THE ETHICS OF NATIONAL SECURITY INTELLIGENCE INSTITUTIONS
THEORY AND APPLICATIONS

Adam Henschke, Seumas Miller, Andrew Alexandra, Patrick F. Walsh and Roger Bradbury
This book explores the ethics of national security intelligence institutions operating in contemporary liberal democracies.

Intelligence collection by agencies such as the CIA, MI6, and Mossad involves practices that are apparently inconsistent with the principles of ordinary morality – practices such as lying, spying, manipulation, and covert action. However, in the defence of national security, such practices may not only be morally permissible but may also under some circumstances be morally obligatory. One approach to the ethics of national security intelligence activity has been to draw from the just war tradition (so-called “just intelligence theory”). This book identifies significant limitations of this approach and offers a new, institutionally based, teleological normative framework. In doing so, it revises some familiar principles designed for application to kinetic wars, such as necessity and proportionality, and invokes some additional ones, such as reciprocity and trust. It goes on to explore the applications of this framework and a revised set of principles for national security intelligence institutions and practices in contemporary and emerging political and technological settings.

This book will be of much interest to students of intelligence studies, ethics, security studies, and international relations.

Adam Henschke is Assistant Professor with the Philosophy Section at the University of Twente in the Netherlands.

Seumas Miller is Professor of Philosophy at the Australian Graduate School of Policing and Security at Charles Sturt University in Australia, a Distinguished Research Fellow at the Uehiro Centre for Practical Ethics at Oxford University, and an Honorary Fellow at the Digital Ethics Centre at Delft University of Technology.

Andrew Alexandra is Adjunct Senior Fellow with the School of Historical and Philosophical Studies at Melbourne University in Australia.

Patrick F. Walsh is Professor of Intelligence and Security Studies with the Australian Graduate School of Policing and Security at Charles Sturt University in Australia.

Roger Bradbury is Emeritus Professor of Complex Systems Science with the Crawford School of Public Policy at the Australian National University in Australia.
The Ethics of National Security Intelligence Institutions
Theory and Applications

Adam Henschke, Seumas Miller, Andrew Alexandra, Patrick F. Walsh and Roger Bradbury
## Contents

*Acknowledgements* vii

1 Institutionalising Intelligence Ethics: The Case for a Just Intelligence Theory 1
   ADAM HENSCHE AND PATRICK F. WALSH

### PART I

**Concepts and Principles for Just Intelligence Institutions** 31

2 On National Security Intelligence: Concepts and Contexts 33
   SEUMAS MILLER

3 On Just Intelligence Operations: Exceptions and Explanations 51
   ADAM HENSCHE

4 National Security Intelligence Activity: The Principles of Discrimination, Necessity, and Proportionality 72
   SEUMAS MILLER

### PART II

**Practices: Just Intelligence Institutions in Action** 87

5 Espionage: Ends and Means 89
   SEUMAS MILLER

6 Covert Action: The Ethics of Secret National Security Operations 105
   ANDREW ALEXANDRA

7 PSYOP and Intelligence Institutions 122
   ANDREW ALEXANDRA
PART III
The Future of Intelligence and the Evolution of Intelligence Institutions 143

8 Privacy as Digital Sovereignty: Rethinking Privacy for International Intelligence 145
   ADAM HENSCHKE

9 Beyond Independence: The Ethics of Trustworthy Intelligence Institutions 163
   ADAM HENSCHKE

10 Changing Practices, Disruptive Technologies, and the Evolution of Intelligence Institutions 185
   ADAM HENSCHKE, PATRICK F. WALSH, AND ROGER BRADBURY

11 The Future of Intelligence Practice: Concluding Lessons for Just Intelligence Institutions 205
   PATRICK F. WALSH AND ADAM HENSCHKE

Index 233
Acknowledgements

The authors gratefully acknowledge the Australia Research Council and the Australian Graduate School in Policing and Security Studies at Charles Sturt University for supporting this research, through the ARC Discovery grant DP180103439, *Intelligence and National Security: Ethics, Efficacy and Accountability*. We also thank Devon Harvey and Andrew Humphrys for their support and patience.

Adam Henschke gratefully acknowledges the Australian Department of Defence Strategic Policy Grant *Confronting Foreign Interference and Cyberwar Challenges* for funding part of this research. He acknowledges support from the Ethics of Socially Disruptive Technologies (ESDiT) program, funded through the Gravitation program of the Dutch Ministry of Education, Culture, and Science and the Netherlands Organization for Scientific Research (NOW grant number 024.004.031). He thanks Leonardo Werner for his help with review and formatting. He also thanks the Philosophy Section at the University of Twente for their support while writing this.

Seumas Miller gratefully acknowledges the European Research Council, the Philosophy Section at Delft University of Technology, and the Uehiro Centre for Practical Ethics at the University of Oxford for supporting this research, through the ERC grant GTCMR. No. 670172, *Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies*. He also thanks the publisher and editors of *Intelligence and National Security* for permission to reproduce some material from his article “National security intelligence activity: a philosophical analysis”, *Intelligence and National Security*, 37:6, 2022, 791–808, DOI: 10.1080/02684527.2022.2076329.
1 Institutionalising Intelligence Ethics
The Case for a Just Intelligence Theory

Adam Henschke and Patrick F. Walsh

The Problem of Ethical Intelligence Institutions

This book explores the ethics of national security intelligence institutions. Intelligence involves practices that are outside of what is normally accepted – acts such as lying, spying, and manipulating people would normally be considered morally problematic, and should be avoided or even prohibited. US General John Magruder, who worked for the Office of Strategic Services, the precursor to the Central Intelligence Agency stated: “Clandestine intelligence operations involve a constant breaking of the rules… To put it baldly, such operations are necessarily extra-legal and sometimes illegal” (John Magruder, quoted in Weiner 2008, 13). However, when we consider intelligence, lying, spying, and manipulating people might be required, and in some situations may be obligatory, even praiseworthy. “From earliest times, intelligence has often involved covert operations intended to influence the course of events by methods ranging from deception to assassination” (Andrew 2019, 2). This book explores the context and reasons why what is normally morally blameworthy becomes permissible and praiseworthy for intelligence, providing resources for distinguishing cases where it is praiseworthy from ones where it is isn’t, and offering ethical reasons for our different judgments. This may seem counter-intuitive: “Some may find the concept odd, if not implausible, that you can have such standards for an activity that seeks… to violate norms of behavior that prevail in other circumstances” (Lowenthal 2017, 111). Drawing from other traditions dealing with morally exceptional behaviour, we develop an account about why and when, in intelligence, it is morally permissible to overlook these norms.

A key part of this story, we suggest, is that intelligence is not simply a set of practices, but it also refers to institutions. James may be an intelligence agent, an individual engaged in a set of specific intelligence acts, but to make sense of what James is doing, we have to see his acts in relation to the wider institution that he is working for. There are an increasing set of works that look at the ethics of intelligence (Bellaby 2014; Omand and Phythian 2018; Perry 2016; Quinlan 2007; Fabre 2022); our work adds the institutional dimension to this discussion. That is, it is not enough to simply look at the acts and practices of intelligence. In order to develop a thoroughgoing intelligence ethics, we need to look at intelligence institutions.
To motivate the discussion, consider this scenario: The political leader of the country Anxietous believes that the neighbouring country Belligerence is planning on interfering in Anxietous’ forthcoming election. Moreover, Anxietous’ leader believes that this interference will be a precursor to Belligerence invading Anxietous. What should Anxietous do? Knowing that the leaders of Belligerence have not been responsive to diplomatic efforts, the leader of Anxietous considers going to war against Belligerence. However, it rapidly becomes apparent that Anxietous has a low chance of defeating Belligerence in a conventional land-based or ground war. Furthermore, as this is a pre-emptive attack, it would likely violate Article 51 of the United Nations charter, and the just war tradition’s Just Cause criterion. Instead, Anxietous considers using a third option, a “Tertia Optio, the president’s option when the first option, diplomacy, is inadequate and the second, war, is a terrible idea” (Jacobsen 2019, 3). This Tertia Optio is the realm of intelligence, of spies, assassinations, and political warfare. The leadership of Anxietous needs to consider if using these secret means and forces short of war will do what is needed to counter the threat posed by Belligerence and to protect their citizens and national security.

There is a second aspect of intelligence implied in this scenario. As described, the leader of Anxietous believes that Belligerence is engaged in these activities and might be planning a military invasion. However, we do not know why they believe this. Are they simply anxious people, seeing threats everywhere? Or do they have good reasons to believe that this is happening, and what it implies? Intelligence plays a vital role in differentiating between unjustified anxiety and justified concern. Here, intelligence’s role is that of providing reliable and usable information for decision-makers. “Better-informed decisions lead to better government and a safer, more secure society” (Omand and Phythian 2018, 1). In the ideal scenario, Anxietous would have functioning and trustworthy intelligence agencies that are monitoring for threats, assessing the likelihood and impacts of those threats, and informing decision-makers properly and reliably, such that the decision-makers make reasonable decisions.

The key function that intelligence plays for policy makers, aside from the essential strategic warning function is decision advantage… providing policy makers with the intelligence that they need to have an advantage in pursuing their goals and in dealing with rival states.

(Lowenthal 2017, 13)

If the leader of Anxietous wakes up one morning after a nightmare and is suddenly convinced that Belligerence is engaged in political interference with plans for an invasion, the heads of the intelligence agencies would be expected to tell the leader that this was just a nightmare and there is no evidence of any such interference or impending attack. If, however, the leader of Anxietous has been informed by the leader of another country that Belligerence was attempting to buy large amounts of weapons, then it would seem reasonable for the intelligence agencies of Anxietous
to investigate if these claims were true, and also investigate if there was any other evidence that Belligerence had plans to attack.

The point of this scenario is to draw out two complementary features of intelligence. First, intelligence actions are typically considered to be a *Tertia Optio*, a third option where diplomacy is not enough but warfare is too much. Second, intelligence practice is concerned with gathering and using information to improve decision-making. In order to make good decisions, leaders must have good reasons for their decisions. This illustrates the key to understanding intelligence. “Good intelligence will address [policy maker’s] uncertainty by attempting to describe which outcomes or reactions are more or less likely and therefore where to focus one’s attention” (Lowenthal 2017, 13). It is about information and decision-making. Moreover, the decision-making, or, at least, the process on the basis of which the final decision is made, involves epistemic activity, for example, information, input, analysis, and dissemination from collectors and analysts, as well as decision-making by their leaders. In short, it is a collective or joint process involving multiple intelligence actors. Accordingly, as we will argue in Chapter 2, intelligence collection, analysis, and dissemination should be understood as *joint epistemic activity that aids national security decision-making, in an environment of competition*.

While this scenario, and the description of intelligence offered, may seem reasonable, we suggest that it exposes a deep moral and political problem for liberal democracies.

For the democracies, retaining such advanced intelligence capabilities is a key part of national security… we believe it is no longer possible to conduct such work without more explicit congressional, parliamentary, and public acceptance of the legal and ethical limits that should be placed on the intelligence agencies lest the manner in which they run their covert activities *undermines the national values and freedoms that they exist to help defend*.  

(Omand and Phythian 2018, ix; emphasis ours)

Liberal democracies face a basic tension when it comes to intelligence. To get information in order to make better decisions, decision-makers, whether they be police, military, or political leaders, need to make hard decisions. Intelligence actors and institutions may need to engage in activities that would not normally be permitted. However, based on the earlier description, these actions and decisions may run in contrast to the ethical and political principles that ground these liberal democracies. This is particularly obvious where liberal democracies declare that their moral authority is derived from their respect for basic human rights, that they have limits on what they can do to their citizens and in their citizen’s name, and that they desire political sovereignty and political autonomy. Many intelligence actions, and even the very existence of intelligence institutions, can run counter to these values and may threaten the trust in, and authority of, other liberal democratic institutions. As such, a comprehensive theory of intelligence practices and institutions is needed to
ensure that liberal democracies do not become the very things that they are fighting
against. Such a theory is normative, as opposed to descriptive, since it is a theory
of what intelligence practices and institutions morally or ethically (we use these
terms interchangeably) ought to be, as opposed to what they might in fact be in
some cases.

This book’s focus is on the ethics of intelligence institutions in liberal democ-
racies. Roughly speaking, liberal democracies are nations that, first, comply with
democratic processes that seek to represent the will of their citizens. Second, they
must comply with individual moral rights, especially individual freedoms. In lib-
eral democracies, individuals have freedom to choose their own idea of the good
life (consistent with a like freedom for others), in which political justice “must
allow for a diversity of doctrines and the plurality of conflicting, and indeed incom-
mensurable, conceptions of the good affirmed by the members of existing demo-
cratic societies” (Rawls 1985, 225). Finally, on this view, it is possible to argue
that if a liberal democracy sees its political authority being founded not just in
some process of agreement and representation, but also in the moral rights inherent
to all humans, then the principles advocated here would apply to people regardless
of their citizenship. Here,

all persons stand in certain moral relations to one another: we are required to
respect one another’s status as ultimate units of moral concern – [this] require-
ment that imposes limits upon our conduct and, in particular, upon our efforts to
construct institutional schemes.

(Pogge 1992, 49)

This description of liberal democracies is deliberately broad and vague, as we
don’t want subsequent discussions to be tied to this or that definition of what a
liberal democracy is, or what it should be. Instead, we intend for this description
to allow us to roughly delineate liberal democracies from authoritarian political
regimes. Here, the authoritarian regimes would have limited or no effective pol-
icies or practices of representation; one particular value or ideology would suffuse
and dominate the people under that rule, and/or actively prevent accountability
through practices that “entail substantive and procedural rule-breaking, interfere
with the preferences and inhibit the civic virtues of those to whom accountability
is owed, and strictly control information flows” (Glasius 2018, 525). Again, here
our description of authoritarianism is broad and vague. We recognise that there will
be overlap between some states that are more or less liberal democratic and some
states that are more or less authoritarian. Further to this, we anticipate that there
will be discussion and disagreement about where which particular states fit on this
spectrum.

As will be argued in later chapters, the justifications for intelligence practices
and institutions by liberal democratic states are dependent upon the ways in which
political and intelligence leaders represent their citizens and the values that these
nations claim to hold. An authoritarian regime may justify its intelligence practices
and institutions by reference to those practices and institutions serving and
providing the political leadership and assisting them to maintain control over the citizenry. This justification is very different from the justification for intelligence practices and institutions in a liberal democracy. In a liberal democracy, intelligence practices and institutions are ultimately justified by their contribution to preserving liberal democracy and, therefore, protecting the rights of its citizens and its democratic processes. Therefore, when national security institutions generally, and intelligence institutions in particular, exercise power over their fellow citizens in a liberal democracy in a manner that violates citizens’ basic moral rights and liberal democratic principles, then that nation is becoming more like an authoritarian one. That is, liberal democracies need to be able to criticise and constrain their intelligence institutions, if these liberal democracies are not to become authoritarian in character. This book offers a set of principles to help protect liberal democracy protect itself against this risk.

Secrecy and Dirty Hands

The history of intelligence stretches back millennia, but it is only recently that these histories have become more open to the public. “For centuries before the Second World War, educated British people knew far more about intelligence operations recorded in the bible that they did about the role of intelligence at any moment in their own history” (Andrew 2019, 1). This points to one feature commonly associated with intelligence – secrecy. Often, secrecy is seen as a defining and essential feature of intelligence.

[S]ecrecy is the key to the definition of intelligence... Without secrets, it is not intelligence. Properly understood, intelligence is that range of activities – whether analysis, collection, or covert action – performed on behalf of a nation’s foreign policy that would be negated if their foreign “subjects” spotted the hand of another country and acted differently as a consequence.

(Warner 2002; emphasis ours)

Historically and in the context of the origins of modern-day national security intelligence agencies, the existence of many of these institutions was kept secret from the public for decades. For example, the existence of UK’s MI6 was only officially admitted by UK PM John Major to the House of Commons on 6 May 1992 (Dorril 2000, 758). While an increasing amount of intelligence may be collected from open sources, the history of modern intelligence from the end of the Second World War, throughout the Cold War, and into the present post 9/11 environment has been one about the ability by intelligence agencies to collect sensitive information without the target or agent’s knowledge (Walsh 2011, 30). Some secret intelligence collection is critically important in circumstances where it is necessary to provide decision-makers forewarning about a target or a threat and its possible intentions. Moreover, the need to control secret information sources and collection methodologies, in order to avoid giving a target or the enemy a “heads up”, has created, by necessity, a culture of secrecy, which has become an important characteristic
of intelligence. This secrecy has resulted in the development of closed information systems, where traditionally the “need to know” principle governed distribution. However, the changing nature of national and transnational threats, where threats can be both foreign and domestic since 9/11, has resulted, to some extent, in a “contradiction between sharing information with decision-makers or other stakeholders quickly, and closed information systems and practices protecting the information” (Walsh 2011, 30).

Consider here Anxietous’ leader lets their citizens know exactly what intelligence operations they were involved by giving a set of highly detailed public announcements. This would easily be picked up by Belligerence, and they would likely change their actions. This would result in a reduction of the capacity for Anxietous to gather intelligence, ultimately resulting in poor decision-making. On this approach, it should be no surprise that the public would have such a limited knowledge of intelligence – in order for it to be intelligence it must be secret, part of a conscious effort “to block information about it or evidence of it from reaching that person, and to do so intentionally” (Bok 1989, 6–7). Chapter 2 argues against secrecy being a necessary condition of intelligence, but recognises that intelligence necessarily involves epistemic competition, and secrecy is one way of trying to successfully engage in that competition.

This need for secrecy, or least control over information, about what a country is doing creates a problem for liberal democracies. “The concept of secrecy, upon which all intelligence services rely regardless of the government they serve, conflicts with the democratic concept of open governments” (Lowenthal 2017, 6). One of the defining features of liberal democracies is that political institutions, and actions conducted in service of those institutions, gain their moral, political, social, and legal authority from the people that the institutions serve. “Good governance therefore is a necessary means to assure these stakeholders and to safeguard their continued support” (Lowenthal 2017, 82). In order for the people to continue granting that authority, they must know what the state is doing in their name. Simply stated, in order for liberal democracies to be properly representative, they must have public accountability.

So here, we find a significant dilemma for intelligence. If secrecy is an important (though not necessary) element of intelligence practices, then it makes no sense to go public with one’s actions, operations, means, or methods. While he was US Director of National Intelligence, James Clapper declared that the disclosures of US and allies’ Signal Intelligence (SIGINT) by Edward Snowden caused profound damage to the national security of the US (Clapper 2014). Making the means and methods of particular SIGINT public was believed to have caused various national security threats to change their own behaviours, to increase the security of their informational practices and communications, and to undermine a key set of tools in the national security arsenal of the US and its allies. In conflict with this, we see Snowden’s motivations being about the public having a right to know not just that they were potentially caught up in a number of SIGINT operations but also what intelligence institutions were doing in their name (Greenwald 2014). If liberal democracies are to be properly representative
of their people’s interests and motivations, then those people surely need to know what the state and its institutions are doing in their name.

What we suggest here is that the dilemma is not so cut and dried. First, we do not live in simple binaries. There is significant middle ground between saying “the actions of the state must be secret” and “the actions of the state must be open and accessible to all”. This book, like any treatment of the ethics of intelligence, recognises this complexity and inhabits the space between these two extremes. There is no conceptual dilemma here. Second to this, there are ways of ensuring accountability without making the actions of the state public. As Genevieve Lester argues, the history of intelligence and national security in a country like the US is not just a history of intelligence actions and operations, but that of the institutions tasked with overseeing those actions, operations, actors, and institutions and holding them to account (Lester 2016). As will be argued in Chapter 9, what is needed is some set of accountability practices that ensure that intelligence institutions are worthy of trust. We can avoid the horns of the dilemma between secrecy and openness by developing a set of institutional accountability measures.

Finally, there are a number of situations and contexts in which secrecy is justified. Consider Operation Mincemeat. During the Second World War, the British needed to deceive the Germans about their future plans. In order to do so, they produced a fake set of documents and placed the documents with a dead body and let the corpse wash up on the Spanish coast. The idea was to convince the Germans “that preparations against Sicily were only a cover for assaults on Sardinia and on southern Greece… The Germans dutifully reinforced Sardinia and the Peloponnese, leaving Sicily alone” (Rothstein and Whaley 2013, 157). Operation Mincemeat required secrecy and potentially played a significant role in the British war effort. We can also consider more common intelligence efforts, like placing someone into an enemy military, terrorist group, or organised crime syndicate. These sorts of covert operations require secrecy to succeed. Moreover, if the secret operative becomes known, it not only puts the mission at risk but also places the lives of those undercover in jeopardy. The group Reporters Without Borders offered a significant criticism of the ways that Wikileaks made particular information publicly available.

Revealing the identity of hundreds of people who collaborated with the coalition in Afghanistan is highly dangerous… It would not be hard for the Taliban and other armed groups to use these documents to draw up a list of people for targeting in deadly revenge attacks.

(quoted in Siddique 2010)

Whether it is at the operational level, or that of individual actors, secrecy might be necessary for the operation to be successful and for the relevant actors’ safety.

One way that ethical discussions have sought to square the circle of justifying ethically problematic behaviour is commonly referred to as “dirty hands”. In dirty hands literature, the basic idea is that people in particular roles may be
required to engage in particular behaviours and/or to request that others engage in particular behaviours that would normally be ethically unacceptable. It captures the situation of “being required on occasion to do what is necessary but what is also wrong at the same time” (Archard 2013, 778). For instance, if Anne was to ask Charles to secretly spy on Becka, a normal ethical criticism would be that both Anne and Charles are violating Becka’s privacy and are worthy of ethical criticism. However, if Anne is the leader of Anxietous’ domestic intelligence agency, Charles is an intelligence agent, and they have reason to suspect that a local citizen Becka is working for Belligerence, then both Anne and Charles may be required to do what is necessary. But this is wrong at the same time as it violates privacy.

The concept of dirty hands brings two additional elements to the analysis of intelligence activity in liberal democracies. First, the concept of dirty hands implies that people in particular roles may have duties that oblige them to act in ways which would not be permitted in normal circumstances. “This manoeuvre has the advantage of capturing something important in the dirty hands literature (and it is also present in the realist literature), namely, the emphasis on the special moral significance of the role of political leadership” (Coady 2011). Originally suggested by Michael Walzer in his paper “Political Action: The Problem of Dirty Hands”, dirty hands scenarios frequently arise for those tasked with making political decisions.

The issue is posed most dramatically in politics for the three reasons that make political life the kind of life it is, because we claim to act for others but also serve ourselves, rule over others, and use violence against them. It is easy to get one’s hands dirty in politics and it is often right to do so.

(Walzer 1973, 174)

The basic argument put forward by Walzer is that political decisions, and people that make political decisions, may have to violate a normal ethical principle.

It means that a particular act of government (in a political party or in the state) may be exactly the right thing to do in utilitarian terms and yet leave the man who does it guilty of a moral wrong. The innocent man, afterwards, is no longer innocent.

(Walzer 1973, 161)

The idea is that the political decision-maker is in a forced choice scenario. In virtue of their role, they have to make particular decisions that would otherwise be morally unacceptable. Moreover, the role of political decision-maker is such that they take into account things that would not naturally feature in a normal relationship. Anne would not normally be required to have Charles spy on Becka, but as Anne is the leader of the domestic intelligence agency, she is required by the role to ask this of Charles. In virtue of his role, Charles is required to follow this command. Standardly, one of the conditions of dirty hands justification is that
the normally forbidden action will generate more good than the harm it does, and that it is the only, or clearly best, way of bringing about the good outcome. These conditions align with principles of proportionality and necessity, to be discussed in Chapter 4.

The concept of dirty hands adds a second element to the moral analysis, an element which distinguishes it from a *simple* consequentialist ethics. On a simple consequentialist analysis, Anne and Charles do the right thing, because it maximises the security for Anxietous, by improving decision-making and protecting against threats from Belligerence and other sources. However, the concept of dirty hands implies that there is a more morally complex decision being made, resulting in the morally justified action nevertheless being morally problematic.

When rules are overridden, we do not talk or act as if they had been set aside, cancelled, or annulled. They still stand and have this much effect at least: that *we know we have done something wrong even if what we have done was also the best thing to do on the whole in the circumstances*.

(Walzer 1973, 171; emphasis ours)

If Becka is a citizen of Anxietous, then she would have legal protections against state surveillance. Moreover, if we consider that privacy is a moral right that all humans have, regardless of their political citizenship, then Becka’s privacy has been abridged or violated by Charles and Anne. What makes the application of the concept of dirty hands distinct from other ethical analyses of such situations is the recognition that *even if the act itself is morally justified, there is still some moral harm or wrong occurring*. Anne and Charles are justified in what they do, even though it violates Becka’s privacy. In contrast, on a consequentialist analysis, albeit a deliberately simple one, what Anne asks of Charles, and what Charles does is the correct thing to do. In this simple consequentialism, given the good outcome, there is nothing morally wrong in what Anne and Charles are engaged in. In contrast, the concept of dirty hands recognises that even if the ends justify the means, there is some “moral remainder”. This moral remainder is what makes the application of the concept of dirty hands distinct from other ethical analysis. *Even if the act itself is morally justified, there is still some moral harm or wrong occurring.*

In contrast, on a consequentialist analysis, albeit a deliberately simple one, what Anne asks of Charles, and what Charles does, is just the correct thing to do. There is nothing morally wrong in what Anne and Charles are engaged in. According to this view,

whether an action is right or wrong *depends only on how it fares with regard to its overall outcomes*. We thus always have to construe an ordering of alternative routes of action from best to worst. What’s right to do is simply to pick the act that ranks highest, and what’s wrong is to pick a course of action that ranks lower… There is no place, however, for an act that is both wrong and right, since that would involve it having overall outcomes that are both best and not
best. We therefore never have to act wrongly to do the right thing, and thus dirty hands scenarios cannot arise.

(Baumann 2021, 472; emphasis ours)

In a simple consequentialism, the outcome is what matters. A more sophisticated consequentialism will take harms into account, and perhaps seek some ways to mitigate them. However, we suggest here that these efforts to recognise and mitigate the harms – including harms to the particular actor’s moral integrity – are an attempt to recognise this moral remainder. For instance, the more sophisticated approach would seek to recognise the rights of those involved in the particular action (Pettit 1988) or may engage in a process that includes justice in its outcomes (Feldman 1995). These more sophisticated accounts recognise and consider the moral remainder in their consequentialist reasoning, making them functionally equivalent to dirty hands. There is not space to explore this further; our point is that dirty hands is not a simple consequentialist ethic, and a more sophisticated consequentialism is in fact recognising and responding to the problem of dirty hands.

Returning to secrecy and intelligence practices and institutions, we would generally hold that spying, lying, manipulation, assassination, etc. are morally and politically wrong. However, given the needs and requirements of political leadership in liberal democracies, specifically where issues of national security and competition or conflict arise, we might see that – in some particular situations at least – such secrecy, spying, lying, manipulation, assassination, etc. are permissible. This is a classic dirty hands formulation – those in relevant political roles must make decisions that violate or override existing ethical, social, or political norms, in virtue of the particular roles that they are in. Further, unlike a simple realist stance which might argue that this is simply the right thing for political leaders to do, there is moral complexity in the decisions made and the actions taken, and there is still moral harm or wrong occurring. The secrecy may be justified, but it is still morally problematic.

To be clear, this is not to say that any and all such acts and operations are justified simply because they are part of a wider intelligence effort. We only need to consider the public backlash at various intelligence agencies following the Snowden revelations that many people around the world are concerned about what intelligence institutions do, and how they do it. Here, we suggest that the role of ethical analysis is to explore how and when particular intelligence acts are justified and where they lack justification. Further to this, our approach includes institutional ethics, in which we also seek to understand the justifications for intelligence institutions. It is not enough to simply ask if a given intelligence act is justifiable but to see that as part of a larger institution, and to ask what the purpose of that institution is and whether that purpose is morally justified. This book is an effort to set both limits and conditions on particular decisions made by individual intelligence officers at the micro-level (so to speak) and also, at the macro-level, on the institutional reach of intelligence agencies. In providing the necessary analyses, we recognise when dilemmas arise and when an all things
considered morally justified action or institutional practice, nevertheless, leaves some moral remainder.

National Security, Liberal Democracy, and Ethical Intelligence

So, the practices and institutions of intelligence in liberal democracies may need to engage in behaviours that would normally be morally impermissible. These may be one-off actions – Charles spying on Becka, or larger operations – the intelligence agency that Anna oversees making a policy decision to engage in covert actions, something they had hitherto not done, by way of responding to the threat that Belligerence poses to Anxietous. An essential feature of dirty hands in the context of national security intelligence practices (as opposed to, for instance, domestic criminal intelligence practices) is that these acts, operations, and policies occur in service of some greater end, national security. Without this purpose, the acts and institutions lack a fundamental element that allows us to understand, critique, and ultimately justify those acts and institutions. To explain this, we offer a brief account of national security, the role it plays in liberal democracy, and how this relates to intelligence and institutions.

National security is a contested concept, with different views through the years offering different ways to understand it. As Arnold Wolfers already argued in 1952, national security is an “ambiguous symbol” (Wolfers 1952). Despite recognising this ambiguity, we should not let the term be whatever anyone decides. As such an approach “may be permitting everyone to label whatever policy he favors with an attractive and possibly deceptive name” (Wolfers 1952, 481). We suggest here that there are three rough ways that national security can be conceptualised. First, national security is just the set of practices conducted by actors and institutions whose function is the protection of the state against foreign threats, particularly the military and related externally oriented intelligence institutions.¹¹ This conception focuses “primarily on the state as the key unit and on the political and military sectors” (Buzan, Wæver, and De Wilde 1998, 11) and is concerned with “Aussenpolitik (foreign relations) [rather than] Innenpolitik (domestic policy including law enforcement)” (Sussex 2022, 25).

A second approach to national security sees it protecting the nation’s people against risks and threats. “As Pufendorf summarises, echoing Hobbes, ‘the general Rule with Sovereigns are to proceed by, is, Salus Populi suprema lex esto; Let the Safety of the People be the supreme Law’ (Skinner 2009, 362). This view draws its inspiration with the rise of society from the state of nature, where people forgo or forfeit some sets of rights to the state, who in turn provides security to its citizens. In the sixteenth century, Sir Edward Coke, a British lawmaker described “the relationship between sovereign and subject in terms of a ‘mutual bond and obligation’, under which the subject owed allegiance or obedience, while the sovereign was bound ‘to govern and protect his subjects’…’”. A more concise and well-known formulation was offered in 1867 by the US lawmaker, John Farnsworth, as “[t]he first duty of the Government is to afford protection to its citizens” (Both quoted in Heyman 1991, 513, 508). On this approach then,
national security is the duty of the state to protect its citizens as a result of the social contract between state and citizen.

A final way to understand national security is through the language of securitisation. In contrast to national security as duty, this approach sees security as “being about survival. It is when an issue is presented as posing an existential threat to a designated referent object” (Buzan, Wæver, and De Wilde 1998, 21). When considering national security, the “the nation is the referent object, and what matters is the survival or at least the persistence of the state” (Henschke 2021, 80).

On the original treatment by Barry Buzan, Ole Wæver, and Jaap De Wilde, using such language, the particular speech act of securitising the nation signifies that the nation is of special importance and, as such, normal ethical and political practices do not apply (Buzan, Wæver, and De Wilde 1998, 1–48). Here, states seek to “create a ‘state of exception’ in which national security questions [are] beyond the reach of the public and legislature and become immune to liberal democracy’s usual checks and balances” (Legrand 2022, 60). Declaring something like intelligence to be in the realm of, or in service of, national security is both a descriptive and normative statement. Intelligence is both in service of protection of the state and as an example of dirty hands, where exceptional practices are permitted.

Intelligence features in all three conceptualisations of national security. Whereas intelligence refers to a set of agencies devoted to protecting the nation, these sets of agencies are just part of the national security institutional framework. As an arm of the state, part of its monopoly of force to use Max Weber’s approach, intelligence agencies are both permitted and required to engage in various behaviours that promote and ensure the security of the state’s citizens. Finally, insofar as intelligence helps identify and respond to threats to the survival or persistence of the state, it becomes a core element of national security.

Rather than decide which of these three concepts of security is the most important, accurate, or correct, we argue that on all three conceptualisations, intelligence is essential for national security. In all three, intelligence centres on “a nation’s efforts to unravel secrets and mysteries, as its leaders attempt to understand world affairs and make decisions in a hostile environment” (Johnson 2017, 6). As will be argued at length in Chapter 2, intelligence is part of an epistemic activity, intended to change and ideally improve the understanding of the world such that decision-makers make better decisions. Liberal democracies face continual challenges, risks, and threats to the safety of their citizens, and to their own survival, and intelligence is needed to know about them, to understand them, and to respond to them effectively.

As already discussed, such responsibilities can sit at odds with the ideas and principles of liberal democracies. Intelligence agencies often fall prey to Lord Acton’s well-known prophecy that… power tends to corrupt, and absolute power corrupts absolutely… History reveals time and again a nation’s secret services have turned their disquieting capabilities for surveillance and manipulation against the very citizens they were meant to shield.

(Johnson 2017, 7)
Take, for instance, the way that the US Federal Bureau of Investigation (FBI) surveilled Martin Luther King, Jr. in the 1960s, and after gathering evidence of his extra-marital affairs, sent him threatening letters that suggested he commit suicide lest these actions be made public (Weiner 2012, 249–250). One Congressional enquiry into US intelligence practices found that the sustained use of such tactics by the FBI in an attempt to destroy Dr. Martin Luther King, Jr., violated the law and fundamental human decency… it demonstrates just how far the Government could go in a secret war against one citizen.

(Church 1976, 219)

Likewise, in a 2004 report by the US Central Intelligence Agency (CIA) Inspector General John Helgerson raised questions about whether CIA officers might face criminal prosecution for the brutal interrogations carried out inside the agency’s network of secret prisons… methods like waterboarding, sleep deprivation, and exploiting the phobias of prisoners… [and perhaps] violated the United Nation’s Convention Against Torture.

(Mazzetti 2014, 118)

While we might consider that secrecy is an important part of intelligence, it can allow for behaviours that are not permitted, even by dirty hands accounts.

Here, however, we see two fundamental features of intelligence in liberal democracies. First, both examples described draw from criticisms offered by internal reviews. The abuses by the FBI and CIA were made known, in part, due to the particular checks and balances of the US government, congressional oversight, and reporting by inspector general. While it is necessary to recognise and find fault with the ways that such checks and balances have operated, these cases indicate something about the nature of intelligence in liberal democracies: The practices and institutions of intelligence should be accountable to their citizens and stated values. Further to this, like many other aspects of liberal democratic government, many problems and failures in intelligence institutions have only been brought to light, and acted upon, due to the efforts of investigative journalists, the so-called “Fourth Estate”. On the rough descriptions offered earlier, such oversight, review, and external criticism would not occur in authoritarian states.

Second, the cases described both fall far short of the stated values of liberal democracy. As we noted at the beginning of this chapter, intelligence is sometimes presented as a space in which ethics don’t apply. As General Magruder said, these sorts of clandestine operations “involve a constant breaking of all the rules” (Magruder, Quoted in Weiner 2008, 13). In addition to the fact that liberal democracies have, albeit limited and at times flawed, oversight and accountability for their intelligence institutions, these practices and institutions can be held up to the norms of liberal democracies and can be found wanting. While we would see these
values as deriving their authority from their moral foundations, the simple fact that liberal democracies claim that values such as liberty, well-being, justice, and so on are important norms of some sort. And these norms “serve the function of creating accountability… Creating accountability is simply what norms do” (Brennan et al. 2013, 39). Here, we do not need to enter into a discussion of the moral truths, rather, we can point to the norms proclaimed by liberal democracies and see if the practices and institutions of intelligence meet those norms.

These two points, that there are some formal and norm-based means of assessing the practices and institutions of intelligence in liberal democracies, mean that we can place limits on those practices and institutions. As will be discussed throughout the book, particular intelligence acts, such as placing King Jr under surveillance and using compromising material in an effort to silence him, and wider institutional decisions, such as the policy to permit the use torture or “torture-lite”,14 are now able to be critically assessed, by reference to the ethical values that liberal democracies use to delineate themselves from authoritarian states. This book is about that story: The ways that liberal democracies rely on intelligence for decision-making in a context of national security competition, and on ways to limit power and abuse that come from these practices.

**Intelligence Practices and Institutions**

Intelligence as a concept and set of dynamic practices cannot exist in a vacuum and needs to be understood by examining what intelligence actors do and the institutional contexts that direct and support their activities. As Ratcliffe suggests, the intelligence process includes some critically important functions regardless of whether this work is being carried out in a military, national security, policing, or private sector capacity. For example, in Ratcliffe’s 3–I model, he explains what intelligence does using a triangular diagram that includes arrows interacting between three areas of activity. Intelligence analysts interpret the environment, their assessments inform decision-making, which hopefully will then have an impact on the threat/risk environment (Ratcliffe 2008, 109–112).

Practising intelligence is highly context-driven. In other words, different types of actors such as collectors, analysts, technical, and admin support staff may be involved depending on agency mission, roles, function, and legislation. Additionally, given the growing diversity and complexity of threats operating in the security environment, it is now often a combination of different intelligence practitioners required at varying times to understand, manage, or disrupt them.

Here, our focus on the main intelligence practitioners is arranged around two large roles: collectors and analysts. Both these roles have become intermingled and, in some intelligence agencies, they are even integrated. Therefore, it is important to keep in mind that these two roles are not entirely separated disciplines in any agency, though for the sake of simplicity and at a very general level, it is possible to distinguish some broad and different characteristics between collectors and analysts. Moreover, in history and modern practice, collectors and analysts are still typically quite distinct, and may have very little to do with each other.
Collectors

Several classes of actors, skilled in a range of disciplines and technical knowledge, are responsible in making sure that intelligence agencies are able to develop an as accurate situational awareness or domain knowledge about threats and risks of greatest concern to governments. Intelligence collection therefore is not just about the technical capability of a collection platform but how this is configured with other capabilities across a nation’s intelligence community. The performance of one collection platform must be evaluated not just at a narrow technical level but also at the institutional level as well.

The three traditional covert collection capabilities are HUMINT, SIGINT, and GEOINT – the latter nowadays more frequently referred to as geo-spatial intelligence. HUMINT or human intelligence is espionage. Prior to the great technological inroads that marked the rising importance of collection capabilities of SIGINT and GEOINT from the early Cold War until the present, HUMINT collection was the main method stretching back to early human history in the bid to obtain secret information not available in the public domain. “[T]hree times over the previous 500 years, Britain faced major invasion threats – from the Armada of Philip II of Spain in 1588, from Napoleon in the early nineteenth century and from Hitler in 1940” (Andrew 2019, 1). Christopher Andrew rightly suggests that while much has been written about the Bletchley Park codebreakers who solved Hitlers ciphers, little was known by scholars at that time about the impressive feats of earlier codebreakers working against Philip II and Napoleon at times of equal great crisis to Britain (Andrew 2019, 1). Modern HUMINT collection is largely dominated by particular intelligence agencies, such as the CIA and FBI in the US, MI5 and MI6 in the UK, the Australian Secret Intelligence Service in Australia, who have developed specialised espionage capabilities over time.

There is usually an elaborate and labour-intensive effort made by a HUMINT (or clandestine) officer to identify, recruit, and manage individuals who have access to valuable information that the home country desires. While in like-minded liberal democratic states, but particularly in the “Five Eyes” countries, it is usual to have declared foreign liaison officers from HUMINT agencies that promote intelligence sharing and trust building. As part of the Five Eyes intelligence sharing arrangements, officers may be embedded within each other’s agencies. There are usually greater risks for undeclared HUMINT officers working in a foreign country, where they are operating under an assumed identify, and their collection efforts are sensitive and riskier, given they are not always under diplomatic protection.

HUMINT collection can be done by civilian or military assets and can be completed in parallel with other covert action operations by special forces. HUMINT is also a collection capability in many policing agencies where it is usually referred to as covert human intelligence source and may include a police officer working undercover in a terrorist or criminal gang and/or the policing agency handling a human source who will have close access to, or knowledge of, illicit activity. In all HUMINT environments, the risks of being exposed can be high, and HUMINT agents and their case officers are, by definition, involved in deceptive behaviour,
which may also require participating in illegal activities in the location of operation
to ensure assumed identities are not revealed.

HUMINT has its benefits in that – in certain circumstances at least – it can be
more cost-effective than applying large technical collection assets like SIGINT
or GEOINT and it can result in the ability to gain close access to a foreign source
and know their intentions. Though we recognise that HUMINT is built around
espionage, which is, by definition, deceptive, the information gathered can also be
deceptive or false, or the source of the information could prove to be unreliable or
even a double agent working for another foreign power.

In contrast to HUMINT, the two main technical collection capabilities, SIGINT
and GEOINT, can provide a scale of collection not usually possible via espionage.
The modern history of western intelligence agencies was largely defined by the
astonishing growth in technological sophistication in collection prowess of SIGINT
and GEOINT. SIGINT includes a number of different interceptions: COMINT for
the interception of communications between two or more persons, TELINT for
the detection of data arising from weapons during testing, and ELINT is used to
gather intelligence by use of electronic sensors. The latter allows the interception
of weapons control signals and radar. As noted by Lowenthal, the advantages of
SIGINT are that it can offer insights into the plans and intentions of threat actors.
Given the technology involved, it allows the collection of vast amounts of informa-
tion that can be done remotely (Lowenthal 2017, 16–50). The disadvantages of
SIGINT are potentially many, including the following: It can be difficult to break
the encrypted communication, it’s expensive, you can end up with vast pools of
information that cannot easily be assessed, and threat actors can use deceptive
communication (Lowenthal 2017). GEOINT or geospatial intelligence collects
images about a range of objects (natural or artificially made) that can be observed
on or below the Earth’s surface that may have national security relevance. What
holds significance varies based on intelligence collection priorities of governments
but can be physical in nature such as terrain, rivers, buildings, roads, towns, and
cities. Modern GEOINT agencies in western countries generally rely on an array
of satellites that transmit images as signals or digital data streams. Intelligence
analysts working with GEOINT collectors normally would request the level of
resolution of imagery required depending on the nature of the target, for example,
person, airport, factory, or building (Lowenthal 2017, 39). Images are normally
influential as stand-alone or attached to other intelligence products for decision-
makers, as a picture can be more compelling evidence of a developing threat/ risk
for a decision-maker than a written report containing SIGINT and HUMINT.
GEOINT, however, is expensive and can only represent one moment in time and
space. Hence, regular GEOINT collection by satellites or unmanned aerial vehicles
(UAVs) over a target is normally required.

In addition to the covert collection sources discussed earlier, a large volume of
information that intelligence agencies collect and use is open source information
(OSINT). OSINT can come from a diverse number of sources including media,
government reports, experts, financial data, and social media. In particular with the
rise of the digital revolution in the late 1990s, social media, or as some refer to it as
Institutionalising Intelligence Ethics

SOCMINT, is providing intelligence agencies with a diverse suite of other information that can be integrated with other data sources on a person or group (Lim 2016; Hayes and Luther 2018). Lim provides a useful description of the variety and utility of social media for intelligence communities (ICs):

Twitter, Facebook, YouTube, Instagram, LinkedIn and sundry social media applications have melded into a “vast digital social commons” capable of facilitating complex analyses of sentiments, semantics, clusters and networks, for instance, in the effort to map, among other things, global Jihadist activity.

(Lim 2016, 629)

There is insufficient space to provide examples of all the contexts in which SOCMINT may be a useful collection source for ICs. But one obvious advantage of SOCMINT’s various platforms (e.g. Facebook and Twitter) is that many provide real-time crowdsourcing information. In crisis situations, such as natural disasters or fast-moving security environments, such as pandemics, riots, radicalisation, or a terrorist attack, citizens can take on the role of journalists – quickly relaying information in real time or near real time that can provide situational awareness to emergency responders, police, and the intelligence community (Stottlemyre 2015, 578–589; Richey and Binz 2015, 347–364).

Analysts

The second major role in the production of intelligence is the analyst. As in the case of collectors, across a typical intelligence agency, there are multiple analyst roles. Their job descriptions will vary depending on the level of decision-making their work supports (e.g. strategic, operational, or tactical), context in which they do this work (e.g. military, national security, law enforcement, compliance, and private sector), and the mandate, roles, and functions of the agency they work for.

In the intelligence studies field, there remains an active discussion of what “intelligence analysis” is and what analysts do (Walsh 2011, 2020; Marrin 2011, 2017; George 2010; George and Bruce 2008). In short, this literature underscores the multidisciplinary nature of intelligence analysis. In its broadest sense, intelligence analysis is an amalgamation of the two broad branches of knowledge, and the practice context determines how aspects of social or natural sciences are deployed (Jøsang, 2016; Walsh 2020). For the sake of simplicity, we define “intelligence analysis” as “both a cognitive and methodological approach to processing and evaluating information – some of which is privileged – in order to produce an assessment for a decision-maker about the security environment” (Walsh 2011, 236). This definition is sufficiently vague that it can be applied in different intelligence contexts.

The analyst must utilise sound critical thinking capabilities in order to synthesise varying levels of valid and reliable information sources to assess the who, what, when, how, and where of a threat or risk and then communicate this effectively to a busy, often non-expert decision-maker. Given that analysts almost never have a
complete and accurate set of information on which to make analytical judgments, their assessments (key judgments) are often the result of inductive reasoning and are probability statements indicating varying degrees of confidence in the judgment being made. Given fragmented information, analytical confirmation bias and other institutional biases are key issues that analysts need to manage in order to improve the rigor of assessments.

A detailed discussion of all these technical skills and knowledge is beyond the scope of this book. Others provide a detailed background knowledge on both analytical techniques and general progress being made in the intelligence analysis area (see, e.g. Dahl 2017; Frank 2017, 579–599; Chang and Tetlock 2016, 903–920; Marrin 2007, 821–846, 2017, 2020, 350–366; Phythian 2017, 600–612; Lahneman and Arcos 2017, 972–985; Shelton 2014, 262–281; Walsh 2011, 2017; Pherson and Heuer 2020). Generally, the key technical and methodological skills, knowledge, and capabilities are social network analysis, structured analytical techniques, data mining/machine learning, as well as specific discipline area such as criminology, strategic studies, languages, psychology, weaponry (e.g. weapon of mass destruction [WMD]), and country/regional knowledge.

**Intelligence as an Institution**

The second major aspect of intelligence practice is to understand how the various roles and duties of different actors (e.g. collectors and analysts) relate to the broader missions of agencies across the intelligence community and to government. A full understanding of intelligence practice needs to go beyond merely examining the role of particular actors to the institutions themselves to view how they interact in a broader organisational context. In short, understanding intelligence practice is about seeing how history, evolving security threats, intelligence community leadership, organisational culture, and political influence shape the mandates, legislation, and resources of different agencies across ICs.

What is still largely missing from the intelligence studies literature is a greater understanding about how institutional factors influence contemporary practice. Our understanding of how intelligence actors perform their duties within broader intelligence institutions has, for several decades now, largely come from studying the history of agencies and their leaders when archives have been released.

For example, intelligence historians have provided a picture of how the impact of two World Wars, the Cold War, and beyond helped develop modern western intelligence community such as the “Five Eyes” communities today. Historical case studies have generated knowledge about a diverse range of issues that shaped the institutional structures of intelligence institutions such as counter-insurgency, covert action (Scott and Hughes 2006, 653–674), intelligence failure, intelligence and decision-making, efficacy, ethics, and accountability (Wark 1993; Best 2014; Kahn 2001; Warner 2014; Gentry 2016, 154–177). All of these studies also provide important knowledge about political and intelligence community leadership and how intelligence was used in a variety of different crises between the end of the Second World War, the Cold War, 9/11, and beyond.
In contrast, contemporary research on the organisational design of intelligence agencies and how it impacts on practice has been more difficult, largely because of culture of secrecy that envelops most ICs. However, in the period leading up to 9/11 and since, scholars have been able to gain insights into how agencies and ICs as a collection of agencies, or what is now more commonly called “the intelligence enterprise”, are structured. Such insights have been made possible due to a number of significant intelligence failures, such as 9/11 and the faulty intelligence assessments of WMD in Iraq. Subsequent events, such as Wikileaks and Snowden, have also enabled scholars to understand more comprehensively, if not completely, both the strengths and weaknesses in institutional arrangements and how they impact practice.

In the US, the 9/11 Commission Report publicly explained the need for intelligence institution redesign – including the need for more effective leadership in order to see such change come into reality (Walsh 2020). In response to the 9/11 Commission Report, the Bush Administration created the Department of Homeland Security (DHS) in 2003. In 2004, the enactment of the Intelligence Reform and Terrorism Prevention Act (IRPTA) led to the establishment of the Office of the Director of National Intelligence (ODNI). The creation of both agencies represents significant institutional reform in the US intelligence community, arguably the most important since the creation of the CIA in 1947. Several scholars and practitioners have questioned whether these latest legislative and policy measures have resulted in just further organisational flaws in US intelligence institutions rather than remedying them. For instance, Hammond argues that in the case of the organisation of the US intelligence institutions, the same contributory historical problems from 1947 that led to the creation of the CIA in response to Pearl Harbour have continued post 9/11, the 2004 creation of the IRPTA and ODNI, and beyond (Walsh 2020; Hammond 2010; Gentry 2015, 637–661).

A final thread relevant to our organisational design theme are organisational cultural issues. Our focus in this section has been on the value that analysis of Five Eyes intelligence institutions can bring to understanding the role of their leadership in the contemporary world. A critical factor in what can be learnt from history is how events, policies, and intelligence leaders themselves have shaped the culture of the organisations they lead. Is it possible, for example, to talk about organisational cultures for the CIA, MI6, or the Royal Canadian Mounted Police (RCMP)? How have they evolved and how do they differ from other agencies within the respective US, UK, and Canadian ICs? Given that the RCMP had its origins in domestic policing forces (Kealey 1992, 179–210), to what extent did an identifiable police culture impact in the early development of key aspects of the Canadian intelligence community? Additionally, can one discern a particular culture in US intelligence institutions that may differ or indeed be similar, for instance, to the Australian intelligence community?

From an organisational cultural perspective, we need to see people in our intelligence institutions as subject to confirmation bias whereby, as Dan Kahan suggests, they “assign weight to new evidence based on its consistency with what they already believe… This tendency limits the likelihood or speed with which people
will revise mistaken beliefs” (Kahan cited in NAS 2019, 8). Groupthink or affinity groups within and across intelligence agencies are clearly powerful influences on the evolution of organisational culture. Moreover, the historical role that leaders have played in shaping groupthink and organisational identity is important for understanding contemporary organisational outlooks in all Five Eyes ICs.

**Institutional Ethics**

This book is concerned with the ethics of intelligence institutions. Here, it is not simply a matter of philosophical theory being mechanically applied to specific problems; instead, there is a complex interplay between theoretical perspectives, on the one hand, and specific ethical intuitions and concrete empirical data, on the other. Whether or not integrated SIGINT databases constitute an infringement of the right to privacy is partly a matter of figuring out what is important about privacy (the ethical theory of privacy), as well as knowing the facts about the particular databases in question and the uses to which intelligence agencies might put them.

And the philosophical theory itself operates at a number of levels of abstraction. There are high-level theoretical claims, such as the principle of maximising the satisfaction of the greatest number or seeking to benefit the least advantaged. But there are also lower-level philosophical theories of specific values, for example, an ethical theory of political freedom, or a specific professional role, for example, the moral purposes and characteristic virtues of an intelligence officer. As recognised by the discussion of dirty hands, these lower-level normative or value theories operate within specific institutional, occupational, and technological settings; they are context-dependent. As such, they grow out of, and are highly sensitive to, specific situations and problems.

Please note that this need to relativise moral theories, perspectives, and principles to institutional and technological context does not imply relativism, that is, the theory that moral statements are not objectively true. The proposition that killing is wrong stands in need of relativisation. In general, it is morally wrong to kill another human being. In some contexts, for example, in a situation of self-defence, it might be morally permissible. However, from the fact that moral principles need to be relativised to context, it does not follow from this that the moral claims implicit in such relativisation are not objectively true.

Much of the philosophical work on ethics undertaken in universities in the English-speaking world in the last century was concerned with higher-order abstract theory, as opposed to lower-order context-dependent theory. However, it has become clear that lower-order context-dependent theory is back on the agenda. The exploration of a particular institutional context, like intelligence, makes this point well.

Philosophers, such as John Rawls, have developed elaborate normative theories concerning the principles of justice that ought to govern social institutions (Rawls 1999). Yet, they have done so in the absence of a developed theory of the nature and purpose of the very entities (institutions, including security institutions such as intelligence agencies) to which the principles of justice in question are supposed to
Institutionalising Intelligence Ethics

apply. Surely, the adequacy of one’s normative account of the justice or otherwise of any given social institution, or system of social institutions, will depend, at least in part, on the nature and point of that social institution or system. For example, the principles of justice governing the distribution of benefits and burdens in relation to prisons differ in substance and application from those operative in relation to universities. This is presumably, in large part, because prisons have a fundamental purpose of preventing ordinary people being harmed by dangerous persons, whereas universities have a fundamental purpose of ensuring the acquisition and transmission of knowledge. And, of course, the fundamental purpose of intelligence agencies differs from both prisons and universities, although it has some affinity with universities (being focused on the acquisition of knowledge and, as such, an epistemic institution) and also with prisons (being focused also on security).

There is, then, a pressing need to develop normative theories of central institutions, including security institutions such as intelligence agencies. It is only in the context of acceptable normative theories of these institutions that many specific practical ethical questions confronted by institutional actors will be able to be adequately answered. It is claimed that when presidents of the US pursue a policy of “stacking” the Supreme Court with judges of their own political persuasion, they overreach the limits of the legitimate authority of their office, corrupt institutional processes, and, over time, do significant institutional damage (Dean 2007). However, this claim crucially depends on a normative theory of government, the role of the judiciary, and the separation of powers; otherwise, the notions of legitimacy, corruption, and institutional damage in play here would have little or no import. Again, when it is claimed that US intelligence agencies have pursued policies of seeking to overthrow democratically elected governments that are regarded as hostile to the US, then they overreach the limits of the legitimate authority of their office, corrupt institutional processes, and, over time, do significant institutional damage. However, this claim crucially depends on a normative theory of intelligence agencies, the need for them not to engage in unlawful activity and to be accountable to their own democratically elected government, notwithstanding their national security function and consequent need for a high degree of secrecy.

Summary

Across the next ten chapters, this book explores a range of conceptual, practical, and institutional aspects of intelligence ethics. Having set the scene for the need for an ethics of intelligence, Part I sets out the book’s range of conceptual and ethical analysis. In Chapter 2, we present a case for intelligence to be understood as institutionalised joint epistemic activity in the service of national security decision-making, in an environment of competition. This definition is important to show how intelligence practices differ from that of military practice. That is, in warfare, the primary activities involve kinetic or physical actions. In intelligence, however, the primary activities are epistemic even if intelligence is used to support the military in warfare. They are about gathering information in order to better understand the world. However, we argue that a comprehensive account of intelligence cannot
intelligence practices are institutionalised joint epistemic activity. A single collector may gather intelligence on a particular target, but this is only part of a comprehensive intelligence practice. Thus, we argue that intelligence collection, analysis, and dissemination constitute joint epistemic activities. Again, however, we argue that a proper definition of intelligence cannot stop there. In order to describe how intelligence operates and to differentiate it from other joint epistemic activity, intelligence must be seen as competitive. Basically, intelligence officers and institutions are in competition with other intelligence officers and institutions, and this competition is necessary to explain intelligence practices and institutions. Finally, we develop the teleological approach to focus our analysis on national security intelligence. This clarification and focus present the case for an institutional approach to intelligence ethics.

Chapter 3 situates approaches to intelligence ethics that draw from and refer to the just war tradition (JWT). On our account, there is good reason to do this – the JWT has a long rich history to draw from. Furthermore, both intelligence and warfare necessarily involve the transgression of regular moral norms. In normal life, spying on someone, exploiting their weaknesses, and coercing them into a particular set of behaviours would be morally impermissible. However, in intelligence, these transgressions are not only permitted but they may also be required and celebrated. Moreover, intelligence requires these practices to be developed, determined, and directed by intelligence institutions. So, much like the ethics of war, in which justified institutional decisions around the resort to warfare are tied to six particular criteria, we present a case for six principles of jus ad intelligentium (i.e. the decision to direct the gathering of intelligence in a particular setting):

- Just cause for intelligence
- Right intention for intelligence
- Legitimate authority for intelligence
- Logical resort for intelligence
- Intelligence that is fit for purpose
- Proportionality for intelligence

Importantly, we show how these six jus ad intelligentium principles differ from the six jus ad bellum criteria. Furthermore, we use the institutional frame to understand how and why these principles differ from other suggested just intelligence theory (JIT) approaches.

Chapter 4 looks more closely at intelligence practices that fit the jus in intelligentia (i.e. what methods can legitimately be used to gather intelligence). As before, the argument is that while the general principles offered in jus in bello are useful starting points, they do not apply in a straightforward way to intelligence. The point of departure is that intelligence practices are justified by reference to the institutional purposes of intelligence, to aid in national security decision-making. Therefore, they differ quite significantly from the jus in bello criteria.

Accordingly, some constitutive principles of Just War Theory, when appropriately revised, are applicable to national security intelligence activity,
Institutionalising Intelligence Ethics

notwithstanding the essentially epistemic character of intelligence activity. Specifically, analyses are offered in this chapter of the key principles of discrimination, necessity, and proportionality. Importantly, the principle of necessity is given a novel analysis according to which it is in reality a set of different principles, depending on the institutional setting in which it is being used. Moreover, the analysis reveals that, as typically used, it consists (in part) of a means/end principle of rationality and one or other versions of a principle of harm minimisation. In addition, it is shown, in general terms, how the principles of discrimination, necessity, and proportionality (or, at least, analogues of these principles) apply, or ought to apply, to national security intelligence activity. To reiterate, the basic argument of Chapter 4 is that we cannot simply take the *jus in bello* criteria and apply them to intelligence practice. Intelligence practices and institutions are fundamentally different from military practices and institutions, and so the *jus in intelligentia* principles need to be developed to suit those practices and institutions.

Part II looks at three particular ethical challenges that are unique to intelligence. The connecting theme between these chapters is that intelligence practices and institutions require actions that are specific to intelligence.

Chapter 5 looks at espionage and, therefore, with the collection and analysis of the secret intelligence of hostile foreign states. There are various issues, or sets of issues, that are salient in relation to espionage. One set of issues concerns the normative theoretical framework justifying espionage (in our restricted sense of that term). In short, what are the purposes or ends that justify the institutional activity of espionage as a means? It is argued in Chapter 2 that espionage and other national security intelligence activities are ultimately justified by the collective moral good of national security.

A second set of issues concerns the particular moral principles that ought to govern the institutional practice of espionage as a means. The principles of discrimination, necessity, and proportionality, discussed in Chapter 4, come to mind and it is assumed that they have application to espionage. However, it is argued that there is an additional principle, namely, a principle of reciprocity in play.

In relation to the need for recourse to a principle of reciprocity, it is argued that espionage is a harmful activity and the moral wrongness of harmful actions can be mitigated if they are reciprocal. However, it is also argued that espionage is frequently, if by no means always, a species of “dirty hands” epistemic activity.

Covert action is the focus of Chapter 6. We start by clarifying what covert action is and putting the practice in its historical and institutional context. We offer a description of covert action as actions undertaken by intelligence agencies with the intention of exerting influence or causing some outcome in a foreign state, without being attributable to those agencies or the governments for which they work. The chapter then explores the justifications for covert actions and looks to sovereign equality and human rights to explain the ethical complexities around these practices. We then finish the chapter by looking at particular institutional aspects of responsibility and authority within democratic states for covert action they undertake.
Chapter 7 delves into the ethically complex area of psychological operations, or PSYOP. Again, the fact that intelligence institutions engage in informational activities that target people’s beliefs and motivations separates it from kinetic actions. PSYOP, we argue, should be seen in the context of speech acts. The chapter then looks at PSYOP in times of peace, PSYOP as a potential cause for war, and PSYOP in times of war. We argue that there is a defeasible right to make use of PSYOP, so there is a distinction between protected uses, where others are not entitled to prevent or retaliate against their use, and unprotected uses, where they do have such a privilege. Second, the impact of PSYOP is mediated through their effect on those to whom they are directed.

Part III of the book looks to the future of intelligence ethics and the future of intelligence. Given that intelligence involves epistemic actions that will frequently involve personal information, Chapter 8 begins the discussion by analysing the concept of privacy. We argue that privacy needs to be understood in at least three different ways. First, a traditional ethical and philosophical account of privacy understands it in reference to two people and the ways that they ought to treat information about each other. We then show that privacy also needs to be understood in a political sense by reference to the relations between individuals and institutions. Of primary importance here are the relations between citizens and their state. However, with the rise of informational institutions spurred by the penetration of the internet into almost every part of our daily lives, we must also recognise the particular relations between consumers and private companies. We then argue that modern national security intelligence practices, in which states are able to gather and direct information against the citizens of other states, require that we think of privacy in a third way, by reference to digital sovereignty.

The focus of Chapter 9 is on the relationships between intelligence institutions and other political institutions. We suggest that there is a commonly held belief that intelligence and politics ought to be independent. On our analysis, this independence is bidirectional: intelligence practices and institutions need to be independent of political influence, and political actors and institutions need to be independent of the influence of intelligence actors. However, we then show that this is a myth, but a noble one that has a sound moral foundation. Looking to this foundation, we argue that what ought to be aimed is that intelligence institutions are worthy of trust. We then offer three different elements of trust – reliability, predictability, and correct intention – to show how the aspirational elements captured in the independence myth can be met by having trustworthy intelligence institutions.

We continue the point of the dynamic and constantly evolving nature of national security intelligence in Chapter 10. Here, we look at three disruptive technologies to show how they are impacting intelligence practices and institutions. Specifically, we look at facial recognition technologies, encryption technologies, and how modern information and communication technologies are driving the evolution of OSINT. Each of these examples, we argue, shows three things. First, the simple application of the just war principles will not meet the current reality of national security intelligence. Second, intelligence institutions need to develop a principled and reflective approach to these changes. Finally, accountability is a fundamental
principle that must be incorporated into intelligence practice and institutions to be considered just.

In the concluding chapter, we draw lessons from the recent COVID-19 pandemic about the relations between national security intelligence practices and institutions and non-national security space. As the COVID-19 pandemic spread around the world, the unique epistemic tools and skills of intelligence were needed to understand what was happening and also to provide guidance for political decision-makers. The basic argument of this chapter is that the interactions between national security institutions and public health institutions presents a very useful way to envision the future of intelligence. In this chapter, we consolidate a number of arguments and principles developed throughout the book, asserting that the *jus ad intelligentium* and *jus in intelligentia* principles are in fact ways of ensuring and assuring the public at large that their intelligence institutions are worthy of trust.

A final note is needed on authorship. While this book has been a collective effort, which each author contributing content and concepts to other authors, each chapter has a particular author or authors. The argument offered by the book – that we need to develop a JIT that recognises and draws from the unique practical and institutional features of intelligence – is held by all of us. Each of us, however, has slightly different frameworks and angles to present this overall argument. As such, there are some differences across the chapters, but the main points, arguments, and positions hold throughout the book.

We outline a range of arguments that support our two main points. First, a JIT is indeed a workable and worthy goal of academic and practical pursuit. But the principles that guide and identify ethical intelligence practices are significantly different from the principles that guide and identify ethical military practices. That is, while we can look to the JWT for inspiration, the actual principles required by a JIT are functionally and fundamentally different from those found in, and discussed by, the JWT. Second, we must recognise intelligence not just as practices but also as institutions. This, we consider, is another functional and fundamental difference between just intelligence and just war that has not been effectively recognised by other discussions of intelligence ethics. While we are confident of our contribution here, we also note that we do not expect our work to be the final word on intelligence ethics. We hope that what follows in this book is part of the ongoing and evolving discussion of intelligence ethics.

Notes

1 Magruder’s point, while referring to laws, is of interest in how he says that intelligence is a breaking of the rules. We take it here to be indicative of a belief in breaking ethical rules or principles.

2 This is a reference to an area of the just war tradition, *jus ad vim*, or “force short of war” that has received some attention in recent years (see Brustetter 2016; Ford 2013). As will be argued in Chapter 2, this account of the ethics of intelligence considers intelligence to be an epistemic action and so is somewhat distinct from the main concerns of *jus ad vim*, though we do recognise that there is an overlap between the two areas.
Note here that despite the quotation from John Rawls, the view of this chapter is not necessarily Rawlsian, nor is our argument dependent upon Rawls’ conception of political justice or his wider political theory. Rawls is used here to indicate the idea of pluralism within liberal democratic nations.

Noting here that this often would only be part of the story. After all, even the citizens of authoritarian regimes have an interest in national security, and legitimate states may have a right to take the steps to protect that.

SIGINT refers to a range of different types of communications interception between individuals via telephone, email, and other related devices. It also includes the detection and tracking of various weapons systems. It can be collected via a number of different ways including ships, planes, ground monitoring, satellites, and uncrewed aerial vehicles.

While we do not necessarily disagree with James Clapper’s assessment here, it is important to note this assessment is necessarily correct.

Privacy is discussed in more detail in Chapter 8.

See, for instance, Philip Pettit’s “The consequentialist can recognize rights” (Pettit 1988).

For more detailed discussions of dirty hands and moral theory, see Nielsen (2007); Meisels (2008); Baumann (2021); de Wijze (2013); Rynard and Shugarman (1999).


By that, we mean intelligence institutions that are focused on external threats, rather than a criminal intelligence institution concerned with domestic issues such as petty crimes. However, there may be overlap between these spaces, and these interstitial spaces need effective policies to navigate such spaces.

For more on securitisation and language, see Buzan, Wæver, and De Wilde (1998); Herington (2012); Balzacq (2011); McDonald (2008).

Max Weber’s influential description of the state is

(a compulsory political association with continuous organization will be called a “state” if and in so far as its administrative staff successfully upholds a claim to the monopoly of the legitimate use of physical force in the enforcement of its order.

(Weber 2012, 154).

See Jessica Wolfendale and Michael Davis for more on these discussions (Wolfendale 2009; Davis 2005).

The “Five Eyes” countries are the US, Canada, UK, Australia, and New Zealand. Reference to the Five Eyes is a recognition of the special intelligence and national security sharing and cooperation that exists between these countries. For more on this, see Kerbaj (2022).

For more on the Five Eyes intelligence community, see Kerbaj (2022). See also the work by David Horner, John Blaxland, and Rhys Crawley for more on this (Horner 2014; Blaxland 2015; Blaxland and Crawley 2016).

This section draws from Seumas Miller’s “Research in Applied Ethics: Problems and Perspectives” (Miller 2008).

References


