitarian debate as it highlights and balances the ethical primacy of the individual against the important and ethical role the community can play.

Furthermore, by exploring the notion of harm and the ethical norms established by the just war tradition, this thesis offers these sub-fields some important contributions. By drawing predominantly upon the work of Andrew Linklater and Joel Fienberg, Chapter One argued that all individuals have a set of vital interests that are preconditions for carrying out the good life and that if these interests are violated in a substantial way then the individual is harmed as a result.[5] Chapter One was then able to advance the existing bodies of literature by arguing that an individual's vital interests should include his physical and mental integrity, his autonomy, liberty, sense of self-worth and privacy. Furthermore, by creating the Ladder of Escalation this thesis made clear how and in what ways the harm caused to individuals can vary from activity to activity. In establishing this list of vital interests, outlining why they are fundamental to the individual and the various ways they can be violated, this thesis has advanced the work done on harm by explicitly codifying some of the general notions that are being discussed in the literature.[6]

By developing and producing a systematic means of outlining how an activity can cause an individual harm, this thesis is also able to offer interesting contributions to the debates that revolve around the ethical acceptability of various activities. For example, the thesis examined how deception, manipulation, seduction, interference with private property, interception of communications and even having one's photograph taken can cause harm to the individual and, in doing so, contributes to each of their relevant debates. For example, the ethic against harm developed throughout the thesis proposes some appealing thoughts on the issues of torture and blackmail. For torture, given the fear of further terrorist attacks like those seen on September 11, 2001 and July 7, 2005, questions regarding how intelligence communities should act when facing extreme scenarios are being re-examined. What the

[5] Feinberg, J. *Moral Limits of the Criminal Law: Vol.1 Harm to Others* (Oxford: Oxford University Press, 1984) pp.31-38; Linklater, A. *The Problem of Harm in World Politics: Theoretical Investigations* (Cambridge: Cambridge University Press, 2011)
[6] Feinberg, J. *Harm to Others* (1984) pp.45-51

ethical framework established in this thesis offers is a new way of examining the debate. The harm ethic presented in this thesis suggested a new way of highlighting the effect torture can have on the individual and outlined what it is about torture that is ethically unacceptable. By examining the different types of activities that qualify as torture in the context of the vital interests put forward in Chapter One, it is possible to understand how torture received the special classification of harm labelled Maximum Harm. By examining this Maximum Harm level with respect to the Just Intelligence Principles it was then also possible to better understand the absolute prohibition that should be placed on torture.

Examining the case of blackmail also gave the opportunity for the harm ethic to offer something new to another existing debate. There is much literature that argues that the prohibition against blackmail is a paradox, given that those actions used are themselves not necessarily ethically prohibited.[7] As a result there has been much effort to detangle this paradox and outline why blackmail should be prohibited. For example, Leo Katz suggests that blackmail is analogous to robbery given that it involves taking property from a target and should be prohibited along these lines.[8] However, conceiving of blackmail in this way fails to engage with blackmail that does not take property but requires the target to carry out a specific act. It would be difficult to call this theft. Furthermore, while Michael Gorr argues that blackmail should be prohibited as it represents an assault, it seems apparent that to classify revealing someone's indiscretion as an assault is too much.[9] Indeed, it could be argued that informing someone of their spouse's adultery is an ethically praiseworthy endeavour and to widen the definition of assault too much is to lose some of the important impact it has. In comparison, what this thesis offers is a way of ethically evaluating blackmail that is not seen in the literature. By examining the way blackmail violates and controls an individual's will and highlighting how autonomy represents a most vital interest for the individual, it is possible to understand why blackmail should be considered ethically unacceptable.

Another contribution offered by this thesis is to the literature dedicated to the just war tradition. As a result of examining the just war tradition in order to develop the Just Intelligence Principles one important contribution is the way the thesis reiterates the contemporary importance of the just war tradition. Nicholas Rengger notes that as the world

[7] See Clark, M. 'There is No Paradox of Blackmail' *Analysis* Vol.54 No.1 (1994) pp.54-61; Lindgren, J. 'Unravelling the Paradox of Blackmail' *Columbia Law Review* Vol.84 No.3 (1984) pp.670-717; and Gorr, M. 'Liberalism and the Paradox of Blackmail' *Philosophy and Public Affairs* Vol.21 No.1 (1992) pp.43-66

[8] Katz, L. 'Blackmail and Other Forms of Arm-Twisting' *University of Pennsylvania Law Review* Vol.141 No.5 (1993) pp.1567-1615

[9] Gorr, M. 'Liberalism and the Paradox of Blackmail' (1992) pp.43-66

moves into the twenty-first century "many of the central aspects of the just war tradition... are becoming ever more etiolated" and that the suitability of the tradition has received attacks from many different quarters.[10] However, while there are those that argue the just war tradition is losing its relevance, by going back to its ethical roots, highlighting its importance in balancing the need to protect the political community with the harm that certain actions can cause, along with a re-examination of the various just war criteria, the importance of the just war tradition is emphasised. Also, by using the just war tradition as the basis for the Just Intelligence Principles it makes clear the versatility of the ethical norms the tradition represents as well as the benefits it can offer the field of intelligence studies. Furthermore, the Just Intelligence Principles themselves offer interesting reinterpretations of the traditional criteria and as such suggest important contributions to the broader just war literature. For example, the redefinition of the principle of discrimination outlined in this thesis challenges and expands on the traditional formulation. According to the traditional view of the principle of discrimination, a relatively strict distinction between legitimate and illegitimate targets is established between combatants and non-combatants. The Just Intelligence principle of discrimination offers a gentle breakdown of this strict dichotomy so as to include new groups as legitimate targets, such as non-combatants who represent varying levels of threat. However, this is a gentle breakdown of the dichotomy in that one of the benefits of the principle of discrimination offered is that the harm allowed is in proportion to the threat the individual represents, meaning that there are still important limits placed on who is a legitimate target.

One final contribution of the work done in this thesis is the flexibility and practical application that the ethical framework represents. That is, it was the intention that the ethical framework would form the basis of a suitable set of legal and cultural rules that can limit and govern the use of intelligence collection. The evaluations made in each of the collection discipline chapters offers important conclusions on the types of rules that should be implemented. As a result, this thesis offers a foundation for outlining rules and regulations for governing the use of intelligence collection. Furthermore, it was not the intention of this thesis to offer an exhaustive examination of all the collection activities used and all the scenarios in which they can be employed. Rather, the ethical framework was designed to be flexible so that its principles can be applied to those activities which have not yet been

[10] Rengger, N. 'On the Just War Tradition in the Twenty-First Century' *International Affairs* Vol.78 No.2 (2008) p.361

discovered. As such, this thesis offers an important way forward when assessing the ethical status of a variety of intelligence collection activities.

Avenues for Further Investigation

While this thesis has endeavoured to develop an ethical framework that offers a full and rigorous evaluation of intelligence collection, there are always more questions to be asked and areas to investigate. One of the contributions of the thesis was to provide the tools necessary for other works on intelligence ethics to be established. One obvious direction for further investigation is how this ethical framework can be translated into practice. The ethical framework established in this thesis offers the opportunity for other works to develop legal rules for intelligence collection. The ethical framework was developed with the intention that it should be applicable to real situations, as demonstrated throughout each chapter with the use of illustrative examples. There is, therefore, a real opportunity for the ethical framework to be developed into a code of conduct in some form.

Another important direction in which this work could be developed involves using the ethical framework created to explore some case examples not yet developed or discussed here. As previously noted, it was not the aim of this thesis to provide an utterly exhaustive examination of all intelligence collection activities, but rather to use the illustrative examples as a means of exploring the ethical framework in greater depth while demonstrating how it might be put into practice. This means that there is opportunity for other works to utilise the ethical framework developed in this thesis in order to evaluate intelligence collection activities that are now beginning to be developed. For example, given the growing role of the Internet and the power to monitor individuals through their electronic activity there is avenue to advance the work started in Chapter Three. Closely related to this is the opportunity to use the work done in this project to ethically evaluate past intelligence collection events. One of the benefits of the just war tradition is that it is a useful tool for ethically evaluating in hindsight actions done or wars started. Similarly, by using the tools developed in this thesis it is possible to evaluate past intelligence collection events and make judgements as to whether the conduct included was ethical or not.

A final opportunity this work offers is the possible development of this ethical framework for application to non-state intelligence actors. The main focus of this thesis was the development of an ethical framework for intelligence carried out by the state with the aim of protecting the political community. However, intelligence collection as a practice is no longer confined to the state. Indeed, there are companies carrying out intelligence collection

for both their own private ends as well as on behalf of other states or political communities. What would be interesting is to see how the work done in this thesis would relate to these different areas, given that the end to which private actors work towards is fundamentally different to that of state-run intelligence institutions. That is, how does the need to make a profit alter the ethical calculations, limits and conclusions as compared to those made in this thesis where the end goal was the protection of the political community.

This thesis posed the problem of how intelligence collection should be ethically evaluated. In brief, intelligence collection is a vital and even indispensible tool for protecting the political community from a variety of internal and external threats. However, intelligence collection involves activities that can cause severe harm to those it targets and, as such, without further justification would not be allowed. As Michael Quinlan argued, "we cannot say that morality must simply be set aside; we have to identify some conceptual structure for legitimising and disciplining the activity of intelligence". [11]

In developing an appropriate ethical framework for intelligence collection it is essential to recognise that it involves a myriad of activities, making an all-encompassing declaration on its ethical status not only unhelpful but impossible. Instead, there is a need for an ethical framework that is nuanced, one able to evaluate different activities and compare them with each other. Furthermore, it is essential that any ethical framework established is able to incorporate both the ethical good intelligence provides the political community while limiting the harm it can cause. In response, this thesis has proposed an ethical framework consisting of two important parts. The first delineates the harm that intelligence collection can cause, making it clear what it is about intelligence collection that gives it a "baggage of unworthiness", while the second outlines a framework that both limits the use of intelligence collection and acknowledges those situations when the harm is justifiable.[12]

By advancing the Ladder of Escalation as the most appropriate ethical framework for evaluating intelligence collection, it is possible to understand the dual quality of intelligence collection: that intelligence collection does indeed cause harm which needs limiting, and that sometimes this harm is necessary in order to protect those for whom a political community carries responsibility.

---

[11] Quinlan, M. 'Just Intelligence: Prolegomena to an Ethical Theory' *Intelligence and National Security* Vol.22 No.1 (2007) p.12

[12] Herman, M. 'Ethics and Intelligence after September 2001' *Intelligence and National Security* Vol.19 No.2 (2004) p.342

Bibliography

Official Material

Annan, K. 'The Secretary-General Address to the General Assembly' *United Nations,* New York, 23rd September 2003. Transcript available at http://www.un.org/webcast/ga/58/statements/sg2eng030923.htm Accessed 1st May 2010

Bush, G. W. 'Notice: Detention, Treatment and Trial of Certain Non-Citizens in the War Against Terrorism' *White House*, November 13 2001, Federal Register Vol.22 No.2 pp.57831-57836 available in *The Torture Papers: The Road to Abu Ghraib* edited Greenberg, K. J. And Dratel, J. L. (Cambridge: Cambridge University Press, 2005) pp.25-28

Cabinet Office, *E-Government: A Strategy for Modernising Government* (1999) CM4310 1999 p.4.
Available at http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm Accessed 1st May 2008

Church Committee *Final Report* Book 1 p.344 Available at
http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm
Accessed 4th April 2009

CIA Website *Intelligence Oversight* https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/intelligence-oversight/ Accessed 1st March 2011

Council of Europe, Parliamentary Assembly: 'Alleged Secret Detention and Unlawful Inter-State Transfers of Detainees Involving Council of Europe Member States' Report by Rapporteur Dick Marty, Doc 10957, 12th June (First Report, 2006). Available at http://assembly.coe.int/Documents/WorkingDocs/doc06/edoc10957.pdf
Accessed 4th November 2010

Council of Europe, Parliamentary Assembly: 'Secret Detentions and Illegal Transfer of Detainees Involving Council of Europe Member States' Report by Rapporteur Dick Marty, Doc.11302rev, 11th June 2007. Available at
http://assembly.coe.int/Documents/WorkingDocs/Doc07/edoc11302.pdf
Accessed 4th November 2010

Department of Justice, Office of Legal Counsel, Memorandum for William J. Haynes, General Counsel, Department of Defence, From: John Yoo, Deputy Assistant Attorney General, 'Application of Treaties and Laws to Detainees', available in *The Torture Papers: The Road to Abu Ghraib* edited Greenberg, K. J. And Dratel, J. L. (Cambridge: Cambridge University Press, 2005)

Home Office *Protecting the Public in a Changing Communications Environment* April 2009 Available at http://www.parliament.uk/deposits/depositedpapers/2009/DEP2009-2754.pdf
Accessed 10th May 2010

House of Lords: Select Committee on the Constitution *Surveillance: Citizens and the State* 2nd Report of Session 2008–09 (6th Feb. 2009) Available at

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/surveillance_report_final.pdf Accessed 9th July 2009

Human Genetics Commission 'Nothing to Hide, Nothing to Fear? Balancing Individual Rights and the Public Interest in the Governance and Use of a National DNA Database' *A Report by the Human Genetics Commission* November 2009. Available at: http://www.hgc.gov.uk/UploadDocs/DocPub/Document/Nothing%20to%20hide,%20nothing%20to%20fear%20-%20online%20version.pdf Accessed 4th April 2010

Intelligence and Security Committee *Rendition* (July, 2007) cm.7171 Online Access: http://www.fas.org/irp/world/uk/rendition.pdf Accessed 7th December 2010

Minutes of the Second Congress of the Communist International, *Evening Session* 4th August 1920. Available at http://www.marxists.org/history/international/comintern/2nd-congress/ch10a.htm Accessed August 2010

Parker, 'Report of The Committee of Privy Counsellors Appointed to Consider Authorised Procedures for the Interrogation of Persons Suspected of Terrorism' (1972) Cmd 4901. Held at *Conflict Archive on the Internet* in collaboration with University of Ulster. Available at http://cain.ulst.ac.uk/hmso/parker.htm#2 Accessed November 2010

Parliamentary Assembly of the Council of Europe *Democratic Oversight of the Security Sector in Member States* Recommendation Doc.1713 (Strasbourg, 23 June 2005) Available at http://assembly.coe.int/Documents/AdoptedText/ta05/EREC1713.htm Accessed 16th April 2008

Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs *Secret Detentions and Illegal Transfers of Detainees by Council of Europe Member States* Doc.11302 (Strasbourg 11th June 2007) Available at http://assembly.coe.int/Documents/WorkingDocs/Doc07/edoc11302.pdf Accessed 16th April 2008

Rose, C., Chief Surveillance Commissioner *Report on Two Visits by Sadiq Khan MP to Babar Ahmad at HM Prison Woodhill* Presented to Parliament by the Secretary of State for the Home Department (February 2008) Cmnd.7336. Available at http://www.official-documents.gov.uk/document/cm73/7336/7336.pdf Accessed 16th April 2008

Secret Intelligence Services Website *Legislation and Accountability* https://www.sis.gov.uk/about-us/legislation-and-accountability.html Accessed 1st March 2011

Tagbua, A. *Article 15-6 Investigation of the 800th Military Police Brigade [The Taguba Report]* (2004) Available at http://www.npr.org/iraq/2004/prison_abuse_report.pdf Accessed 1st May 2007

United States Marine Corp 'Signals Intelligence' *Marine Corp War Fighting Publication* 2-15 (1999) Available at http://www.fas.org/irp/doddir/usmc/mcwp2-15-2.pdf Accessed 16th April 2008

Media Material

BBC News 'Extent of Council Spying Revealed' 26th March 2009 Available at http://news.bbc.co.uk/1/hi/7964411.stm Accessed 1st May 2009 Accessed 9th July 2009

BBC News 'Giant Database Plan Orwellian' October 15th 2008. Available at http://news.bbc.co.uk/1/hi/uk_politics/7671046.stm
Accessed 1st November 2008

BBC News 'Plan to Monitor all Internet Use' Monday 27th April 2009. Available at http://news.bbc.co.uk/1/hi/8020039.stm Accessed 29th April 2009

BBC News 'Warning over Phone Calls Database' 15th July 2008. Available at http://news.bbc.co.uk/1/hi/uk_politics/7507627.stm Accessed 1st November 2008

Chakrabarti, S. BBC Radio Four *Analysis*: *Secrets and Mysteries Broadcast Date: 19th April 2007 CD number: PLN716/07VT1015*

Cobain, I., Grey, S. and Norton-Taylor, R. 'Destination Cairo: Human Rights Fears Over CIA Flights' *The Guardian* 12th September 2005. Available at
www.guardian.co.uk/print/0,,5283268-105744,00.html Accessed 6th November 2010

Dempsey, J. 'German Foreign Minister Under Fire On Human Rights - Europe - International Herald Tribune' *The New York Times* 31st January 2007. Copy available at http://www.nytimes.com/2007/01/31/world/europe/31iht-berlin.4421471.html?scp=1&sq=German%20Foreign%20Minister%20Under%20Fire%20over%20Guantanamo%20Bay%20Detainee&st=cse Accessed 6th November 2010

Grey, S. and Natta, D. 'Thirteen with the C.I.A. Sought by Italy in a Kidnapping' *New York Times* 25th June 2005. Available at
http://www.nytimes.com/2005/06/25/international/europe/25milan.html
Accessed 6th November 2010

Pincus, W. 'Silence of 4 Terror Probe Suspects Poses Dilemma' *Washington Post* October 21st (2001) A06

Quinlan, M. BBC Radio Four *Analysis*: *Secrets and Mysteries Broadcast Date: 19th April 2007 CD number: PLN716/07VT1015*

Rose, D. 'They Tied Me Up Like a Beast and Began Kicking Me' *The Guardian* 16th May 2004. Available at http://www.guardian.co.uk/world/2004/may/16/terrorism.guantanamo. Accessed 4th November 2010

Safire, W. 'You are a Target' *The New York Times* 12th November 2002 p.A35

Shane, S. 'Outfitting Spies with New Tools: Moral Compass' *New York Times* 28th January 2006 A1

Wakefield, J. 'Surveillance Cameras to Predict Behaviour' BBC News 1st May 2002. Available from http://news.bbc.co.uk/1/hi/sci/tech/1953770.stm Accessed 20th May 2009

Civil Society Material

Amnesty International, *Amnesty International: Report on Torture* (London: Duckworth, 1973)

Amnesty International *Cruel. Inhuman. Degrades Us All: Stop Torture and Ill-Treatment in the "War on Terror"* 31st July 2005 Available at http://www.amnesty.org/en/library/asset/ACT40/010/2005/en/69c95ca2-d4c6-11dd-8a23-d58a49c0d652/act400102005en.pdf Accessed 4th November 2010

Amnesty International, 'UK: Human Rights: A Broken Promise' 23rd February 2006. Available at http://www.amnesty.org/en/library/asset/EUR45/004/2006/en/cc167867-d45b-11dd-8743-d305bea2b2c7/eur450042006en.pdf. Accessed 7th November 2010

Isaacs, R. 'What constitutes Suspicious Behaviour and What to do About it?' *The Lubrinco Group* Available at http://www.lubrinco.com/articles/Informed%20Sources%20November%202003.pdf. Accessed May 1st 2009

JUSTICE *Keeping the Right People on the DNA Database: Science and Public Protection* July 2009 Available at http://www.justice.org.uk/images/pdfs/Home%20Office%20NDNAD%20cnsltn%20response%20july%2009.pdf Accessed 4th April 2010

Liberty *DNA Retention* Available at http://www.liberty-human-rights.org.uk/human-rights/privacy/dna-retention/index.php Accessed 4th April 2010

Reprieve 'Enforced Disappearance, Illegal Interstate Transfer, and Other Human Rights Abuses Involving the UK Overseas Territories' (2007). Online Access: http://www.statewatch.org/news/2008/feb/uk-usa-reprieve-submission-FASC.pdf

Academic Sources

Adler, J. E. 'Lying, Deceiving, or Falsely Implicating' *The Journal of Philosophy* Vol.94 No.9 (1997) pp.435-452

Aginger, J and Hemmager, E. 'Unusual Neural Conditions Following Hunger Period of 1945-46' *Archive of Psychiatry* Vol.186 (1951) pp.483-495

Aid, M. M. and Wiebes, C. 'Introduction to the Importance of Signals Intelligence During the Cold War' *Intelligence and National Security* Vol.16 No.1 (2001) pp.1-26

Alexander, L. 'Self-Defence and the Killing of Non-Combatants: A Reply to Fullinwider' *Philosophy and Public Affairs* Vol.5 No.4 (1976) pp.408-415

Allen, T. B. and Polmer, N. *Merchants of Treason: America's Secrets for Sale* (New York: Delacorte Press, c1988)

Allhoff, F. 'A Defence of Torture: Separation of Cases, Ticking-Time Bombs, and Moral Justification' *International Journal of Applied Philosophy* Vol.19 No.2 (2005) pp.243-264

Allodi, F. 'Somoza's National Guard: A Study of Human Rights Abuses, Psychological Health and Moral Development', in *The Politics of Pain Torturers and their Masters* edited Crelinsten, F. D. and Schmid, A. P. (Leiden: Center for the Study of Social Conflicts, 1993), pp.125–140

Allridge, P. 'Attempted Murder of the Soul: Blackmail, Privacy and Secrets' *Oxford Journal of Legal Studies* Vol.13 No.3 (1993) pp.368-387

Altman, I. 'Privacy – A Conceptual Analysis' *Environment and Behaviour* Vol.8 No.1 (1976) pp.7-29

Anderson, K. 'What to do with Bin Laden and Al Qaeda Terrorists?: A Qualified Defence of Military Commissions and United States Policy on Detainees at Guantanamo Bay Naval Base', *Harvard Journal of Law and Public Policy* Vol.25 No.2 (2001) pp.591-635

Andrew, C. *Defence of the Realm: The Authorised History of MI5* (London: Penguin Books, 2010)

Andrew, C. *For the Presidents Eyes Only* (New York: Harper Collins Publishers, 1995)

Andrew, C. *Her Majesty's Secret Service: The Making of the British Intelligence Community* (London: Viking Press, 1986)

Andrew, C. and Gordievsky, O. *Instructions from the Centre: Top Secret Files on KGB Foreign Operations 1975-1985* (London: Sceptre, Hodder & Stoughton, 1993)

Andrew, C. and Mitrokhin, V. *The Mitrokhin Archive: The KGB in Europe and the West* (London: Allen Lane, 1999)

Aquinas, T. 'From *Summa Theologiae'*, in *International Relations in Political Thought* edited by Brown, C., Nardin, T. and Rengger, N. (Cambridge: Cambridge University Press, 2002)

Armstrong, G. and Norris, C. *The Maximum Surveillance Society: The Rise of CCTV* (Oxford: Berg, 1999)

Arneson, R. 'Shame, Stigma and Disgust in the Decent Society' *The Journal of Ethics* Vol.11 No.1 (2007) pp.31-63

Baber, H. E. 'How Bad is Rape' *Hypatia* Vol.2 No.2 (1987) pp.125-138

Baier, A. 'Why Honesty is a Hard Virtue' in *Identity, Character and Morality* (Cambridge: MIT, 1990) pp.259-281

Ball, K. and Webster, F. 'The Intensification of Surveillance' in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age edited* by Ball, K. and Webster, F. (London; Sterling, VA: Pluto Press, c2003) pp.1-15

Bannister, J., Fyfe, N. and Kearns, A. 'Closed-Circuit Television and the City' in *Surveillance, Closed-Circuit Televisions and Social Control* edited by Norris, C., Moran, J and Armstrong, G. (Aldershot: Ashgate, 1998) pp.19-40

Baron, M. W., Pettit, P. and Slote, M. *Three Methods of Ethics* (Oxford: Blackwell, 1997)

Barron, J. *KGB: The Secret Work of Soviet Secret Agents* (New York: Bantam Books, 1974)

Barry, B. *Justice as Impartiality* (Oxford: Oxford University Press, 1998)

Barry, B. 'Some in the Disputation Not Unpleasant' in *Impartiality, Neutrality and Justice: Re-Reading Brian Barry's Justice as Impartiality* edited by Kelly, P. (Edinburgh: Edinburgh University Press, 2000) pp.186-257

Basoglu, M., Jaranson, J. M., Mollica, R., and Kastrup, M. 'Torture and Mental Health: A Research Overview' in *The Mental Health Consequences of Torture* edited by Gerrity, E. Keane, T. M. and Tuma F. (New York: Kluwer, 2001) pp. 35–62

Basoglu, M., Livanou, M. and Crnobaric, C. 'Torture vs Other Cruel, Inhuman, and Degrading Treatment: Is the Distinction Real or Apparent?' *Archives of General Psychiatry* Vol.64 (2007) pp.277-285

Bauman, Z. *Intimation of Postmodernity* (London: Routledge, 1992)

Bayles, M. D. 'A Concept of Coercion' in *Nomos XIV: Coercion* edited by Pennock, J. R. (Chicago: Aldine, 1972) pp.16-29

Bazelan, D. 'Probing Privacy' *Georgia Law Review* Vol.2 No.1 (1997) pp.587-620

Beaney, W. 'The Right to Privacy and American Law' *Law and Contemporary Problems* Vol.31 (1966) pp.253-271

Bellamy, A. J. *Just Wars: From Cicero to Iraq* (Cambridge; Malden, MA: Polity Press, 2006)

Bellamy, A. J. 'No Pain No Gain? Torture and Ethics in the War on Terror' International Affairs Vol.82 No.1 (2006) pp.121-148

Benn, S. I. 'Privacy, Freedom and Respect for Persons' in *Nomos XIII: Privacy* edited by Rennock, J. R. And Chapman, J. W. (New York: Atherton Press, 1971) pp.1-26

Benn, S. I. and Peters, R. S. *Social Principles and the Democratic State* (London: Allen and Unwin, 1959)

Bennetto, J. *Police and Racism: What Has Been Achieved 10 Years After the Stephen Lawrence Inquiry Report?* (London: Equality and Human Rights Commission, 2009)

Bentham, J. *The Panopticon Writings edited by* Bozovic, M. (London: Verso, 1995)

Bentham, J., Burns, J. H. and Hart, H. L. A. editors *An Introduction to the Principles of Morals and Legislation* (Oxford: Clarendon, 1996)

Berlin, I. *Four Essays on Liberty* (Oxford: Oxford University Press, 1969)

Bexton, W. H. Heron, W. and Scott, T. 'Effects of Decreased Variation in Sensory Environment' *Canadian Journal of Psychology* Vol.8 No.2 (1954) pp.70-76

Beytagh, F. 'Privacy and the Free Press: A Contemporary Conflict in Values' *New York Law Forum* Vol.20 No.3 (1975) pp.453-514

Biderman, A. D. "Communist Techniques of Coercive Interrogation" Air Force Personnel and Training Research Center Development Report Vol.132 (Lackland Air Force Base, Texas, 1956)

Black, H. C. *Black's Law Dictionary* 8th Edition (St. Paul MN: West Publishing Company, 1999)

Blakeley, R. 'Why Torture?' *Review of International Studies* Vol.33 No.3 (2007) pp.373-394

Bloustein, E. 'Group Privacy: The Right to Huddle' in *Individual and Group Privacy* edited by Bloustein, E. (New Brunswick: Transaction Books, 1978) pp.123-188

Bogard, W. T*he Simulation of Surveillance* (Cambridge: Cambridge University Press, 1996)

Bok, S. *Lying: Moral Choice in Public and Private Life* (New York: Vintage Books, 1979)

Boyle, J. *Shamans, Software and Spleens: Law and the Construction of the Information Society* (Cambridge, Mass.; London : Harvard University Press, 1997)

Brandeis, L. And Warren, S. 'The Right to Privacy' *The Harvard Law Review* Vol.4 No.5 (1980) pp.193-220

Breckenridge, A. C. *The Right to Privacy* (Lincoln: University of Nebraska Press, 1970)

Breckinridge, S. D. *The CIA and the U.S. Intelligence System* (Boulder, Colo.: Westview Press, 1986)

Brettle, J. and Rice, S. *Public Bodies, Private States: New Views on Photographic Representation and Gender* (Manchester: Manchester University Press New York, 1994)

Brown, I. and Karff, D. 'Terrorism and the Proportionality of Internet Surveillance' *European Journal of Criminology* Vol.6 No.2 (2009) pp.119-134

Butler, J. *Precarious Lives: The Powers of Mourning and Violence* (London: Verso, 2004)

Carmola, K. 'The Concept of Proportionality: Old Questions and New Ambiguities' in *Just War Theory: A Reappraisal* edited by Evans, M. (Edinburgh: Edinburgh University Press, 2005) pp.93-113

Carson, T. L. 'Bribery, Extortion, and "The Foreign Corrupt Practices Act"' *Philosophy and Public Affairs* Vol.14 No.1 (1985) pp.66-90

Cast, A. D. and Burke, P. J. 'A Theory of Self-Esteem' *Social Forces* Vol.80 No.3 (2002) pp.1041-1068

Chisholm, R. M. and Feehan T. D. 'The Intent to Deceive' *The Journal of Philosophy* Vol.74 No.3 (1997) pp.144-159

Cholbi, M. 'The Murderer at the Door: What Kant Should Have Said' *Philosophy and Phenomenological Research* Vol.59 No.1 (2009) pp.17-46

Clark, I. *Waging War: A Philosophical Introduction* (Oxford: Clarendon, 1988)

Clark, M. 'There is No Paradox of Blackmail' *Analysis* Vol.54 No.1 (1994) pp.54-61

Clarke, A. C. 'Extra-Terrestrial Relays: Can Rocket Stations Give World-Wide Radio Coverage' *Wireless World* (October, 1945) pp.305-308

Clarke, R. 'Information Technology and Dataveillance' *Communications of the ACM* Vol.31 No.5 (1988) pp.498-512

Clausewitz, C. *On War*, ed. and trans. Howard, M and Paret, P. (Princeton, N.J.: Princeton University Press, 1989)

Clover, J. S. '"Remember, We're the Good Guys": The Classification and Trial of the Guantanamo Detainees' *South Texas Law Review* Vol.45 No.1 (2003) pp.351-395

Coase, R. H. 'Blackmail' *Virginia Law Review* Vol.74 No.4 (1988) pp.655-676

Coates, A. J. *The Ethics of War* (Manchester: Manchester University Press, 1997)

Cohen, R. *Threat Perception in International Crisis* (Madison: University of Wisconsin Press, 1979)

Cohen, S. and Golan, D. *The Interrogation of Palestinians during the Intifada: Ill-treatment, 'Moderate Physical Pressure' or Torture?* (Jerusalem: Israeli Information Center for Human Rights in the Occupied Territories, 1991)

Colby, W. and Forbath, P. *Honorable Men: My Life in the CIA* (New York: Simon and Schuster, 1978)

Colitt, L. *Spymaster: The Real Life Karla, His Moles and the East German Secret Police* (London: Robson, 1996)

Conroy, J. *Unspeakable Acts, Ordinary People: The Dynamics of Torture* (New York: Knopf, 2000)

Cooley, C. H. *Human Nature and the Social Order* (Charles Scriber and Sons, 1902)

Costanzo, M., Gerrity, E. and Lykes, M. B. 'Psychologists and the Use of Torture in Interrogations' *Analyses of Social Issues and Public Policy* Vol.7 No.1 (2007) p.7-20

D'Andrade, K. 'Bribery' *Journal of Business Ethics* Vol.4 No.4 (1985) pp.239-248

Daniels, N. 'Wide Reflective Equilibrium and Theory Acceptance in Ethics' *The Journal of Philosophy* Vol.76 No.5 (1979) pp.256-282

Darwall, S. 'Introduction' in *Consequentialism* edited by Darwall, S. (London; Blackwell Publishers, 2003) pp.1-8

Darwell, S. 'Introduction' in *Deontology* edited by Darwell, S. (Oxford: Blackwell, 2002) pp.1-9

Davis, K. 'Final Note on Case of Extreme Isolation' *American Journal of Sociology* Vol.52 (1947) pp.432-437

De Jong, J. T., Komproe, I. H., Van Ommeren, M., El Masri, M., Araya, M., Khaled, N., Van de Put, W. A. C. M., and Somasundaram, D. J. 'Lifetime Events and Posttraumatic Stress Disorder in Four Post-Conflict Settings' *Journal of the American Medical Association* Vol.286 (2001) pp.555–562

Dempsey, J. X. and Flint, L. M. 'Commercial Data and National Security' *The George Washington Law Review* Vol.72 (2004) pp.1459-1502

DePaul, M. R. 'Two Conceptions of Coherence Methods in Ethics' *Mind* Vol.96 No.384 (1987) pp.463-481

Dershowitz, A. *Why Terrorism Works: Understanding the Threat, Responding to the Challenge* (London: Yale University Press, 2002)

Diffie, W. and Landau, S. *Privacy On The Line: The Politics Of Wiretapping And Encryption* (Cambridge: MIT Press, 1998)

Dorril, S. *The Silent Conspiracy: Inside the Intelligence Services in the 1990s* (London: Mandarin, 1994)

Driberg, T. *Ruling Passions: The Autobiography of Tom Driberg* (London: Quartet, 1978)
Dulles, A. *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering in a Free World* (Guildford: Lyons Press, 2006)

Dupont, A. 'Intelligence for the Twenty-First Century' *Intelligence and National Security* Vol.18 No.4 (2003) pp.15-39

Dzhirkvelov, I. *Secret Servant: My Life with the KGB and the Soviet Elite* (New York: Simon & Schuster, 1989)

Edwards, A. S. 'Effects of Loss of 100 Hours' Sleep' *American Journal of Psychology* Vol.54 (1941) pp.80-91

Epstein, E. *Deception: The Invisible War Between the KGB and CIA* (New York: Simon and Schuster, 1989)

Erskine, T ''As Rays of Light to the Human Soul?' Moral Agents and Intelligence Gathering' *Intelligence and National Security* Vol.19 No.2 (2004) pp.359-81

Erskine, T. 'Assigning Responsibilities to Institutional Moral Agents: The Case of States and Quasi-States' *Ethics & International Affairs* Vol. 15 No.2 (2001) pp.67-85

Erskine, T. *Embedded Cosmopolitanism: Duties to Strangers and Enemies in a World of 'Dislocated Communities'* (Oxford: Oxford University Press/British Academy, 2008)

Erskine, T. 'Embedded Cosmopolitanism and the Case of War: Restraint, Discrimination and Overlapping Communities' *Global Society* Vol.14 No.4 (2000) pp.569-590

Erskine, T. 'Locating Responsibility: The Problem of Moral Agency in International Relations' in *The Oxford Handbook of International Relations* edited by Reus-Smit, C. and Snidal, D. (Oxford: Oxford University Press, 2008) pp.699-707

Evans, M. 'Moral Theory and the Idea of a Just War' in *Just War Theory: A Reappraisal* edited by Evans, M. (Edinburgh: Edinburgh University Press, 2005) pp.1-24

Evans, M. D. *International Law Documents* 8th edition (London: Blackstone Press, 2007)

Fairfield, P. *Public/Private* (London: Rowman & Littlefield Publishers, 2005)

Fallows, J. 'Foreword' in *Brave New War: The Next Stage of Terrorism and the End of Globalization* by Robb, J. (Hoboken, NJ: John Wiley and Sons 2007)

Farber, I., Harlow, H. and West, L. 'Brainwashing, Conditioning and DDD' *Sociometry* Vol.20 No. 4 (1957) pp.271-285

Feinberg, J. *Moral Limits of the Criminal Law: Vol.1 Harm to Others* (Oxford: Oxford University Press, 1984)

Feinberg, J. 'The Idea of a Free Man' in *Educational Judgments: Papers in the Philosophy of Education* edited by Doyle, J. F. (London: Routledge, 1973) pp.143-165

Feinberg, J. 'Voluntary Euthanasia and the Inalienable Right to Life' *Philosophy and Public Affairs* Vol.7 No.2 (1978) pp.93-123

Forster, E. M. *The Machine Stops* (DodoPress, 1909)

Foucault, M. *Discipline and Punish: The Birth of the Prison* (Harmondsworth: Penguin, 1979)

Fox, R. 'Someone to Watch Over Us: Back to Panopticon?' *Criminology and Criminal Justice* Vol.1 No.3 (2001) pp.251-276

Frankfurt, H. 'Freedom of the Will and the Concept of the Person', *Journal of Philosophy* Vol.68 No.1 (1971), pp.5-20

Fried, C. 'Privacy: A Moral Analysis' *Yale Law Review* Vol.77 No.1 (1969) pp.475-949

Freund, P. 'Privacy: One Concept of Many?' in *Nomos XIII: Privacy* edited by Rennock, J. R. And Chapman, J. W. (New York: Atherton Press, 1971) p.182-198

Froomkin, A. M. 'The Death of Privacy?' S*tanford Law Review* Vol.52 No.5 (2000) pp.1461-1543

Fyfe, N. *Surveillance, Closed Circuit Television, and Social Control* (Aldershot: Ashgate, 1998)

Fyfe, N. R. and Bannister, J. 'City Watching: Closed Circuit Television Surveillance in Public Spaces' *Area* Vol.28 No.1 (1996) pp.37-46

Gandy, O. *The Panoptic Sort: A Political Economy of Personal Information* (New York: Westview Publishers, 1993)

Gardner, J. 'Complicity and Causality' *Criminal Law and Philosophy* Vol.1 No.2 (2007) pp.127-141

Garfinkle, S. *Database Nation: The Death Of Privacy In The 21st Century* (California: O'Reilly & Associates, 2001)

Gecas, V. 'The Self-Concept' *Annual Review of Sociology* Vol.8 (1982) pp.1-33

Gellman, B. and Priest, D. 'U.S. Decries Abuse but Defends Interrogation' *Washington Post* December 26th (2002)

Geraghty, T. *The Irish War* (London: HarperCollins Publishers Ltd, 2000)

Gerety, T. 'Redefining Privacy' *Harvard Civil Rights-Civil Liberties Law Review* Vol.12 (1977) p.262-3

Gewirth, A. ‘Are There Any Absolute Rights’ *The Philosophical Quarterly* Vol.31 No.122 (1981) pp.1-16

Gibb, J. *Who’s Watching You?* (London: Collins & Brown, 2005)

Gibson, J. ‘Factors Contributing to the Creation of a Torturer’ in *Psychology and Torture* edited by Suedfeld, P. (Washington, D.C.: Hemisphere, 1990)

Gibson, J. ‘Training People to Inflict Pain: State Terror and Social Learning’ *Journal of Humanistic Psychology* Vol.31 No.2 (1991) pp.72-78

Giddens, A. *The Nation State and Violence* (Berkeley: California University Press, 1987)

Gill, P. ‘Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'?’ *Intelligence and National Security* Vol.24 No.1 (2009) pp.78-102

Goldstein, I. ‘Pleasure and Pain: Unconditional, Intrinsic Values’ *Philosophy and Phenomenological Research*, Vol. 50, No. 2. (1989) pp.255-276

González Castresana, C. ‘Torture as a Greater Evil’ *South Central Review* Vol.24 No.1 (2007) pp.119-130

Gordievsky, O. *Next Stop Execution: The Autobiography of Oleg Gordievsky* (London: Macmillan, 1995)

Gorr, M. ‘Liberalism and the Paradox of Blackmail’ *Philosophy and Public Affairs* Vol.21 No.1 (1992) pp.43-66

Gottschick, J. ‘Neuropsychiatric Disease Among German Prisoners of War in the United States’ *Archive of Psychiatry* Vol.185 (1950) pp.491-510

Govier, T. *Dilemmas of Trust* (London: McGill University Press, 1998)

Graham, T. and Hansen, K. *Spy Satellites and Other Intelligence Technologies that Changed History* (London: University of Washington Press, 2007)

Green, R. K. and Pawlak, E. J. ‘Ethics and Manipulation in Organisations’ *The Social Service Review* Vol.57 No.1 (1983) pp.35-43

Greenberg, D. F. *The Construction of Homosexuality* (Chicago; London: University of Chicago Press, 1988); and Moran, L. J. ‘Justice and Its Vicissitudes’ *The Modern Law Review* Vol.54 No.1 (1991) pp.146-161

Greenwood, T. ‘Reconnaissance and Arms Control’ *Scientific American* Vol.228 (1973) p.14-25

Grendron, A. ‘Just War, Just Intelligence: An Ethical Framework for Foreign Espionage’ *International Journal of Intelligence and Counter Intelligence* Vol.18 No.3 (2005) pp.398-434

Grey, S. *Ghost Plane: The True Story of the CIA Torture Program* (New York: St. Martin's Press, 2006)

Gross, H. 'Privacy and Autonomy' in *Privacy: Nomos XIII* edited by Pennock, J. R. and Chapman, J. W. (New York: Atherton Press, 1971) pp.169-181

Guiora, A. N. and Page, E. M. 'The Unholy Trinity: Intelligence, Interrogation and Torture' *Case Western Research Journal of International Law* Vol.37 (2006) pp.427-447

Gutwirth, S. *Privacy and the Information Age* (Oxford: Rowman & Littlefield Publishers, 2002)

Hakimi, M. 'The Council of Europe Addresses CIA Rendition and Detention Program' *The American Journal of International Law* Vol.101 No.2 (2007) pp.442-452

Hallborg, R. 'Principles of Liberty and the Right to Privacy' *Law and Philosophy* Vol.5 No.2 (1986) pp.175-218

Haritos-Fatouros, M. 'The Official Torturer: A Learning Model for Obedience to the Authority of Violence' in *The Politics of Pain Torturers and their Masters* edited Crelinsten, F. D. and Schmid, A. P. (Leiden: Center for the Study of Social Conflicts, 1993), pp.141–160

Harris, D. A. 'Driving While Black and Other Traffic Offences: The Supreme Court and Pretextual Traffic Stops' *The Journal of Criminal Law and Criminology* Vol.87 (1999) pp.544-582

Hart, H. L. A. *Concept of Law* (Oxford: Clarendon Press, 1976)

Haslett, D. W. 'What is Wrong with Reflective Equilibrium' *The Philosophical Quarterly* Vol.37 No.148 (1987) pp.305-311

Hastedt, G. *Controlling Intelligence* (London: Cass, 1991)

Hausman, D. and McPhereson, M. *Economic Analysis and Moral Philosophy* (Cambridge: Cambridge University Press, 1996)

Hebb, D. O. 'Experimental Deafness' *Canadian Journal of Psychology* Vol.8 No.3 (1954) p.152-56

Heinz, W. S 'The Military, Torture and Human Rights: Experiences from Argentina, Brazil, Chile and Uruguay', in *The Politics of Pain Torturers and their Masters* edited Crelinsten, F. D. and Schmid, A. P. (Leiden: Center for the Study of Social Conflicts, 1993), pp.73–108

Helmholz, R. H. 'The Roman Law of Blackmail' *Journal of Legal Studies* Vol.30 No.1 (2001) pp.33-52

Helweg-Larsen, P., Hoffmeyer, H. and Kiefer, J. *Famine Disease in German Concentration Camps: Complications and Sequels* (Scandinavia: Med Scan, 1952)

Hepworth, M. *Blackmail: Publicity and Secrecy in Everyday Life* (London: Routledge, 1975)

Herman, B. *The Practice of Moral Judgement* (Harvard University Press, 1996)

Herman, M. 'Ethics and Intelligence after September 2001' *Intelligence and National Security* Vol.19 No.2 (2004) pp.342-58

Herman, M. *Intelligence Services in the Information Age: Theory and Practice* (London: Frank Class, 2001)

Herman, M. 'Why Should Intelligence Professional Attend to Intelligence Ethics?' in 'A Symposium on Intelligence Ethics' *Intelligence and National Security Special Addition* Vol.24 No.3 (2009) pp.366-386

Herring, J. *Criminal Law: Texts, Cases and Materials* (Basingstoke; New York: Palgrave Macmillan, 2009)

Hinkle, L. E. 'The Physiological State of the Interrogation Subject as it Affects Brain Function' in *The Manipulation of Human Behaviour* edited by Biderman, A. D. and Zimmer, H. (New York; London: John Wiley & Sons Inc, 1961) pp.19-50

Hirsch, A. 'The Ethics of Public Television Surveillance' in *Ethics and Social Perspectives on Situational Crime Prevention* edited by Hirsch, A., Garland, D. and Wakefield, A. (Oxford: Hart Publishing, 2000) pp.59-76

Hobbes, T. *De Cive* [On the Citizen] edited and translated by Tuck R. and Silverthorne, M. (Cambridge: Cambridge University Press 1998)

Hoch, P. H., Cattell, J. P. and Pennes, H. H. 'Effects of Mescaline and Lysergic Acid (d-LSD-25)' *The American Journal of Psychiatry* Vol.108 (1952) pp.579-584

Hollinsworth, M. and Fielding, N. *Defending the Realm: MI5 and the Shayler Affair* (London: André Deutsch, 1999)

Horowitz, D. L. 'The Courts as Guardians of the Public Interest' *Public Administration Review* Vol.37 No.2 (1977) pp.148-154

Hughes, R. G. and Scott, L. ''Knowledge is Never Too Dear': Exploring Intelligence Archives' in *Exploring Intelligence Archives: Enquiries into the Secret State* edited by Hughes, R. G., Jackson, P. and Scott, L. (Abingdon, Oxon, England ; New York : Routledge, 2008) pp.13-40

Hunsinger, G. 'Torture Is the Ticking Time-Bomb: Why the Necessity Defense Fails' *A Journal of Theology* Vol.47 No.3 (2008) pp.228-239

Hurka, T. 'Proportionality in the Morality of War' *Philosophy and Public Affairs* Vol.33 No.1 (2005) pp.34-66

Huxley, P. *Blackstone's Statutes on Evidence 11th Edition* (Oxford: Oxford University Press, 2010)

Ikuenobe, P. 'The Meta-Ethical Issue of the Nature of Lying: Implications for Moral Education' *Studies in Philosophy and Education* Vol.21 (2002) pp.37-63

Innes, J. *Privacy, Intimacy and Isolation* (Oxford: Oxford University Press, 1996)

Isenberg, A. 'Deontology and the Ethics of Lying' *Philosophy and Phenomenological Research* Vol.24 No.4 (1964) pp.463-480

Isenbergh, J. 'Blackmail from A to C' *University of Pennsylvania Law Review* Vol.141 No.5 (1993) pp.1905-1933

Jackson, P. and Scott, L. 'The Study of Intelligence in Theory and Practice' *Intelligence and National Security* Vol.19 No.2 (2004) pp.139-169

Johnson, J. T. *Morality and Contemporary Warfare* (London: Yale University Press, 2001)

Johnson, L. 'Ethical Intelligence: A Contradiction in Terms?' in 'A Symposium on Intelligence Ethics*' Intelligence and National Security Special Addition* Vol.24 No.3 (2009) pp.366-386

Johnson, L. *Secret Agencies: US Intelligence in a Hostile World* (London: Yale University Press, 1996)

Johnson, L. 'Spies' *Foreign Policy* No.120 (2000) pp.18-26

Jones, J. M. 'Is Ethical Intelligence a Contradiction in Terms?', in *Ethics of Spying: A Reader for the Intelligence Professional Volume 2* edited by Goldman, J. (Plymouth: Scarecrow Press, 2010) pp.21-33

Kahn, H. *On Escalation: Metaphors and Scenarios* (London: Pall Mall Press, 1965)

Kant, I. *Fundamental Principles of the Metaphysics of Morals* (London: Longmans, 1926)

Kant, I. *Groundwork of the Metaphysics of Morals* translated and edited by Gregor, M. (Cambridge: Cambridge University Press, 1998)

Kant, I. *Practical Philosophy* translated and edited by Gregor, M. (Cambridge: Cambridge University Press, 1999)

Kasachkoff, T. 'Killing in Self-Defense: An Unquestionable or Problematic Defense?' *Law and Philosophy* Vol.17 No.5/6 (1998) pp.509-531

Kasher, A. 'The Principle of Distinction' *Journal of Military Ethics* Vol.6 No.2 (2007) pp.152 - 167

Keefe, P. R. *Chatter: Dispatches From The Secret World Of Global Eavesdropping* (New York: Random House, 2005)

Kennedy, R. *Race Crime and the Law* (New York: Patheon, 1997)

Kessler, R. *Inside the CIA: Revealing the Secrets of the Most Powerful Spy Agency* (New York: Pocket Books, 1994)

Kessler, R. *The CIA at War: Inside the Secret Campaign Against Terror* (New York: St. Martin's Press, 2003)

Keys, A. *The Biology of Human Starving* (Minneapolis: University of Minneapolis Press, 1950)

Khalil, F., Lawarree, J. and Yun, S. 'Bribery Versus Extortion: Allowing the Lesser of Two Evils' *The RAND Journal of Economics* Vol.41 No.1 (2010) pp.179-198

Kang, J. 'Information Privacy in Cyberspace Transactions' *Stanford Law Review* Vol.50 No.4 (1998) pp.1193-1294

Kiralfy, A. *The Burden of Proof* (Abingdon: Professional, 1987)

Knorr, K. 'Threat Perception' in *Historical Dimensions of National Security Problems* edited by Knorr, K. (Lawrence: University Press of Kansas, I976)

Konvitz, M. 'Privacy and the Law: A Philosophical Prelude' *Law and Contemporary Problems* Vol.31 No.2 (1966) pp. 272-280

Kutz, C. 'Causeless Complicity' *Criminal Law and Philosophy* Vol.1 No.3 (2007) pp.289-305

Lackey, D. P. *The Ethics of War and Peace* (London : Prentice Hall International, 1989)

Laidler, K. *Surveillance Unlimited: How We've Become the Most Watched People on Earth* (Thriplow: Icon, 2008)

Lamond, G. 'Coercion, Threats and the Puzzle of Blackmail' in *Harm and Culpability* edited by Smith, A. and Simester A. (Oxford: Oxford University Press, 1996) pp.215-238

Langbein, J. H. *Torture and the Law of Proof: Europe and England in the Ancien Régime* (Chicago; London: University of Chicago Press, 1977)

Laslett, H. R. 'An Experiment on the Effects of Loss of Sleep' *Journal of Experimental Psychology* (1924) Vol.7 pp.45-58

Laufer, R. and Wolfe, M. 'Privacy as a Concept and Social Issue: A Multidimensional Developmental Theory' *The Journal of Social Issues* Vol.33 No.3 (1977) pp.22-42

Lessig, L. *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

Lever, A. 'Why Racial Profiling is Hard to Justify: A Response to Risse and Zeckhauser' *Philosophy and Public Affairs* Vol.33 No.1 pp.94-110

Lewis, D. *Sexpionage: The Exploitation of Sex by Soviet Intelligence* (London: H. Hanau Publications, 1976)

Lindgren, J. ‘Unravelling the Paradox of Blackmail’ *Columbia Law Review* Vol.84 No.3 (1984) pp.670-717

Lindley, R. *Autonomy* (Basingstoke: Macmillan, 1986)

Linklater, A. ‘Citizenship, Humanity and Cosmopolitan Harm Conventions’ *International Political Science Review* Vol.22 No.3 (2001) pp.261-277

Linklater, A. ‘The Harm Principle in Global Ethics’ *Global Society* Vol.20 No.3 (2006) pp.329-343

Linklater, A. *The Problem of Harm in World Politics: Theoretical Investigations* (Cambridge: Cambridge University Press, 2011)

Locke, J. *Second Treatise of Government: and, A Letter Concerning Toleration* by Laslett, P. (Cambridge: Cambridge University Press, 1960)

Lowenthal, M. *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003)

Luban, D. ‘Liberalism, Torture and the Ticking Bomb’ *Virginia Law Review* Vol.9 No.6 (2005) pp.1425-1461

Luhmann, N. *Trust and Power: Two Works by Niklas Luhmann* translated by Davis, H., Raffan, J. and Rooney, K with introduction by Poggi, G. (Chichester: Wiley, 1979)

Lukes, S. ‘Liberal Democratic Torture’ *British Journal of Political Science* Vol.36 (2006) pp.1-16

Lyon, D. ‘An Electronic Panopticon? A Sociological Critique of Surveillance Theory’ *The Sociological Review* Vol.41 No.3 (1993) pp.653-678

Lyon, D. *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001)

Lyon, D. *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity Press, 1994)

Lyon, D. ‘The Search for Surveillance Theories’ *Theorising Surveillance: The Panopticon and Beyond* edited by Lyon, D. (Devon: Willan, 2006) pp.3-20

Mackie, J *Ethics: Inventing Right and Wrong* (London: Penguin, 1977)

Mahon, J. E. ‘Kant and the Perfect Duty to Others Not to Lie’ *British Journal for the History of Philosophy* Vol.14 No.4 (2006) pp.653-685

Malott, R. W. *Principles of Behaviour* (London: Pearson/Prentice Hall, 2008)

Mannheim, B. F. ‘Reference Groups, Membership Groups and the Self Image’ *Sociometry* Vol.29 No.3 (1966) pp.265-279

Marbles, W. 'Psychology of Treason' in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal 1955-1992* edited by Westerfield, H. B. (New Haven; London: Yale University Press, 1995) pp.70-82

Marx, G. 'Ethics for the New Surveillance' *The Information Society* Vol.14 No.3 (1998) pp.171-185

Marx, G. 'Some Concepts that May be Useful in Understanding the Myriad Forms and Contexts of Surveillance' *Intelligence and National Security* Vol.19 No.2 (2004) pp.226-248

Marx, G. *Undercover: Police Surveillance in America* (Berkeley: University of California Press, 1988)

Mathiesen, T. 'The Viewer Society: Michelle Foucault's Panopticon Revisited' *Theoretical Criminology* Vol.1 No.2 (1997) pp.215-234

Mayer, R. 'What's Wrong With Exploitation' *Journal of Applied Philosophy* Vol.24 No.2 (2007) pp.137-150

McCahill, M. 'Beyond Foucault: Towards a Contemporary Theory of Surveillance' in *Surveillance, Closed-Circuit Television and Social Control* edited by Norris, C., Moran, J. and Armstrong, G. (Aldershot: Ashgate, 1998) pp.41-65

McCoy, A. W. *A Question of Torture: CIA Interrogation, from the Cold War to the War on Terror* (New York: Henry Holt and Company, 2006)
McCready, D. 'When is Torture Right?' *Studies in Christian Ethics* Vol.20 No.3 (2007) pp.383-398

McKenna, J. C. 'Ethics and War: A Catholic View' *American Political Science* Vol.54 No.3 (1960) pp. 647-658

McMahan, J. 'Innocence, Self-Defence and Killing in War' *The Journal of Political Philosophy* Vol.2 No.1 (1994) pp.193-221

McMahan, J. 'On the Moral Equality of Combatants' *Journal of Political Philosophy* Vol.14 No.4 (2006) pp.377-393

Merton, R. *Social Theory and Social Structure* (New York: Free Press, 1968)

Mill, J. S. *On Liberty* Edited by Gray, J (Oxford: Oxford University Press, 1991)

Mill, J. S. *Utilitarianism* edited by Crisp, R. (Oxford: Oxford University Press, 1998)

Miller, A. *The Assault on Privacy* (Ann Arbor: The University of Michigan Press)

Miller, R. B. *Interpretations of Conflict, Ethics, Pacifism and the Just War Tradition* (Chicago; London: University of Chicago Press, 1991)

Miller, S. B. *The Shame Experience* (Hillsdale: Analytic, 1985)

Mills, A. *The Assault on Privacy: Computers, Databanks and Dossiers* (Michigan: University of Michigan Press, 1971)

Misztal, B. A. *Trust in Modern Societies: The Search for the Bases of Social Order* (Cambridge: Blackwell Publishers, Inc., 1996)

Monagham, H. P. 'Of Liberty and Property' *Cornell Law Review* Vol.62 No.1 (1977) pp.405-444

Montague, P. 'The Morality of Self-Defense: A Reply of Wasserman' *Philosophy and Public Affairs* Vol.18 No.1 (1989) pp.81-89

Morgan, R. E. *Domestic Intelligence: Monitoring Dissent in America* (Austin: University of Texas Press, 1980)

Nagel, T. *Mortal Questions* (Cambridge: Cambridge University Press, 1979)

Nagel, T. *The View From Nowhere* (Oxford: Oxford University Press, 1986)

Norman, R. *Ethics, Killing and War* (Cambridge: Cambridge University Press, 1995)

Northcott, C. 'The Role, Organisation and Methods of MI5' *International Journal of Intelligence and Counterintelligence* Vol.20 No.3 (2007) pp.453-479

Nussbaum, M. *Hiding from Humanity: Disgust, Shame and the Law* (Princeton: Princeton University Press, 2004)

Nussbaum, M. *Women and Human Development: The Capabilities Approach* (Cambridge: Cambridge University Press, 2000)

Olson, J. M. *Fair Play: The Moral Dilemmas of Spying* (Washington, D.C.: Potomac Books Inc., 2006)

Omand, D. 'Reflections on Secret Intelligence' in *The New Protective State: Government, Intelligence and Terrorism* edited by Hennessy, P. (London: Continuum, 2007) pp.97-122

Omand, D. 'The Dilemmas of Using Secret Intelligence for Public Security' in *New Protective State: Government, Intelligence and Terrorism* edited by Hennessy, P (London: Continuum, 2007) pp.142–69

Orend, B. *Morality of War* (Peterborough: Broadview Press, 2006)

Orwell, G. *Nineteen Eighty Four* (London: Penguin Books, 1987)

Oscar. G. 'Data Mining and Surveillance in the Post 9/11 Environment' in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* edited by Bell, K. and Webster, F. (2003) pp.26-41

Otsuka, M. 'Killing the Innocent in Self-Defense' *Philosophy and Public Affairs* Vol.23 No.1 (1994) pp.74-94

Parent, W. A. 'Privacy, Morality and the Law' *Philosophy and Public Affairs* Vol.12 No.4 (1983) pp.269-288

Parker, J. *Total Surveillance: Investigating the Big Brother World of E-Spies, Eavesdroppers and CCTV* (London: Piatkus, 2000)

Parkinson, J, and Walker, C. *Blackstone's Counter-Terrorism Handbook* (Oxford: Oxford University Press, 2009)

Parry, J. 'Escalation and Necessity: Defining Torture at Home and Abroad' in *Torture: A Collection* edited by Levinson, S. (Oxford; New York: Oxford University Press, 2004) pp.145-164

Parry, J. 'Interrogating Suspected Terrorists: Should Torture be an Option?' *University of Pittsburgh Law Review* Vol.63 No.1 (2001) pp.743-766

Parry, L. A. *The History of Torture in England* (Montclair, N.J: Patterson Smith, 1975)

Patten, J. W. 'Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places' *Ethics and Information Technology* Vol.2 (2000) pp.181-187

Pekel, K. 'Integrity, Ethics and the CIA: The Need for Improvement' *Central Intelligence Agency Washington D.C. Center for the Study of Intelligence* (1998) pp.1-10

Pennock, J. R. 'Coercion: An Overview' in *Nomos XIV: Coercion* edited by Pennock, J. R. (Chicago: Aldine, 1972) pp.1-16

Peters, E. *Torture* (New York: Basil Blackwell, 1985)

Pfaff, T. and Tiel J. 'The Ethics of Espionage' *Journal of Military Ethics* Vol.3 No.1 (2004) pp.1-15

Phillips, M. 'Bribery' *Ethics* Vol.94 No.4 (1984) pp.621-636

Phillips, R. *War and Justice* (Norman: University of Oklahoma Press, 1984)

Polyviou, P. *Search and Seizure: Constitutional and Common Law* (London: Duckworth, 1982)

Priebe, S. and Bauer, M. 'Inclusion of Psychological Torture in PTSD Criterion' *American Journal of Psychiatry* Vol.152 (1995), pp.1691–1692

Quinlan, M. 'Just Intelligence: Prolegomena to an Ethical Theory' *Intelligence and National Security* Vol.22 No.1 (2007) pp.1-13

Quinlan, M. 'The Future of Covert Intelligence' in *Agents for Change: Intelligence Services in the 21st Century edited by* Shukman, H. (London: St Ermin's Press 2000) pp.61-71

Raab, C. D. 'Joined-Up Surveillance: The Challenge to Privacy' in *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* edited by Bell, K. and Webster, F. (London; Sterling, VA: Pluto Press, 2003) pp.42-61

Rachels, J. *The Elements of Moral Philosophy* (New York; London: McGraw-Hill, 1993)

Rawls, J. *Theory of Justice* (Cambridge: Harvard University Press, 1971)

Raz, J. *The Morality of Freedom* (Oxford: Clarendon, 1986)

Regan, R. *Just War: Principles and Cases* (Washington, D.C: Catholic University of America Press, 1996)

Reiman, J. 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' *Computer and High Technology Law Journal* Vol.11 (1995) pp.27-44

Reiman, J. 'Privacy, Intimacy, and Personhood' *Philosophy and Public Affairs* Vol.5 No.1 (1976) pp.26-44

Rengger, N. 'On the Just War Tradition in the Twenty-First Century' *International Affairs* Vol.78 No.2 (2008) pp.353-368

Rescher, N. *Welfare: The Social Issue in Philosophical Perspective* (Pittsburgh: University of Pittsburgh Press, 1972)

Richelson, J. T. *A Century of Spies: Intelligence in the Twentieth Century* (New York: Oxford University Press, 1995)

Richelson, J. T. 'Intelligence: The Imagery Dimension' in S*trategic Intelligence: The Intelligence Cycle* Volume 2 edited by Johnson, L. K. (London: Praeger Security International, 2007) pp.61-74

Richelson, J. T. *The U.S. Intelligence Community* (Boulder, Colo.: Westview Press, 2008)

Richelson, J. T. and Ball, D. *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries* (Boston: Allen & Unwin, 1985)

Robinson, M. 'The Construction and Reinforcement of the Myth of Race Crime' *Journal of Contemporary Criminal Justice* Vol.16 (2000) pp.133-156

Rodley, N. S. *The Treatment of Prisoners Under International Law* (Oxford; New York: Oxford University Press, 2009)

Rosenberg, M. 'The Self-Concept: Social Product and Social Force' in *Social Psychology: Sociological Perspectives* edited by Rosenberg, M. and Turner, R. H. Transaction (New York: Basic Books, 1990) pp.593-624

Rosenberg, M., Schooler, C., Schoenbach, C. and Rosenberg, F. 'Global Self-Esteem and Specific Self-Esteem' *American Sociological Review* Vol.60 (1995) pp.141-56

Ross, W. D. *The Right and The Good* (Oxford: Clarendon Press, 1930)

Rubinstein, I., Lee, D. and Schwartz, P. 'Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches' *The University of Chicago Law Review* Vol.75 No.1 (2008) pp.261-285

Rudinow, J. 'Manipulation' *Ethics* Vol.88 No.4 (1978) pp.338-347

Rule, J. *Private Lives and Public Surveillance* (London: Allen Lane, 1973)

Sawatsky, J. *Men in the Shadows: The RCMP Security Service* (Toronto: Doubleday, 1980)

Scanlon, T. M. and Daney J. 'Intention and Permissibility' *Supplement to the Proceedings of the Aristotelian Society* Vol.74 No.1 (2000) pp.301-317

Scarry, E. 'Five Errors in the Reasoning of Alan Dershowitz', in *Torture: A Collection* edited by Levinson, S. (Oxford; New York: Oxford University Press, 2004) pp.281-290

Scarry, E. *The Body in Pain: The Making and Unmaking of the World* (New York: Oxford University Press, 1985)

Schechter, J. L. and Deriabin, P. S. *The Spy Who Saved the World: How a Soviet Colonel Changed the Course of the Cold War* (London: Brassey's, 1992)

Scott, R. *History of Torture Throughout the Ages* (Montana: Kessinger Publishing, 2003)

Selznick, P. 'The Idea of a Communitarian Morality' *Californian Law Review* Vol.75 No.1 (1987) pp.445-463

Shils, E. 'Privacy: Its Constitution and Vicissitudes' *Law and Contemporary Problems* Vol.31 No.2 (1966) pp. 281-306

Shpiro, S. 'Intelligence Ethics in Israel: Why Do We Need Intelligence Ethics' in 'A Symposium on Intelligence Ethics' *Intelligence and National Security Special Addition* Vol.24 No.3 (2009) pp.366-386

Shue, H. 'Torture' *Philosophy and Public Affairs* Vol.7 No.2 (1978) pp.124-143

Shulsky, A. N. *Silent Warfare: Understanding the World of Intelligence* (Oxford: Brassey's, 1991)

Shulsky, A. N. and Schmitt, G. J. *Silent Warfare: Understanding the World of Intelligence* (Washington, D.C.: Brassey's, 2002)

Silove, D. M., Steel, Z., McGorry, P. D., Miles, V., and Drobny, J. 'The Impact of Torture on Posttraumatic Stress Symptoms in War-Affected Tamil Refugees and Immigrants' *Comprehensive Psychiatry* Vol.43 (2002) pp.49–55

Simitis, S. ‘Reviewing Privacy in an Information Age’ *University of Pennsylvania Law Review* Vol.35 No.3 (1987) pp.707-746

Singer, D. J. ‘Threat Perception and the Armament Tension Dilemma’ *Journal of Conflict Resolution* Vol.2 No.1 (1958) pp.90-105

Slobogin, C. ‘Government Data-Mining and the Fourth Amendment’ *The University of Chicago Law Review* Vol.75 No.1 (2008) pp.317-341

Slim, H. *Killing Civilians: Methods, Madness and Morality in War* (Basingstoke: Palgrave, 2002)

Smart, J. J. C. and Williams, B. *Utilitarianism: For and Against* (London: Cambridge University Press, 1973)

Solove, D. ‘Conceptualising Privacy’ *California Law Review* Vol.90 No.4 (2002) pp.1087-1156

Solove, D. *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004)

Somnier, F. and Genefke, I. ‘Psychotherapy for Victims of Torture’ *British Journal of Psychiatry* Vol.149 (1986) pp.323-329

Spiller, G. *The ‘Sense’ of Pain (and Pleasure)* (London: Farleigh Press, 1938)

Steinberger, P. J. ‘Public and Private’ *Political Studies* Vol.47 No.2 (1999) pp.292-313
Steinhoff, U. ‘Torture – The Case for Dirty Harry and against Alan Dershowitz’ *Journal of Applied Philosophy* Vol.23 No.3 (2006) pp.337-353

Suedfeld, P. *Psychology and Torture* (New York; London: Hemisphere Publishing Corporation, 1990)

Sullivan, W. C. *The Bureau: My Thirty Years in Hoover’s FBI* (New York: Norton, 1979)

Sussman, D. ‘What’s Wrong with Torture?’ *Philosophy and Public Affairs*, Vol.33 No.1 (2005) pp.1-33

Tangney, J. P. and Dearing, R. L. *Shame and Guilt* (London: Guilford Press, 2002)

Taylor, G. *Pride, Shame and Guilt* (Oxford: Clarendon Press, 1985)

Taylor, P. *Beating the Terrorists? Interrogation in Omagh, Gough and Castlereach* (London: Penguin, 1980)

Taylor, S. A. and Snow, D. ‘Cold War Spies: Why they Spied and How they got Caught’ *Intelligence and National Security* Vol.12 No.2 (1997) pp.101-125

Thomson, J. J. ‘Self-Defence’ *Philosophy and Public Affairs* Vol.20 No.4 (1991) pp.283-310

Thomson, J. J. 'The Right to Privacy' *Philosophy and Public Affairs* Vol.4 No.4 (1975) pp.295-314

Thomson, J. *Rights, Restitution and Risk: Essays in Moral Theory* (Cambridge: Harvard University Press, 1986)

Todd, R. W. 'Electronics and the Invasion of Privacy' in *Privacy* edited by Young, J. B. (1978) pp.309-318

Turner, J. T. *Just War Tradition and the Restraint of War: A Moral and Historical Inquiry* (Princeton: Princeton University Press, 1981)

Turner, W. *Hoover's FBI: The Men and Myth* (New York: Dell Publishing, 1971)

Turow, S. 'What's Wrong with Bribery' *Journal of Business Ethics* Vol.4 No.4 (1985) pp.249-51

Twigge, S., Hampshire, E. and Macklin, G. *British Intelligence: Secrets, Spies and Sources* (Kew: National Archives, 2008)

Urban, M. *UK Eyes Alpha: The Inside Story of British Intelligence* (London: Faber, 1996)

Vassall, J. *Vassall: The Autobiography of a Spy* (London: Sidgewick & Jackson, 1975)

Viera, J. D. 'Images as Property' in *Image Ethics: The Moral Right of Subjects in Photographs, Film and Television* edited by Gross, L., Katz, J. and Ruby, J. (Oxford: Oxford University Press, 1988) pp.135-162

Waldron, J. 'Torture and Positive Law: Jurisprudence for the White House' *California Law Review* Vol.106 No.6 (2005) pp.1681-1750

Wall, D. 'Policing the Internet: Maintaining Law and Order on the Cyberbeat' in *The Internet, Law and Society* edited by Akdeniz, Y., Walker, C. and Wall, D. (Harlow: Longman, 2000) pp.154-174

Waller, J. *Becoming Evil: How Ordinary People Commit Genocide and Mass Killing* (Oxford: Oxford University Press, 2002)

Walzer, M. *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: BasicBooks, 2000)

Walzer, M. *Obligations: Essays on Disobedience, War, and Citizenship* (Cambridge, MA: Harvard, 1970)

Warnock, G. J. *The Object of Morality* (London: Methuen, 1971)

Webster, W. 'CCTV Policy in the UK: Reconsidering the Evidence Base' *Surveillance and Society* Vol.6 No.1 (2009) pp.10-22

Weinstein, M. A. 'The Uses of Privacy in the Good Life' in *Privacy: Nomos XIII* edited by Pennock, J. R. and Chapman, J. W. (New York: Atherton Press, 1971) pp.88-104

Westin, A. F. *Privacy and Freedom* (London: Bodley Head, 1967)

Whitaker, R. *The End of Privacy: How Total Surveillance Is Becoming a Reality* (New York: The New Press, 2000)

Winder, W. 'The Development of Blackmail' *The Modern Law Review* Vol.5 No.1 (1941) pp.21-50

Wise, D. *Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million* (New York: HarperCollins Publishers, 1995)

Wisnewski, J. J. *Understanding Torture:* (Edinburgh: Edinburgh University Press, 2010)

Wright, P. and Greengrass, P. *Spycatcher: The Candid Autobiography Of A Senior Intelligence Officer* (New York: Viking, 1987)

Wolf, M with McElvoy, A. *Memoirs of a Spymaster: The Man Who Waged a Secret War Against the West* (London: Pimlico, 1998)

X, Mr. with Henderson, B. E. and Cyr, C. C. *Double Eagle: The Autobiography of a Polish Spy who Defected to the West* (New York: Ballantine Books, 1983)