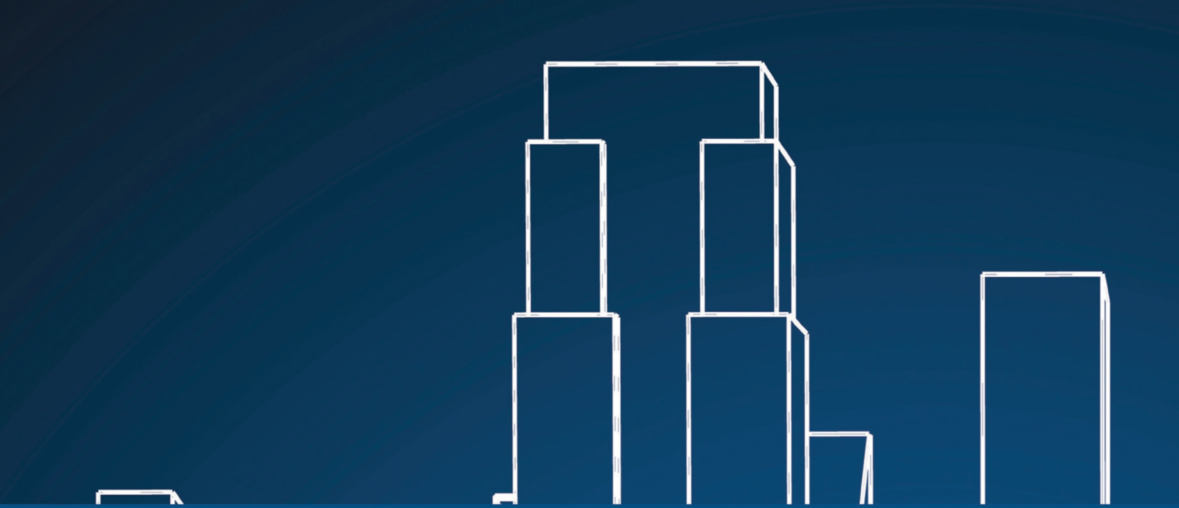

Studies in Intelligence

THE ETHICS OF NATIONAL SECURITY INTELLIGENCE INSTITUTIONS

THEORY AND APPLICATIONS

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

ROUTLEDGE

The Ethics of National Security Intelligence Institutions

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.

Studies in Intelligence
General Editors: Richard J. Aldrich, Claudia Hillebrand and Christopher Andrew

Intelligence Analysis in the Digital Age
Edited by Stig Stenslie, Lars Haugom, and Brigt H. Vaage

Conflict and Cooperation in Intelligence and Security Organisations
An Institutional Costs Approach
James Thomson

National Security Intelligence and Ethics
Edited by Seumas Miller, Mitt Regan, and Patrick F. Walsh

Intelligence Agencies, Technology and Knowledge Production
Data Processing and Information Transfer in Secret Services during the Cold War
Edited by Rüdiger Bergien, Debora Gerstenberger and Constantin Goschler

State-Private Networks and Intelligence Theory
From Cold War Liberalism to Neoconservatism
Tom Griffin

India's Intelligence Culture and Strategic Surprises
Spying for South Block
Dheeraj Paramesha Chaya

Big Data, Emerging Technologies and Intelligence
National Security Disrupted
Miah Hammond-Errey

The Ethics of National Security Intelligence Institutions
Theory and Applications
Adam Henschke, Seumas Miller, Andrew Alexandra, Patrick F. Walsh and Roger Bradbury

For more information about this series, please visit: www.routledge.com/Studies-in-Intelligence/book-series/SE0788

The Ethics of National Security Intelligence Institutions

Theory and Applications

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

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2024
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-367-61756-1 (hbk)
ISBN: 978-0-367-61760-8 (pbk)
ISBN: 978-1-003-10644-9 (ebk)

DOI: 10.4324/9781003106449

Typeset in Times New Roman
by Newgen Publishing UK

The Open Access version of this book was funded by The University of Oxford

Contents

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).[1] 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.

DOI: 10.4324/9781003106449-1

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[2] 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 democracies. 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 liberal 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 incommensurable, conceptions of the good affirmed by the members of existing democratic societies" (Rawls 1985, 225).[3] 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] requirement 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 policies 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 protecting the political leadership and assisting them to maintain control over the citizenry.[4] 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)[5] by Edward Snowden caused profound damage to the national security of the US (Clapper 2014).[6] 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[7] 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.

> [T]he 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.[8] 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;[9] 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,[10] 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 it 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.[12] 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,[13] 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,[15] 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 information 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

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.[16] 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[17]

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 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 stop there – 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, 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 Brunstetter 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] Privacy is discussed in more detail in Chapter 8.

[8] See, for instance, Philip Pettit's "The consequentialist can recognize rights" (Pettit 1988).

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

[10] See Seumas Miller's *Social Action* and *The Moral Foundations of Social Institutions* for deeper discussions of institutional ethics (Miller 2010, 2001).

[11] 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.

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

[13] 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).

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

[15] 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).

[16] 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).

[17] This section draws from Seumas Miller's "Research in Applied Ethics: Problems and Perspectives" (Miller 2008).

References

Andrew, Christopher. 2019. "The Secret World". In *The Secret World*. London: Penguin Random House.

Baumann, Marius. 2021. "No Fact of the Matter". *Metaphilosophy* 52(3–4): 466–478. https://doi.org/10.1111/meta.12498

Bellaby, Ross. 2014. *The Ethics of Intelligence*. Abingdon: Routledge. https://doi.org/10.4324/9780203383575

Best, Richard A. 2014. "Leadership of the U.S. Intelligence Community: From DCI to DNI". *International Journal of Intelligence and CounterIntelligence* 27(2): 253–333. doi:10.1080/08850607.2014.872533

Blaxland, J. 2015. *The Official History of ASIO: Volume II – The Protest Years 1963–1975*. Sydney: Allen & Unwin.

Blaxland, J. and R. Crawley. 2016. *The Official History of ASIO: Volume III – The Secret Cold War 1975–1989*. Sydney: Allen & Unwin.

Bok, Sissela. 1989. *Secrets: On the Ethics of Concealment and Revelation*. New York: Vintage Books.

Brennan, Geoffrey, Lina Eriksson, Robert E. Goodin, and Nicholas Southwood. 2013. *Explaining Norms*. Oxford: Oxford University Press.

Brunstetter, Daniel. 2016. "Jus Ad Vim: A Rejoinder to Helen Frowe". *Ethics & International Affairs* 30(1): 131–136.

Buzan, Barry, Ole Wæver, and Jaap De Wilde. 1998. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers.

Chang, Welton and Philip E. Tetlock. 2016. "Rethinking the Training of Intelligence Analysts". *Intelligence and National Security* 31(6): 903–920.

Church, Frank. 1976. *Foreign and Military Intelligence Book 2: Intelligence Activities and the Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate Together with Additional, Supplemental, and Seperate Views*. Washington DC: U.S. Government Printing Office.

Clapper, James. 2014. "Clapper: Snowden Caused 'Profound Damage'". *BBC News*, 29 January. www.bbc.com/news/av/world-us-canada-25954640

Coady, CAJ (Tony). 2011. "The Problem of Dirty Hands". The Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/archives/spr2014/entries/dirty-hands/

Dahl, Erik J. 2017. "Getting beyond Analysis by Anecdote: Improving Intelligence Analysis through the Use of Case Studies". *Intelligence and National Security* 32(5): 563–578. doi:10.1080/02684527.2017.1310967

Davis, Michael. 2005. "The Moral Justifiability of Torture and Other Cruel, Inhuman, or Degrading Treatment". *International Journal of Applied Philosophy* 19: 161–178.

Dean, John. 2007. *Broken Government: How Republican Rule Destroyed the Legislative, Executive, and Judicial Branches*. New York: Viking Press.

Dorril, Stephen. 2000. *MI6: Fifty Years of Special Operations*. Notting Hill: Fourth Estate.

Fabre, Cécile. 2022. *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence*. Oxford, New York: Oxford University Press.

Feldman, Fred. 1995. "Adjusting Utility for Justice: A Consequentialist Reply to the Objection from Justice". *Philosophy and Phenomenological Research* 55(3): 567–585. https://doi.org/10.2307/2108439

Ford, Shannon Brandt. 2013. "Jus Ad Vim and the Just Use of Lethal Force-Short-of-War". In *Routledge Handbook of Ethics and War: Just War in the 21st Century*, edited by Fritz Allhoff, Nicholas G. Evans, and Adam Henschke. 63–75. Abingdon: Routledge.

Frank, Aaron. 2017. "Computational Social Science and Intelligence Analysis". *Intelligence and National Security* 32(5): 579–599. doi:10.1080/02684527.2017.1310968

Gentry, John. A. 2015. Has the ODNI Improved US Intelligence Analysis? *International Journal of Intelligence and CounterIntelligence* 28(4): 637–661.

Gentry, John. A. 2016. "Managers of Analysts: The Other Half of Intelligence Analysis". *Intelligence and National Security* 31(2): 154–177. doi:10.1080/02684527.2014.961244

George, Roger Z. 2010. Beyond Analytic Tradecraft. *International Journal of Intelligence and CounterIntelligence* 23(2): 296–306. doi:10.1080/08850600903566124

George, Roger Z. and James B. Bruce. 2008. *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington DC: Georgetown University Press.

Glasius, Marlies. 2018. "What Authoritarianism Is … and Is Not: A Practice Perspective". *International Affairs* 94(3): 515–533. https://doi.org/10.1093/ia/iiy060

Greenwald, Glen. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

Hammond, Thomas H. 2010. "Intelligence Organizations and the Organization of Intelligence". *International Journal of Intelligence and CounterIntelligence* 23(4): 680–724. doi:10.1080/08850601003780987

Hayes, Rebecca M. and Kate Luther. 2018. *#Crime: Social Media, Crime, and the Criminal Legal System*. Dordrecht: Springer.

Henschke, Adam. 2021. "Ethics and National Security: A Case for Reasons in Decision-Making". In *The Palgrave Handbook of National Security*, edited by Michael Clarke, Adam Henschke, Matthew Sussex, and Tim Legrand. 73–92. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-53494-3

Herington, Jonathan. 2012. "The Concept of Security". In *Ethics and Security Aspects of Infectious Disease Control: Interdisciplinary Perspectives*, edited by Michael J. Selgelid and Christian Enemark, 7–25. Aldershot: Ashgate.

Heyman, Steven. 1991. "The First Duty of Government: Protection, Liberty and the Fourteenth Amendment". *Duke Law Journal* 41: 507–571.

Horner D. 2014. *The Official History of ASIO: Volume I – The Spy Catchers 1949–1963*. Sydney: Allen & Unwin.

Jacobsen, Annie. 2019. *Surprise, Kill, Vanish: The Secret History of CIA Paramilitary Armies, Operators, and Assassins*. New York: Hachette.

Johnson, Loch. 2017. *National Security Intelligence*. 2nd ed. Cambridge: Polity Press. https://books.google.com.au/books?hl=en&lr=&id=GkO9DgAAQBAJ&oi=fnd&pg=PT6&dq=National+Security+Intelligence+2nd+edition+&ots=lhnOWUBmPd&sig=dUQYmxhERtrcnx9AMWi3prWrago&redir_esc=y#v=onepage&q=National%20Security%20Intelligence%202nd%20edition&f=false

Jøsang, Auden. 2016. *Subjective Logic: A Formalism for Reasoning under Uncertainty*. Berlin: Springer.

Kahn, David. 2001. "An Historical Theory of Intelligence". *Intelligence and National Security* 16(3): 79–92. doi:10.1080/02684520412331306220

Kealey, Gregory 1992. "The Surveillance State: The Origins of Domestic Intelligence and Counter-Subversion in Canada, 1914–21". *Intelligence and National Security* 7(3): 179–210. doi:10.1080/02684529208432165

Kerbaj, Richard. 2022. *The Secret History of the Five Eyes: The Untold Story of the Shadowy International Spy Network, through Its Targets, Traitors and Spies*. London: Blink Publishing.

Lahneman, William J. and Rubén Arcos. 2017. "Experiencing the Art of Intelligence: Using Simulations/Gaming For Teaching Intelligence and Developing Analysis and Production Skills". *Intelligence and National Security* 32(7): 972–985.

Legrand, Tim. 2022. “National Security and Public Policy: Exceptionalism versus Accountability”. In *The Palgrave Handbook of National Security*, edited by Michael Clarke, Adam Henschke, Matthew Sussex, and Tim Legrand, 53–72. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-53494-3_3

Lester, Geneveive. 2016. *When Should State Secrets Stay Secret?* Cambridge: Cambridge University Press.

Lim, Kevjn. 2016. “Big Data and Strategic Intelligence”. *Intelligence and National Security* 31(4): 619–635.

Lowenthal, Mark M. 2017. *The Future of Intelligence*. Cambridge: Polity Press.

Marrin, Stephen. 2007. Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities. *Intelligence and National Security*, 22(6): 821–846. doi:10.1080/02684520701770634

Marrin, Stephen. 2011. *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. Abingdon: Routledge.

Marrin, Stephen. 2017. “Understanding and Improving Intelligence Analysis by Learning from Other Disciplines”. *Intelligence and National Security* 32(5): 539–547. doi:10.1080/02684527.2017.1310913

Mazzetti, Mark. 2014. *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth*. New York: Penguin.

McDonald, Matt. 2008. “Securitization and the Construction of Security”. *European Journal of International Relations* 14(4): 563–587. https://doi.org/10.1177/1354066108097553

Meisels, Tamar. 2008. “Torture and the Problem of Dirty Hands”. *Canadian Journal of Law & Jurisprudence* 21(1): 149–173. https://doi.org/10.1017/S0841820900004367

Miller, Seumas. 2001. *Social Action: A Teleological Account*. Cambridge, New York: Cambridge University Press.

Miller, Seumas. 2008. “Research in Applied Ethics: Problems and Perspectives”. *Philosophia*. www.springerlink.com/content/k25135l83v43260q/

Miller, Seumas. 2010. *The Moral Foundations of Social Institutions: A Philosophical Study*. Cambridge: Cambridge University Press.

NAS. 2019. *A Decadal Survey of the Social and Behavioural Science: A Research Agenda for Advancing Intelligence Analysis*. Washington DC: The National Academies Press.

Nielsen, Kai. 2007. “There Is No Dilemma of Dirty Hands”. In *Politics and Morality*, edited by Igor Primoratz, 20–37. London: Palgrave Macmillan. https://doi.org/10.1057/9780230625341_2

Omand, David and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Oxford: Oxford University Press.

Perry, David L. 2016. *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation*. Washington DC: Rowman & Littlefield.

Pettit, Philip. 1988. “The Consequentialist Can Recognise Rights”. *The Philosophical Quarterly* 38(150): 42–55.

Pherson, Randolph H. and Richards J. Heuer Jr. 2020. *Structured Analytic Techniques for Intelligence Analysis*. Washington DC: CQ Press.

Phythian, Mark. 2017. “Intelligence Analysis and Social Science Methods: Exploring the Potential for and Possible Limits of Mutual Learning”. *Intelligence and National Security* 32(5): 600–612.

Pogge, Thomas W. 1992. “Cosmopolitanism and Sovereignty”. *Ethics* 103(1): 48–75.

Quinlan, Michael. 2007. “Just Intelligence: Prolegomena to an Ethical Theory”. *Intelligence and National Security* 22(1): 1–13. https://doi.org/10.1080/02684520701200715

Ratcliffe, Jerry. 2008. *Intelligence-Led Policing*. Devon: Willan Publishing.

Rawls, John. 1985. "Justice As Fairness: Political Not Metaphysical". *Philosophy and Public Affairs* 14(3): 223–251.

Rawls, John. 1999. *A Theory of Justice*. Cambridge: Harvard University of Press.

Richey, Melonie K. and Mathias Binz. 2015. "Open Source Collection Methods for Identifying Radical Extremists Using Social Media". *International Journal of Intelligence and CounterIntelligence* 28(2): 347–364. doi: 10.1080/08850607.2014.962374

Rothstein, Hy and Barton Whaley. 2013. *The Art and Science of Military Deception*. Norwood: Artech House. http://site.ebrary.com/id/11069368

Rynard, Paul and David Shugarman, eds. 1999. *Cruelty and Deception: The Controversy over Dirty Hands in Politics*. Peterborough: Broadview.

Scott, Len and R. Gerald Hughes. 2006. "Intelligence, Crises and Security: Lessons from History". *Intelligence and National Security* 21(5): 653–674.

Shelton, Allison M. 2014. "Teaching Analysis: Simulation Strategies in the Intelligence Studies Classroom". *Intelligence and National Security* 29(2): 262–281.

Siddique, Haroon. 2010. "Press Freedom Group Joins Condemnation of WikiLeaks' War Logs". *The Guardian*, 13 August 2010. www.theguardian.com/media/2010/aug/13/wikileaks-reporters-without-borders

Skinner, Quentin. 2009. "A Genealogy of the Modern State". *Proceedings of the British Academy* 162(325): 34.

Stottlemyre, Steven A. 2015. "HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence". *International Journal of Intelligence and CounterIntelligence* 28(3): 578–589. doi: 10.1080/08850607.2015.992760

Sussex, Matthew. 2022. "Understanding National Security: The Promises and Pitfalls of International Relations Theory". In *The Palgrave Handbook of National Security*, edited by Michael Clarke, Adam Henschke, Matthew Sussex, and Tim Legrand, 23–52. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-53494-3_2

Walsh, Patrick F. 2011. *Intelligence and Intelligence Analysis*. Abingdon: Routledge.

Walsh, Patrick F. 2020. *Intelligence Leadership and Governance: Building Effective Intelligence Communities in the 21st Century*. Abingdon: Routledge.

Walzer, Michael. 1973. "Political Action: The Problem of Dirty Hands". *Philosophy and Public Affairs* 2(2): 160–180.

Wark, Wesley. 1993. "Introducing the Study of Espionage: Past, Present, Future". *Intelligence and National Security* 8(3): 1–13.

Warner, Michael. 2002. "Wanted: A Definition of 'Intelligence'". *Studies in Intelligence* 46(3). www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html

Warner, Michael. 2014. *The Rise and Fall of Intelligence: An International Security History*. Washington DC: Georgetown University Press.

Weber, Max. 2012. *The Theory of Social and Economic Organization*. Connecticut: Martino Fine Books.

Weiner, Tim. 2008. *Legacy of Ashes: The History of the CIA*. New York: Anchor.

Weiner, Tim. 2012. *Enemies: A History of the FBI*. New York: Random House Incorporated.

Wijze, Stephen de. 2013. "Punishing 'Dirty Hands' – Three Justifications". *Ethical Theory and Moral Practice* 16(4): 879–897. https://doi.org/10.1007/s10677-012-9396-x

Wolfendale, J. 2009. "The Myth of 'Torture Lite'". *Ethics & International Affairs* 23: 47–61. https://doi.org/10.1111/j.1747-7093.2009.00189.x

Wolfers, Arnold. 1952. "'National Security' as an Ambiguous Symbol". *Political Science Quarterly* 67(4): 481–502. https://doi.org/10.2307/2145138

Part I

Concepts and Principles for Just Intelligence Institutions

In the next three chapters, we present and outline the key concepts that underpin and explain our just intelligence theory (JIT). Here, we outline the idea of intelligence as institutionalised joint epistemic activity. Further, we clarify intelligence as competitive, indeed adversarial, epistemic activity, and contain intelligence by reference to the collective good of national security. This gives the rationale for how and why we use intelligence in the particular way that we do and forms the foundation for our institutional approach to national security intelligence.

Following this, we look to ideas of moral exceptionalism that are found in the just war tradition (JWT) that motivate a number of approaches to the JIT (Bellaby 2014; Miller, Regan and Walsh 2021). In Chapter 3 we show how the *jus ad bellum* criteria need to be adapted such that they can be useful in the national security intelligence context. Importantly, our approach highlights what role intelligence institutions play in relation to just intelligence principles. Chapter 4 closes Part I by looking at the ways that just intelligence practices ought to occur. Again, we initially rely on three principles: discrimination, necessity and proportionality. We adjust these three principles in a manner that enables their application to intelligence practice.

DOI: 10.4324/9781003106449-2

2 On National Security Intelligence

Concepts and Contexts

Seumas Miller

National security intelligence activity is a relatively specialised form of institutional activity. Moreover, this activity is paradigmatically epistemic (from the Greek word, “episteme”, meaning knowledge) or knowledge-focused activity; it is an activity that has as its end or purpose the collection, analysis, and dissemination of discrete information, extended descriptions of events and threats, numerical, visual, and other non-linguistic data, and so on.

Naturally, political, military, police, and intelligence personnel read newspapers, watch TV, and learn about current affairs from their friends; indeed, as a consequence, they may be well-informed about current affairs. However, by engaging in such epistemic activity these personnel are not, thereby, necessarily engaging in national security intelligence activity, even if the current affairs in question include military and other national security matters. For one thing, in becoming well-informed about current affairs in this manner, they are not engaging in essentially adversarial activity; they are not seeking information that the newspaper or TV journalists (let alone their friends) are trying to prevent them from attaining. By contrast, intelligence officers in national security organisations seek to access the secrets of hostile nation states and non-state actors while preventing these adversaries from accessing their own secrets. For another thing, such informal, current affairs-oriented, epistemic activity is not necessarily undertaken jointly with colleagues, under instruction from their political, military, police, or intelligence superiors, and in the service of their institutional role; it is not institutional (epistemic) activity undertaken qua institutional role occupant.

In short, national security intelligence activity is in essence institutionalised, joint epistemic activity that is focused on matters of national security and undertaken against state or organised non-state adversaries by intelligence officers acting qua intelligence officers. As such, national security intelligence activity stands in contrast with informal epistemic activity undertaken by an individual acting of his or her own accord who is seeking to be well-informed on current affairs.

While national security intelligence activity is adversarial activity, it is not kinetic adversarial activity as is, for instance, much of the activity of combatants, e.g., when they shoot enemy combatants, or of police officers, e.g., when they

DOI: 10.4324/9781003106449-3

restrain suspects. Epistemic activity, even the acquisition of secret knowledge from an adversary trying to keep it secret, is importantly different from kinetic activity. That said, epistemic activity often relies on kinetic activity, e.g., knowledge of an enemy's position may rely on reconnaissance flights, and kinetic activity relies on epistemic activity, e.g., combatants need to *know* who to shoot at. Moreover, the distinction between the epistemic and the kinetic is not always clear-cut. For instance, some national security "intelligence" activities, such as so-called psyops (see Chapter 7), are seemingly in part epistemic and in part kinetic.

Philosophical analysis of fundamental concepts and theories used in national security intelligence activity has been minimal and, where it exists, largely limited to ethical issues, as in the application of the constitutive principles of Just War Theory to secret intelligence. On the other hand, in recent years the definition of intelligence in national security (including the military) has achieved a great deal of attention, albeit not by philosophers (Breakspear 2013; Marrin 2018; Gill 2018; Stout and Warner 2018; Barnea 2020). Yet the definition of intelligence remains unresolved. Moreover, a complete and correct one will not be offered here. Rather in this chapter an initial characterisation of national security intelligence is offered; that is, in the light of the national security intelligence literature, a list of the main features of national security intelligence are described. Moreover, the concept of intelligence is located in relation to cognate concepts, notably knowledge. It is suggested that ideally intelligence is knowledge, as Sherman Kent argued many years ago in his influential work (Kent 2015, chap. 1), although we need to keep in mind (as Kent did) the differences between, on the one hand, knowledge of existing conditions and events that have already taken place and, on the other hand, predictions, and between descriptive knowledge and evaluations, as well as various other distinctions. Further, according to the characterisation offered here, intelligence is a teleological concept (i.e. defined in terms of its end or purpose) and (relatedly) institutionally relative (i.e. relative to some institution). Accordingly, military intelligence is intelligence that serves the ends or purposes of military institutions; as such, it belongs to a different category than, say, police intelligence. In addition to this initial characterisation of national security intelligence, this chapter provides a philosophical analysis of the notion of knowledge which, it is argued, lies at the heart of national security intelligence activity. This notion of knowledge is then applied to national security intelligence activity, with the understanding that knowledge is a state or product that results from such activity (again, as Kent made clear (Kent 2015, chap. 9). In the third section (Joint Epistemic Action and Epistemic Institutions), the notion of joint epistemic action (and some related notions) is introduced and applied to national security collection, analysis, and dissemination. National security intelligence activity is cooperative or joint in nature; indeed, as mentioned earlier, it is a form of institutional activity and intelligence agencies are a species of epistemic institution. Given this, important questions arise about how intelligence officers could be morally responsible for the intelligence that the institutions that they work for provide to their political masters. Here, the notion of collective moral responsibility understood as joint moral responsibility is salient.

Characterising Intelligence

There are a number of general points, some of which are fairly obvious and oft stated and which can serve to characterise, if not define, intelligence as a phenomenon (Miller 2022a). Note that we need to keep in mind the threefold distinction between intelligence as the informational, cognitive, or epistemic product of intelligence activity, as opposed to the activity itself and the agent (whether an individual or organisation (Miller 2022a, chap. 5) of the activity[1].

First, as mentioned earlier, the contexts in which such intelligence is collected and analysed are adversarial. The adversaries are institutions, such as the Central Intelligence Agency (CIA) and MI6, often acting, at least in the modern world, in the service of nation states. Such national security intelligence institutions seek to access the secrets of their adversaries while preventing their adversaries from accessing their own secrets. Moreover, they engage in various forms of deception and disinformation against these adversaries. However, ultimately, they are acting, at least normatively speaking, in the service of the moral rights (specifically, *joint rights*) (Miller 2010, 66–76; Miller 2016, chap. 3) of their citizens to a collective good (Miller 2010, 66–76), namely, security and, more specifically, in the case of the intelligence agencies of interest to us, national security. As such, national security intelligence activity is, or ought to be, ultimately directed to the realisation of a collective good. That is, it is institutionalised joint epistemic activity directed to a collective end, which is a collective good (discussed later). Moreover, intelligence activity involves, or at least is implicated in, the exercise, or attempted exercise, of power (Miller 2017, chap. 2; Phythian 2013), influence, and the like, albeit in a normative context (by virtue of citizens' joint moral right to the collective good of security, which good ought to be the collective end of said activity). Thus, the military intelligence officers of nation state A at war with nation state B are collecting and analysing intelligence on the enemy forces of B in order to facilitate their defeat on the battleground.

Second, given these adversarial contexts, inevitably secrecy is of the utmost importance (Bok 1982); it is critical that information about police or military operations, methods, tactics, strategies, and goals be kept secret for them to successfully realise their institutional purposes (and, thereby, discharge their moral obligations to the citizenry to ensure their security). This is, of course, not to deny that there is typically much that is common knowledge (Smith 1982) between adversaries in these contexts. For instance, each side knows that the other side has access to knowledge that is in the public sphere.

Third, intelligence is in the service of kinetic activity, such as bombing installations or waging war, and, therefore, needs to be actionable by the relevant decision-makers (e.g. police leaders, military commanders, and politicians). Accordingly, intelligence officers need to be responsive to decision-makers but also, if their intelligence is ultimately to be beneficial, somewhat independent of decision-makers so that it is evidence-based and not vitiated by political interference. Intelligence officers may even, at times, need to "speak the truth to power" rather than tell their superiors what they want to hear. However, many intelligence agencies focused on the epistemic activity of national security intelligence are also engaged in kinetic activity (Stout and Warner 2018), such as sabotage (including by way of cyberattacks, as in the case of the Stuxnet virus), interference in elections, funding dissidents, cross-border kidnappings, arming secessionists, and assassinations.

Fourth, some distinction needs to be maintained between intelligence as "raw data" and intelligence as the epistemic product of some process of analysis and evaluation according to different criteria, including the likelihood that it is true, its importance (assuming that it is true), and (relatedly) the reliability of its source. Hence, the distinction between collectors and analysts.

Fifth, in the light of the above-mentioned distinctions between collectors, analysts, and decision-makers operating in an adversarial context, it makes sense to introduce *some* notion of an intelligence cycle (Treverton 2001; Phythian 2013) involving not only a one-way circular process in which intelligence is directed to be collected, analysed, and acted on by decision-makers who in turn direct further intelligence to be collected – doing so in part because of the actions of adversaries (including in response to the actions consequent on the decisions of one's own decision-makers). The process is not simply circular but also (at least ideally) two-way interactive at each of the points in the "circle", as is the case between intelligence officers and decision-makers.

Sixth, intelligence can be categorised in various ways according to its source, mode of communication, content, and potential use. For instance, regarding its potential use, intelligence can be categorised as strategic, tactical, or operational. National security intelligence activity is institutional, whether it be strategic, tactical, or operational activity. Nevertheless, one can distinguish a number of institutional levels at which it is conducted. Tactical and operational intelligence activity might be regarded as activity undertaken at the micro-institutional level, whereas matters such as the purpose, structure, resources, and culture of an intelligence agency, and its institutional relationships to, for instance, government or the military forces it serves, might be regarded as activity conducted at the macro-institutional level. However, there might need to be a further distinction between the activities conducted at these two levels and activities such as the design of a national intelligence strategy and the establishment of bulk databases by security agencies for national security purposes. Accordingly, this intermediate level might be referred to as the mezzo institutional level.

Intelligence can also be categorised (inter alia, according to its source and mode of existence) as human intelligence (HUMINT), signals intelligence (SIGINT), social media intelligence (SOCMINT), open source intelligence (OSINT), imagery intelligence (IMINT), and geospatial intelligence (GEOINT). In recent times, various forms of electronic intelligence, notably metadata (phone or email data other than content, such as the phone number of the caller and the receiver, and the time and duration of call), have emerged as of great importance in the context of end-to-end encryption impeding access to content. Moreover, OSINT and SOCMINT are increasingly important intelligence sources. Thus, intelligence agencies have increased their uses of data mining and analytics technologies, notably machine learning techniques and computer vision algorithms.

The content of intelligence is multifarious. Content can include discrete items of information, such as the name of a foreign agent, or larger fragments of epistemic material, such as a list of associates or the strategic plan of the enemy. The content might be a fact, a formula, a map, an image, an opinion, an ideological claim, an expressed emotion, a video clip, or a narrative about a sequence of events. Importantly, intelligence content is holistic. Any particular item of intelligence only has significance in the context of a larger structure of intelligence content. Thus, the movement of troops within a nation-states own borders might constitute a national security problem for another nation-state or it might not depending on whether the state moving its troops was regarded as belligerent by virtue of its past actions, the troops were well armed, battle-prepared and large in number, and were moved close to the border with the other state.

Seventh, while the raw data collected by intelligence officers (whether human intelligence or electronic intelligence) consist of linguistic (spoken and written) and non-linguistic materials such as images, videos, maps, diagrams, etc., once analysed and disseminated to decision-makers, it exists in large part in a form such that it is (i) expressed or expressible in a language and, therefore, communicable; (ii) epistemic (or knowledge focused) and, as such, capable of being true or false, correct or incorrect, probable or improbable, evidence-based or not; (iii) stored somewhere, such as in an investigator's notebook or in a security organisation's databank (Miller and Gordon 2014).

Eighth, information and intelligence are closely related concepts. Both information and intelligence, at least in many of their forms, can be thought of as statements stored in some information system. Moreover, both information and intelligence, as we will use the terms in this article, are epistemically evaluable, i.e., either true or false (albeit, perhaps unverifiable), correct or incorrect, accurate or inaccurate, or probable or improbable. However, neither information nor intelligence is *necessarily* true (or necessarily correct, accurate, or probable). This is, of course, true of disinformation masquerading as bona fide intelligence and also of much "raw" intelligence. But it is also true of intelligence that has been subjected to analysis and is well-evidenced. Finally, neither information nor intelligence necessarily has a good, let alone decisive, justification. Accordingly, neither information nor intelligence is necessarily knowledge. On the other hand, a piece of information or of intelligence might be true and might have a good and decisive justification; *some* information and *some* intelligence is knowledge.

Ninth, notwithstanding that information and intelligence are closely related concepts, they are not the same thing; specifically, intelligence is information, but information is not necessarily intelligence. For instance, the information from the surgeon that my ankle is broken is not necessarily intelligence, given the irrelevance, let us assume, of my medical condition to the activities of intelligence agencies. On the other hand, this information might be intelligence if, for instance, I am a fugitive whose whereabouts is being sought by an intelligence agency.

Tenth, as mentioned earlier, intelligence, whether it be criminal intelligence, market intelligence, or military intelligence, is defined relative to some institutional purpose or function (Miller 2021). Accordingly, we should accept a teleological (purpose-based) or functional account of intelligence; intelligence is, by definition, information or data (expressible as a statement or, more likely, structured set of statements) that are acquired for various institutional purposes. Moreover, intelligence is institutionally relative in that it is relative to the purposes of some institution. So military intelligence is a different category of intelligence from criminal intelligence because military institutions have a somewhat different institutional purpose than police organisations.

If the primary purpose or function of an institution is knowledge (understood broadly in the sense of evidence-based understanding), then the institution is an *epistemic* institution. Thus, universities, news organisations, and, arguably, intelligence agencies are epistemic institutions.

What of national security intelligence, the collection, analysis, and dissemination of which is, let us assume, the primary purpose of many intelligence agencies (Miller 2021)? National security intelligence is sometimes collected and analysed by military organisations, sometimes by police organisations, but paradigmatically by intelligence agencies whose institutional purpose is internal and/or external national security, e.g., the CIA, NSA, GCHQ, MI5, MI6, Mossad, RAW, ASIO, etc. Accordingly, what makes information or other data collected by these agencies national security intelligence is that these agencies collect and analyse this information in the service of national security – national security being their primary institutional purpose. This immediately raises the vexed question as to what national security is; after all, the content of the term "national security" is notoriously ill-defined, indeterminate, shifting, open-ended, and contestable. For instance, the US National Intelligence Strategy has as one of its purposes to promote liberal democracy. Importantly, national security should not simply be understood as national interest since the latter notion is very permissive and could license all manner of individual and collective rights violations. For instance, it might be in the national interest of a nation state to increase its territory by invading a neighbouring nation state. Perhaps the Russian invasion of Ukraine might ultimately be thought to have been in Russia's national interest, assuming that Russia ends up acquiring not only Crimea but, say, also the Donbas industrial region of eastern Ukraine. Again, it might be thought to be in the national interest of some nation state to enslave a population, or to otherwise engage in widespread, serious rights' violations, to increase its own wealth. Historically, the slave trade was thought to be an economic imperative and, therefore, in the interest of, for instance, the US during the 18th century. The Chinese incarceration of hundreds of thousands of Uighurs in oil and resources-rich Xinjiang might be thought by members of the Chinese communist party to be in the national interest. However, let us assume that national security intelligence is intelligence pertaining to serious internal or external (direct or indirect) threats to the nation state itself, or to one of its fundamental political, military, criminal justice or economic institutions, and that these threats might emanate from state or non-state actors, such as terrorist groups. So national security intelligence includes military intelligence, but also some criminal intelligence and economic intelligence, since the latter may have national security implications. Consider, for instance, intelligence on drug cartels destabilising governments or on fighter aircraft being built by private companies. Note also that while national security threats (as opposed to safety threats) are necessarily posed by state or non-state (and, therefore, human) actors, the conditions under which these security threats emerge might have arisen as a result of other, including non-human, sources, such as (at least in some cases) pandemics, famines, or water shortages consequent on climate change.

Knowledge and the Aims of Intelligence Collection and Analysis

Intelligence is, as we have seen, an epistemic notion and, *ideally* (but not always or even typically), it consists of knowledge understood as evidence-based understanding; that is, it is true or correct or accurate or probably true, or some such. Accordingly, intelligence officers aim at, or ought to aim at, knowledge (discussed later) and possess associated traits of objectivity, a capacity for judgement in relation to what is important and what is not, and relevant expertise (including jointly held expertise (Miller 2019)), such as a specific language, but also be able to work to a deadline (Kent 2015).

Consistent with the claim that national security intelligence activity is ultimately undertaken in the service of kinetic action undertaken by other agencies, we suggest, nevertheless, that the fundamental (proximate) *point* of intelligence collection and analysis is knowledge (Miller 2022a, 2022b; Miller and Gordon 2014; Pili 2019; Miller 2021) and, more specifically, knowledge expressed in statements – since such knowledge needs to be disseminated to others, notably decision-makers, and not "left in the head" of the intelligence officer (let alone in the database of the intelligence agency). In short, intelligence officers *ought* to have the acquisition of knowledge as their principal aim or end. Accordingly, a necessary condition for being a good intelligence officer is that one aims at knowledge. So an otherwise highly skilled intelligence officer who did not have knowledge as his *overriding* aim, but rather a desire to, for instance, please her political masters, would not be a good intelligence officer. For example, the highly skilled officer who, nevertheless, ignores counter-evidence when forced to choose between getting to the truth of the matter (and, thereby, coming to have knowledge) and providing confirmation of a view of her political masters, is not a good intelligence officer.

We saw earlier that intelligence collection, analysis, and dissemination are the means to a further end, namely, kinetic action. Nevertheless, the acquisition of knowledge is *also* an end-in-itself for intelligence officers, notwithstanding the further requirement that the truths acquired be actionable. For the activities of intelligence collection and analysis are not related to knowledge merely as means to end, but also conceptually. Truth is not an external contingently connected end which some intelligence activities might be directed towards if the intelligence officers happened to have an interest in truth, rather than, say, an interest in falsity. Rather, truth is internally connected to intelligence activity. Thus, aiming at truth is aiming at truth as an end-in-itself. This is consistent with also aiming at truth as a means to some other further end, such as winning a war. In other words, supposed intelligence activity which *only* aimed at truth as a means to some other end would not be genuine intelligence activity or would be defective qua intelligence activity, since for such a pseudo-intelligence officer truth would not be internal to his or her activity. Such a pseudo-intelligence officers would abandon truth-aiming if, for example, it turns out that the best means to the officer's end is not, after all, truth, but rather falsity. Obviously, such pseudo-intelligence officers would be extremely dangerous since their intelligence would be very unreliable. For they are not simply officers who aim at (and more often than not acquire) the truth but who, nevertheless, often present false reports to their political masters (or other "clients"), knowing them to be false (or, more likely, to be somewhat misleading because unpalatable truths are omitted or downplayed). Rather, these pseudo-intelligence officers do not aim at truth in the first place. That is, having little interest in the truth, they do not seek the truth and, as a result, do not themselves acquire knowledge; therefore, they do not have knowledge to pass on to their political masters. Of course, in the real world such pseudo-intelligence officers are unlikely to exist in a pure form. However, in an intelligence agency lacking independence and in which intelligence officers' desire to please, or, more likely, a desire not to antagonise, their political masters (as in the case of many Soviet intelligence officers who served under Stalin), the commitment to the truth might well weaken, especially when one considers the inherent difficulties in acquiring accurate and significant national security intelligence from adversaries determined to maintain information security. As a consequence, such intelligence officers might initially have the practice of reporting what they know to be false or misleading on some occasions when it is politically or otherwise expedient to do so. However, over time, they might end up largely abandoning the practice of evidence-based truth-seeking in favour of selective data collection and skewed analyses in the service of personal, political, or other non-epistemic agendas, that is, they might end up becoming something akin to pseudo-intelligence officers.

There is an important institutional implication of the above discussion. As we have just seen, whereas the primary institutional purpose of national security intelligence agencies is essentially epistemic, the realisation of this epistemic purpose serves a larger national security purpose only realisable by the kinetic activity of other institutions, such as the military. Accordingly, there is an institutional division of labour; the intelligence agency provides knowledge (or weaker epistemic goods) to the decision-makers, such as politicians or military or police leaders, who in turn act (or refrain from acting) on that knowledge. In order for this institutional division of labour to function successfully, it is critical that the intelligence provided is reliable, trustworthy, and, therefore, that the epistemic activity of the intelligence agencies is not unduly influenced or otherwise undermined by the institutions which they serve, notably by their political masters. Accordingly, consistent with an appropriate level of responsiveness to their political masters' national security intelligence demands, it is necessary that intelligence officers' professional commitment to the epistemic purposes of their intelligence agencies override any personal loyalty they might have to their political masters; indeed, on occasion, they may need to speak unpalatable truths to power. However, it is also necessary that intelligence officers have an overriding professional commitment to the epistemic purposes of their intelligence agencies rather than seeking to realise the ultimate national security outcomes that might or might not flow from the decisions of the politicians, military leaders, and other decision-makers who act on their intelligence. It is important that intelligence officers do not engage in institutional overreach.

Thus far, we have been using an unanalysed notion of knowledge and a somewhat loose one. In what follows, we need to keep in mind a threefold distinction between intelligence, knowledge, and certainty. Here we need to distinguish between knowledge and so-called intelligence, on the one hand, and knowledge and certainty, on the other.

Knowledge is to be distinguished from intelligence in the sense of unanalysed "information" – including unsubstantiated reports, hearsay, and the like – that is collected by intelligence officers. Intelligence in this sense is more likely to be true than, for instance, blatant lies or ideology. However, intelligence is often unconfirmed; some intelligence is at best *prima facie* true. Intelligence may have some evidential backing, but even if it does, this backing might not be sufficiently strong to warrant it being believed..

It is also important to distinguish between knowledge and certainty. If someone has certainty, then s/he cannot be mistaken. However, there is very little that intelligence officers could not be mistaken about.

Let us now return to the matter of defining the notion of knowledge (Moser 1989). By definition, knowledge is at least true belief (or accurate structure of beliefs or the like) and, given that, as we saw earlier, the knowledge in question is expressed in a language, then knowledge is true, *stated* belief. If knowledge is at least true belief, then an existing state of affairs, e.g., a dead body, is not a matter of knowledge until it, so to speak, "enters the head" of someone and becomes the content of a belief. However, in order for belief (either a single belief or a structure of beliefs) to be knowledge, it must be *true* (or accurate or the like); false beliefs are not knowledge.

Truth is attained by the intelligence officer when he or she has a true belief that, for instance, Kim Philby is spying for the Soviets. However, truth in the sense of true belief is not sufficient. The intelligence officers need to be able to justify their true beliefs by recourse to evidence. Moreover, this justification must consist in reasons, namely, good and (hopefully) decisive reasons; a bad reason is an unacceptable justification and a good reason is not necessarily sufficient to warrant true belief (there might be, for example, a countervailing good reason not to hold that belief). Hopefully, there will be a set of good reasons which cumulatively should constitute a decisive reason for the investigator's true belief. However, if this is not the case, then decisions will need to be made on the basis of probabilities or (in the case of unacceptable outcomes) even possibilities.

Accordingly, intelligence officers ought to have as a goal *justified* true beliefs. But justified true beliefs are knowledge. So knowledge is the goal of the officer, specifically, knowledge expressed in statements.

But why does the intelligence officer need a rational justification? Why is not the truth (true belief or, at least sincerely held true statement) sufficient? First, speaking generally, beliefs need to be grounded in reasons if they are to be rationally held beliefs, as opposed to irrational or non-rational ones. Here reasons are the means by which we reliably determine which beliefs are true and which are false (and, therefore, which structures of belief are accurate or inaccurate, probable or improbable, and so on). An irrational person might accidentally possess true beliefs. But, as Plato famously argued centuries ago in the *Theaetetus* and elsewhere, accidental true beliefs do not constitute knowledge. For example, taking a hallucinogenic drug might cause you to believe that Y is a terrorist, and Y might in fact be a terrorist. But your true belief that Y is a terrorist would not thereby constitute knowledge. This is because hallucinogenic drugs are not a reliable method (we are assuming) for arriving at the truth.

Indeed, not only should your true belief be based on the use of a reliable method, but you should also be competent in the use of that method on pain of it being mere luck that you arrived at the truth using that method (Sosa 2015). Consider a novice intelligence officer who uses a method that is reliable when used by those competent in its application but who is himself incompetent in the use of the method, as might be so in an instance of the use of a complex code to decipher the enemy's communications. Because the novice officer in question is incompetent under normal circumstances, he would not succeed in correctly deciphering the messages; rather his efforts would simply generate a meaningless string of letters. However, as a result of pure luck, on a particular occasion his incompetent use of the code delivers the same result as a competent use of the code would have delivered. Accordingly, while his misuse of the method delivered the correct result on this one occasion by sheer luck, arguably he does not know that this result is correct. Thus if his misuse of the method was discovered by the senior analyst, his result would not be believed.

The second reason a rational justification is required is because, institutionally speaking, the intelligence official needs to be able to justify his or her beliefs, his or her statements, to others and do so by means of the provision of good and decisive reasons. To the extent that intelligence officers know how to use reliable methods, in fact use these methods and, thereby, come to acquire true beliefs, then intelligence agencies embody a general principle of epistemic rationality.

Thus far, we have largely been concerned with intelligence activity as, at least implicitly, the epistemic activity of individuals, as indeed much of it is. However, it is also a collective epistemic undertaking; it is a joint epistemic activity.

Joint Epistemic Action and Epistemic Institutions

National security intelligence activity is cooperative or joint in nature; indeed, it is a form of institutionalised epistemic activity.[2] As such, it is a species of joint *epistemic* activity, where joint *activity* is understood as a complex structure consisting in large part of joint epistemic *action*. Note that joint epistemic activity (unlike joint epistemic action) typically consists in part in individual *non-joint* action that is not constitutive of a joint epistemic action (even though such individual action is ex hypothesis constitutive in part of the joint activity). When James Bond performs the single individual act of stealing some secrets from a KGB agent, he is not engaged in joint action, notwithstanding that his single action is constitutive of the joint *activity* of MI6, supposing he is acting qua MI6 spy.

The activities of other security agencies are also forms of cooperative, institutional activity, and, therefore, they are also species of joint activity and, therefore, of joint action; however, they are predominantly species of joint *kinetic* activity. Accordingly, we can distinguish epistemic institutions, such as universities and national security intelligence agencies, from non-epistemic (especially kinetic) institutions, such as police and military institutions.

As suggested earlier, and argued in detail elsewhere (Miller 2010; Miller 2016, chap. 3), security agencies are, or ought to be, established to realise collective ends, which are collective goods, namely security (to which the relevant citizens have joint rights), and inevitably do so via institutionalised joint activity (specifically, multi-layered structures of joint action (Miller 2001, 173–179; Miller 2010, 47–52). Intelligence agencies are no exception. However, as already stated, the characteristic joint activity which they perform is essentially joint *epistemic* activity (Miller 2018; Pili 2019) (at least, insofar as the intelligence agencies in question do not engage in so-called covert action, such as sabotage, targeted killing, and other kinetic activity). Importantly, joint epistemic action, as is the case with epistemic action more generally, is a necessary condition for kinetic action but not a sufficient one. Rather, roughly speaking, it stands to kinetic action as beliefs stand to action (other than to *mental* actions, such as judgements), more generally. That is, it is mediated by affective and, especially, conative (as opposed to cognitive) states, such as intentions, ends, and the like. Hence, an intelligence report stating that Saddam Hussein is building weapons of mass destruction (WMDs) does not, in and of itself, cause a kinetic response, such as war; rather the kinetic response depends on a decision to act (or not act), based in part on the intelligence report but also in part on some goal or end, such as to prevent Hussein from possessing an arsenal of WMDs. In short, knowledge does not, in and of itself, generate kinetic action.

This indirect relationship between knowledge and action and, therefore, between epistemic, including joint epistemic, action and kinetic action (and, in turn, the outcome of kinetic action) has important implications for our understanding of responsibility and, specifically, moral responsibility. Roughly speaking, intelligence officers have *some degree* of moral responsibility for the actions of their political masters, given that the latter make morally significant decisions based, in part, on intelligence reports. However, their political masters are, nevertheless, morally responsible for their own actions (and the reasonably foreseeable outcomes of their actions), notwithstanding their reliance on intelligence reports. Thus, President Bush and Prime Minister Blair were morally responsible for waging war against Saddam Hussein and, therefore, for the disastrous outcomes of that conflict. However, insofar as intelligence officers provided them with incorrect intelligence, they must also bear some responsibility. On the other hand, the latter responsibility of intelligence officers is diminished to the extent that the intelligence they provided, namely, that there was insufficient evidence that Hussein was developing WMDs, was ignored.

The notion of joint action is a familiar one in the philosophical literature (Miller 1992; Miller 2001, chap. 2; Bratman 1993). An example of a joint action is two people lifting a table. Moreover, we can distinguish between epistemic actions and non-epistemic, notably kinetic actions. Roughly speaking, epistemic actions are actions directed to an epistemic end, such as knowledge. An example of an epistemic action is an intelligence officer deciphering a coded message. Elsewhere we have argued that these two notions can be brought together to yield the notion of joint epistemic action, and a relational individualist analysis of joint epistemic actions has been provided (Miller 2015, 2018). An example of a joint epistemic action is a team of intelligence officers jointly breaking a code.

Joint epistemic actions involve two or more persons jointly pursuing a common or collective goal or end (Fallis 2007; Miller 2008, 2015, 2018; Pili 2019). Consider, for example, members of a counterterrorist national security task force identifying, surveilling, and, potentially, arresting suspected terrorists. Each participant involved in a particular operation intentionally does his or her epistemic part. For instance, an intelligence analyst identifies person X as a potential terrorist and a surveillance team conducts surveillance on X. On the basis of the information gained, the commander decides to use an undercover officer to establish a relationship with X. Finally, on the basis of evidence gained by the undercover officer, X is arrested by uniformed police officers (since, let us assume, the members of the national security task force in question do not have the legal power to effect arrests). Moreover, there is interdependence among the epistemic actions of each participant; each believes (or at least hopes) that the others will do their parts and, indeed, relies on at least some of the others to do their part if the shared epistemic end is to be realised. Moreover, there is interdependence between the epistemic end (to determine whether or not X is a terrorist) and the kinetic end (to arrest X, if he proves to be a terrorist). Further, there is typically interdependence with respect to the possession of the epistemic end. Since no single participant could realise the ultimate end on their own (or could only do so with difficulty), each only has the end if the others do. Finally, it is a matter of mutual true belief among participants that each has the (interdependent) end and beliefs in question. So each has these true beliefs, believes the others have them and that they believe he or she has them, and so on (Smith 1982).

There are a number of points to notice about joint epistemic action on this account. First, while each participant has beliefs with respect to the actions of other participants, no participant *necessarily* has any intentions with respect to the actions of others. Rather, each participant only necessarily has intentions with respect to their own actions. That said, such intentions with respect to the actions of others *might* be present in some cases, such as those involving authority relations between participants. A superior might issue a direct order to a subordinate to do their part in some joint epistemic action and in issuing the order also intend that the subordinate perform the act in question. Second, joint epistemic action typically involves mental acts (Geach 1957), such as judgments, and behavioural actions, such as communicating and physical evidence gathering. We are assuming that what makes an action an epistemic action is that its goal or end is epistemic, and that this point applies both to individual and joint epistemic actions. Third, in the case of morally significant joint epistemic actions, the participants are jointly morally responsible for the action or its outcomes. The joint epistemic actions performed by intelligence officers typically have moral significance, given that they are directed to national security ends, i.e., ideally, to the collective moral good of national security.

Intelligence Agencies as Epistemic Institutions

As argued elsewhere (Miller 2010), joint action is the basic building block of joint activity and, therefore, of social institutions. Similarly, joint epistemic action is the basic building block of joint epistemic activity, and therefore, of epistemic institutions, such as intelligence agencies (Miller 2022a).

Intelligence agencies are institutions in the sense of organisations or systems of organisations, as opposed to less complex social forms, such as conventions or social norms, on the one hand, and more complex and complete social forms, such as societies or nation states, on the other hand. An institution (in this sense) consists of an embodied (occupied by human persons) structure of differentiated roles (Miller 2010, chap. 2; Miller 2022a, 2022b) – as well as, typically, additional non-human components, e.g., buildings and other artefacts. These roles are defined in terms of tasks, and rules (including conventions and social norms, as well as explicit laws and regulations) governing the performance of those tasks. Moreover, there is a degree of interdependence among these roles, such that the performance of the constitutive tasks of one role cannot be undertaken or, at least, cannot be undertaken except with great difficulty or considerable inefficiency, unless the tasks constitutive of some other role or roles in the structure have been undertaken or are being undertaken. Further, these roles are often related to one another hierarchically, and hence involve different levels of status and degrees of authority. Finally, on teleological and functional accounts and, in particular, on the joint action-based teleological account favoured here, these roles are related to one another, in part, in virtue of their contribution to the *ends* or *functions* of the institution; and the . realisation of these ends or functions normally involves interaction not only between the members of the institution in question but also between these internal institutional actors and external actors who might be members of other institutions or, alternatively, might be non-institutional actors.[3] Thus, intelligence officers interact with one another and also with political, military, and police decision-makers.

Organisational action typically consists in a multi-layered structure of joint actions (Miller 1992, 2001, chap. 5, 2010, chaps. 1 and 2, 2022a; 2022b). One relevant illustration of the notion of a layered structure of joint actions is a foreign interference task force comprising three (let us assume for purposes of simplification) teams: a national security threat intelligence team (TI) focused on, inter alia, foreign intelligence agencies seeking to hack into national security institutions in order to steal secrets, destroy databases, interfere in democratic elections, and the like; an investigative team (INV) tasked with investigating, inter alia, the nature of the threat and identifying the source of the threat – a difficult task, given the attribution problem, and the likelihood of credible deniability; and a response team (RES) that comprises, in part, decision-makers who need to decide on the appropriate defensive response (e.g. "patching" a defect in the system's software that is being exploited by the hackers), or (potentially) offensive response (e.g. interfering with a foreign authoritarian government's surveillance systems). Suppose at an organisational level, a number of joint actions ("actions") are severally necessary[4] and jointly sufficient to achieve some collective end, e.g., to prevent or mitigate hacktivists seeking to steal secret intelligence. Thus, the joint epistemic action of the TI team gives early warning to the INV team which performs the joint epistemic action of determining the source of the attack and disseminating this information to the RES team, which performs the joint epistemic action of determining the appropriate defensive or offensive response before initiating that response (i.e. the kinetic action). We are here assuming that the "action" of TI is, in fact, a joint epistemic action, as is the "action" of INV and the "action" of RES. Moreover, assume also that the "action" of TI, the "action" of INV, and the "action" of RES are severally necessary and jointly sufficient to achieve the collective end of preventing or mitigating the ongoing cyberattack. These "actions", taken together, constitute a fourth joint action, which comprises the three joint actions of TI, INV, and RES, respectively.

At the first level, there are individual actions directed to three distinct collective ends: the collective ends of (respectively) monitoring and identifying threats, investigating actual attacks, and responding to these attacks, whether defensively or offensively (or both). Thus, at this level, there are three joint actions, namely, those of (respectively) TI (a joint epistemic action), INV (a joint epistemic action), and RES (a joint epistemic action followed by a kinetic joint action)). However, taken together, these three joint actions constitute a single (second level) joint action. The collective end of this second level joint action is to mitigate the effects of the ongoing cyberattack(s); and from the perspective of this second level joint action, and its collective end, these (first level joint) constitutive actions are (second level) individual actions.

Note that typically in organisations, not just the nature, but also the extent, of the individual contributions made to the collective end will differ from one team member to another. Note also that (as mentioned earlier) the collective end of the organisation (and of particular joint actions) will exist in the minds of the participants under different descriptions; indeed, in some instances, it might be more accurately characterised as a set of overlapping individual ends. In addition, as is often the case with long-term ends or with the ends of complex actions, the content of these collective ends is initially underspecified and only receives further specification as the joint activity proceeds.

Note finally that here, as elsewhere in institutional arrangements, the role structure within each of the sub-joint actions is maintained, in part, by the commitment of each or most of the participants to the collective end constitutive (respectively) of each of these sub-joint actions. Likewise, there is a need for a coordinating structure comprising, in part (let us assume), a committee consisting of the leadership of the foreign interference task force and of each of the three teams (TI, INV, and RES, respectively). This structure, and therefore the committee, exists to ensure that each of the sub-joint actions does, in fact, contribute to the larger joint action. Needless to say, without appropriate ongoing coordination, the larger joint action would not be successfully performed. Importantly, this coordination consists, in large part, in ensuring that the pursuit of the collective ends of each of the sub-joint actions meshes appropriately with the pursuit of the overall collective end of the larger overall joint action.

This appropriate meshing relies, in part, on all (or, at least, most) of the participants in the larger overall joint action being aware that their participation in their sub-joint actions is ultimately in the service of the ultimate collective end of (in this case) mitigating the effects of the ongoing cyberattacks. Therefore, they need to willingly (including occasionally as a result of their own discretionary decisions) adjust their contributory individual and sub-joint actions, accordingly, i.e., they need to have adopted the ultimate collective end of the larger joint action (even if this is not often in the forefront of their minds because it does not need to be – rather their focus needs to be on their own individual contributory action and their own local collective ends). It is an illusion to imagine that the actions to be performed by most institutional role occupants can be reduced to mechanically performed tasks under the complete control (at least in principle) of those in authority. Hence, the need for role occupants engaged in the core activity of an institution to understand (at least to some extent) and pursue (even if indirectly and often unconsciously) the collective end(s) of the institution to which they belong. Certainly, this is necessary if an institution is to be successful over time and, in particular, if an *epistemic* institution is to be successful over time.

Obviously, given the crucial role of institutions and institutional actions in the prevention of cyberattacks seeking to steal secret intelligence, it is important, for the purposes of this chapter, that the activity of organisations that are institutions can be understood in purely individualist terms and by recourse to the core notion of joint action (including that of joint epistemic action); hence, the significance of the technical notion of a multi-layered structure of joint action. Moreover, since those responsible for joint actions, including joint epistemic actions, are individuals then these individuals, including intelligence officers, can (at least in principle) be held morally responsible (jointly morally responsible (Miller 2006; 2014)) for their intelligence activity.

Conclusion

Let me conclude this chapter by noting some differences between national security intelligence agencies and other epistemic institutions (Miller 2022b). As argued earlier, national security intelligence is an epistemic notion, and ideally, it consists of knowledge, i.e., it is true or correct or accurate or probably true, or some such. Thus, intelligence officers aim at, or ought to aim at, knowledge as is the case with both academics and journalists. However, unlike academics, but like journalists, generally speaking, this knowledge is not new knowledge but is *secret knowledge* acquired from knowledgeable sources. Moreover, in the case of intelligence officers, unlike academics and (to a lesser extent) journalists, the sources of this knowledge are typically highly resistant to it being acquired, as in the case of secret intelligence acquired about foreign military organisations. Indeed, intelligence officers confront foreign *counter-intelligence* operations. Further, unlike knowledge acquired by journalists for public dissemination, national security intelligence is typically secret intelligence acquired (again, following on a process of collection and analysis) in the service of the collective end of national security and, as such, is not for public consumption. Indeed, even within a national security intelligence organisation, intelligence (or knowledge resulting from the collection and analysis of intelligence) might only be disseminated on a "need to know" basis, although intelligence officers are often said to be prone not to provide such intelligence or knowledge to their fellow officers even when they need to possess it. Finally, as mentioned earlier, national security intelligence needs to be actionable by political leaders and security agencies. For instance, national security intelligence in relation to a planned foreign military attack might require, at the very least, putting in place defensive measures and, indeed, might require a pre-emptive attack. In this respect, national security intelligence differs somewhat from both the knowledge sought by academics and that sought by journalists.

Notes

[1] An earlier version of the material in this section appeared in Miller 2022b.

[2] An earlier version of the material in this section appeared in Miller 2022b.

[3] Of course, institutions have other general properties such as institutional cultures.

[4] This is not strictly correct; rather, typically, some threshold set of actions is necessary to achieve the end.

References

Barnea, Avner. 2020. "Strategic Intelligence: A Concentrated and Diffused Intelligence Model." *Intelligence and National Security* 35(5): 701–16. doi:10.1080/02684527.2020.1747004

Bellaby, David. 2014. *Ethics of Intelligence*. London: Routledge.

Bok, Sissela. 1982. *Secrets: On the Ethics of Concealment and Revelation*. New York: Pantheon Books.

Bratman, Michael E. 1993. "Shared Intention." *Ethics* 104(1): 97–113. doi:10.1086/293577

Breakspear, Alan. 2013. "A New Definition of Intelligence." *Intelligence and National Security* 28(5): 678–93. doi:10.1080/02684527.2012.699285

Fabre, Cecile. 2022. *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence*. Oxford: Oxford University Press.

Fallis, Don. 2007. "Collective Epistemic Goals." *Social Epistemology* 21(3): 267–80. doi:10.1080/02691720701674106

Geach, Peter. 1957. *Mental Acts*. London: Routledge.

Gill, Peter. 2018. "The Way Ahead in Explaining Intelligence Organization and Process." *Intelligence and National Security* 33(4): 574–86. doi:10.1080/02684527.2018.1452566

Kent, Sherman. 2015. *Strategic Intelligence for American World Policy*. Princeton: Princeton University Press.

Marrin, Stephen. 2018. "Evaluating Intelligence Theories: Current State of Play." *Intelligence and National Security* 33(4): 479–90. doi:10.1080/02684527.2018.1452567

Miller, Seumas. 1992. "Joint Action." *Philosophical Papers* 21(3): 275–97. doi:10.1080/05568649209506386

Miller, Seumas. 2001. *Social Action: A Teleological Account*. New York: Cambridge University Press.

Miller, Seumas. 2006 "Collective Moral Responsibility: An Individualist Account." *Midwest Studies in Philosophy* 30(1): 176–93. doi:10.1111/j.1475-4975.2006.00134.x

Miller, Seumas. 2008. "Collective Responsibility and Information and Communication Technology." In *Information Technology and Moral Philosophy*, edited by Jeroen Van Den Hoven and John Weckert. 226–250. Cambridge: Cambridge University Press.

Miller, Seumas. 2010. *The Moral Foundations of Social Institutions: A Philosophical Study*. New York: Cambridge University Press.

Miller, Seumas. 2014. "Police Detectives, Criminal Investigations and Collective Moral Responsibility." *Criminal Justice Ethics* 33(1): 21–39. doi:10.1080/0731129x.2014.906094

Miller, Seumas. 2015. "Joint Epistemic Action and Collective Moral Responsibility." *Social Epistemology* 29(3): 280–302. doi:10.1080/02691728.2014.971908

Miller, Seumas. 2016. *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*. New York: Oxford University Press.

Miller, Seumas. 2017. *Institutional Corruption: A Study in Applied Philosophy*. New York: Cambridge University Press.

Miller, Seumas. 2018. "Joint Epistemic Action: Some Applications." *Journal of Applied Philosophy* 35(2): 300–18. doi:10.1111/japp.12197

Miller, Seumas. 2019. "Joint Abilities, Joint Know-How and Collective Knowledge." *Social Epistemology* 34(3): 197–212. doi:10.1080/02691728.2019.1677799

Miller, Seumas. 2021. "Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity." *Social Epistemology* 35(3): 211–31. doi:10.1080/02691728.2020.1855484

Miller, Seumas. 2022a "Epistemic Institutions: A Joint Epistemic Action-Based Account." *Nous-Supplement: Philosophical Issues* 32: 398–416.

Miller, Seumas. 2022b "National Security Intelligence Activity: A Philosophical Analysis." *Intelligence and National Security* 37: 791–808.

Miller, Seumas and Ian Gordon. 2014. *Investigative Ethics: Ethics for Police Detectives and Criminal Investigators*. London: Wiley-Blackwell.

Miller, Seumas, Regan, Mitt and Patrick Walsh (eds.). 2021. *National Security Intelligence and Ethics*. London: Routledge.

Moser, Paul K. 1989. *Knowledge and Evidence*. Cambridge: Cambridge University Press.

Phythian, Mark (ed.). 2013. *Understanding the Intelligence Cycle*. Abingdon: Routledge.

Pili, Giangiuseppe. 2019. "Intelligence and Social Epistemology – Toward a Social Epistemological Theory of Intelligence." *Social Epistemology* 33(6): 574–92. doi:10.1080/02691728.2019.1658823

Smith, Neilson V. 1982. *Mutual Knowledge*. London: Academic Press.

Sosa, Ernest. 2015. *Judgment and Agency*. Oxford: Oxford University Press.

Stout, Mark and Michael Warner. 2018. “Intelligence Is as Intelligence Does.” *Intelligence and National Security* 33(4): 517–26. doi:10.1080/02684527.2018.1452593

Treverton, Gregory F. 2001. *Reshaping National Intelligence for an Age of Information*. Cambridge: Cambridge University Press.

3 On Just Intelligence Operations

Exceptions and Explanations

Adam Henschke

Intelligence, joint epistemic action for national security decision-making in a context of competition, can be understood to have normative content. However, here we need to highlight significantly different views on intelligence. On the one hand, given the connection between these joint epistemic actions and national security, some argue that intelligence is a space free of ethics. "[W]hy should we be concerned at all with ethics in this field – is it not quintessentially one where Machiavelli and *realpolitik* have to rule?" (Quinlan 2007, 1). To speak of intelligence by reference to national security is to effectively claim that there is no connection to ethics. What matters is power, success, survival, or some other non-ethical value. On the other hand, however, reference to national security is in fact the thing that gives intelligence an ethical foundation. "Secret intelligence is needed and depended upon to protect against a range of external and internal threats… As a key tool of the state, it is the duty of intelligence organisations to detect, locate and prevent any threat to the political community" (Bellaby 2014, 2). This goes to the idea that actions and institutions that act in service of national security are ethically justified by those aims.

> [D]iscussions of national security are typically threaded through with attempts to justify the nation, its existence and what the state must do to protect either its people or its own persistence. That is, ethical reasoning is central to any discussion of national security.
>
> (Henschke 2021, 81)

Here, it seems we may be at an impasse: If people cannot agree whether intelligence admits of a relation to ethics, perhaps it is fool's errand to find a path through. However, I suggest that there is a way forward that accepts part of the premise that ethics has no place in intelligence while arguing for an ethics of intelligence. What I suggest here is that the first path recognises something quite important about intelligence – it is a realm in which normal interpersonal ethics do not apply. However, as we will argue, looking at the concepts and history of this sense of exceptionalism leads us back to the second path, a realm where ethics do apply.

DOI: 10.4324/9781003106449-4

The argument in this chapter develops as follows. It begins by explaining the challenge of whether there is a connection between intelligence and ethics. There is considerable reason to think that the relation between intelligence and ethics is different from a more "normal" way of doing ethics. It then looks at the notion of ethical exceptionalism and explores how the related field of military ethics has grappled with the same problem. From here, some of the main ideas of the just war tradition (JWT) are introduced, and they show how a range of people have sought to build a bridge between the JWT and "just intelligence". Drawing from Chapter 2, the chapter suggests that the bridge between just war and just intelligence needs to be built from a foundation of institutional ethics. That is, it is not enough to simply take the principles of just war and apply them to intelligence. The institutional nature of intelligence is such that the ethics principles of intelligence need to be significantly reconsidered and reshaped to make them workable for intelligence.

This Fundamentally Repugnant Philosophy: On Ethics and Intelligence

Does it make sense to speak of ethics in intelligence? Consider this contrast between war and the shadowy world of spies and saboteurs. "War, like sport, was to be a gentleman's game. Guerrilla warfare was most ungentlemanly, based as it was on treacherous principles like sabotage and subversion" (Jacobsen 2019, 18). The Doolittle Report on the Covert Activities of the Central Intelligence Agency described the position of the US in the Cold War as one where immoral actions must be permitted.

> Hitherto acceptable norms of human conduct do not apply. If the United States is to survive, long-standing American concepts of "fair play" must be reconsidered. We must develop effective espionage and counterespionage services and must learn to subvert, sabotage and destroy our enemies by more clever, more sophisticated and more effective methods than those used against us. It may become necessary that the American people be made acquainted with, understand and support this fundamentally repugnant philosophy.
>
> (Quoted in Weiner 2008, 125)

While we can disagree with the idea that war is a gentleman's game like sport, the practice of intelligence seems to suggest something that is morally tainted.

The reason for this is that, when considered in a context of typical human interactions, the work of intelligence is indeed likely to be immoral. A very simple ethics tells us not to lie to people, not to manipulate them for our own ends. In contrast to war, where soldiers are supposed to engage in fair combat, poisoning, kidnapping, and assassinating one's enemy is duplicitous, cowardly, and not the realm of gentlemen. As the US Secretary of State said, when closing down the State Department's code breaking department in 1929, "gentlemen do not read each other's mails" (Quoted in Faini 2020, 73). It is wrong for me to read your private correspondence, a violation of your right to privacy. And, insofar as intelligence involves the gathering of secrets on people, then it is violating their privacy.

There are two primary foundations for the moral values that underpin the sense of repugnance about the secret and cowardly world of intelligence. First is what we would call traditional ethical values. Here, ethics, at its most simple, can be reduced to whether a person suffers as a result of your particular decisions, or whether you are showing them the respect that they are owed in virtue of them being a human. To spy on someone, to kidnap them, poison them, assassinate them, and so on will clearly cause them to suffer. And, as per a very simplified consequentialist analysis, this is morally impermissible.[1] Similarly, to lie to them, cheat them, to deceive or manipulate them for your own ends violates their basic dignity. In Immanuel Kant's classic formulation, one should "*act that you use humanity, whether in your own person or in the person of any other, always at the same time as an end, never merely as a means*" (Kant 1997, 38; emphasis original). By denying them the truth, and manipulating them, you are reducing them to mere means and not giving them the respect that they are due.

If we reduce human interactions to one-to-one relations and look for the key values that underpin and guide our interactions, then we ought not cause suffering in others, and we ought not violate a person's dignity by lying to them and so on. Assuming that intelligence as a practice requires these basic practices, on a very simple reductive analysis, not only is intelligence a space that seems free of ethics, but it is also likely to be inherently unethical.

The second foundation of moral values is related to a person's character. As cited earlier, warfare is conducted by gentleman, people of dignity and honour. Intelligence, by contrast, is conducted by liars, thieves, and cowards – people lacking dignity and honour. As people like Shannon French and Shannon Vallor have argued, there is a significant tradition that links warfare to virtue. Warriors operate under a code, and

> this code of honor seems to hold the warrior to a higher ethical standard than that required for an ordinary citizen… The warriors themselves police strict adherence to these standards: with violators being shamed, ostracized, even killed by their peers.
>
> (French 2005, 4)

Vallor argues

> Self-sacrifice is a core component of military service because the highest expression of ethical service is that in which one wholly gives oneself for another, or more properly, for many others – one's fellow unit and service members, one's family and friends back home and their progeny, one's fellow and future citizens, and fellow and future members of the human community.
>
> (Vallor 2014, 174)

Insofar as intelligence involves practices that are neither honourable nor involve sacrifice in the same way as the warrior, then the intelligence practitioner lacks the special character of the warrior.

This is of course a nonsense, a myth. While it is undoubtedly true that those who serve in the military have and adhere to codes of conduct or honour, and they make considerable sacrifices to protect their people and the lives of others, to say that war is conducted by gentlemen is simply not true. War is bloody and brutal, and may require a person to put their lives on the line, but may also require the sacrifice of traditional ethics in order to achieve a particular military goal. As per the JWT, while it may be reasonable to say that a soldier or commander had ethical justification for their actions, we might also see that they are exposed to significant moral harms in pursuit of these goals. The moral injury of soldiers is an area that is gaining more attention,[2] and some have argued that soldiers can suffer moral exploitation by the militaries for whom they fight (Robillard and Strawser 2016).

At the same time, intelligence as a practice and the larger institutions of intelligence may also be ethically justified or obligatory, and those engaged in intelligence may be morally praiseworthy for their actions and for the sacrifices that they make in service of intelligence. Going back to our definition of intelligence, "[b]etter-informed decisions lead to better government and a safer and more secure society" (Omand and Phythian 2018, 1). Insofar as we want to commend the character of those who work to protect the lives and human rights of fellow citizens or others around the world, then those engaged in intelligence ought also to be praiseworthy. So, just as we ought to be critical of the idea that war is the realm of good manners and fine conduct, we also ought to be critical of the idea that intelligence is the realm of liars, deceivers, and the dishonourable.

However, we do need to recognise that there is a moral dissonance where intelligence is concerned.

> Let's be blunt about what we do. There is no dishonour in it. We steal secrets for a living. If we do not steal secrets for a living then we ought to shut the doors and do something else for a living.
>
> (George Tenet, quoted in Omand and Phythian 2018, 9)

As discussed in Chapter 2, intelligence is joint epistemic activity in an environment of competition. This puts intelligence at odds with how a good person would normally conduct himself or herself. It is widely accepted that it would be wrong for Jones to lie to Jane. And Jane would violate Jones' right to privacy if she was to read his emails, to track his phone, or tell other people about his movements. While we might see that those engaged in intelligence practice are good people, we also recognise that intelligence requires morally problematic actions.

Exceptionalism or Business as Usual? Just War and Just Intelligence

A number of people writing on intelligence ethics have sought to square the circle by drawing from the JWT. Sir David Omand and Mark Pythian, for example, develop a theory of just intelligence (JIT) from the JWT (Omand and Phythian 2018, 72–109). Ross Bellaby's intelligence ethics seeks to do similar (Bellaby 2014, 15–47). While we do not wholly agree with their approaches (see later and in Chapter 4), there is good reason to look to the JWT for a way of assessing the ethics of intelligence practice and institutions.

First and foremost, the JWT has a long history. Its roots go back to the ancient Greeks, with Plato, Aristotle, and perhaps even Thucydides[3] setting the foundation for moral reflection on war (Reichberg, Syse, and Begby 2006, 3–46). The JWT provides a deep resource from which to draw guidance and understanding. Many of the finest moral philosophers have grappled with deep moral challenges faced by decisions around war, and it makes sense to use this tradition and the insights it has generated over thousands of years to help guide responses to modern challenges.

Second to this, there is an important similarity between the JWT and the ethics of intelligence. The JWT, at its core, grapples with the idea of whether it is ethically permissible to do things that are normally impermissible. Killing someone is typically seen as one of the most morally problematic things that one can do. In normal life, if Jane was to kill Jones, Jane would be tracked down, charged with murder, and if convicted, and sentenced to a long jail term. Yet, when in combat, if Jane and Jones were soldiers in opposing militaries, they would both be permitted to try to kill the other. And, given other factors, at the end of the war, they might both be treated like heroes. This, of course, simplifies things incredibly; there are constraints on what warfighters can do in war, and there is considerable scholarship that suggests that the reasons why Jane and Jones fight might bear upon their moral status.[4] However, the simple point remains – what is generally morally impermissible may become permissible when in situations of conflict like war.

The practice of intelligence is similar. Intelligence involves many actions and decisions that would not normally be permissible. "At its most basic level, intelligence involves theft, or acquiring things whose owners do not want them shared" (Omand and Phythian 2018, 10). While it might be wrong for Jones to lie to Jane in normal life, if Jones is an undercover agent investigating Jane, he might need to lie to her to gain her trust. Or, consider that they are married and Jones is an intelligence agent. Imagine that Jane asks him something about his work; Jones may need to lie to Jane about aspects of his role. Not only is he permitted to lie to his wife, but he might even be obliged to lie. Likewise, given the idea of intelligence as some joint action conducted in a competitive context, if Jane works for an intelligence agency tasked with placing threats under surveillance, she may have to find ways to gather information on Jones. Yet, in normal life, this spying would not just violate Jones' moral right to privacy but may also break the law.

The point here is that the needs of war and the needs of intelligence – specifically national security intelligence – permit and may require actions that are typically impermissible. Furthermore, both competition in war and in intelligence involve the use of government institutions to pursue and protect the security of the nation, its people, and perhaps its values. In this way, they are both similar in that an ethics of intelligence is like an ethics of war – when is it permissible to engage in normally prohibited activities, and what can and cannot be done when that permission is granted? The JWT has developed a set of principles that seek to offer ways that the decisions and acts of war can be understood, and perhaps ethically justified. Given the long tradition in the ethics of war, it makes sense to see how those questions have been answered elsewhere.

One general view of the ethics of war, and perhaps the ethics of intelligence, is to see them both as forms of moral exceptionalism. That is, to hold that in the context of war, and perhaps epistemic competition, certain acts and decisions are excepted from normal morality. "[N]othing else is remotely like war. As Cheyney Ryan puts it, we must confront 'war-as-its-own reality'. Analogies with ordinary life only mislead" (Shue 2008, 111). Given this difference, we might see that war and, perhaps, intelligence are cases for exceptionalism. "The semantics of exceptionalism mandate that something is being *excepted* vis-à-vis some category" (Allhoff 2012, 40). War, on this view, is a special situation, a case of moral exceptionalism in which the normal moral rules and principles do not apply.

> [G]iven the characteristic features of war – the fact that war precisely consists of wounding and killing people and damaging and destroying objects – the specific rules for conduct in war, if any notion of such rules can be intelligible at all, must be radically different in content from the specific standards for conduct in ordinary life.
>
> (Shue 2008, 87)

Importantly for the JWT, this is not to say that no rules apply, rather it is that there are different and exceptional rules that apply in warfare. One of the defining features of the JWT has been the effort to develop and justify those rules. Intelligence is similar – to reword Henry Shue's statement from earlier, *given the characteristic features of national security intelligence – the fact that this epistemic competition consists of lying and manipulating people and damaging and destroying the truth – the specific rules for conduct in intelligence, if any notion of such rules can be intelligible at all, must be radically different in content from the specific standards for conduct in ordinary life*. As in war, the normal rules do not apply, and as in war, some exceptional rules must be developed.

However, this exceptionalism of intelligence is not something new. Like war, intelligence is not a new phenomenon. Spying, for instance, is frequently referred to as the "second oldest profession".[5] As Christopher Andrew shows, the history of intelligence stretches back through human history. "The Old Testament (also known as the Tanakh, the Hebrew Bible) contains more references to spies than any published history of Britain or most other countries" (Andrew 2019, 14). So, on this, intelligence is hardly exceptional in terms of its occurrence. The point here is that the ethical principles around intelligence, like war, are constant features in our world, and both involve regular practices. What we need to do is develop principles that explain, justify, and guide good behaviour. In order to identify and develop those principles for intelligence, we can follow the path set by the JWT, to look to ordinary moral values and seek to develop them for the particular context of interest.

> [T]o be recognizable as normative standards, the rules for the conduct of war cannot be detached from ordinary moral moorings, even if the specific rules appropriate for *ordinary contexts no longer apply*. So, this suggestion is that different specific standards from the specific standards that apply to ordinary life – all life outside war – apply inside war.
>
> (Shue 2008, 87; my emphasis)

Likewise, the suggestion is that different specific standards from the standards that apply to ordinary life – all life outside intelligence – apply inside intelligence. The ordinary moral moorings remain constant; the exceptions relate to the particular principles derived from these moorings and how and when they are applied.

What we need to do, therefore, is to look to the context of intelligence and develop specific principles for this context. It is here that our account for an ethics of intelligence differs from those that apply the just war principles to intelligence. While their approach, to look to the general principles that allow for normally impermissible actions and decisions, is reasonable, the *institutional context* of intelligence needs to be considered as an essential aspect of just intelligence. As we argued in Chapter 2, intelligence is not simply an epistemic activity but a joint epistemic activity conducted in a context of competition. That is, it is an institutional action, and a model of just intelligence needs to recognise that institutional aspect in order to properly translate the general ethical principles to intelligence.

From the Just War Tradition to a Theory of Just Intelligence

The JWT approaches question about the ethics of warfare by clustering questions of permissibility around three main themes. First, questions of when it is permissible to go to war. Second, what one can permissibly do in war. And third, what one must do after war ends. These are referred to as the *jus ad bellum*, *jus in bello*, and *jus post bellum*, respectively. Further, there has recently been interest in other aspects around warfare, such as *jus ad vim* or "force short of war" (Ford 2013; Brunstetter 2016), the ethics of unarmed conflict (Gross and Meisels 2017), and the ethics of cyberwarfare (Allhoff, Henschke, and Strawser 2016). For the purposes of this book, we will focus primarily on *ad bellum here* and *in bello* in Chapter 4. I also note that the following discussion draws directly from Seumas Miller's "Rethinking the just intelligence theory of national security intelligence collection and analysis: The principles of discrimination, necessity, proportionality and reciprocity" (Miller 2021). However, the particular form of the JIT principles derived from Miller's work and their ultimate expression are my final take on Miller's view.

Roughly speaking, according to JWT, the armed forces of a collective political entity, a nation state such as Anxietous, are morally justified in waging war against the armed forces of another collective political entity, Belligerence, if and only if:

1 Anxietous' purpose in waging war is collective self-defence against Belligerence's military aggression, or defence of others against military aggression. Call this just cause for war (JCW).

2 Anxietous uses lethal force only to the end of bringing about the cessation of Belligerence's aggression. Call this right intention for war (RIW).
3 Anxietous' armed forces are waging war under a legitimate political authority. Call this legitimate authority for war (LAW).
4 There is no alternative means of defence against Belligerence, and so Anxietous wages war as a last resort. Call this last resort for war (LRW).
5 Anxietous has a reasonable chance of winning the war against Belligerence. Call this probability of success for war (PSW).
6 It is probable that if Anxietous wages war against Belligerence, the consequences, all things considered, will be better than if Anxietous does not. Call this proportionality of war (PW).
7 Anxietous only deliberately uses lethal force against morally legitimate targets, that is, against Belligerence's combatants (identifiable by virtue of their uniforms and the fact that they bear their arms openly) but not Belligerence's civilians ((i) principle of discrimination), an extent of violence that is necessary to the end of winning the constitutive battles of the war and, ultimately, the war itself ((ii) principle of military necessity), and the violence is not disproportionate ((iii) principle of proportionality).

Notice that condition (7) is essentially the so-called *jus in bello* of JWT, according to which combatants on both the just and the unjust side are (at least on the traditional view) moral equals. Conditions (1)–(6) constitute the so-called *jus ad bellum*. The focus in this chapter is on the *ad bellum* criteria. Seumas Miller returns to the discussion of the *in bello* criteria and their relation to intelligence in Chapter 4.

The six *ad bellum* principles have been the topic of discussion since the time of the ancient Greeks. These are supported by vast bodies of scholarly debate.[6] Given the basic recognition of the moral exceptionalism around warfare, the six principles can serve as a starting point to develop a JIT. However, the *ad bellum* principles need to be adapted significantly to the context of intelligence. That is, we cannot simply lift a principle like JCW and drop it into the intelligence context.

One significant reason for this is that war and intelligence are quite different contexts of application. The JWT, particularly the *ad bellum* criteria, is concerned with decisions about when it is morally permissible to go to war. This notion relies on a somewhat binary analysis – are states at peace or are they at war? The *ad bellum* principles are intended to clarify and guide when it might be justified to move from peace to war. "One issue that arises in attempting this parallel [between war and intelligence] concerns the fact that war is an exceptional state, while, in the contemporary world, intelligence activity is a constant state of affairs" (Omand and Phythian 2018, 85). Intelligence, however, does not sit on this binary. In part because intelligence practices happen constantly, the institutions of intelligence are always active in some way or another. Note also that we "do not talk of 'going to intelligence', or 'resorting to intelligence' as we do of 'going to war' or 'resorting to war'…" (Omand and Phythian 2018, 85). It is not sensible to say that a given nation is in a condition of non-intelligence and then it shifts to a condition of intelligence. Rather than placing intelligence in a binary state, the criteria of the *jus ad bellum* need to be significantly adapted to create a sensible set of *jus ad intelligentiam* criteria.

Also note that the morally acceptable purposes of war (essentially, defence against military aggression) constitute a much narrower, determinate, and less open-ended (e.g. wars but not national security concerns in general have a start and finish date) set of national security concerns than those that might legitimately motivate intelligence activities. While the notion of intelligence as joint epistemic group action within a context of national security competition is tightly described, it does include and perhaps allow a wide range of activities. Wire taps, remote surveillance, setting honey traps, pushing propaganda, perhaps even engaging in efforts to replace political leaders, these all fit within the wide set of activities that intelligence is involved in. Furthermore, intelligence is not simply involved in collection, but analysis. Likewise, the institutions that are engaged in these behaviours are wide and varied, from military intelligence, to international signal intelligence (SIGINT), to domestic human intelligence (HUMINT). In short, the range of actions and institutions involved in the competitive epistemic actions are wide and varied. On this, intelligence is always ongoing. What matters is which sorts of operations are permitted by the relevant intelligence authorities and institutions. As recognised in Bellaby's "ladder of escalation", intelligence is always happening, what differs is where the intelligence operation sits in relation to harms, needs, and justifications. "[A]s the level of harm goes up, according to the number, severity and range of vital interests violated, so too must the justification" (Bellaby 2014, 31).

This gives us the first way to develop the notion of JCI. Given that intelligence is ongoing, what a JCI principle must offer is guidance in whether a particular intelligence operation is justified. Here we see a fundamental difference between JCW and JCI. In order for Anxietous to be justified in going to war, there must be an act of aggression by Belligerence, either against Anxietous or, perhaps – though this is more controversial – against one of their allies. Anxietous is therefore acting in self-defence or defence of another. Yet, as defined, intelligence is an epistemic action.

> [G]iven that it is the duty of intelligence agencies to provide the very information that is then used to establish the just cause, we are faced with how to make the initial ethical calculation without carrying out some form of intelligence collection.
>
> (Bellaby 2014, 34)

Bellaby goes on to note that "the intelligence operative must engage with the evidence available and determine what action is best given the range of possibilities" (Bellaby 2014, 34). While this makes sense, we suggest that more nuance is needed. As described, it is unclear whether the JCI is about a specific intelligence action carried out by a specific intelligence agent, or whether the JCI is about more general intelligence operation, which is decided higher up an institutional chain of command. On an institutional approach, and following a separation into *jus ad intelligentiam* and *jus in intelligentia*, the JCI must be seen as the high-level decisions about institutional operations and policies.

This highlights the strength of taking a teleological approach (described in Chapter 2) and links the JCI to national security. The British legislation regarding intelligence

> limits the work of the agencies to only three statutory functions: upholding national security, detecting and preventing serious crime, and safeguarding economic well-being (the latter being qualified as having to originate from outside the nation and be of national security concern).
>
> (Omand and Phythian 2018, 75)

As Omand and Pythian note, national security is typically not defined (Omand and Phythian 2018, 76). However, we can consider national security as relating to the special responsibility of the state to secure its citizens and to maintain its own survival (Henschke 2021, 80). National security intelligence is justified when the joint epistemic actions support decision-making that protects or improves the security of its citizens and maintains its own survival. However, recall that our definition of intelligence and national security relates to joint epistemic actions in a context of competition. The role of intelligence is unique in that it is not simply about improved government decision-making; it is about improved government decision-making in relation to threats. Thus, we offer the first of the *jus ad intelligentiam* criteria, the JCI: The national security intelligence agencies of a collective political entity, A (a nation state), are morally justified in collecting, analysing, and disseminating intelligence in relation to an individual or collective political actor, B (e.g. a nation state, violent non-state actor, such as a terrorist group, etc.), if and only if:

> Just Cause for Intelligence (JCI): A’s purpose in undertaking these intelligence activities is to enable decision making that protects against any national security threat posed by B; and/or to enable decision making that gives a competitive national security advantage against B.

On this definition, and drawing from Bellaby’s ladder of escalation, we would expect basic background intelligence to be gathered on the potential threats posed to a country’s citizens and survival, and if/when there is reason to suspect that there is a threat, then the relevant intelligence institutions would engage in a potential escalation of intelligence operations to gain more information and certainty about that threat, and how the nation’s decision-makers should respond to that threat.

The second principle is the RII. Again, recall that we are looking at this in relation to *jus ad intelligentiam*, the high-level considerations about wide-scale intelligence operations and the basic conditions around the use and existence of intelligence institutions. In war, the RIW is something like the reason that a war is being fought to protect the nation, its people, or others against unjust aggression. A RII is similar in spirit but different in practice. The simplest way to think of the

RII is that the intelligence operation and institution must act in ways that protect the security of its citizens and the state. This ties directly to the JCI.

There are two complementary ways to consider a RII. First is how the intelligence operation or institution matches to the JCI. Consider two contrasting uses of intelligence to illuminate this point. An intelligence operation by Anxietous is authorised that installs listening devices in the meeting room where Belligerence's leaders are deciding on a course of military action. Anxietous is now able to monitor and know if Belligerence poses a national security threat to its citizens or survival. In the second scenario, an intelligence operation by another nation called Competitor, is authorised that installs listening devices in the meeting room where Competitor nation's leaders and Defender are deciding on a course of economic development, such as resource extraction. Competitor is now able to monitor and know if Defender poses an economic threat to its national interest. In the first instance, Anxietous' intention matches to the JCI. In the second scenario, however, Competitor's intention is *not* about national security. Competitor's economic well-being, while important, is significantly different from Anxietous' survival. In short, only Anxietous' intention would count as RII, Competitor's would not.

The second way to consider the RII is as integrity. Omand and Pythian, for instance, write that the right intention for intelligence "could be characterized as integrity of the motive on the part of those initiating and authorizing the operations" (Omand and Phythian 2018, 79). While integrity is an important indicator of RII, it is itself not the RII. For instance, the decision-makers in Competitor might have a motive that sincerely connects their operation to the nation's interests, but this is not the correct motive. Integrity is more a characterisation of the intention and its relation to the JCI, than being the RII. As such, this account of RII is offered:

> Right Intention for Intelligence (RII): A undertakes these intelligence activities only for the ultimate purpose of enabling the protection against or the competitive advantage over the threat to its national security posed by B.

To be clear here, in the comparison between Anxietous and Competitor, only Anxietous has the intention of protecting its citizens and country against the *national security threat* posed by Belligerence. Competitor's intention is about national interest, and not national security.

The next *jus intelligentiam* criterion is LAI. In war, the legitimate authority criterion may reflect two main concepts. First, is the person who makes a decision to go to war the relevant role holder? In the US, for instance, the President is the Commander in Chief. A member of Congress would not be the relevant person to decide to go to war. A second concept looks at whether the person making a decision to go to war actually represents the interests of people in whose name a war will be fought. On the first, the role-based concept, we ask who is the person that can legitimately make such a declaration; are they the legitimate role holder, and is the role one that allows for such decisions to be made? On the second, the recognition-based concept, we ask if the person has the moral authority to make such decisions; do they represent the moral will of the people that the war would be fought for?

When considering LAI, we have different considerations in play. As there are typically multiple people in nation's national security institutions who can and should make decisions regarding intelligence, we need question if a particular role holder has legitimacy to make intelligence decisions or not. Consider here controversies over the use of metadata by various government agencies in Australia. In the mid-2010s, the Australian government brought in new changes to metadata legislation regarding which government agencies could access citizen's metadata. Among the agencies seeking access to this information was the National Measurements Institute (NMI), which wanted "warrantless access to Australians' metadata to help them hunt down supermarkets skimping on [meat] portions" (Farrell 2016). On this example, the NMI lacked legitimacy. Second to this, "[I]ntelligence activity needs to be conducted in a democracy in accordance with the authority provided by the rights compliant domestic law" (Omand and Phythian 2018, 81). Here, we return to the principle of authority – an agency that is seeking to engage in intelligence activity needs to be acting in accordance with basic human rights, lest it lack moral and legal authority. To this end then, the LAI is offered:

> Legitimate Authority of Intelligence (LAI): A's intelligence agencies are collecting, analyzing, and disseminating the intelligence in question under a legitimate political authority.

In order to be an LAI, an institution must have some relevant connection to national security, and must be acting in accordance with the moral foundations that underpin national security, namely, the protection of the lives and rights of its citizens, perhaps also the lives and rights of all people, and the survival of the state itself, and must be authorised to do so by the appropriate political authority.

So far, the first three JIT principles are concerned with the institutions of intelligence, and how they relate to the purposes of those institutions. Our understanding of intelligence is not just about the institutions of intelligence but intelligence as joint epistemic actions. Being concerned with epistemic action, intelligence is about the production and communication of information for improved national security decision-making. This leads us to recognise a second fundamental conceptual difference between war and intelligence. War involves kinetic activity, the use of physical means to defeat an enemy by killing their soldiers and destroying the materiel necessary for them to fight the war. Intelligence is fundamentally different; it is about the knowledge of national security threats and how to respond to them.

Here, another fundamental different between LRW and the last resort of intelligence needs to be recognised. In the JWT, the recourse to war should be a last resort. While what this "last resort" amounts to in practice is open to discussion, as a basic principle, the idea is that as many options as possible to resolve conflict between states or organised parties should be attempted prior to the use of large-scale violence.

> Given the horrors of war, moral as well as physical, a just recourse to war should be marked by extreme reluctance and a sense of moral tragedy and foreboding. A hasty recourse to war is an unjust recourse to war. The move to war is to be justified only when all other means short of war have been exhausted.
>
> (Coates 1997, 189)

As discussed, intelligence is a practice that is ongoing, regardless of whether one is at peace or at war. Moreover, in order to know if one should engage in war, diplomacy, covert actions, or other means of conflict and competition, one needs intelligence.

In one sense, then, intelligence is in fact a *first* resort. In line with the concept of intelligence as being a necessary part of good decision-making, intelligence is necessary prior to any other action. As Bellaby notes,

> given that it is the duty of intelligence agencies to provide the very information that is then used to establish the just cause, we are faced with a paradox on how to make the initial ethical calculation without carrying out some form of intelligence collection.
>
> (Bellaby 2014, 34)

At the same time, however, intelligence operations differ significantly. Since the end of epistemic activity is (roughly speaking) knowledge, and, therefore, as a matter of logic, one embarks on an epistemic project from a position of ignorance – and with a set of questions to be answered, for example, Is there a threat? What is the nature of the threat? – the content of the end is in an important sense, and by definition, unknown. Accordingly, any prior moral assessment of the contemplated epistemic action is necessarily radically incomplete, since it depends, in large part, on the moral costs attaching to the realisation of the epistemic end, i.e., of being in possession of the answers to the questions sought – something which is, to reiterate, by definition, unknown. So while it might be sensible to say that intelligence is a first resort, not all intelligence means and methods can justifiably be used in the early stages of threat detection and analysis. I suggest here is that the principle be adapted such that it is a *logical resort*; what intelligence steps are taken are logical progression from simple threat awareness, right up to intelligence activities that directly interfere with the political processes of the target country.

Again, Bellaby's notion of the ladder of escalation is useful here. As the awareness of a potential threat increases, more invasive intelligence operations are permitted. On his account "as the level of harm goes up… so too must the justification" (Bellaby 2014, 31). As the potential threat to a country's citizens or survival increases, we would expect an effective intelligence institution to be aware of the threat, its evolution, and any increases, and ideally, for that intelligence to provide more information on how decision-makers can respond to, and mitigate or eliminate, that threat. Here we offer a principle of logical resort for intelligence:

> Logical Resort for Intelligence (LRI): As awareness of a potential national security threat increases, more intelligence operations that serve national security are permitted.

So decisions whether to wage war, apply economic sanctions, or merely use diplomacy are predicated on intelligence. In short, the relationship between any JWT and JIT is not that of theories that mirror one another by virtue of the structurally similar activities (national security intelligence collection/analysis/dissemination and waging war, respectively), but rather that of theories of dissimilar activities. These activities, nevertheless, stand in (roughly speaking) the relationship of knowledge to action; kinetic action presupposes epistemic action since the decision to perform a kinetic action (or not to do so) presupposes knowledge with respect to the why, how, what, when, where, who, etc. of the kinetic action in question (and its alternatives).

However, to be clear, similar to the LRW criterion, intelligence does need constraints. Where there are means and methods that either respect human rights, like privacy, or political principles, like state sovereignty, that would do a sufficient job of guiding decision-making, those alternative means and methods ought to be used first. We return to this point in our discussion of the *in intelligentia* necessity criterion. The principle here is considered in relation to the decision to activate intelligence operations.

This leads to the next principle – probability of success. In the JWT, the PSW is controversial. It might be understood to mean that Anxietous has a reasonable chance of success at winning. Or might simply be that Anxietous has some mere possibility of success. Either way, the basic idea of PSW is that, given that war is immensely destructive, even if there is a just cause for war, the relevant political and military leaders need to consider if going to war is worth the death and destruction it would cause. Given that intelligence is not about winning a war (even military intelligence is not about winning a war, but how can intelligence aid in decisions that win the war), how then are we to see an equivalent principle for the JIT? What I suggest here is to look again at intelligence as an institutional process, in which there is a joint epistemic action in service of national security in a context of competition.

Here, we ask if the intelligence operation or institution is *fit for purpose*. That is, does a particular intelligence operation, or does the intelligence institution, aid in national security decision-making? The first part of this question concerns basic competence. Given that a particular intelligence operation will be engaged in some competitive epistemic activity, is the outcome of that activity likely to improve national security decision-making? Similarly, we can ask if the particular intelligence institution does indeed improve national security decision-making? In one sense, however, we face a similar paradox to that of the LRI principle – how do we know if a particular intelligence operation or institution aids in national security decision-making? Much like the PSW criterion, we will only "know" this in hindsight. But this has significant institutional implications.

To explain the idea of whether an intelligence operation is fit for purpose, consider intelligence failures. In the lead up to the 2003 invasion of Iraq, there were a series of significant intelligence failures. One of the most significant was the reliance of US and then UK intelligence on a single unreliable source codenamed Curveball. This informant provided information that played a significant role in the belief that Saddam Hussein's regime had the capacity for mobile weapons manufacturing (Drogin 2007). With the benefit of hindsight, Curveball's testimony and claims would have been dismissed, and decision-makers would have admitted that there was no credible evidence of weapons of mass destruction in Iraq. We can imagine a counterfactual, in which decision-makers knew that Curveball's intelligence was deeply unreliable and would not have made the decision that they did. The reason the intelligence provided by Curveball was not fit for purpose is that it came from only one source, was not sufficiently supported by other independently sourced information, and insufficient effort was made to assess Curveball's reliability. Given the gravity of the decision being made, relying on a single source, unsupported (and indeed contradicted by other intelligence), and from an increasingly unreliable source, the specific intelligence being provided was not fit for that serious decision. Here, we have a useful general tool to ask if intelligence is fit for purpose: Given that intelligence is justified by reference to whether it improves national security decision-making, we can ask if a particular decision would have been made with better, more accurate, or more reliable intelligence. If the decision would be different, then the initial intelligence was not fit for purpose.

A reasonable challenge to this is whether this is at all practical: Surely, if decision-makers had access to the right intelligence, they would make the best decision, and hypothesising about counterfactuals does little to help us in practice. However, this is where the institutional focus becomes essential. In the case of Curveball, the intelligence operation was not fit for purpose, something only realised afterwards. But such reflection and recognition of failure should prompt wholescale review and redesign of the relevant intelligence institutions. The intelligence failures for Curveball were multiple and spread throughout the entire national security decision-making process. As such, the operational failure is indicative of a wider institutional failure. Tim Weinar's *Legacy of Ashes: The History of the CIA*, for example, argues that "the most powerful country in the history of Western Civilization has failed to create a first-rate spy service. That failure constitutes a danger to the national security of the United States" (Weiner 2008, xvii). On Weiner's account, the CIA is not fit for purpose as an institution. Less critical, but making the same point, the 9/11 Commission found that one of the main contributing factors to the successful Al Qaeda attacks on the US on September 11, 2001 was a failure of different intelligence agencies to share relevant information (National Commission on Terrorist Attacks Upon the United States 2004, 83–84). A subsequent congressional report stated that "[i]n the aftermath of the 9/11 attacks in 2001, a consensus emerged that information sharing, especially between intelligence offices and law enforcement officials, had been deficient and had contributed to the failure to detect the plot in advance" (Best Jr. 2011). Here, we see that the intelligence failings do not necessarily arise from any individual intelligence actor failing. Rather, the failure is a high-level institutional failure to properly communicate and coordinate the different sets of information they had. I thus suggest that a principle of fit for purpose ought to be included in the *ad intelligentiam* set:

> Fit For Purpose Intelligence (FFPI): Does the intelligence operation and/or institution reliably assist in national security decision making?

The final principle is that of proportionality. Proportionality is at once the most simple of principles and the most complicated, whether considering just war, just intelligence, or other applications. At its most simple, the principle of proportionality is easy to understand – one should simply choose an option which the benefits outweigh the cost. If you lost a $5:00 note while out walking, but it would cost you $10:00 in petrol to drive to where you lost the money, this would be disproportionate. The costs are more than the benefits. Proportionality is a very common and eminently sensible principle.

> A simple analysis goes like this: if my life was at risk, and your only option to save me was to punch me in the face, then the punch (relevant harm) would be proportional to saving my life (relevant benefit). However, if I was being annoyed by a fly and you punched me in the face in order to get rid of the fly, then the punch (relevant harm) would be in excess to getting rid of the fly (relevant benefit); the punch is disproportional.
>
> (Henschke 2018, 225)

However, when we start to consider proportionality in detail, it becomes far more complicated. In making a proportionality calculation, we are making a comparison between at least two different sets of things. And for that calculation to make sense, we have to clarify what comparisons are being made. "[A]s the punch example shows, the things being compared determine the assessment – saying a punch is proportional or disproportional is meaningless until we know what the punch is being compared to" (Henschke 2018, 224). To make sense of these calculations then, we can conduct proportionality assessments in at least five ways: "appropriateness of means to ends, action versus inaction, economic costs/benefits, comparison between different ends and as a comparison between a simple act and a complex action" (Henschke 2018, 224). Spelling these five assessments out, we have the following taxonomy:

- On appropriateness, the means are compared with the ends being sought. Punching me in the face to get rid of a fly is like cracking a nut with a sledgehammer, the means (punch) are excessive when compared to the ends (fly).
- On action versus inaction, proportionality instead focuses on deciding whether one should act by comparing acting with not acting. The choice is between punching me in the face versus doing nothing, so allowing the fly to remain. On this, it seems that acting (punching me) is excessive compared to doing nothing.

- A third way "simply" compares the costs and benefits. For example, if you and I have a $500 bet that you cannot punch the fly that is resting on my face, then (maybe) the benefits ($500) outweigh the cost (me being punched).
- A fourth way of understanding proportionality instead assumes that one must act and then seeks guidance by comparing different ends – in order to avoid the fly, we compare punch in the face with moving inside. One option (punching) seems excessive compared to the other option (moving inside).
- Finally, we compare a simple act with a complex action. For instance, a simple act, punching me to kill a fly is excessive. But compare this to a situation where I have a deadly fear of flies and am driving a bus full of people on a busy freeway. Assuming that there is no other way to kill the fly, the fly must be killed immediately, lest I lose control of the car, and you alert me to the fact you are about to punch me, then on complex set action, punching me is no longer excessive (Henschke 2018, 224–225).

Following this taxonomy, the relevant proportionality considerations for intelligence, we need to ask if the means being used are proportionate to the ends. This goes directly to the JCI and utilises Bellaby's ladder of escalation. We need also to ask if the action of intelligence is preferable to *inaction*. While this might seem fairly easy – insofar as intelligence is an epistemic activity, then surely it is better to know what is happening than to be in a state of ignorance. However, we must also ask what the risk of the intelligence operation being discovered is and if the costs of that will be significant or not. For instance, the public disclosure that the US had spied on Angela Merkel, leader of an allied nation, may have done more damage than if they had not spied on her. In terms of the costs, here we would be interested in the economic costs of a particular intelligence operation and the economic costs of running an intelligence institution. In particular, if they fail the fit for purpose intelligence (FFPI) principle, then they would be disproportionate. The fourth way of considering proportionality would then consider the range of options at hand. Note that this would be intelligence in contrast with war, diplomacy, etc. and would also need to compare different intelligence operations. "In intelligence work, the preferred way of collecting the relevant information entails a lesser or no ethical risk – for example from open sources" (Omand and Phythian 2018, 84). Obviously, here we see a bleed between this notion of proportionality and the logical resort principle.

Assuming that they give the same support to decision-making, some intelligence operations, like open source intelligence, would be preferable to invasive surveillance, covert operations, etc. So, the PI, simply stated, might look like *the good of the intelligence actions should outweigh the bads*. However, as just stated, in order for this to actually be useful, we need to add some more detail to it.

> Proportionality for Intelligence (PI): the good of the Intelligence actions should outweigh the bads, including comparisons between the appropriateness of means to ends, compared to inaction, economic costs and benefits, across a range of different options, and between simple acts and complex actions.

By adding detail and nuance to the PI, we have a better and more useful principle to guide action.

Conclusion

The basic points being made in this chapter are that intelligence practices and institutions require a set of moral principles in order to engage in joint epistemic actions that serve national security in a competitive environment. Much like the questions around use of organised force in warfare, we agree with the work done by Bellaby, Omand, Pythian, and others that draws from the JWT to develop a JIT. Where we differ, however, is in the explicit recognition of the particular ways that the practice of intelligence and the importance of the role that intelligence institutions play in how to develop and apply the principles of just intelligence.

This allows us to develop and present a form of moral exceptionalism in which the principles of *jus ad bellum* are the starting point to develop principles for *jus ad intelligentiam*. We do not seek to reject those principles, as the JWT provides a deep well from which to draw inspiration and guidance. Instead, we have argued that intelligence practices and institutions are unique, and the principles must be developed to match the reality of intelligence. We thus offer these six criteria for *jus ad intelligentiam*:

Just cause for intelligence (JCI): A's purpose in undertaking these intelligence activities is to enable decision-making that protects against any national security threat posed by B and/or to enable decision-making that gives a competitive national security advantage against B.

Right intention for intelligence (RII): A undertakes these intelligence activities only for the ultimate purpose of enabling the protection against or the competitive advantage over the threat to its national security posed by B.

Legitimate authority of intelligence (LAI): A's intelligence agencies are collecting, analysing, and disseminating the intelligence in question under a legitimate political authority.

Logical resort for intelligence (LRI): As A's awareness of a potential national security threat increases, more intelligence operations that serve national security are permitted.

Fit for purpose intelligence (FFPI): Does the intelligence operation and/or institution reliably assist in national security decision-making?

Proportionality for intelligence (PI): the good of the intelligence actions should outweigh the bads, including comparisons between the appropriateness of means to ends, compared to inaction, economic costs and benefits, across a range of different options, and between simple acts and complex actions.

As with the JWT, these six principles are likely to be controversial and contested. There will be debate about the particular formulation of each principle, over its inclusion in the *jus ad intelligentiam*, how each of these principles works in relation to the other principles, whether each must be met, and to what degree, in order for a particular intelligence operation to be considered just. However, much like the JWT, we consider this a strength of the JIT. By outlining a set of criteria, we hope not only to improve particular decision-making but also to increase the tools that are used to reflect upon intelligence decisions.

Naturally, this analysis is so far incomplete. One of the great strengths of the JWT is the separation of analysis into *jus ad bellum* and *jus in bello*. Following the work of Jeff McMahan, particularly his publication of *Killing in War* (McMahan 2009), much recent scholarship on the JWT has explored and challenged this distinction between the decisions around going to war and the decisions made in war. However, one stands on this discussion, the distinction is highly useful to help focus attention on very different aspects of intelligence practice. Chapter 4 looks more closely at the decisions made in regard to specific intelligence practices, the *jus in intelligentia*.

Notes

[1] I note here that this is deliberately simplified and lacks any nuance or sophistication. On a more considered utilitarian reasoning, for instance, it might be permissible to poison someone to avert some larger catastrophe. I return to this point later in this section.

[2] See, for instance Frame 2015; Dobos 2023; Bandura 2002.

[3] Thucydides is often presented as "a political realist, not an idealist or "just war" thinker" (Reichberg, Syse, and Begby 2006, 3). However, as Cian O'Driscoll argues, there is perhaps more of a connection between Thucydides and the just war tradition (O'Driscoll 2014).

[4] See, for instance McMahan 2009.

[5] Phillip Knightly, for instance, uses the phrase as the title to his book on the recent history of spies and spying (Knightley 1980).

[6] See, for example: (Walzer 2006; Orend 2013; McMahan 2009; Coates 1997; Steinhoff 2007; French 2005).

References

Allhoff, Fritz. 2012. *Terrorism, Ticking Time-Bombs, and Torture*. Chicago: University of Chicago Press.

Allhoff, Fritz, Adam Henschke, and Bradley Jay Strawser, eds. 2016. *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press.

Andrew, Christopher. 2019. *The Secret World*. London: Penguin Random House.

Bandura, Albert. 2002. "Selective Moral Disengagement in the Exercise of Moral Agency". *Journal of Moral Education* 31(2): 101–119. https://doi.org/10.1080/0305724022014322

Bellaby, Ross. 2014. *The Ethics of Intelligence*. Abingdon: Routledge. https://doi.org/10.4324/9780203383575

Best Jr., Richard A. 2011. "Intelligence Information: Need-to-Know vs. Need-to-Share". Washington DC: Congressional Research Office. www.fas.org/sgp/crs/intel/R41848.pdf

Brunstetter, Daniel. 2016. "Jus Ad Vim: A Rejoinder to Helen Frowe". *Ethics & International Affairs* 30(1): 131–136.

Coates, Tony J. 1997. *The Ethics of War*. Manchester: Manchester University Press.

Dobos, Ned. 2023. “Pharmacological Prophylaxes against Moral Injury”. *Monash Bioethics Review*. https://doi.org/10.1007/s40592-022-00167-3

Drogin, Bob. 2007. *Curveball: Spies, Lies and the Man behind Them: The Real Reason America Went to War in Iraq*. New York: Ebury Press.

Faini, Matteo. 2020. *Spies and Their Masters: Intelligence–Policy Relations in Democratic Countries*. Abingdon: Routledge.

Farrell, Paul. 2016. “Lamb Chop Weight Enforcers Want Warrantless Access to Australians’ Metadata”. *The Guardian*, January 19. www.theguardian.com/world/2016/jan/19/lamb-chop-weight-enforcers-want-warrantless-access-to-australians-metadata

Ford, Shannon Brandt. 2013. “Jus Ad Vim and the Just Use of Lethal Force-Short-of-War”. In *Routledge Handbook of Ethics and War: Just War in the 21st Century*, edited by Fritz Allhoff, Nicholas G. Evans, and Adam Henschke. 63–75. Abingdon: Routledge.

Frame, Tom, ed. 2015. *Moral Injury: Unseen Wounds in an Age Barbarism*. Sydney: UNSW Press.

French, Shannon E. 2005. *Code of the Warrior: The Values and Ideals of Warrior Cultures throughout History*. New York: Rowman & Littlefield.

Gross, Michael L. and Tamar Meisels. 2017. *Soft War: The Ethics of Unarmed Conflict*. Cambridge: Cambridge University Press.

Henschke, Adam. 2018. “Conceptualising Proportionality and Its Relation to Metadata”. In *Intelligence and the Function of Government*, edited by Daniel Baldino and Rhys Crawley. 221–242. Carlton: Melbourne University Press.

Henschke, Adam. 2021. “Ethics and National Security: A Case for Reasons in Decision-Making”. In *The Palgrave Handbook of National Security*, edited by Michael Clarke, Adam Henschke, Matthew Sussex, and Tim Legrand. 73–92.Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-53494-3

Jacobsen, Annie. 2019. *Surprise, Kill, Vanish: The Secret History of CIA Paramilitary Armies, Operators, and Assassins*. London: Hachette UK.

Kant, Immanuel. 1997. *Groundwork of the Metaphysics of Morals*. Edited by Mary Gregor. Cambridge: Cambridge University Press.

Knightley, Phillip. 1980. *The Second Oldest Profession: Spies and Spying in the Twentieth Century*. London: W. W. Norton & Company.

McMahan, Jeff. 2009. *Killing in War*. Oxford: Clarendon Press.

Miller, Seumas. 2021. “Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity”. *Social Epistemology* 35(3): 211–231.

National Commission on Terrorist Attacks Upon the United States. 2004. “The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States”. Washington, DC: US Government.

O’Driscoll, Cian. 2014. “Thucydides and the Just War Tradition: Unlikely Bedfellows?” In *A Handbook to the Reception of Thucydides*, edited by Christine Lee and Neville Morley, 373–390. Hoboken: Wiley-Blackwell.

Omand, David and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Oxford: Oxford University Press.

Orend, Brian. 2013. *The Ethics of War*. 2nd ed. Vancouver: University Of Alberta.

Quinlan, Michael. 2007. “Just Intelligence: Prolegomena to an Ethical Theory”. *Intelligence and National Security* 22(1): 1–13. https://doi.org/10.1080/02684520701200715

Reichberg, Gregory, Henrik Syse, and Endre Begby, eds. 2006. *The Ethics of War: Classic and Contemporary Readings*. Hoboken: Wiley-Blackwell.

Robillard, Michael and Bradley J. Strawser. 2016. “The Moral Exploitation of Soldiers”. *Public Affairs Quarterly* 30(2): 171–195.

Shue, Henry. 2008. “Do We Need a ‘Morality of War’?” In *Just and Unjust Warriors: The Moral and Legal Status of Soldiers*, edited by David Rodin and Henry Shue. 401–428. Oxford: Oxford University Press.

Steinhoff, Uwe. 2007. *On the Ethics of War and Terrorism*. Oxford: Oxford University Press.

Vallor, Shannon. 2014. “Armed Robots and Military Virtue”. In *The Ethics of Information Warfare*, edited by Luciano Floridi and Mariarosaria Taddeo, 169–185. New York: Springer.

Walzer, Michael. 2006. *Just War and Unjust Wars*. 4th ed. New York: Basic Books.

Weiner, Tim. 2008. *Legacy of Ashes: The History of the CIA*. New York: Anchor.

4 National Security Intelligence Activity

The Principles of Discrimination, Necessity, and Proportionality

Seumas Miller

While the so-called just intelligence theory (JIT) – comprising *jus ad intelligentiam* and *jus in intelligentia* – provides a useful starting point in the construction of a normative framework for national security intelligence activities, ultimately it may not be serviceable, first, in respect of some of the particular constitutive principles and, second, in respect of its fundamental division between jus ad bellum and jus in bello, or rather in its application to national security intelligence, between jus ad intelligentiam and jus in intelligentia. Regarding the first point, consider the just war theory (JWT) principle of last resort. While war ought to be a last resort, intelligence collection and analysis ought to be a first resort. Regarding the second point, consider that the practices of national security intelligence collection and analysis, and the principles that govern these practices, such as the principles of necessity and proportionality, continue in a more or less seamless manner before, during, and after the waging of war. Thus, while it is not morally permissible for combatants to deliberately shoot dead the combatants of an adversarial nation state during peacetime, it is morally permissible, and perhaps morally obligatory, for intelligence officers to collect and analyse intelligence about an adversarial nation state during peacetime (as well as during war). This is, of course, not to say that what might count as necessity or proportionate national security intelligence collection activity during war does not differ from what might so count during peacetime.

On the other hand, some constitutive principles of JWT are, appropriately revised, applicable to national security intelligence activity, notwithstanding the essentially epistemic character of intelligence activity. Specifically, analyses are offered in this chapter of the key principles of discrimination, necessity, and proportionality (Miller 2022a, 2022b, 2021a, 2021b). Importantly, the principle of necessity has been 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. In doing so, a threefold distinction is invoked, namely, that between the macro-, mezzo-, and

DOI: 10.4324/9781003106449-5

micro-institutional levels. Our concern in the last section of this chapter will be with the mezzo-institutional level (e.g. the establishment of bulk databases by security agencies for national security purposes) and the micro-institutional level (e.g. the conduct of a specific operation utilising data from a bulk database).

The Principle of Discrimination

Consistent with relevant liberal democratic regulatory regimes, harmful internal (at least) national security intelligence activities are, or ought to be, conducted in accordance with the principles of necessity and proportionality. Moreover, in the context of JWT (Walzer 1997) these principles are typically applied in conjunction with a third principle, namely, the principle of discrimination[1] (Green 1993).The principle of discrimination, or rather the various analogues of the principle of discrimination (given that, strictly speaking, this principle only applies to combatants engaged in war), is involved in national security intelligence activities insofar as it is generally assumed that innocent persons ought not to be deliberately harmed or have their rights violated. Accordingly, it would be one thing for police to intercept and access the metadata and content of the phone calls and emails of a known terrorist or foreign espionage agent on an ongoing basis for intelligence purposes, and quite another for this to be done to an ordinary citizen known to be innocent of any crime, for example, on the off chance that some useful intelligence might be picked up (Miller and Gordon 2014). Surveillance of the terrorist or spy would, in this instance, be a *morally justified infringement* of the right to privacy (Miller and Gordon 2014; Miller 2009), whereas surveillance of the innocent citizen would evidently be a *violation* of the right to privacy. Accordingly, the principle of discrimination (or, at least, an analogue of it) ought to be applied to national security intelligence activities. However, its application in these activities is somewhat different from its application in kinetic military and policing contexts. Speaking generally, its application to national security intelligence activities is far more permissive.

Importantly, unlike the targets of, for instance, military combatants (Miller 2016a), the targets of intelligence activities can sometimes be innocent civilians, for example, deliberately and deceptively gaining information about a terrorist from the terrorist's innocent relative might be morally justified, whereas deliberately killing the terrorist's innocent relative would certainly not be. Moreover, intelligence activities ultimately aimed at identifying terrorists and thwarting acts of terrorism often now involve the application of machine learning techniques to bulk databases that consist mainly of the communication and other data of innocent civilians – indeed, frequently innocent fellow citizens, as well as innocent foreign citizens. In other words, the data of innocent civilians are deliberately collected and accessed (or, at least, filtered and accessed).

It can be argued that while the bulk data of these innocent persons are "read" by a machine or, perhaps, "seen" by human eyes in an anonymised form, it is for the most part not seen (in the appropriate privacy infringing sense).[2] Of course, the particular data items that result from the application of the machine learning process are de-anonymised and, ultimately, seen by human eyes; however, the argument might continue, such data meet the standard of reasonable suspicion already applicable to intelligence gathering/investigation by law enforcement agencies, and does so by virtue of being the result of that very process. Whatever the merits of this argument as a justification for the application of machine learning techniques to bulk databases by way of mitigating the degree and extent of intrusion into the privacy of innocent citizens (Sorell 2018; Miller 2018b), nevertheless, this intrusion into the privacy of innocent civilians is deliberately done, albeit as a means to an end. As such, it is not analogous to the principle of discrimination as it applies to the use of lethal force by combatants in war; combatants, to reiterate, are not permitted to *deliberately* kill innocent civilians (whether they be civilians of the enemy state or not), even as a means to some further legitimate end. The reason for this difference between the principle of discrimination as it applies to intelligence activities and as it applies to the use of lethal force reflects the much greater moral significance that attaches to deliberately overriding an innocent person's right to life than to deliberately overriding their right to privacy. This difference, in significance, in turn, reflects, indeed, in large part, is derived from, the much greater moral weight that attaches to life than to privacy. Hence, there is a (more or less) absolute legal prohibition on deliberately killing the innocent (even in wartime), but not on deliberately overriding their privacy (even in peacetime).

A final point regarding the principle of discrimination as it applies to national security intelligence activities pertains to differences between internal and external national security threats. Intelligence activities directed at external threats to national security, for example, threats posed by foreign powers, are much less constrained than those directed at internal threats, for example, home-grown terrorists; indeed, in war, there are few, if any, constraints on intelligence activity. Arguably, this is not how it should be; after all, the innocent citizens of enemy authoritarian states do have moral rights, including privacy rights (whatever their legal rights might be or, more likely, not be). However, it does seem that, given the purpose of the intelligence activities in question is national security, and governments and their security agencies have special *partialist* duties in respect of their own citizens (Miller 2016a, chap. 3), it is to be expected that the principle of discrimination and, for that matter, the principles of necessity and proportionality might justifiably be applied in a more permissive manner externally than internally.

The Principle of Necessity

The principle of necessity,[3] that is of interest in this chapter, is applied in circumstances in which harm (including, for ease of exposition, in the sense of the infringement of a moral right[4]) is typically caused by members of security agencies, including members of national security intelligence agencies, to those targeted in their operations and caused by virtue of the inherently harmful method used, for example, surveillance (infringement of the right to privacy), arrest (infringement of the right to freedom of movement), and use of lethal force. The principle of necessity is typically illustrated by recourse to a standard situation of personal self-defence in which the defender (Defender) has a choice between these two (effective) means (harmful methods) to preserve his or her life – killing or disarming his or her attacker (Attacker). It is generally held that he or she ought to disarm Attacker since it is *not necessary* for him or her to kill Attacker.[5] By parity of reasoning, if an intelligence officer (Officer) has a choice between two (effective but harmful) means to collect information on a suspected terrorist or spy (Suspect), who is, let us assume, operating in the Officer's domestic environment – namely, either to collect metadata from Suspect's phone or to intrusively surveil Suspect by means of miniature cameras and listening devices placed in his home – Officer ought to simply rely on metadata since it is *not necessary* to engage in intrusive surveillance. However, from the mere fact that one of two available means is not necessary to realise some end, it does not follow that it ought not to be chosen. After all, ex hypothesis, neither of the two available means is a necessary means to achieve the end in question (given the other one is available), and it would be irrational (other things being equal) not to choose any of the available means to one's ends.

What is going on here? Clearly, the idea is that the less harmful means morally ought to be chosen, and the harm in question is harm to the target, for example, to Attacker or to Suspect. In our self-defence example, Defender ought to choose to disarm Attacker rather than kill him because disarming Attacker is the less harmful means to achieve the end of preserving Defender's life. Likewise, in our intelligence example, Officer ought to choose to collect Suspect's metadata but not his communicative content and visual data since this is the less harmful means – being less of an infringement of Suspect's privacy[6] – to achieve the end of acquiring the desired information.

However, *qua means to the end of preserving Defender's life*, disarming Attacker is no better than killing Attacker. Indeed, disarming Attacker might be a worse choice qua means to that end since, for example, it might be less effective (the chances of failure are greater) or less efficient (the effort required is greater) than killing him or her. Again, qua means to the end of acquiring information, accessing Suspect's metadata is no better in our scenario (we have assumed) than intrusively surveilling Suspect. Indeed, if anything, merely accessing Suspect's phone metadata is presumably a worse choice qua means to that end since, for example, it might be less effective (some relevant information might only be found in the content of his or her conversations or from the visual data). Nevertheless, it might continue to be insisted that the less harmful means morally ought to be chosen. Why so? Evidently, there is another end in play here. The end in question is the moral end to minimise harm to persons from which can be derived the moral principle to minimise harm to targets. Moreover, given the possibility of so-called collateral damage, there is also the derived principle of minimising harm to bystanders. Further, given the possibility of harm being done by targets or third parties to the user of harmful methods, we can derive a third principle from the general moral end of minimising harm to persons; the principle of minimising harm to the users of the harmful methods in question, such as Defender, police officers and intelligence officers (who will, in each case henceforth in this section, for ease of exposition, be referred to as operators, i.e. users of a harmful method). We return to this threefold distinction between minimising harm to targets, bystanders, and operators later.

As we have seen, in each of our scenarios, there is a harmful means to an end. However, in each of our scenarios, there are two *conceptually independent* ends, for example, in our personal self-defence scenario, the end of preserving Defender's life and the end of minimising harm to Attacker. While conceptually independent, these two ends can come into conflict under some circumstances, for example, in a self-defence scenario in which Defender must kill Attacker or be killed by Attacker. In the intelligence collection scenario, there is the end of collecting the desired intelligence and – as in the self-defence scenario – the end of minimising harm to those from whom intelligence is being collected, in particular (although the harm minimisation in question is typically that of minimising the degree or extent of infringement of the right to privacy). In each of the two scenarios, the two ends are conceptually independent. This is obvious from the fact that one could have as an end to defend oneself and yet not have as an end to minimise harm to others.[7] This may well be so if, for instance, Defender decides to kill Attacker to preserve Defender's life, notwithstanding that Defender could easily have chosen the equally effective means of disarming Attacker. Likewise, the conceptual independence of the two ends in play in the intelligence collection scenario is obvious, since one could have as an end to collect the desired intelligence and yet not have as an end to minimise harm to targets (by minimising the degree and extent of the infringement of privacy rights). This may well be so if, for instance, Officer decided to intrusively surveil the target, notwithstanding that Officer could easily have chosen the equally effective means (let us now assume) of relying exclusively on the metadata.

So, we need to distinguish between two conceptually independent ends in the application of the necessity principle in both self-defence scenarios and intelligence collection scenarios: the end definitive of the activity in question (e.g. preserving one's life, acquiring national security intelligence) and the end of minimising harm to the target. However, in discussing applications of the principle of necessity, we also need to stress the differences between the ends definitive of kinetic activity, such as interpersonal self-defence, and the ends definitive of intelligence activity. Clearly, the ends definitive of intelligence activities (e.g. knowledge of terrorists, or foreign espionage agents, and their plans) and those definitive of kinetic activities (e.g. arrest of suspects, destruction of enemy military forces) are different and, accordingly, the end implicit in the application of the principle of necessity in an intelligence collection context will be different. Moreover, the (harmful) means to realise the ends definitive of intelligence activities and to realise the specific ends implicit in an application of the necessity principle in an intelligence collection context will also be different.[8] So drawing analogies between military, law enforcement, and national security intelligence activities in respect of the principle of necessity relies on moving to a high level of abstraction. Further, in intelligence activities, the notion of necessity in play is very often a permissive one. For instance, intelligence activities that utilise bulk data are often not necessary, strictly speaking, rather they are the most effective – and perhaps least resource intensive – means to a national security end (see later).

The description of the principle of necessity, that has been provided thus far, omits a key feature of this principle as it operates in the contexts in question, namely, that its constitutive end – that of preserving Defender's life or, in the other scenario, of collecting desired intelligence – is a moral end (i.e. identifying, neutralising, or mitigating a national security threat, we are assuming). Accordingly, the principle of necessity is not, after all, *merely* a principle of rationality, rather it has, in the contexts in question, a moral loading by virtue of the moral quality of the ends in play. Accordingly, it is, after all, a moral principle, at least in these contexts. What morally justifies Defender's act of killing Attacker is, in part, the moral weight attaching to Defender's life, the preservation of which is Defender's end. It is also true that preserving Defender's life (the end) needs to be weighed against the loss of Attacker's life (the harmful means). Specifically, the moral principle of proportionality applies in relation to weighing morally significant ends and means. Moreover, an analogous argument operates in the case of intelligence collection that is the means to a legitimate national security end (e.g. removing the terrorist threat to innocent lives). Officer's acquisition of the national security intelligence (the end) needs to be weighed against the infringement of Suspect's right to privacy (the harmful means).

Now neither the negative moral weight of the harmful method nor the positive moral weight of the end of preserving Defender's life or of collecting national security intelligence is constitutive of the necessity principle *qua principle of necessity.* The necessity principle qua principle of necessity pertains to the necessity of a means (Defender killing Attacker or Officer infringing Suspect's right to privacy) to an end (preserving Defender's life or Officer acquiring national security intelligence, respectively). But, evidently, an action is a means to an end irrespective of the moral quality of either the action or the end that it serves.[9] Moreover, an action that is a necessary means to some end is a *necessary* means irrespective of the moral quality of the action or its end. Nevertheless, the principles of necessity, or rather principle of necessity, as they apply in the interpersonal, military, law enforcement, and national security intelligence contexts in question, are moral principles by virtue of their implicit reference in each case both to a harmful means and a moral (indeed, morally worthy, let us assume) end. So each of these principles of necessity is a moral principle at the core of which is a means/end principle of rationality; and each of these principles of necessity *qua principle of necessity* is merely a principle of rationality.

The upshot of the discussion thus far is that the principles of necessity in the institutional contexts in question (military, law enforcement, and national security intelligence) are moral principles, each of which has at its core a means/end principle of rationality. The means/end principle of rationality states that (other things being equal) one ought to choose the means to one's ends and, if there is a necessary means, then one ought to choose it. However, each principle of necessity is different from the others by virtue of the different moral ends in play in these various institutional contexts (as well as, typically, the different harmful means used in the service of these ends). Thus, in military contexts, the principle of necessity is referred to as the principle of military necessity and implicitly refers to the moral end of winning the war, battle, or other military engagement in question. On the other hand, in a law enforcement context, the principle of necessity might refer to the moral end of preserving the life of the defender, be that a citizen or the officer himself/herself. By contrast with these essentially kinetic ends, the principle of necessity, as it applies in national security intelligence activity, has an epistemic (and morally significant) end: to acquire knowledge relevant to the protection of national security.

Moreover, as we saw earlier, these principles of necessity are applied in circumstances in which harmful methods are being used, notably, by members of security agencies (the operators) against their targets but also in interpersonal contexts by, for instance, Defender against their Attacker. Accordingly, as also mentioned, there is a harm minimisation principle associated with each of these principles of necessity. The harm minimisation principle is a principle of morality, and it states that one ought to minimise harm to persons and, therefore, if there are two (or more) means to a given end, then (other things being equal) one ought to choose the least harmful. Of course, to reiterate, the ends specified in the family of related principles of necessity applicable in different security contexts vary. As will become clear, this point is also relevant to our understanding of the harm minimisation principle, and, therefore, it is important to reflect on its scope in the interpersonal self-defence, kinetic military, kinetic law enforcement, and national security intelligence contexts of its application. In each of these contexts, we need to keep in mind the threefold distinction, made earlier, with respect to the harm minimisation principle, namely, harm to targets, harm to bystanders, and harm to operators (i.e. to reiterate, Defender, police officer, intelligence officer, or combatant using the harmful method in question). It is only the *harm to target* version of the harm minimisation principle that has been identified earlier as implicated in the versions of the necessity principle thus far discussed. This is to be expected, given the circumstances in question all involve the use of harmful methods by the operator (e.g. intelligence officer) against the target.[10]

Let us consider further the various harm minimisation principles implicated in different versions of the principle of necessity. The harm minimisation principle in play in the application of the principle of necessity in internal national security intelligence operations is focused on minimising harm to the criminal or suspected criminal (as well as to innocent third parties, i.e. (typically) fellow citizens of the intelligence officers), that is, it is the harm to targets version of the principle (and also the harm to bystanders version). As such, it is not focused on minimising harm to the intelligence officer, himself/herself, that is, the one conducting the surveillance or collecting and analysing the data (the operator). Indeed, there is, typically, no need to go beyond the minimise harm to targets principle (and, perhaps, minimise harm to bystanders principle) and invoke the minimise harm to operators principle in such contexts unless, of course, the intelligence officer is an informant or undercover operative. Consider, by contrast, kinetic law enforcement, that is, situations involving the use of lethal force (in particular) by police officers. In this latter case, police officers ought to minimise harm to themselves (as well as to offenders and to innocent members of the public). As such, the minimise harm to operators principle seems applicable and, indeed, is implicated in the application of the necessity principle in these contexts. The principle that police officers should not use lethal force against a suspect unless it is necessary implies, first, that they ought not do so if there are non-lethal methods available (minimise harm to the target) or if using lethal force would put the lives of bystanders at serious risk (minimise harm to bystanders), but, secondly, that. they may do so if to do otherwise would put their own lives at serious risk (minimise harm to operators).[11]

Now, consider kinetic military operations and, in particular, the harm minimisation principle implicated in the principle of military necessity. Here, there is also a dis-analogy with respect to harm minimisation as it applies to intelligence activities. The harm minimisation end implicated in the principle of military necessity applies when war is already underway and, important to our concerns here, might *not* have a focus on minimising harm to enemy combatants in, for instance, an ambush or firefight. Indeed, quite the reverse, in such circumstances, it might be focused on *maximising* harm to enemy combatants, for example, if the most effective military strategy is to degrade enemy forces. So the harm minimisation principle implicated in the principle of military necessity is *not* the principle of minimising harm to targets, rather it is the principle of minimising harm to bystanders (as opposed to targets). In this respect, the harm minimisation principle implicated in the principle of military necessity is also dis-analogous to the harm minimisation principle implicated in the principle of necessity, as it applies in law enforcement, since the police ought to minimise harm to criminals, and as it applies in internal national security intelligence activity, since intelligence officers ought to minimise harm to targets in their domestic intelligence activities (if not in their foreign intelligence activities – see Chapter 5). Related points can be made with respect to the operation of the principle of proportionality. If it was necessary to slaughter most of a much larger enemy force in order to win a battle, this would not necessarily be regarded as a disproportionate measure, assuming innocent civilians' lives and the lives of one's own combatants – belonging to the much smaller armed force – were not put at significant risk. One reason for this difference is evidently that in internal (at least) national security operations, as in law enforcement, more generally, there is a presumption of innocence and, therefore, a strong presumption in favour of refraining from harming criminals, that is, prior to conviction "criminals" are, legally speaking, merely suspects .

The Principle of Proportionality

What of the principle of proportionality? In the light of our earlier analysis of the necessity principle in terms of a means/end principle of rationality at its core, a moral end, and an implied principle of harm minimisation in its contexts of use, what is to be morally weighed in applications of the proportionality principle? As already mentioned, the application of the principle of necessity in the earlier described scenarios requires moral weight to be attached to the relevant moral ends in question (e.g. the life of Defender, the national security intelligence collected, winning the battle), relative to the harm caused by the harmful means, for example, the death of Attacker, infringement of privacy, foreseen but unintended death of some innocent civilians. Moreover, obviously the ends in question need to be (actually or prospectively) realised if they are to be given moral weight; so, the use of the harmful methods needs to be successful. As we have seen, the harm done as a result of the use of harmful methods is (at least potentially) harm to the target, to bystanders, and/or to the operator (e.g. the user of the harmful method). However, as we have also seen, not all of these harms are present in some settings, for example, there might be no harm done (or in prospect of being done) to intelligence officers engaged in surveillance; and not all of these harms, even if present, are necessarily given negative moral weight in the application of the proportionality principle in a given institutional setting, for example, harm done to enemy combatants might not be. It follows from this that there are different versions of the proportionality principle in play in different institutional settings (as, we saw, was the case with the necessity principle). However, speaking generally, the proportionality principle ascribes positive moral weight to the ends realised (the ends constitutive of self-defence, law enforcement, national security intelligence activity, or military action) and negative moral weight to the harms caused by the use of harmful means. This is, in part, simply a reflection of a general principle of rationality. After all, other things being equal, it is surely irrational to choose to perform an action as a means to one's end in circumstances in which the benefit (or moral good) of the end is outweighed by the cost (including moral cost) of the means. To this extent, the application of the principle of necessity implies the application of a principle of proportionality with respect to means and end. However, the various proportionality principles give negative moral weight to some harms that are not part of the means to the end, for example, harms to bystanders. Indeed, in theatres of war – settings in which the principle of military necessity applies – the accompanying principle of proportionality is largely focused on avoiding disproportionate harm to bystanders, that is, to innocent civilians (Walzer 1997).

Note that the necessity principle and all relevant harm minimisation principles might be complied with and yet the proportionality principle not be complied with. Thus, in order to prevent a pickpocket escaping, it might be necessary for a police officer to shoot the pickpocket in the leg, and this might be the least harmful means available, for example, the only alternative to allowing the pickpocket to escape would be for the officer to shoot the pickpocket dead. However, this action would be disproportionate. So, compliance with the necessity principle and all relevant harm minimisation principles is not a sufficient condition for compliance with the proportionality principle. Conversely, it is possible to comply with the proportionality principle and yet fail to comply with relevant harm minimisation principles. It might not be disproportionate for an intelligence officer to intrusively surveil a known terrorist, notwithstanding that an equally effective, less intrusive means was available. However, to do so would be a failure to comply with the principle of minimising harm to targets and, given the latter is (as we saw earlier) implicated in the relevant necessity principle, it would also be a failure to comply with the necessity principle.

Please also note that the proportionality principle presupposes the application of the principle of discrimination. Thus the *deliberate* bombing of these innocent civilians (as opposed to their foreseeable but unintended deaths) is ruled out by the principle of discrimination, irrespective of any proportionality considerations. As we saw earlier, by contrast with the bombing of innocent civilians, the principle of discrimination, as it applies to intelligence collection, is far more permissive. Does the principle of proportionality, nevertheless, presuppose the principle of discrimination in national security intelligence activities?

Harm in terms of privacy infringements is easy or, at least, easier to justify in the case of suspects – and certainly known offenders, for example, known terrorists – than in the case of innocent citizens. Hence, the application of the principle of proportionality presupposes the principle of discrimination in play; it might be disproportionate to collect intelligence by means of an intrusive method from a person believed to be innocent of any serious crime but not disproportionate if the target were a known terrorist or foreign spy.

Jus ad intelligentiam, Jus in intelligentia, and the Mezzo-/Micro-Level Distinction

Whereas there is a relatively clear-cut distinction between the decision to wage war and decisions made in the actual conduct of war and, therefore, between the jus ad bellum and the jus in bello, matters are somewhat different when it comes to national security intelligence collection/analysis/dissemination and, therefore, the (alleged) distinction between the jus ad intelligentiam and the jus in intelligentia. National security intelligence activity (i.e. collection, analysis, and dissemination) is a continuous, ongoing, more or less seamless (indeed, cyclical – hence, the so-called intelligence cycle) activity in relation to threats and enemies that come and go; unlike war, it has no determinate end state, the cessation of hostilities that is being aimed at (perhaps understood in terms of winning the war).[12] Moreover, national security intelligence activity does not mirror kinetic activity, such as waging war, but rather stands to it in the general relationship of knowledge to action, that is, as its logical precursor. Accordingly, the existence and application of the alleged jus ad intelligentiam/jus in intelligentia dualism – as opposed to the existence and application of particular constitutive principles, for example, the principles of necessity and proportionality – is, to say the least, open to question; there seems to be a lack of conceptual fit between the phenomenon (national security intelligence activity) and this dual theoretical framework.

That said, national security intelligence activity exists at macro-, mezzo-, and micro-institutional levels (at least, and as long as these distinctions are understood as being a fairly loose ones). Our interest here is with the distinction between the mezzo- and the micro-institutional levels. The micro level is the level of specific operations. This is the level which has been the focus of most of the discussion earlier, a level at which the principles of discrimination, necessity, and proportionality are manifestly applied. But national security intelligence activity also exists at a mezzo level in a manner that has implications for the application of the principles of necessity and of proportionality, in particular. Consider, in this connection, national security intelligence bulk data collection.

At the micro level, the application of the principles of necessity, proportionality, and discrimination is on specific intelligence operations directed at particular targets, for example, collecting information concerning the associates of a suspected terrorist. Questions to be addressed include the following ones: Is intrusive surveillance necessary and proportionate? Would the less intrusive collection of metadata to determine callers/persons called be sufficient? Our focus thus far in this chapter has been on the micro-institutional level. But what of the mezzo level?

Key ethical issues at the mezzo level pertain to the necessity and proportionality of the establishment and general uses of the bulk databases themselves.[13] In his influential UK report, David Anderson (Anderson 2016) distinguishes between bulk interception, bulk acquisition, bulk equipment interference (e.g. hacking into computerised devices and copying material), and bulk personal data sets (e.g. electoral roles, passport databases, driving licence databases, national insurance numbers, passenger name records from flights [PNRs]). He also distinguishes between databases held by the security agencies and their accessing of databases held by other agencies, for example, private sector firms. His concern was with the former. Regarding the necessity of establishing and utilising these databases, Anderson said: "The bulk powers play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield. Where alternative methods exist, they are often less effective, more dangerous, more resource-intensive, more intrusive or slower" (Anderson 2016, chaps. 5–8)". Clearly given, for instance, the existence of alternative methods that are merely more resource-intensive, this is a relatively weak and, therefore, permissive notion of necessity.[14]

Anderson did not address the question of proportionality in his report. In order to do so, we would need to distinguish between the proportionality of establishing a particular database for national security purposes, as opposed to accessing and analysing (for national security purposes) an existing database created for a purpose other than national security. Moreover, the weight to be accorded to the right to privacy in any such application of the principle of proportionality is a complex matter, not the least because of the close (conceptual?) relationship between privacy and other fundamental rights, such as the right to individual autonomy in the context of the liberal democratic concern not to allow individual autonomy vis-à-vis the state to be compromised. Evidently, the application of the principle of discrimination at this mezzo-institutional level is problematic insofar as the databases in question necessarily contain the data of citizens innocent of any national security breach; indeed, most of the data in many of the databases in question pertain to innocent citizens. Nor is this problem necessarily entirely resolved, even if it is considerably mitigated, by virtue of, for instance (and as mentioned earlier), the anonymised form in which the personal data in these databases exist in the collection and filtering, etc. phases of the national security intelligence process.

There is also the question of the relationship of the micro level to the mezzo level (and, ultimately, of the mezzo level to the macro level) from the perspective of the application of the principles of discrimination, necessity, and proportionality. For instance, successful micro-level counterterrorism (CT) operations that rely on bulk data might be aggregated so as to justify the existence and accessing of bulk databases for national security purposes in terms of the principle of necessity (as per Anderson's report mentioned earlier). Again, taken in aggregate, the nature and extent of the infringements of privacy of innocent citizens resulting from the accessing of databases of personal information might be held not to be disproportionate to the aggregated outcomes of successful CT operations that relied on the accessing in question. Note that compliance with the principles of necessity and proportionality at the mezzo level does not entail compliance with these principles at the micro level, that is, it does not entail compliance with these principles on each and every specific intelligence collection operation. This is, in part, because micro-level operations might be ultimately justified in terms of their contribution to mezzo-level outcomes. For instance, spreading the intelligence gathering net wide and over a long period of time might enable the joining of dots on a terrorist network and its activities, notwithstanding that the accessing of the personal data of a given person, who was not a suspect but merely thought (falsely, as it turns out, let us assume) to be a potential associate, might not – *considered on its own* – be justified by the principles of discrimination, necessity, or proportionality.

The principle of proportionality needs to take into account not only the somewhat vague character of the end of national security (definitive, as we saw earlier, of the principle of necessity) and the obstacles faced by intelligence officers, for example, high-level encryption, but also potential future harms arising from national security intelligence activities and, in particular, from the utilisation of bulk data. To reiterate, privacy concerns in this area are somewhat mitigated by the fact that the bulk data collected and analysed are typically in an anonymised form (e.g. by means of machine learning techniques), and, therefore, arguably, only the privacy rights of genuine suspects are infringed or, perhaps, seriously infringed (i.e. the individuals identified upon completion of the analysis). However, these harms, such as the weakening individual autonomy vis-à-vis the state arising from extensive privacy infringements by intelligence agencies, and a diminution in public trust (a collective good [Miller 2010]) as a consequence of the secret nature of national security intelligence activities, may be incremental in character, difficult to quantify, and collective in character. Please also note that considered at the mezzo level the harms in question are potentially various in terms of the taxonomy of harms mentioned earlier. For instance, since intelligence officers are themselves citizens, their intelligence activities might turn out to be (indirectly and incrementally) a form of collective *self*-harm, given their membership of the collective harmed.

Accordingly, it can be difficult to know exactly where to draw the line between proportionate and disproportionate intelligence activities when it comes to the utilisation of bulk data for national security purposes. Consider, in this connection, the potential utilisation of integrated biometric and non-biometric databases. One prominent concern about the inadequacy of privacy protections is the potential for "function creep", where the use of information taken for a particular purpose is used for other purposes for which consent was not obtained. The underlying concern in relation to "function creep" is the one adumbrated earlier, namely, the threat to individual autonomy posed by comprehensive, integrated biometric and non-biometric databases utilised by governments and their security agencies in the service of ill-defined notions of necessity and national security and, at least potentially, without appropriate regulatory constraints and democratic accountability.

Conclusion

In this chapter, it has been argued that some of the key constitutive principles of JWT are appropriately revised, applicable to national security intelligence activity, notwithstanding the essentially epistemic character of intelligence activity. Specifically, analyses have been offered of the principles of discrimination, necessity, and proportionality. Importantly, the principle of necessity has been 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 or versions of these principles) apply, or ought to apply, to national security intelligence activity. In doing so, a threefold distinction has been invoked, namely, that between the macro-, mezzo-, and micro-institutional levels. The concern in the last section of this chapter has been with the mezzo-institutional level (e.g. the establishment of bulk databases by security agencies for national security purposes) and the micro-institutional level (e.g. the conduct of a specific operation utilising data from a bulk database).

Notes

[1] Sometimes referred to as the principle of difference.

[2] For more on bulk data and the state, see Cate and Dempsey (2017).

[3] Earlier versions of the material in this section appeared in Miller (2021a) and Miller (2021b).

[4] In other contexts, it is important to distinguish harms from rights violations, since, arguably, there can be rights violations without harm, for example, a violation of a right to privacy which is never disclosed to the person whose right to privacy is violated.

[5] There is a voluminous literature on the moral justification for killing in personal self-defence. See, for instance, Leverick (2009). Regarding the necessity principle, see, for instance, Lazar (2012). Regarding the proportionality principle, see, for instance, Hurka (2005) and Uniacke (2011, 253–272). See also Miller (2016a, 2021a, 2021b).

[6] There might also be resource considerations; intrusive surveillance is more resource-intensive. But this is another matter.

[7] And vice versa, since one could have as an end to minimise harm to other but not have as an end to defend one's own life.

[8] This is not to say that they might not, on occasion, be similar, for example, depriving a target of their freedom, or even using or threatening physical harm, in order to "loosen their tongue".

[9] There might be some exceptions to this, for example, the moral end of being treated respectfully.

[10] Naturally, there might be scenarios in which the defender could minimise harm to himself/herself by, for instance, using his or her arm to shield his or her head from a baseball bat wielding attacker, thereby, incurring a broken arm rather than a broken skull. However, such scenarios are not at issue here.

[11] Or would put the lives of bystanders at risk (minimise harm to bystanders). The applicability of two or more of the harm minimisation principles gives rise to important moral questions. If the principles come into conflict, for example, should a police officer put his or her own life at risk to save an innocent bystander's life?

[12] See Phythian (in Omand and Phythian 2018, 85) for this kind of point and Omand (in Omand and Phythian 2018, 91–92) for a response to it.

[13] David Omand recommends the distinction between laws and their application as being serviceable in the attempt to understand how jus ad intelligentiam and jus in intelligentia might relate to national security intelligence activities. See Omand and Phythian (2018, 99).

[14] Assuming, of course, that the principle of necessity is what Anderson had in mind. But if he did not have the principle of necessity in mind, what principle did he have in mind? See Macnish (2018, chap. 5) for an account of the ethical issues in this area.

References

Anderson, David W. K. 2016. *Report of the Bulk Powers Review*. Great Britain: Home Office.

Cate, Fred H. and James Dempsey (eds.). 2017. *Bulk Collection: Systematic Government Access to Private Sector Data*. Oxford: Oxford University Press.

Green, Leslie C. 1993. *The Contemporary Law of Armed Conflict*. Manchester: Manchester University Press.

Hurka, Thomas. 2005. "Proportionality in the Morality of War." *Philosophy and Public Affairs* 33(1): 34–66.

Lazar, Seth. 2012. "Necessity in Self-Defence and War." *Philosophy and Public Affairs* 40: 3–44.

Leverick, Fiona. 2009. *Killing in Self-Defence.* Oxford: Oxford University Press.

Macnish, Kevin. 2018. *The Ethics of Surveillance*. London: Routledge.

Miller, Seumas. 2009. *Terrorism and Counter-Terrorism: Ethics and Liberal Democracy*. Oxford: Blackwell.

Miller, Seumas. 2010. *The Moral Foundations of Social Institutions: A Philosophical Study*. New York: Cambridge University Press.

Miller, Seumas. 2016a. *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*. New York: Oxford University Press.

Miller, Seumas.2018b. "Machine Learning, Ethics and Law." *Australian Journal of Information Systems* 22: 1–13.

Miller, Seumas. 2021a. "Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity." *Social Epistemology* 35(3): 211–31. Doi:10.1080/02691728.2020.1855484

Miller, Seumas. 2021b. "Truth-Seeking and the Principles of Discrimination, Necessity, Proportionality and Reciprocity in National Security Intelligence Activity." In *National Security Intelligence and Ethics*, edited by Seumas Miller, Mitt Regan, and Patrick Walsh, 21–38. London: Routledge.

Miller, Seumas. 2022a "Epistemic Institutions: A Joint Epistemic Action-Based Account." *Nous-Supplement: Philosophical Issues* 32: 398–416.

Miller, Seumas. 2022b "National Security Intelligence Activity: A Philosophical Analysis." *Intelligence and National Security* 37: 791–808.

Miller, Seumas and Ian Gordon. 2014. *Investigative Ethics: Ethics for Police Detectives and Criminal Investigators*. London: Wiley-Blackwell.

Omand, David and Mark Phythian. 2018. *Principled Spying*. Oxford: Oxford University Press.

Sorell, Tom. 2018. "Bulk Collection, Intrusion and Domination." In *Philosophy and Public Policy*, edited by A. Cohen, 39–60. Lanham, MD: Rowman and Littlefield.

Uniacke, Suzanne. 2011. "Proportionality and Self-Defence." Law and Philosophy 30(3): 253–272.

Walzer, Michael. 1997. *Just and Unjust Wars*. 2nd ed. New York: Basic Books.

Part II

Practices

Just Intelligence Institutions in Action

In this part, we discuss three particularly challenging but characteristic practices of intelligence institutions. In doing so we explore and expand the concepts and principles introduced in Part I. The three practices are espionage, covert action, and PSYOP . We have chosen these three practices in part because they involve morally exceptional activities distinctive of national security intelligence activity. As such, they display the contrast with military and policing activities, and further strengthen our argument that the ethics of national security intelligence is different from military ethics and police ethics, albeit there is also some overlap. In short, these chapters serve to underpin a central thesis of this book, namely that national security intelligence practices and institutions are distinctive and call for novel ethical analyses, including ones that seemingly justify activities that are inconsistent with so-called common morality (Gendron 2005; Quinlan 2007; Marrin 2018; Miller 2016b; 2021a; 2021b; Pili 2019; Fabre 2022).

DOI: 10.4324/9781003106449-6

5 Espionage

Ends and Means

Seumas Miller

On Espionage

The activity of espionage, or, more colloquially, spying, is conducted by externally focused national security intelligence agencies, such as the CIA, MI6, Mossad, and RAW (Research and Analysis Wing – the foreign intelligence agency of India), in the service of national security, and paradigmatically concerns the collection of secret intelligence possessed and protected by hostile foreign governments. Such collection might take the traditional form of secret intelligence being passed by a so-called "mole" inside a government agency or national security intelligence agency to an adversarial national security intelligence agency. Or it might take the more recent form of cyber-espionage in which, for instance, the secret intelligence of the former is stored in an electronic database and hacked by an expert hacker employed by the latter (Miller 2016b; Miller and Bossomaier 2024).

Espionage in our favoured sense is to be distinguished from industrial espionage but also from the use of informants and undercover operatives to collect intelligence on domestic criminal organisations, including terrorist groups. That said, at times, externally focused national security agencies, such as the CIA, spy upon non-state actors operating within a foreign country, such as terrorist groups and other criminal groups, and do so for national security purposes.

Accordingly, a paradigm case of espionage is the activity of the Cambridge spy ring that comprised Anthony Blunt, Guy Burgess, John Cairncross, Kim Philby, and Donald McLean who were recruited by the Soviet Union in the 1930s and collected British secret intelligence while working for the British government in various capacities, including British intelligence agencies such as MI5 and MI6, and disseminated it to their KGB handlers in Soviet Russia. Another paradigm of espionage is the activity of double-agent Colonel Oleg Gordievsky of the KGB who eventually became head of the KGB's bureau in London and who from the mid-1970s to the mid-1980s provided secret intelligence to MI6. A paradigm case of cyber-espionage was Titan Rain. In the period 2003–2007 Chinese military hackers attacked the computers of US government agencies, and UK defence and foreign ministries. Using a variety of techniques, such as trojan horses, the hackers accessed these network computers and extracted as much data as they could (Miller and Bossomaier 2024).

DOI: 10.4324/9781003106449-7

We need to distinguish secret or confidential intelligence from open-source intelligence (OSINT). OSINT is not secret or confidential and includes such material as court reports and media reports.[1] Secret intelligence also needs to be distinguished from disinformation. Disinformation in this sense is false "information" that is deliberately presented as correct information. It includes false information that is presented as secret intelligence, such as happened in Operation Fortitude conducted during the Second World War in which false information regarding the location of the Allies' D-Day invasion was in effect communicated by the Allies to the German High Command. This deception was effected by means of the creation of "phantom" armies at various locations at which there were in fact no actual Allied armed forces. Disinformation, in this sense, also includes false "information" that is publicly disseminated, as occurs in so-called information "warfare". An example of this is the Soviet campaign, INFEKTION, waged by the KGB in the 1980s to spread the idea that the US invented AIDS.

Our concern in this chapter is with espionage as characterised earlier and, therefore, with the collection and analysis of the secret intelligence of hostile foreign states. Importantly, discrete "items" of secret intelligence, once collected and analysed, exist as elements or fragments of epistemic networks or structures and it is these fragments or networks (once they become sufficiently complete for the purpose at hand) that enable decision-makers to act on intelligence. Thus, the confirmed intelligence, indeed knowledge, that Osama bin Laden is at a particular location in Pakistan only makes sense relative to an epistemic network of known facts or beliefs about al Qaeda, its operations, that he was the leader, and remains an influential member, of Al Qaeda, and so on.

Individual items or fragments of intelligence are collected by multiple intelligence officers, diplomats, and others. Accordingly, the construction of an epistemic network or epistemic fragment, existing in the form of, say, an intelligence report, is the outcome of joint epistemic action (see Chapter 2). Accordingly, at least in principle, the contributors, including collectors and analysts, to an intelligence report disseminated to a political, intelligence, police, or military decision-maker can be ascribed collective, in the sense of joint, responsibility for that report (Miller 2006, 2015). Moreover, if the report is morally significant, as many such reports are, the contributors can reasonably be ascribed joint *moral* responsibility for it (although some may have a greater individual responsibility as elements of the joint responsibility than others [Miller 2006; Miller 2015]). Ideally, such reports, once acted upon by decision-makers, further the legitimate national security purposes of the nation state in question and, therefore, the contributors to the report are worthy of moral praise.

Thus, the collection, analysis, and dissemination of the secret intelligence of hostile foreign states is conducted by the cooperative or joint epistemic activity (Miller 2015, 2018a) of members of intelligence agencies, such as the CIA, MI6, Mossad, RAW, MSS (China's Ministry of State Security), and the FSB (Russian Federation's Federal Security Service). Accordingly, such secret intelligence activity is institutionalised joint epistemic activity that is, or ought to be, focused on matters of national security and undertaken against foreign state adversaries by intelligence officers qua institutional role occupants (assisted by others). Naturally, such activity may be undertaken in the service, not of national security but, rather, of the national interest more broadly understood. If so, it might not be morally justified. Moreover, there is a grey area in relation to informants and others involved in this activity who might or might not be regarded as institutional role occupants but rather those who assist institutional role occupant qua role occupants without themselves being role occupants. We note that intelligence collectors engaged in espionage might have a cover. However, this in itself would not entail that they are not intelligence officers. Moreover, double agents, such as Kim Philby and Oleg Gordievsky, occupy two *competing* institutional roles at the same time, in their cases one with the KGB and the other with MI6. Since these roles are in competition with one another, a person occupying both roles cannot undertake both effectively, yet, in order to function as double agents, they do need to occupy both roles.

There are various issues, or sets of issues, that are salient at this point. 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?[2] We have argued in Chapter 2 that espionage and other national security intelligence activities are ultimately justified by the collective moral good of national security. Moreover, this collective good is *in part* constituted by prior, natural (as opposed to institutional), individual, moral rights, such as personal security. We address this issue later.

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 we will assume that versions of these principles have application (although the specifics of their application to particular espionage practices, and particular non-standard instances of these practices, may well be problematic). However, we argue for an additional principle, namely, a principle of reciprocity (Miller 2016b).

In relation to the need for recourse to a principle of reciprocity, we note that espionage is a harmful activity, and the moral wrongness of harmful actions can be mitigated if they are reciprocal. However, we also note that espionage is frequently, if by no means always, a species of "dirty hands" epistemic activity. In this respect, espionage is analogous to covert action (see Chapter 6). Roughly speaking, dirty hands actions are pro tanto morally wrong actions performed as a means to a morally good end (see Chapter 1). Dirty hands action often involve deliberately doing wrong to an innocent person, and the reciprocating action may involve deliberately doing wrong to another innocent person, i.e., a person other than the initial wrongdoer. In such cases, the principle of reciprocity defended in this chapter may not apply (see further discussion below).

Espionage is frequently (but not necessarily always) a species of dirty hands action since spies are frequently citizens of the state that they are spying on, and these citizens may have a pro tanto moral duty not to divulge their state's secret intelligence to foreign states (Piaff and Tiel 2004; Perry 2016, 2021; Fabre 2022). In these cases, espionage is not only unlawful in the state being spied on but also – given the spies are citizens of this state – treason. Naturally, treason is a pro tanto moral wrong, at least in nation states that are not beyond the pale, i.e., nation states that have a degree of moral legitimacy that is sufficient to warrant a moral and legal (under domestic and international law) entitlement to protect their national security and, therefore, much of their secret intelligence.

There is a third set of issues pertaining to quite specific collection practices such as, for instance, the use of blackmail and other coercive measures to recruit foreign agents, the recruitment of criminals to provide secret intelligence, and so-called false flag operations. In the case of criminals turned informants, their effectiveness may depend on their continued engagement in very serious criminal activity.[3] In the case of false flag operations, the foreign agent recruited is deceived in relation to who he or she is working for and the purposes to which the secret intelligence collected will be put. For instance, he might think he is working for the CIA when in fact he is working for the FSB.

Blackmail, false flag operations, and the use of criminals are typically instances of dirty hands action, assuming they are undertaken in the service of the moral good of national security. However, for reasons of space, we will not address this third set of issues further beyond making the following two general points. First, these three kinds of case add to the stock of instances of espionage that are dirty hands actions. Second, and relatedly, it is unclear why such practices, or at least the occasional instance of such practices, could *never* be morally justified all things considered, notwithstanding the various moral problems that they give rise to, e.g., the potential unreliability and actual violation of autonomy involved in the use of coercive measures in recruitment of foreign agents. Naturally, the practice of, say, blackmail, could justifiably be banned in a national security intelligence agency, while on a one-off occasion it might be justified and, indeed, used. In this scenario, the practice has not been institutionalised, even if in some (presumably) highly unusual and extreme circumstance it is used. This is not to say that such "one-off" uses might not generate a so-called slippery slope. At any rate, the reason it is hard to see that such practices, and, especially, a one-off instance of such a practice, could never be morally justified all things considered is that the practice, or its one-off use, may well be necessary (given the strenuous efforts of foreign intelligence agencies to protect their secret intelligence) and not disproportionate (even if it violates the principle of discrimination), given what is often at stake in national security contexts, including defeat in war.[4]

Espionage: The Ends

According to the normative teleological theory of institutions (Miller 2010), and, therefore, of national security intelligence institutions, normatively speaking, institutions have as their raison d'etre or institutional purpose the production or maintenance of a collective good (Miller 2010: 66–80; Miller 2016a Ch. 3; Miller 2022a; Miller 2022b; Miller and Bossomaier 2024 Ch. 2) such as, for instance, national security. This collective good is produced or maintained by means (at least in large part) of the joint activity (including via layered structures of joint action – see Chapter 2) of the occupants of the constitutive roles of the institution in question.

Moreover, in the case of many institutions, this collective good is, in large part, an aggregation of prior needs-based, individual moral rights of members of the relevant polity or community, e.g., an individual's needs-based right to personal security from lethal threats. However, at the collective level, i.e., at the level of the polity or community, these moral rights are *joint* moral rights. Thus, a single member of a nation state has his or her moral right to national security *interdependently* with his or her fellow members. Indeed, the right to, say, the national security of Australia is a jointly held right of all Australians (including, residents who are not citizens, let us assume) *qua Australians*, i.e., qua members of the nation state, Australia. Accordingly, this jointly held right is not a prior, natural (as opposed to institutional) individual right, rather it is a joint *institutional* right (although it is a general, rather than a special, institutional right since special institutional rights are tied to particular institutions, as, for instance, the institutional rights of intelligence officers might be tied to national security intelligence agencies (Miller 2010; Miller 2016a Ch. 2).

Further, national security is not only a collective good in the sense that it is jointly produced or maintained, it is also a public good in the economists' sense in that it is non-rivalrous and non-excludable. That is, if a single member of the polity enjoys national security – such as security from foreign invasion – then others are not thereby prevented from doing so, and, indeed, it is more or less impossible for a single member of the polity who is enjoying national security to exclude others from doing the same (although one or a few of them might be excluded from enjoying, for instance, personal security).

Finally, the content of national security, i.e., what is protected or secured from domestic or foreign attacks, includes *necessarily* collective goods, such as sovereignty, and also institutions, such as (in modern liberal democracies) elected governments, police services, critical infrastructure, and so on. In short, national security is not reducible to aggregated personal security or, indeed, any other simple aggregation of prior, natural, individual moral rights. For instance, sovereignty or self-government is not simply the expression of an aggregation of prior, natural, individual moral rights to freedom or, in the case of a dictatorship, the claimed moral right of a single person, the dictator. For one thing, at least in the case of democracies, sovereignty is based in part on the exercise of *joint* moral rights to participate in political decision-making. For another, the decision-making roles and processes constitutive of sovereignty, even in a dictatorship, are institutionalised and pertain to the nature and future direction of the nation as a whole, i.e., of an irreducibly collective entity, and of its constitutive institutions.

The maintenance and production of the collective good of national security depends, in part, on knowledge of threats to national security and how to effectively combat them; that is, it depends on national security intelligence. Accordingly, national security intelligence agencies have been established in large part to provide the required national security intelligence. Moreover, since the realisation of national security intelligence agency's fundamental purpose entails the acquisition of the secrets of hostile foreign states and the protection of its own secrets from them, national security intelligence agencies need to engage in espionage, especially in relation to threats to national security emanating from hostile foreign states. In short, espionage is a necessary means to protect national security. Nevertheless, if undertaking espionage is to be morally acceptable to the liberal democracies whose intelligence agencies are undertaking it, then it needs to be governed by various moral principles including, as we have seen, discrimination, necessity, and proportionality, but also, as is argued in the next section, reciprocity.

As we have seen, espionage consists, in large part, in acquiring the secret intelligence of hostile states. It is also important to protect one's own secret intelligence from access by hostile foreign states. However, the latter typically requires preventing the disclosure of one's own secret intelligence even to one's own citizens. Accordingly, the joint moral right of the citizens of the liberal democracy, Democracy, to national security ultimately morally justifies not only the collection of the secret intelligence of a hostile foreign state, Hostile, and, correspondingly, the protection of the secret intelligence possessed by their own intelligence agencies from access by Hostile, but also the non-disclosure of this secret intelligence to the citizens of Democracy. Yet, it might seem that the citizens of Democracy have a joint moral right to access this secret intelligence, given that it is a necessary part of the means to protect their national security, i.e., it is done for them and they, presumably, need to consent to it, although the consent of current citizens may not be sufficient, given they may have obligations to accommodate the interests (and rights?) of the past and future citizens of Democracy in the continuation and, therefore, national security of Democracy.

Here, we need to distinguish the notional rights in play. First, there may well be a joint right of the citizens of Democracy to have secret intelligence collected from Hostile and to have Democracy's secret intelligence protected from disclosure, i.e., kept secret, including, from the citizens themselves. Call this the joint right of the citizens of Democracy to secret intelligence acquisition and non-disclosure. The basis of this derived joint right, supposing it exists, is the citizens' joint right to national security.[5] However, it would not follow from this that the citizens have a countervailing moral right, joint or otherwise, to access such secret intelligence, given that the citizens acting by themselves cannot acquire secret intelligence (at least to the extent required) but rather must rely on their national security intelligence agencies to do so.

It might be thought that members of the citizenry have a joint right to access this information, since it is ultimately their security that is being protected by its non-disclosure (and they must consent to the protection of their security and the means by which it is protected). Assume that A has a right that Protector protect A from Aggressor and that Protector has a concomitant duty to protect A from Aggressor. Now assume that in order for Protector to protect A from Aggressor, Protector needs to ensure that neither Aggressor nor A has Protector's secret knowledge of the means (K-Means) Protector uses to protect A. In these circumstances, it seems that A does not have a right to K-Means (other than perhaps, in general terms, including that Means is a morally justified means), or that, if A does have such a right, it is overridden by Protector's duty to protect A, given A has not waived A's right to be protected by P. In short, A cannot have it both ways; A cannot have a right to be protected by Protector (and, therefore, Protector's duty to protect A) and, simultaneously, a right to access information that would prevent Protector from discharging Protector's duty to protect A.

In this example, in order for Protector to discharge Protector's duty to protect A, Protector needs to have a degree of operational autonomy and the latter brings with it the requirement of a degree of epistemic opacity in respect of Protector's activities and methods, i.e., Protector must have secret knowledge. This notion of the operational autonomy of security agencies is a familiar one; for instance, the operational autonomy of the police is a well-established principle in liberal democracies, albeit it is autonomy in the context of a requirement for responsiveness and accountability to government and, ultimately, to the citizenry (Miller and Blackler 2005 Ch. 2; Miller and Gordon 2014 Ch. 4). Moreover, there is a further point to be made here, namely, that of investigative independence and, relatedly, the independence of intelligence agencies (again, subject to responsiveness and accountability [see later]). This exists in part because the police and national security agencies, including national security intelligence agencies, may need to investigate and, therefore, collect intelligence on their fellow citizens, including their democratically elected leaders if, for instance, there is a suspicion that they are engaged in treason.

Thus far, we have argued that there are good reasons why a law enforcement or national security intelligence agency ought not permit, for instance, its "tradecraft" to be known outside the agency. Are there countervailing reasons in favour of public disclosure that have not yet been canvassed?

It might be thought that secret intelligence is owned in some sense by the citizens. However, knowledge of the tradecraft of a national security intelligence agency, at any rate, is evidently not owned by ordinary citizens; they did not develop it and cannot use it if they did own it. Rather the relevant practitioners developed it and use it in the service of national security. So, any alleged right of access to tradecraft is seemingly not based on ownership. Naturally, some information, i.e., secret intelligence held by a national security intelligence agency is owned by individual citizens or businesses, e.g., information pertaining to the design of a new fighter plane developed by a private company. However, such information would not be owned by all or even most citizens. Moreover, the privacy rights of the citizens are not implicated in the case of such tradecraft, as would be the case if it was a personal information. But some personal information is also secret intelligence, e.g., the personal information of a suspected mole, KP. However, again, the personal information of KP is not owned by all or even most of KP's fellow citizens. Further, public interest is not available to provide the justification for a putative citizens' right to know a national security intelligence agency's tradecraft, as it is available in the case of some secret or confidential information obtained and disclosed by journalists. Indeed, the reverse is evidently the case; it is not in the public interest for secret information concerning a national security intelligence agency's tradecraft to be publicly disclosed because doing so would undermine national security.

There is a rather different and far more compelling argument for disclosure of secret intelligence, namely, democratic accountability (mentioned earlier). Democratic accountability requires that citizens know what activities their national security intelligence agencies are engaged in and, in particular, that these activities are actually being conducted in the service of national security and are compliant with the laws that their representative bodies have enacted. However, such accountability does not require public disclosure, and certainly not public disclosure of tradecraft and other secret intelligence the public disclosure of which would undermine national security. Rather a trusted citizens' representative, e.g., an elected official or committee composed of elected officials, or some person or committee appointed by the elected officials, could have the task of scrutinising the activities of a national security intelligence agency in detail, and, thereafter, of reporting back to the government, and via the government to the citizenry *in general terms*, what the agency was engaged in and whether it was compliant with relevant laws and government policies. Such a representative or representative body would need to be trusted by the government and the citizenry, on the one hand, and by the national security intelligence agencies, on the other, if it was adequately to discharge this sensitive role.

Espionage as Means: The Principle(s) of Reciprocity

In Chapter 4 it was argued that the principles of discrimination, necessity, and proportionality apply to national security intelligence activity, although not in the same manner as they apply to waging war (as constitutive of either the jus ad bellum or the jus in bello).[6] Analyses of the principles of necessity and proportionality, and of their relationship to one another and to the principle of discrimination in their application to national security intelligence activity, including espionage, have also been provided in Chapter 4. It is now time to argue that there is an additional normative principle governing espionage. This is a principle of reciprocity (see Miller and Walsh 2016). Reciprocity is not a constitutive principle of just war theory (JWT) or, therefore, just intelligence theory (JIT), nor is it a principle of Fabre's rights-based account of espionage (Fabre 2022), although it does feature in Skerker's account (Skerker 2021), albeit in a different manner to that advanced here.

Espionage raises legitimate privacy concerns, as well as confidentiality concerns. Privacy concerns arise when spies access the personal information of ordinary citizens. Confidentiality concerns arise when spies access the confidential or secret information held by government agencies, including foreign national security intelligence agencies. Other things being equal, national security intelligence agencies are entitled to protect such information, including secret intelligence collected for legitimate national security purposes, against espionage. Moreover, other things being equal, foreign citizens who are not members of national security agencies, or other relevant institutions, are entitled to the protection against espionage of their personal information to which they have privacy rights. The confidential and private information in question includes so-called metadata insofar as its collection may constitute a breach of confidentially and privacy rights, as might be the case if, for instance, it enable a person's movements to be tracked.

Here we need to keep in mind the distinction between morality and legality. Consider the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008. It mandates the monitoring of, and data gathering from, foreigners who are outside the US by the National Security Agency (NSA). This activity is, therefore, legal, but is it moral, given US citizens could not legally be subject to such monitoring and data gathering?

Such monitoring of, and data gathering from, foreign citizens is morally problematic insofar as privacy is regarded as a *human* right and, therefore, a right of all persons, US citizens or not. Moreover, these inconsistencies between the treatment of US citizens and foreigners are perhaps even more acute or, at least obvious, when it comes to the infringement of the rights to privacy and, for that matter, confidentiality of non-US citizens in liberal democratic states allied with the US, e.g., EU citizens.

Intelligence-gathering surveillance, and so on, of citizens by domestic law enforcement agencies is reasonably well defined and regulated, e.g., in accordance with probable cause/reasonable suspicion principles and requirements for warrants, hence, the feasibility of simply extending the law enforcement model to metadata collection within domestic jurisdictions. This law enforcement model evidently does not need to help itself to a principle of reciprocity. However, this domestic law enforcement model is too restrictive, and not practicable, in relation to external national security intelligence gathering from, e.g., hostile foreign states during peacetime, let alone in wartime. That is, the domestic law enforcement model is too restrictive to be adequate to the task of regulating espionage.

The privacy rights of the members of the citizenry during wartime are curtailed under emergency powers, and the privacy and confidentiality rights of enemy citizens are almost entirely suspended. Military intelligence-gathering during wartime has few privacy constraints and, given what is at stake in all-out wars, such as the Second World War, this may well be justified. This is not to say that the principles of necessity and proportionality are not applicable. Surely they are. However, their application is less restrictive, given what is at stake in war. That said, these are extreme circumstances and the suspension of privacy rights is only until the cessation of hostilities. Accordingly, this military model of intelligence-gathering is, arguably, too permissive in relation to secret national security intelligence gathering from, for example, fellow liberal democracies during peacetime.

The intelligence-gathering activities, mentioned earlier, including cyber-espionage, of the NSA do not fit neatly into JWT or, for that matter, the law enforcement model. At any rate, the question arises as to whether some different additional moral principle(s) needs to be invoked in relation to espionage, in particular. Evidently, some principle of reciprocity (Miller 2016b; 2021a; 2021b; 2023) needs to be invoked.[7]

This is not to say that a principle of reciprocity justifies espionage in a manner that enables it to replace or override the primary justification in terms of national security. The idea is not that if state A engages in espionage against state B, then state B is entitled to engage in espionage against state A, *and* this justification replaces the justification in terms of national security. Rather the primary justification for B to engage in espionage against A is and remains B's national security (and likewise for A). Hence, if A is known to have hostile intentions against B, then B is entitled to engage in espionage targeting A. Moreover, if A is an authoritarian state, albeit one that is not beyond the pale (as totalitarian states are) and, therefore, has legitimate national security concerns, then even if A does not, in fact, have any hostile intentions against B, nevertheless, B might be morally entitled to engage in espionage against A to assure itself that A had no hostile intentions, given that A's disregard for the moral rights of its own citizens creates a presumption that A would not shrink from engaging in hostile actions against B, if A judged this to be in its interest. Notice that in justifiably accessing A's secret intelligence in the service of B's national security, B might, nevertheless, commit the pro tanto wrong of compromising A's national security (e.g. with respect to A's military capabilities or spy networks) and, therefore, A might be morally entitled to protect itself against B's espionage activities and, indeed, to conduct its own espionage activities against B in order to determine, for instance, the extent to which A's secret intelligence has been compromised as a consequence of B's espionage activities. Here, there are two conclusions to be drawn. First, even if each and every state only ever conducted espionage in the service of its own national security (as opposed to, for instance, in the service of its national interest, such as its expansionist ambitions), espionage would likely, nevertheless, be a pervasive activity among nation states, at least as long as there are authoritarian states. Second, espionage in the service of national security may well be a contingent liberty right (although one subject to limitations and constraints), a right that all nation states possess (other than states beyond the pale) in the current circumstances of the world order (but might not do in other circumstances – hence it is a contingent liberty right).

The primacy of the justification of espionage in terms of national security and its status as a contingent liberty right is consistent with the applicability of the principle of reciprocity at a number of levels. At the micro level, for instance, the principle might morally justify specific practices that might otherwise not be morally justified. Consider the practice of blackmail. Suppose that intelligence officers in A's national security intelligence agency, frustrated in their attempts to access B's secret intelligence, decide to have recourse to the practice of blackmailing B's intelligence officers (as opposed to blackmailing ordinary citizens or those in government agencies other than security agencies), a practice that yields results. By virtue of the principle of reciprocity, arguably B's intelligence officers would be entitled to engage in the practice of blackmailing A's intelligence officers in the service of B's national security, notwithstanding that B had hitherto banned this practice because they reasonably regarded it as immoral. Here, the principle of reciprocity provides a justification for pro tanto wrongdoing, i.e., engaging in blackmail, but does so only in the context that, first, in some circumstances it is the most effective means to realise the collective good of national security and, second, that intelligence officers have, let us assume, freely undertaken the role of intelligence officer knowing that blackmail is authorised and practised, and, therefore, that they might be the perpetrators of it (or, since the adversarial intelligence agency practises blackmail, victims of it). Naturally, it does not follow from this that *any* practice, no matter how harmful or wrongful, is morally justified by the principle of reciprocity in this context. For instance, the practice of torturing intelligence officers would not be morally justified, even if the adversary state practised it (and even if, should it be introduced, this would be common knowledge among intelligence officers who would, therefore, have the opportunity of resigning their positions or not undertaking them in the first place).

At the macro level, the application of a principle of reciprocity might also make a difference, notwithstanding the primacy of the justification for espionage in terms of the collective good of national security. Here, we should distinguish between a retrospective and a prospective principle of reciprocity (Miller 2016b) and, in addition, keep in mind the distinction between the *partialist* collective good of *our* national security or that of *their* national security, e.g., an adversarial state's national security, on the one hand, and, on the other hand, the impartial collective good of global security – a collective good, in part, constituted by the aggregated national security of each of the nation states.

The retrospective principle of reciprocity takes its inspiration from the ancient prescription, "an eye for an eye and a tooth for a tooth" and, therefore, from lex talionis. On this version of the principle, if one is wronged, e.g., attacked, then one is morally entitled to respond in kind, irrespective of whether it is necessary for the specific purpose of, say, self-defence. Consider, in this connection, espionage conducted in the service of national interest (e.g., the secret intelligence acquired provides an economic advantage in a competitive arms market), as opposed to espionage conducted in the service of national security. According to the principle of reciprocity, a defender is not entitled to do more harm to an attacker than the attacker did, or intended to do, to the defender. This might limit the amount of damage that a state, A, is entitled to do by means of espionage to the national security of another state, B, in the service of A's own national security. For instance, in response to B's relatively harmless espionage activities targeting A, A's espionage activities in relation to B might compromise B's entire defensive strategy, thereby rendering B vulnerable to an attack from C. Here A's response would violate the principle of reciprocity.

However, while the prescription "an eye for an eye and a tooth for a tooth" limits harmful activity in this manner, it is, nevertheless, excessively permissive; it would license reciprocal attacks on others for any purpose whatsoever, just so long as this attack was not more harmful than the one it was in response to. Accordingly, we need to place a restriction on the principle, a restriction with respect to the purposes it is to serve.[8] Thus, a morally acceptable version of this retrospective principle would justify nation state, A, engaging in espionage against nation state, B, in circumstances in which B had engaged, or was engaging, in espionage on A, but only if A's espionage was in the service of A's national security (as opposed to, e.g., merely in A's national interest).

The prospective principle of reciprocity is a tit-for-tat principle in the service of bringing about a morally desirable future state of affairs from an impartial perspective, as opposed to being in the service of the partialist good of a single nation's national security (whether retrospectively or prospectively). The state of affairs in question is an equilibrium state among nation states, more specifically, a morally justifiable equilibrium under the rule of international law. As such, this prospective principle is not a tit-for-tat principle in the service, merely, of any single state's national security, much less of any single state's national interest (in the manner of rational choice theories). Of course, in this equilibrium state of affairs, there would not be espionage activities among participating nation states, e.g., liberal democracies, or, at least, espionage activities would be few and far between. So this principle does not justify harmful actions in the manner of its sister retrospective principle, rather it has as its purpose to eliminate, or at least greatly reduce, harmful actions and do so from an impartialist perspective, the harmful activity in question being espionage. Accordingly, the end point of the application of this prospective principle of reciprocity is to establish among relevant nation states a social contract, the content of which is the equilibrium state in which espionage among members is eliminated or, more realistically, substantially reduced. However, this equilibrium state which is the principle's *raison d'etre* is at best a long-term goal; it is unlikely to be achieved anytime soon.

On the one hand, the US and its allies cannot be expected to defend their national security, and for that matter their legitimate national interests, with their hands tied behind their backs. So their recourse to espionage seems justified, and the retrospective principle of reciprocity taken in conjunction with the collective good of national security provides a specific moral justification for this. On the other hand, understood as a prospective tit-for-tat procedure in the service of bringing about a social contract, the principle of reciprocity requires the moral renovation of espionage, including cyber-espionage, as it is currently conducted. Second, a couple of suggestions: (i) the clustering of nation states and (ii) a demarcation between government and security personnel, on the one hand, and ordinary citizens, on the other.

It is now commonplace for like-minded liberal states to share secret intelligence to some degree or another. For instance, the US, UK, Canada, Australia, and New Zealand – the so-called "Five Eyes" – share information gathered from other states. These nation states are, so to speak, allies in espionage, notably cyber-espionage; for example, they share intelligence. They are the members of my first cluster. There are, of course, other liberal democratic states outside the Five Eyes, such as various EU countries, which have "shared core liberal democratic values" with one another and with the Five Eyes and, specifically, a commitment to privacy rights. This is a second cluster.

The members of these two clusters have privacy-respecting laws and associated accountability measures in their domestic settings. However, they ought to make good on their claims to respect privacy rights as human rights by developing privacy-respecting protocols governing their intelligence-gathering activities in relation to one another. Of course, determining the precise content of such protocols is no easy matter, given, e.g., that there are often competing national interests in play, even between liberal democracies with shared values and many common political interests. But there does not appear to be any in-principle reason why such protocols could not be developed; and the fact that this might be difficult is no objection to attempting to do so. Moreover, since adherence to the protocols in question would consist, insofar as it is practicable, in ensuring compliance with some of the standard moral principles protecting privacy and confidentiality rights already in place in liberal democracies (but not authoritarian states), such as probable cause or reasonable suspicion and use of judicial warrants, these two clusters would essentially consist of an extension of the law enforcement model to espionage conducted within and between these countries. Clearly such an extension is unlikely, if not impossible, in the case of authoritarian states since these lack any commitment to privacy (and other) individual rights even in their domestic settings.

Further, such a process of clustering of liberal democratic states would be in accordance with the prospective principle of reciprocity; each of these nation states would need to agree to, and actually comply with, the privacy-respecting protocols in question, but each might be deterred from not doing so by the tit-for-tat procedure of the prospective principle. This is, of course, not to say that those who agree to comply with the protocols/laws will *never* breach them. But this is true of protocols and laws in general.

What of authoritarian states known to be supporting international terrorism and/or engaging in hostile covert political operations, including espionage and cyber-espionage, e.g., Russia, China and North Korea?

In respect of authoritarian states of this kind, the retrospective principle of reciprocity reigns. Accordingly, there are few, if any constraints on intelligence-gathering and analysis, including cyber-espionage, if it is done in the service of a legitimate political interest such as national security.[9] Nevertheless, it is important to demarcate within such an authoritarian state between the government and its security agencies, on the one hand, and private citizens, on the other. Notwithstanding the applicability of the retrospective reciprocity principle, the need to respect the privacy rights of private citizens in authoritarian states remains, perhaps all the more so given these rights (and, for that matter, human rights in general) are routinely violated by their own governments.

So a stringent principle of discrimination ought to govern espionage, including cyber-espionage, directed at authoritarian states. At the very least, the citizens of these states ought to be able to differentiate between morally justified infringements of the privacy and confidentiality rights of members of their government and its security agencies, on the one hand, and violations of their own privacy and confidentiality rights, on the other, and be justified in believing that whereas the former might be routine, the latter are few and far between.

Conclusion

The concern in this chapter has been with 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 were identified as salient in relation to espionage and that have been addressed in this chapter. 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?

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 was assumed that versions of these have application to espionage. However, an additional principle was argued for, namely, a principle of reciprocity.

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

Notes

[1] There is also information that is not in the public sphere but which is not secret or confidential, since although not directly accessible by those external to the organisation that holds it, nevertheless, would be made available to anyone who asked for it.

[2] Elsewhere, I have also argued that espionage is justified by the collective good of national security which is, in turn, based in part and indirectly on prior natural individual moral rights, such as the right to personal security. See Miller and Walsh (2016); Miller (2021a, 2021b,2022a; 2022b). Relatedly, and more recently, Cécile Fabre deploys the notion of collective goods and argues that espionage is justified by the prior, individual (natural, i.e. non-institutional?) moral rights of the citizens on whose behalf it is conducted (Fabre 2022).

[3] See Omand and Phythian (2018, chap. 4) for a good discussion of the issue of recruiting criminals such as the notorious "Stakeknife" during the "Troubles" in Norther Ireland.

[4] See Perry (2016, 2021) for discussion of these issues.

[5] See Fabre (2022, 43).

[6] This has also been argued in effect by Omand and Phythian (2018), albeit the argumentative detail is somewhat different.

[7] Reciprocity-based principles are related to, but distinct from, consent-based principles. In relation to the latter applied to espionage, see Piaff and Tiel (2004).

[8] Espionage would also by virtue of this introduction of a purpose, thereby, be subject to a necessity principle in the sense of necessary means but not to a harm minimisation. See Chapter 4. Regarding harm minimisation, the reciprocity principle does limit harm to equivalent harm. The reciprocity principle is consistent with a principle of discrimination. On principles of reciprocity and their application see Miller (2016b; 2021a; 2021b; 2023).

[9] There are important questions here concerning what counts as a legitimate purpose, particularly in the context of the blurring of the distinction between a political interest and an economic interest, e.g., China's cyber-theft operations. For reasons of space I cannot pursue these here.

References

Fabre, Cécile. 2022. *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence.* Oxford: Oxford University Press.

Gendron, Angela. 2005. "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage." *International Journal of Intelligence and Counter-Intelligence* 18(3): 398–434.

Marrin, Stephen. 2018. "Evaluating Intelligence Theories: The State of Play." *Intelligence and National Security* 33: 479–90.

Miller, Seumas. 2006. "Collective Moral Responsibility: An Individualist Account." In *Midwest Studies in Philosophy*, edited by Peter A. French, XXX: 176–93.

Miller, Seumas. 2010. *The Moral Foundations of Social Institutions: A Philosophical Study*. New York: Cambridge University Press.

Miller, Seumas. 2015. "Joint Epistemic Action and Collective Moral Responsibility." *Social Epistemology* 29(3): 280–302.

Miller, Seumas. 2016a. *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force.* New York: Oxford University Press.

Miller, Seumas. 2016b. "Cyber-attacks and 'Dirty Hands': Cyberwar, Cyber-Crimes or Covert Political Action?" In *Binary Bullets: The Ethics of Cyberwarfare*, edited by F. Allfhoff, A. Henschke, and B J. Strawser, 228–50. Oxford: Oxford University Press.

Miller, Seumas. 2018a. "Joint Epistemic Action: Some Applications." *Journal of Applied Philosophy* 35(2): 300–18.

Miller, Seumas. 2021a. "Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity." *Social Epistemology* 35(3): 211–31. doi:10.1080/02691728.2020.1855484

Miller, Seumas. 2021b. "Truth-Seeking and the Principles of Discrimination, Necessity, Proportionality and Reciprocity in National Security Intelligence Activity." In *National Security Intelligence and Ethics*, edited by Seumas Miller, Mitt Regan, and Patrick Walsh, 21–38. London: Routledge.

Miller, Seumas. 2022a. "Epistemic Institutions: A Joint Epistemic Action-based Account." *Nous-Supplement: Philosophical Issues* 32(1): 398–416.

Miller, Seumas. 2022b. "National Security Intelligence Activity: A Philosophical Analysis." *Intelligence and National Security* 37: 791–808.

Miller, Seumas. 2023. "War, Reciprocity and the Moral Equality of Combatants." *Philosophia* August: 1–8. https://link.springer.com/article/10.1007/s11406-023-00678-1

Miller, Seumas and Ian Gordon. 2014. *Investigative Ethics: Ethics for Detectives and Criminal Investigator.* Hoboken: Wiley-Blackwell.

Miller, Seumas and John Blackler. 2005. *Ethical Issues in Policing*. Aldershot: Ashgate.

Miller, Seumas and Patrick Walsh. 2016. "NSA, Snowden and the Ethics and Accountability of Intelligence Gathering." In *Ethics and the Future of Spying: Technology, Intelligence Collection and National Security*, edited by Jai Galliott and W. Reed, 193–204. New York: Routledge.

Miller, Seumas and Terry Bossomaier. 2024. *Cybersecurity, Ethics and Collective Responsibility*. New York: Oxford University Press.

Omand, David and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Oxford: Oxford University Press.

Perry, David. 2016. *Partly Cloudy: Ethics in War, Covert Action and Interrogation.* 2nd ed. London: Rowman & Littlefield.

Perry, David. 2021 "Ethics in the Recruiting and Handling of Espionage Agents 1." In *National Security Intelligence and Ethics*, edited by Seumas Miller, Mitt Regan, and Patrick F. Walsh, 63–88. London: Routledge.

Piaff, Tony and Tiel, Jeffrey R. 2004. "Ethics of Espionage." *Journal of Military Ethics* 3(1): 115.

Pili, Giangiuseppe. 2019. "Intelligence and Social Epistemology: Towards a Social Epistemological Theory of Intelligence." *Social Epistemology* 33(6): 574–92.

Quinlan, Michael. 2007. "Just Intelligence: Prolegomena to an Ethical Theory." *Intelligence and National Security* 22(1): 1–13.

Skerker, Michael. 2021 "The Rights of Foreign Intelligence Targets." In *National Security Intelligence and Ethics*, edited by Seumas Miller, Mitt Regan, and Patrick F. Walsh, 89–106. London: Routledge.

Walsh, Patrick and Seumas Miller. 2016. "Rethinking 'Five-Eyes' Security Intelligence Collection Policies and Practices Post 9/11/Post-Snowden." *Intelligence and National Security* 31(3): 345–68.

6 Covert Action

The Ethics of Secret National Security Operations

Andrew Alexandra

"Covert action", in the sense in which it is used in this chapter, refers to actions which are 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. While actions of this kind have a venerable pedigree, it appears that it is only in the twentieth century that they have been clearly distinguished, conceptually and organisationally, from other forms of state-sponsored activities.

Covert action can be seen as a kind of intermediate means for the projection of national influence, sitting between diplomacy and military action (though the borders between these various means are not always sharp). However, while there are well-developed conventions and international law regulating diplomatic and military relations between states, norms governing covert action remain underdeveloped.

Covert operations came to the fore in the Cold War. While the US and the USSR understood themselves as engaged in a bitter struggle to promote competing ideologies, the balance of nuclear terror acted to deter direct military confrontation. George Kennan, who headed the US State Department's Policy Planning Staff, in a paper written in 1948 for the US National Security Council (NSC) recommended "the inauguration of organized political warfare", which he defined as "all the means at a nation's command, short of war, to achieve its national objectives" (Rudgers, 2000). Covert operations were integral to such political warfare and the definition of such operations subsequently adopted by the NSC in 1948 was, accordingly, extremely accommodating. The NSC saw covert operations as all activities conducted or sponsored by this Government against hostile foreign states or groups or in support of friendly foreign states or groups but which are so planned and executed that any US Government responsibility for them is not evident to unauthorised persons and that if uncovered the US Government can plausibly disclaim any responsibility for them[1] (US Department of State 1948).

The two defining features of covert operations in the NSC description are that they are sponsored by the government in support of friendly states or groups, or in opposition to hostile ones, and that (it is intended that) they cannot be attributed to their sponsor.

DOI: 10.4324/9781003106449-8

One way in which attribution can be prevented is by an action being undertaken secretly, so those from whom it is meant to be concealed remain unaware of its occurrence. Many of the things that are generally counted as covert operations (such as secret funding of political movements) are in fact done surreptitiously. However, what makes these actions covert in the sense in which the term is used by the NSC is not that they are undiscovered, or even that it is intended that they remain so, but rather that the identity of their sponsor will not be apparent to "unauthorised" persons. Where the action is visible, lack of attributability depends on "plausible deniability". Whether a denial is plausible is not inherent to its content, as truth or falsity are, for example. It is, rather, the function of a judgment made by a hearer, who assesses the claim on the basis of its fit with their prior beliefs and commitments, their ability to gather and interpret relevant information and, especially, their assessment of the trustworthiness of the source of the claim. These factors can vary from time to time and person to person, and they can be manipulated.

It follows that the same action can be – or intended to be – covert in relation to one potential audience, but not to another. Typically, of course, those responsible for notionally covert action intend that their identity should remain hidden from everyone else except, perhaps, public officials who have oversighting or reviewing authority. However, it is possible that an action is meant to be covert only to some of those affected by it. Consider, for example, the poisoning of Sergei Skripov – a former Russian military officer and British double agent – and his wife Yulia by the Novichok nerve agent in England in 2018. Evidence that the poisoning was carried out by Russian state agents was not difficult to discover and was convincing enough for the UK government and allies to institute weighty sanctions against Russia, and for the Western press to accept their claims of Russian responsibility. On the other hand, the Russian government's denial of involvement appears to have been found plausible by the majority of its own citizens, with the *Moscow Times* reporting that a survey published by the independent Levada Center pollster [in October 2018] says that 28 percent of Russians believe that British intelligence services were behind Skripals' poisoning, with only 3 percent saying they believe their own intelligence officers carried out the attack. Another 56 percent said that "it could have been anyone" (*The Moscow Times* 2018).

It seems that the Russian government in fact wanted its role in the Skripov's poisoning to be apparent to members of its security establishment to act as a warning against following Sergei Skripov's example, while veiling it from its populace. If so, it was intended that the poisoning be covert in relation to the Russian general public, but not to others, including the British public. Or consider the actions of the Soviet and American governments in hiding from their respective publics their involvement in serious aerial conflict with each other during the Korean War (Carson 2018, 1–2), apparently so that they would not face popular pressure to escalate fighting. Here, it seems that each government wanted their conflict to be covert relative to both their own and their opponent's population, but not to the military and political commanders of their opponents. (And they both succeeded.)

The definition of covert action does not provide any reasoned principle(s) for determining the grounds on which covert actions should (or shouldn't) be undertaken, nor the means to be used in such actions. Immediately following its definition of covert operations, the NSC provided a list of the kind of actions which might count as covert operations, including activities related to propaganda, economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anti-communist elements in threatened countries of the free world, and excluding armed conflict by recognised military forces, espionage, counter- espionage, and cover and deception for military operations. But in the absence of any account of the reasons why covert action should be undertaken, this list must be seen as open ended. Covert actions are identified not by the means used, or the ends aimed at, but simply by the intention that their sponsor should not be held responsible for them (US Department of State 1948).

In short, apart from their being state sponsored and (supposedly) non-attributable by some audience, there is no essential feature which specific covert actions must have in common. They can be undertaken for a range of reasons, making use of any means to achieve the goals of their sponsors, and they can be intended to be covert for some audiences, but not others. Indeed, over the past 70 years, all the major powers have invested substantial resources in a broad range of covert actions, from funding for political parties, to provision of weapons to armed groups, to assassination and attempted regime change, and beyond. According to Loch Johnson, the CIA – and no doubt the KGB as well – has counterfeited foreign currency to trigger inflationary pressures in target countries; depressed the world price of certain agricultural products vital to the economies of adversaries – especially devastating in one-crop economies; contaminated oil supplies; cultivated parasites that might destroy crops; diluted pesticides bought in the international marketplace by nations hostile to the US; and engaged in … cloud-seeding in the skies over enemy territory (Johnson 2020, 673).

While some of these actions have been comically ineffective, many have had really significant impact, supporting major insurgencies in Afghanistan and Nicaragua in the 1980s, contributing to regime change in Iran in 1953 and Chile in 1973 and influencing electoral politics in many states (O'Brien 1995).[2] So, for example, the CIA spent over $US75 million trying to influence the outcome of Italian elections in the period between 1948 and 1975.

Justifying Covert Action

Despite the intentions of those responsible, details of much covert action, including the identity of its originators, have been revealed over the past 70 years.[3] In many cases, these revelations have generated controversy. For example, in the 1960s the US engaged in covert action in Chile, originally with the aim of preventing the election to President of the socialist Salvador Allende, and after his election in 1970, providing support to the growing opposition to his regime, opposition which culminated in his violent overthrow in 1973 and the imposition of a military dictatorship.[4] On the one hand, it would seem that the actions of the CIA contributed to the overthrow of a democratic regime and its replacement by a cruel and repressive dictatorship. But, it has been claimed that these actions were justified in the global geopolitical context of the time, lessening the likelihood of a communist takeover of much of South America and furthering legitimate national interests of the US.

In what follows, we discuss the ethical assessment of covert action. Such an assessment has to consider a wide variety of situations, since there is no in-principle restriction on the sorts of actions which can be undertaken covertly, and in practice a very wide range of sorts of actions have been so undertaken. Moreover, these actions have had a variety both of targets, from individuals to regimes to political movements, and of motivations. This is not to say that we can't make some ethical generalisations about covert action, most of which is – in Kennan's words – a form of "political warfare" – involving harm to its targets. As with actual warfare, "political warfare" is subject to ethical constraints, particularly the principles of discrimination, which aim to protect civilians by prohibiting directly targeting them, necessity, which dictates that the least harmful means to achieve the desired goal is taken, and proportionality, which requires that the harm done is proportionate to the wrong being prevented or overcome. Moreover, in as much as covert action *is* a form of political warfare, we also need to consider its political dimension, in particular, whether covertness is compatible with the norms of openness and accountability which are fundamental in legitimate, especially democratic, polities.

Covert Action as "Political Warfare"

Relations between states are now ideally supposed to conform to the "rules-based international order", the broad architecture of international governance developed since the end of the Second World War. There are two broad sets of principles within that architecture relevant to justification of covert action, at least where it is undertaken without the knowledge and permission of the state in which it occurs. These are the principles of sovereign equality, and the protection and promotion of human rights.

Sovereign Equality

The principles of sovereign equality as outlined in the *Declaration on the Principles of International Law* (United Nations 1970) hold the following:

- States are legally equal.
- Every state enjoys the rights inherent in full sovereignty.
- Every state is obligated to respect the fact of the legal entity of other states.
- The territorial integrity and political independence of a state are inviolable.
- Each state has the right to freely choose and develop its own political, social, economic, and cultural systems.

- Each state is obligated to carry out its international obligations fully and conscientiously and to live in peace with other states.

Given these principles, there is a presumption against unwanted interference by one state in the internal affairs of another. Any form of covert action that is not undertaken with the knowledge of the government within whose territory it occurs would seem to violate Principle 4, since presumably the rights to "territorial integrity and political independence" imply at least a right to know about the activities of foreign governments that are taking place within their borders. Moreover, particular kinds of covert action, such as secret funding of political parties and other forms of intervention in elections, violate specific principles such as the right of each state to "choose and develop its own political, social, economic and cultural systems".

The presumption against interference is not, however, absolute. Both international law and philosophical theory accept that it follows from the principles of sovereign equality that a state can be justified in taking hostile action against another state, given the satisfaction of certain conditions. This goes to the principle of reciprocity, introduced in Chapter 4. So, in international law, a state can be justified in taking so-called "countermeasures", even where those measures are normally forbidden, in response to the wrongful acts of another state, provided that they are done with the aim of bringing about the end of the wrongful acts, they are proportional to the wrongs they are trying to stop, and they cease when the wrongful acts do. It seems impossible that an action which is normally forbidden in international law could satisfy these conditions if undertaken covertly, where the identity of the sponsoring state is hidden from the offending state, since that state would not know why it is occurring and, hence, what they need to do to stop it.

Nevertheless, there are situations where states may be justified in taking covert action. According to just war theory, one of the necessary conditions for justifiably going to war is that it is a last resort – that is, all feasible alternative means of resolving a dispute have been tried. The requirement to explore feasible alternative courses of action before going to war may justify resort to covert action, where it is less harmful, and more effective, than alternatives in curtailing escalation short of war. Similarly, covertness may be justified where it is used not to prevent war but, rather, to prevent escalation once military action has begun. These kinds of cases are theoretically possible and have existed in actuality, as in the Korean War case outlined earlier, but they will be rare.

Further, the logic, which justifies the prohibition on the pre-emptive use of military force, does not apply to covert action intended to protect computer systems, at least presently. Permitting pre-emptive military action would threaten to generate an international Hobbesian state of nature, giving each state a reason to go to war against potential adversaries whenever they calculate that it is to their advantage to do so, for the fear that if they wait, they will become the victim of their now more powerful adversaries. And the need for pre-emption can be lessened by the development of powerful military defences, which deter attack and provide reassurance. Matters are quite different with the computer networks now central to both civil life and military capacity. Currently, at least, it appears that it is impossible to make these networks fully[5] secure as demonstrated by the recent "SolarWinds" and Microsoft Exchange hacks.[6] Cyber-space will be one of the most, if not the most, important battlefields in future wars. Given the apparent vulnerability of computer systems and the havoc that could be wreaked through disabling government and civilian systems, requiring that a state waits until an attack has happened or is imminent, would place an insurmountable handicap on second movers in hostilities. To deter serious, possibly deadly, cyberattacks, it may be necessary for states to convince potential adversaries that they possess the capacity and willingness to respond in kind if attacked. Doing so may require the covert infiltration of networks so that they can be disabled at a later date, as well, perhaps, as actually using offensive cyber weapons in a targeted way to demonstrate capacity. A state is justified in, in effect, taking other states' cyber facilities hostage: they will be attacked if, but only if, an attack is made on its own facilities.[7]

Our focus in this section has been on the kind of violation of the principle of sovereign equality by one state which may give another state reason to take covert action against it. However, such action can only be justified if it is also in accord with the principles of discrimination, proportionality, and necessity, outlined earlier.

Many of the kinds of covert actions in Loch Johnson's list, quoted earlier, clearly violate discrimination. For example, Johnson speaks of the CIA diluting pesticides bought in the international marketplace by nations hostile to the US. Note that it is unlikely that these pesticides were actually bought by "the nation", if this meant to refer to the government of the nation. Rather they were almost certainly bought by individuals and businesses domiciled in the nation. The immediately intended effects of the covert actions, presumably, are to undermine the capacity of farmers in that nation to protect their crops, resulting in less food, higher prices, and so on. In turn, the resultant social unrest is likely to make it harder for the incumbent regime to maintain control, encourage dissident groups, and the like. It is the effect on the regime which is the goal of the action, but this is achieved by means of acting on the users of the pesticide and those who depend on them. They are the proximate targets of the covert action, and the regime is the distal targets. Since the civilian population have done nothing to lose their immunity against intentional harm, such actions are morally illegitimate.

Human Rights

The second set of principles, which has been used to justify covert action, derives from the recognition of human rights, as enunciated in the Universal Declaration of Human Rights. In response to atrocities in Rwanda and elsewhere, the international community accepted the doctrine of the "Responsibility to Protect" (R2P), which licenses interventions, up to and including military intervention, where necessary to prevent large-scale violations of basic human rights through genocide, war crimes, and the like (United Nations, n.d.).

There is a tension, at least, between the principles of sovereign equality and those supporting human rights, at least if they are taken to license interventions which would otherwise be prohibited, as per R2P. How can the "territorial integrity and political independence" of a state really be inviolable, as supposedly guaranteed by Principle 4 of international law, when foreign troops may be authorised by the UN to intervene to protect some of its citizens, even where the state itself has not violated any of its obligations to other states? Addressing that question is obviously far beyond the ambit of this chapter. What is relevant here is that R2P presupposes that states can be permitted – perhaps even required – to intervene in the internal affairs of other states to protect the human rights of the citizens of those states. Covert action could not be one of the means used in an R2P operation, since any action undertaken in its name has to be debated and approved in the UN. However, the premises underpinning R2P – that sovereignty does not entail a right to violate basic human rights and that other states can be entitled to act to prevent such violations – could be used in the justification of covert action where it could be shown that such action was necessary to prevent egregious violation of rights (and even if this could be shown, it is difficult to see how ongoing denial of involvement could be necessary, given that by hypothesis such action is morally justified).

To this point, covert action has not, in fact, generally featured as part of the direct responses to atrocities such as the Rwanda massacre, which "shock the conscience of mankind" and stimulated the development of R2P. Defence of human rights has, however, been appealed to in justifying covert action supporting regime change or helping favoured groups obtain or retain political power. Loch Johnson, for example, endorsed Lori Damrosch's claim that "a political system that denies basic political rights is … no longer a strictly internal affair" (Damrosch, quoted in Johnson 1992, 288), and added that "Tyrants who suppress human rights and the political participation of their citizens undermine whatever claim they may have had to protection from outside influence based upon the noninterventionist norm, for the human rights norm is a powerful countervailing claimant" (Johnson 1992, 288). Similarly, Michael Reisman and James E. Baker hold that "Genuine self-determination is … the basic postulate of political legitimacy" and see covert operations which … "increase the probability of the free choice of peoples about their government and political structure as possibly justified, especially where such operations are the only way to achieve this" (Reisman and Baker 1992, 74–75).[8]

On the face of it, there is an air of paradox about claiming to act to increase people's self-determination, while doing so in ways which are intended to deny them knowledge about the means used to do so, and the identity of those using those means, and hence the possibility of their deciding for themselves whether they support what is being done. However, covert action might be justified as a necessary condition for political self-determination. Consider, for example, the rule of a tyrannical regime which violently represses any expression of dissent, or a fledgling democracy which is trying to organise a free and fair election, but lacks the resources to do so, or a national election where one political party is receiving substantial funding from a foreign power, giving it an unfair advantage over its competitors. In these kinds of cases, covert action may be intended to remove the barriers to, or provide the resources for, political self-determination. Corstange and Marinov (2012) have drawn a useful distinction between what they call partisan as against process intervention. Slightly modifying the original meaning of the distinction, let us say that partisan intervention involves (covert) support for a particular group or cause for purposes the intervening state favours, and process intervention provides (covert) support for the creation and exercise of political and civil rights (through the running of free and fair elections, for example), without the intention of influencing the way in which those rights are exercised. So, process intervention aims to remove a block to free choice, rather than influencing the choice that is made.

Covert process action is undertaken to facilitate free choice, and its motivation is altruistic. Altruistically promoting free choice is morally admirable, so covert action which does this is to that extent a good thing. However, it is not unproblematic. In the first place, such action faces the same burden of justification as (non-covert) foreign intervention in general. Even if a repressive regime has forfeited its legitimacy, so that the citizens of a state have a right to overthrow it, it does not follow, as J.S. Mill and others have pointed out, that foreign states have the same right (Mill 1973)[9]. Mill argued that self-determination was not something that could be granted or imposed by outside actors: only through the determined and coordinated action of a people themselves could they develop both the capacity to self-govern and an appreciation of the value of doing so. Intervening in the name of self-determination retards the development of that capacity by the people on whose behalf that intervention is made and is likely to make the viability of the new regime dependent on ongoing support by the interveners.

This is not to say that even those who hold that there is a presumption against intervention deny that what we have called process intervention can ever be acceptable. Mill, for example, thought it might be justified to bring an end to a long-running and bloody civil war, or to aid in a struggle to remove a colonising power. Nevertheless, it is difficult to justify covert process intervention. First, there is the question of why covertness is required. Consider covert funding of political parties, of the kind both the US and the USSR engaged in in post-war Italy and elsewhere. Let us assume that at least in the case of the US this was an example of process intervention, aiming simply to restore the balance that had been disrupted by the Soviet funding of its preferred parties. Why did the US funding need to remain covert? Could not the US simply point to the distortion of the democratic process caused by the USSR and explain how its own actions were correcting that distortion? To the extent to which the US actions were in fact aimed at restoring balance, there appear to be a number of non-exclusive answers to these questions. Knowledge that a party was being supported by a foreign power would undercut its credibility: was there an explicit or implicit quid quo pro demanded – could the party be relied on to make decisions simply on the basis of its judgment of national interest, rather than taking into account the interests of its foreign paymaster? Moreover, knowing that a party was receiving foreign support would reveal that it was actually less well-supported by the local population than it had appeared. And however pure the motives and methods of foreign funders might be, the very notion of political autonomy implies that foreign involvement is unwelcome, as the common prohibition on foreign funding of elections shows.[10]

While ideally process intervention removes barriers to self-determination without affecting the choices that would be made if those barriers did not exist, the tools of covert action mean that in practice this ideal of neutrality is unlikely to be realised, as the history of actual covert interventions shows. As well as simply providing funding for friendly political movements and civil society organisations, foreign agencies in Places such as Chile and Italy have engaged in bribery of politicians, construction of "front" organisations purporting to represent members of the community, and the planting of secret propaganda. Much of that propaganda is "black" – the presentation of false and damaging claims about the intentions of a group which purports to come from that group. Such actions are both deceptive – creating the impression that favoured groups and causes enjoyed greater local support than they did, and disfavoured ones less – and manipulative[11] – attempting to change people's behaviour without those they were trying to influence realising how they were being acted on. Deceiving and manipulating people in the name of promoting their self-determination is obviously difficult to justify, to say the least.

Responsibility, Authority, and Covert Action

The discussion of liberal democratic values and particular political principles leads us to a specific problem for the resort to covert action by intelligence institutions in liberal democracies. As discussed in Chapter 1, on the one hand, liberal democracies define themselves, in part, by notions of representativeness and accountability – the state generally is legitimate insofar as it represents the will of its citizens and is accountable to them. On the other hand, covert action is – *by definition* – an institutional action or operation which is intended, designed, and carried out to be publicly deniable. Assuming that in liberal democracies sovereignty rests with the people, they are ultimately responsible for actions which are taken (supposedly) on their behalf by the executive arm of the government and in the case of covert action by the groups funded to carry out such action. Thus, the citizens of the given state and these other bodies stand in a principal-agent relationship. Even though it is the agent who acts, and is thus causally responsible, moral responsibility lies with the principal, at least where the agent acts within the remit given to them by the principal (as recognised in the legal doctrine of vicarious responsibility). Here, by granting the intelligence actors and institutions the authority to act in their name – or at least to the extent to which they do so – the citizens of a given state bear some moral responsibility for those covert actions.

In a genuine principal-agent relationship, the principal has authority over the agent – the agent acts according to the stated will of the principal. Given that the agent, rather than the principal, is acting, the principal is not fully in control of what is done. It is this gap between wish and act which allows for so-called "agency problems", which arise when the agent has relevant knowledge which the principal lacks, either about how to achieve their task or about the extent to which they are actually working to achieve it, and when they have a conflict of interests, where it is in the interest of the agent to act in a way which is not in the principal's interest.

Agency problems are overcome or prevented through reducing the asymmetry of information between principal and agent by installing monitoring and accountability mechanisms, and by aligning their incentives for action. Accountability has two important roles in the principal-agent relationship. It has a regulatory function, imposing a discipline on agents to act as they should, by requiring them to justify their action if asked, to face sanctions or provide restitution if they have failed to act appropriately, and so on.[12] But it also provides information which the principal needs in order to refine and alter their views about what should be done. Accountability, in its informational function, is thus an aspect of the authority a principal has over their agent, not something separate from it.

In the case of state agencies, authority and accountability are mediated through the legislative and executive branches of the government. Popular authority over elected representatives is exercised indirectly, typically through lobbying and electoral pressure, which also tends to align the incentives of politicians with those of their constituents, while accountability is promoted through reporting requirements, parliamentary debate, freedom of information laws, the funding of oversighting bodies, such as anti-corruption commissions and auditors-general and the like, as well as through reporting and discussion in the media. The various public sector agencies are in turn accountable to the executive through reporting, auditing, and so on.

This standard chain of accountability for state bodies obviously cannot hold in the case of secret government action, despite a presumption that the actions of public officials should be open to public scrutiny. That presumption may, however, be defeasible, where secrecy facilitates more effective decision-making and action, and particularly where it would be impossible without it. While it would be incoherent to think that the public could decide on a case-by-case basis whether state action should be kept secret, there is nothing incoherent in thinking that there can be general principles governing the use of secrecy by state officials which respect the ideals of popular sovereignty by, for example, being open for public discussion and debate. Where secrecy is seen as desirable citizens can authorise the legislative to develop laws allowing and regulating secret (including covert) action, the executive to direct its agencies to undertake secret action in accordance with those laws, and agencies to provide accounts of such action to oversighting authorities. Indeed, modern states have increasingly put in place structures of just such a character, where a small subset of the legislative and executive become proxies for the general population.[13]

Arguments for state secrecy are consequentialist in nature: their strength depends on contingent matters of fact. Satisfactory consequentialist reasoning looks both at considerations in favour of a course of action and those against and compares it to alternatives where they exist. There is a range of different kinds of situations where secrecy may be desirable, from the workings of the deliberative process, to the decisions issuing from that process, to the actions which are taken as a result. Different considerations may apply in each of these situations. Decision-makers may be more likely to base their decisions on the merits of the case where they do not have to take account of personal costs associated with possibly being seen to advocate – or even consider – unpopular positions, or changing their mind as new information comes to light. Thus, the protection given to jury and cabinet deliberations. And secrecy about decisions and consequent action may be necessary where openness would be self-defeating, making effective action impossible, as in wartime.

At the same time, there are weighty consequentialist considerations against state secrecy. While sometimes secrecy may lead to better decisions, decision-making is often improved through wide consultation and contestation. And secrecy provides cover for ineptitude, corruption, and illegality. The truncation of the chain of accountability inherent in state secrecy is problematic for both the regulatory and informational functions of accountability. Without public accountability, it is at least possible that those secretly making and acting on decisions will be motivated by short-term political or personal advantage, ideology or favouritism, without fear of sanction. Lacking reliable information about what action is taken and why, and what its effects are, popular opinion remains ill-formed, so that even views about the justifiability of the principles governing secrecy are not properly informed.

Covert action inherits these difficulties, with added problems of its own. Conceptually, covertness, understood as "plausible deniability", differs in an important respect from the kind of secrecy involved in the cases discussed earlier. The secrecy of jury deliberations, or about the sailing of troop ships, say, involves constructing an impenetrable veil to prevent outsiders from seeing what is happening. But, as noted earlier, successfully keeping action covert does not involve hiding what is happening, but rather obscuring who is responsible for it. "Plausible deniability" implies a willingness to actually deny if necessary, and denial, to put it plainly, involves lying, or at least deception. Governmental deception of the citizenry is clearly more problematic than the kind of simple secrecy discussed earlier, where citizens can know that there is an area of activity hidden from their gaze. Government deception, on the other hand, leads misinformed citizens to falsely believe that they have knowledge on which they can base their opinion about government action, subverting the proper relationship of authority and accountability between state and citizen.

Practically, there is a tension between the organisational arrangements fostered by the need for plausible deniability and effective accountability. One way of increasing deniability is by insulating political decision-makers from direct responsibility for covert action by, for example, informing subordinates about the kinds of outcomes which are seen as desirable, without providing specific instructions, or by "outsourcing" action – by funding and assisting third parties. The independence of these groups from the state which has initiated the action they undertake makes it easier for the state to deny responsibility, while making it harder both to control what is done[14] and to demand accountability. And, as history teaches us, even when it is state actors who are directing covert action, accountability is often lacking.[15]

Moreover, the supposed "plausible deniability" of covert action provides incentives for states to mislead their citizens not just about those actions but about other matters as well. As noted earlier, plausibility is not inherent to the content of a claim, as truth or falsity are, for example, but is a function of a hearer's prior beliefs and commitments, their ability to gather and interpret information and, especially, their assessment of the trustworthiness of the source of the claim. Hence, a state, or its agencies, engaging in covert action has an incentive to try to affect the background beliefs of its citizens about such things as their benign behaviour in the international arena compared to the malevolence of its rivals, its commitment to human rights, the integrity of its institutions, and so on, independently of their truth.[16]

The successful denial of covert action leads citizens to have false beliefs about their government. But, as noted earlier, that denial is not always uncontested, particularly in countries with a relatively free press.[17] In the face of such contestation, citizens may come to doubt the veracity of their government[18] or of the media, or both. Indeed, in the US, which possesses both a large national security establishment and a lively tradition of investigative journalism disclosing supposedly covert action by state agencies, public faith in both the government and the media has declined over the past several decades to disturbingly low levels, well beneath those found in other democratic states and apparently even below those in some authoritarian states.[19] While the causes of these trends are obviously multi-factorial, the disjunction between claims of the media and those of the government in these matters is surely a contributing factor.

The straining of trust between state and citizens, and between citizen and citizen, must count as one of the actual bad consequences of covert action in the case of the major Western democracies, especially the US. But there have been others. Revelations of US and British involvement in supposedly covert action has fuelled the antagonism to these countries which has resulted in terrorist atrocities against their people, most notably the 9/11 attack. As Chalmers Johnson writes in a discussion of the long-term consequences of American covert action: "Even though the American people may not know what has been done in their name, those on the receiving end certainly do… Not surprisingly, sometimes these victims try to get even" (Johnson 2004) Moreover, knowledge of past covert action has generated such mistrust of Western governments in parts of the world that they are likely to be seen as responsible for outrageous interference even when they are not[20]with consequential hostility to citizens of those governments. We return to the issues of trust, intelligence, and institutional accountability in Chapter 9.

Conclusion

In this chapter, we have considered the ethics of covert action as they concern international relations and relations between citizens and their government. In both cases, it is clear that there must be a presumption against the use of covert action. In the case of international relations, though covert operations can be, and occasionally have been, consensual, most of them fit George Kennan's description of “political warfare”. While all states pay at least lip service to the “rules-based international order”, covert actions, which aim to obscure the responsibility of a state for hostile action against other states, subvert that order, which depends on state accountability for its integrity. Domestically, the inherent nature of covert action conflicts with the proper relationship between citizens and state, interfering with the accountability state agents owe to the citizens on whose behalf and at whose behest they are supposedly acting. And in both cases, the veil which covert action draws over state action facilitates corrupt, illegal, immoral of simply inept behaviour.

It does not follow that covert operations could never be, or as a matter of fact never have been, justified. As noted earlier, for example, covert action might actually be required if it is the only feasible way to avoid war, or its escalation. But such action should be considered only in extreme circumstances, and where there is no feasible alternative.

Notes

[1] Similar definitions are found in the CIA’s *A Consumer's Guide to Intelligence* (1995) “An operation designed to influence governments, events, organizations, or persons in support of foreign policy in a manner that is not necessarily attributable to the sponsoring power; it may include political, economic, propaganda, or paramilitary activities” (p. 38, quoted in Rudgers 2000, 249), and in the US Intelligence Authorization Act of 1991. According to the Act

(e) … . the term “covert action” means an activity or activities of the US Government to influence political, economic, or military conditions abroad, where it is intended that the role of the US Government will not be apparent or acknowledged publicly, but does not include the following:

(1) activities the primary purpose of which is to acquire intelligence, traditional counter-intelligence activities, traditional activities to improve or maintain the operational security of the US Government programmes, or administrative activities;

(2) traditional diplomatic or military activities or routine support to such activities;

(3) traditional law enforcement activities conducted by US Government law enforcement agencies or routine support to such activities; or

(4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of the US government agencies abroad.

[2] According to O’Brien, “both the CIA and the KGB soon rapidly developed covert action arms that far outweighed their intelligence collection missions” (O’Brien 1995, 432).

[3] Speaking of US action, Gregory Treverton claimed that “In all likelihood, the record shows, covert operations will become known, and America will be judged for having undertaken them” (Treverton 1987, 1005). While there are factors particular to the US which contribute to the likelihood of its covert action becoming known, it is noteworthy how much has also come to be known about the covert activities of the USSR (see e.g. Levin 2019).

[4] For details of US covert action in Chile, see the “Church Report” prepared by a committee of the US Senate (1975). For one theoretical perspective on that action, see Petras and Morley (2016). For a contrary view and a challenge to what has become the received

view about US involvement in the overthrow of the Allende government in Chile in 1973, see Falcoff (2003).

[5] For explanation as to why this is, see Nicole Perlroth (2021).

[6] The Solarwinds hack, attributed to Russian state actors, involved the insertion of a"backdoor" into widely used software, allowing infiltration of corporate and government networks, including the US State and Treasury Departments, the Pentagon, the Department of Homeland Security, the Department of Energy, and the National Nuclear Security Administration. The Microsoft Exchange hack, attributed to Chinese state backed actors, infected email server software across hundreds of thousands of mainly small organisations. For further details and discussion see Chesney (2020) and Aitel et al. (2021).

[7] The Stuxnet computer worm is an example. For discussion of some of the ethical issues raised by its use, see Peter W. Singer (2015).

[8] On the other hand, John Rawls claims that at least in the case of what he calls "decent" states – where basic human rights are guaranteed – the denial of the "rights of liberal democratic citizenship", such as civic equality, democratic governance, free speech, and association, does not justify humanitarian intervention (Rawls 2001, 32–33, 73).

[9] Michael Walzer (1977, 2015) expresses a similar view, albeit from a more communitarian position. For criticism of Walzer's view, see Luban (1980). For a discussion of the continuities and differences between Mill and Walzer, see Michael W. Doyle (2009). Coady, Dobos, and Sanyal (2018) provide a sample of contemporary philosophical thinking about humanitarian intervention.

[10] Approximately 70% of the world's states prohibit foreign financing of elections, see The International Institute for Democracy and Electoral Assistance 2023.

[11] For further discussion of the evils of manipulation in the context of covert action, see Charles Beitz (1989).

[12] See Mark Bovens (2007) for more on accountability and public administration.

[13] For a description of oversighting and accountability arrangements for agencies engaged in covert action in the US and an assessment of their (limited) efficacy, see (DeRosa 2021 and Lester 2015).

[14] Indiscriminate US support for the mujahidin in Afghanistan in their fight against the Soviet-backed government which helped lead to the rise of the Taliban and to Afghanistan becoming a base for anti-western terrorism is a paradigm example. For a detailed account, see Steve Coll (2004).

[15] The Iran-contra affair is a well-known example (Walsh 1993).

[16] Jacob Rowbottom (2017) distinguishes communicative inputs and outputs about government policy. Inputs contribute to discussion about what this should be, and should be free from governmental direction and influence. Once policy is decided, government communications legitimately inform and direct. Of course, there are many ways in which governments can, and do, generate and influence communicative inputs other than through official channels. For a relevant discussion, see Ted Galen Carpenter (2021).

[17] See Treverton (1987, 1005).

[18] Timothy Melley (2012) discusses the way in which the image of the national security establishment as a malign leviathan counter-posed to virtuous individuals has become a trope of popular culture in the US.

[19] For attitudes to the government, see Pew Research Centre (2021); for attitudes to the media, see Knight Foundation (2020).

20 So, false rumours that the US was responsible for the 1979 attack on the Grand Mosque in Mecca sparked violent demonstrations and attacks on US embassies in a number of countries (Coll 2004).

References

Aitel, Dave, Perri Adams, George Perkovich, and J. D. Work. 2021. "Responsible Cyber Offense." *Lawfare*. August 2. Accessed April 25, 2023. www.lawfareblog.com/responsible-cyber-offense

Beitz, Charles R. 1989. "Covert Intervention as a Moral Problem." *Ethics & International Affairs* 3(1): 45–60. https://doi.org/10.1111/j.1747-7093.1989.tb00211.x

Bovens, Mark. 2007 "Analysing and Assessing Accountability: A Conceptual Framework 1." *European Law Journal* 13(4): 447–68.

Carpenter, Ted Galen. 2021. "How the National Security State Manipulates the News Media." Cato Institute. March 21. Accessed April 25, 2023. www.cato.org/commentary/how-national-security-state-manipulates-news-media

Carson, Austin. 2018. *Secret Wars*. New Jersey: Princeton University Press.

Chesney, Robert. 2020. "The CIA, Covert Action and Operations in Cyberspace." *Lawfare*. July 15. Accessed April 25, 2023. www.lawfareblog.com/cia-covert-action-and-operations-cyberspace

CIA. 1995. *A Consumer's Guide to Intelligence*. Office of Public Affairs.

Coady, C. A. J., Ned Dobos, and Sagar Sanyal, eds. 2018. Challenges for Humanitarian Intervention*: Ethical Demand and Political Reality*. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780198812852.001.0001

Coll, Steve. 2004. *Ghost Wars: The Secret History of the CIA, Afghanistan and Bin Laden, from the Soviet Invasion to September 10, 2001*. London: Penguin.

Corstange, Daniel and Nikolay Marinov. 2012. "Taking Sides in Other People's Elections: The Polarizing Effect of Foreign Intervention." *American Journal of Political Science* 56(3): 655–70.

DeRosa, Mary B. 2021. "Congressional Oversight of US Intelligence Activities." In *National Security Intelligence and Ethics*, edited by Seumas Miller, Mitt Regan, and Patrick F. Walsh, 216–31. New York: Routledge.

Doyle, Michael P. 2009. "A Few Words on Mill, Walzer, and Nonintervention." *Ethics & International Affairs* 23(4): 349–69. https://doi.org/10.1111/j.1747-7093.2009.00228.x

Falcoff, Mark. 2003. "Kissinger & Chile: The Myth That Will Not Die." *Commentary* 116(4): 41.

Johnson, Chalmers. 2004. "Abolish the CIA." *London Review of Books*. October 21. www.lrb.co.uk/the-paper/v26/n20/chalmers-johnson/abolish-the-cia

Johnson, Loch K. 1992. "On Drawing a Bright Line for Covert Operations." *The American Journal of International Law* 86(2): 284–309.

Johnson, Loch K. 2020. "Reflections on the Ethics and Effectiveness of America's 'Third Option': Covert Action and US Foreign Policy." *Intelligence and National Security* 35(5): 669–85.

Knight Foundation. 2020. "American Views 2020: Trust, Media and Democracy." Accessed April 24, 2023. https://knightfoundation.org/reports/american-views-2020-trust-media-and-democracy/

Lester, Genevieve. 2015. *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence*. Cambridge: Cambridge University Press.

Levin, Dov. 2019. "Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset." *Conflict Management and Peace Science* 36(1): 88–106. https://doi.org/10.1177/0738894216661190

Luban, David. 1980. "The Romance of the Nation-State." *Philosophy & Public Affairs* 9(4). www.jstor.org/stable/2265007

Melley, Timothy. 2012. *The Covert Sphere: Secrecy, Fiction, and the National Security State*. New York: Cornell University Press.

Mill, John Stuart. 1973. "A Few Words on Non-Intervention." In *Essays on Politics and Culture*, edited by Gertrude Himmelfarb. Gloucester: Peter Smith.

O'Brien, Kevin A. 1995. "Interfering with Civil Society: CIA and KGB Covert Political Action during the Cold War." *International Journal of Intelligence and Counter Intelligence* 8(4): 431–56.

Perlroth, Nicole. 2021. *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. London: Bloomsbury.

Petras, James and Morris Morley. 2016. "On the U.S. and the Overthrow of Allende: A Reply to Professor Sigmund's Criticism." *Latin American Research Review* 13(1): 205–21. https://doi.org/10.1017/s0023879100030806

Pew Research Center. 2021. "Public Trust in Government: 1958–2021." Accessed April 24, 2023. www.pewresearch.org/politics/2021/05/17/public-trust-in government-1958-2021/

Rawls, John. 2001. *The Law of Peoples: With "The Idea of Public Reason Revisited"*. Cambridge, Mass: Harvard University Press.

Reisman, William M. and Baker, James E. 1992. *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law*. New Haven: Yale University Press.

Rowbottom, Jacob. 2017. "Government Speech and Public Opinion: Democracy by the Bootstraps." *Journal of Political Philosophy* 25(1). https://doi.org/10.1111/jopp.12101

Rudgers, David F. 2000. "The Origins of Covert Action." *Journal of Contemporary History* 35(2): 249–62. https://doi.org/10.1177/002200940003500206

Senate, U. S. 1975 "Covert Action in Chile 1963–1973." In *94th Congress 1st Session, Washington*, vol. 18.

Singer, Peter W. 2015. "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons." *Case Western Reserve Journal of International Law* 47(1): 79. https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1009&context=jil

The International Institute for Democracy and Electoral Assistance. 2023. "Political Finance Database." Accessed April 24, 2023. www.idea.int/data-tools/data/political-finance-database

The Moscow Times. 2018. "Only 3 Percent of Russians Believe Moscow Was behind Skripal Attack, Poll Says." October 25. www.themoscowtimes.com/2018/10/25/only-3-percent-russians-believe-moscow-was-behind-skripal-attack-poll-says-a63297

Treverton, Gregory F. 1987. "Covert Action and Open Society." *Foreign Affairs* 65(5): 995. https://doi.org/10.2307/20043198

United Nations. 1970. "Declaration on the Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations." Resolution A/RES/25/2625, October 24, 1970.

United Nations. n.d. "United Nations Office on Genocide Prevention and the Responsibility to Protect." www.un.org/en/genocideprevention/about-responsibility-to-protect.shtml

U.S. Department of State. 1948. "Foreign Relations of the United States, 1945–1950: Intelligence Activities." Accessed April 24, 2023. https://history.state.gov/historicaldocuments/frus1945-50Intel/d292

Walsh, Lawrence E. 1993. *Final Report of the Independent Counsel for Iran/Contra Matters*. Vol. 1. US Court of Appeals for the District of Columbia Circuit, Division for the Purpose of Appointing Independent Counsel.

Walzer, Michael. 1977. *Just and Unjust Wars*. New York: Basic Books.

Walzer, Michael, 2006, 'Mill's "A Few Words on Non-Intervention": A Commentary.' In *J.S. Mill's Political Thought: A Bicentennial Reassessment*, 347–56. Cambridge: Cambridge University Press.

7 PSYOP and Intelligence Institutions

Andrew Alexandra

There are many discussions of psychological operations (PSYOP)[1] in international relations and military strategy literature, but there is no canonical definition. Along with cognates such as propaganda, information operations, military deception, and the like, it is given a variety of senses by different commentators in different contexts. A typical definition, published by the US Army, describes PSYOP as "[t]he planned use of propaganda and other measures to influence the opinions, emotions, attitudes, and behavior of hostile, neutral, or friendly groups in such a way as to support the achievement of national objectives".[2]

It is noteworthy how broad this definition is. It does not say who undertakes the "planned operations" – there is no requirement that PSYOP be directly carried out by government agencies, for instance. The "selected information and indicators" could be anything that influences "emotions, motives, objective reasoning and… behavior": it could be purportedly factual information, but it could also be songs, poems, or other cultural products. The targets of influence range from individuals to governments, and presumably everything in between, while the kinds of behaviour which PSYOP is supposed to influence them to undertake is equally open-ended. Taken in its broadest possible sense, then, on this definition "PSYOP" refers to the full gamut of such deliberate influence over attitudes to potentially or actually antagonistic states or other political entities, aimed at both domestic and foreign audiences, during both war and peace.

In official and military circles, and as used in this chapter, PSYOP has tended to have a more limited extension, referring to specific kinds of activities and operations, undertaken or sponsored by state bodies, particularly intelligence agencies and the military, directed at non-compatriots, and in the service of national security, as broadly understood. So, during wartime, PSYOP units in armies have undertaken non-kinetic actions, such as dropping leaflets on enemy forces encouraging them to surrender, or providing information to civilians in occupied areas about their rights and duties in relation to the occupiers (Jowett and O 'Donnel 1986, 118–152), while in peacetime state-funded organisations have beamed radio broadcasts into foreign countries to sow distrust of the government or to generate positive attitudes to the government of the broadcaster (Puddington 2000; Rid 2020; Singer and Brooking 2018).

DOI: 10.4324/9781003106449-9

Though the psychological element in warfare (and international relations) has long been recognised, PSYOP, as a dedicated element in national security institutions, is a relatively recent development.[3] Success in the "total wars" of the nineteenth and twentieth centuries required the mobilisation of all the resources of the society, which in turn depended on the willing involvement of all sectors of the population. The innovations in communications technology and techniques of persuasion and the new insights into human psychology, which facilitated the growth of mass media, advertising and public relations, provided the tools to be used, on the one hand, to shore up domestic support and, on the other, to subvert it in foreign settings.

As the power of those tools, especially the internet, has grown, so has the capacity of PSYOP.[4] Social media platforms such as Facebook and WhatsApp have, literally, billions of users, who transmit enormous number of messages and (usually unwittingly) generate vast amounts of data. Exploitation of that data has allowed much more precise targeting of messages, including advertisements, to individuals and groups. It has also facilitated research which investigates group behaviour, such as the "viral" spread of (mis)information, and provides the basis for techniques and technologies which can predict and manipulate such behaviour (so-called "social physics", or nudging).[5] Advances in artificial intelligence and machine learning suggest that it will soon be impossible to detect the difference between human and artificial agents on the internet, allowing the creation of a multitude of fake identities that can interact believably with users. Jointly, these developments mean that there is little resemblance between current and future PSYOP operations on the one hand and those of even the recent past on the other: PSYOP can now reach far more people, much more cheaply and rapidly than previously, transmitting vastly greater amounts of information and interacting with users in ways which were previously impossible, while making it much harder to detect the origin of the information they are receiving. Both law and ethical theory have yet to come to terms with these developments, with the discussion of the ethics of war in particular still centred on kinetic force.

PSYOP as Speech

The essence of PSYOP is communicating with an audience, with the intention to influence them to hold certain beliefs or attitudes, and ultimately to act in accordance with the sender's intentions. PSYOP, then, mainly operates through the use of language or, more broadly, expression.[6] The ethical assessment of PSYOP thus falls within the category of the ethics of speech (where speech is understood as referring to linguistic communication in general).

There is, of course, broad agreement about a right to freedom of speech (Fish 1994; Schauer 1982; Sadurski 1999; Sunstein 1993; D. van Mill 2017). This does not mean that anyone has a right to say anything they want. It does imply that the onus is on those who want to limit the expression of others to justify that constraint. Rights are often spoken as "hedges", delimiting an area which is protected from outside encroachment. So, to say that someone has a right to speak (about some topic) means that others are not entitled to prevent them from doing so. Importantly, it does not follow from this that if someone has a right to speak about something, there are no moral constraints on what they say: that *others* are not entitled to prevent us from saying something doesn't mean that *we* should feel free to say whatever we like, or be immune from criticism for saying it. We shouldn't lie or deceive, or gratuitously offend others or belittle, demean, or shout them down. And we should also be conscious of the pragmatic effects of our speech: getting a reputation as a liar or a blowhard may make it less likely that others will engage with us, or take our point of view seriously.

There are, then, two broad tasks for an account of the right to free speech. First, we need to specify the limits of the right. Speech that is within the boundary of the right is protected from coercive interference while speech outside it is not. Second, we have to outline the moral and pragmatic constraints on our exercise of the right to free speech. Undertaking these tasks presupposes an account of the grounds of the right to free speech – that is, what it is for. In chapter 2 of *On Liberty*, John Stuart Mill provided the most influential account of the justification for free speech, arguing for protecting "the fullest liberty of professing and discussing, as a matter of ethical conviction, any doctrine, however immoral it may be considered" (Mill 1971). Mill thought that allowing the expression and contestation of ideas was the best way of generating true beliefs – and hence effective action – among a population, while holding that it also promoted the morally desirable traits of critical thought and independence of mind.

On this approach, freedom of speech is best characterised as freedom of discussion, a characterisation which helps to set the limits to the right to free speech. Speech which contributes to discussion and the pursuit of truth, no matter how apparently implausible or offensive, is protected – others are not permitted to prevent or punish it – while speech which does not, isn't. So, slander and libel which falsely or unfairly destroy a person's good reputation fall outside the range of protected speech, as does fraudulent advertising, and "fighting words", which aim to insult and provoke. Seeing free speech as grounded in the mutual pursuit of truth also helps us to understand how we should constrain ourselves in its exercise. Talking over the top of someone, for instance, or making it clear that we think of them as our intellectual inferior, is clearly incompatible with mutual engagement in the pursuit of truth. Understanding the right to free speech as grounded in our interest in coming to well-informed and thoroughly reasoned beliefs also implies what might be called a right to hear – to have access to the views of others.

Whether some utterance counts as protected or not cannot be determined simply by its content, we also need to look at its context. In chapter 3 of *On Liberty*, Mill considers the example of the claim that "corn dealers are starvers of the poor" (Mill 1971). Printed in a book, or uttered in a parliamentary debate, this would count as protected speech, since it is a contribution to reasoned discussion, the merits of which can be explored and debated. But proclaimed by an agitator in front of an enraged mob outside a corn dealer's house, it wouldn't be protected, because it is, in Mill's words, "a positive instigation to some mischievous act", which achieves its effect by acting on its listeners' emotions, rather than their reason (Mill 1971).

Three comments are in order here. First, "instigation" and related terms such as "incitement" can have both a purely causal sense as well as a purposeful one. A Police Officer might incite a riot, for example, by their heavy-handed arrest of a member of an ethnic minority, without any intention of doing so. And an agitator might intentionally incite a riot by making an incendiary speech in front of an aroused crowd. Second, from the fact that some utterance falls into the category of unprotected speech it does not follow that it should be prohibited, or that those responsible for it should be sanctioned, since there may be weightier reasons against taking such action. If sanctions are imposed, however, those sanctioned cannot claim that their right to free speech has been violated. Finally, rights can both conflict and overlap. The most important right overlapping with the right to free speech, for our purposes, is the right of free association. The right of free association is two-sided – on the one hand, the right to associate with those we choose to and on the other hand, to not associate with those we don't want to. When applied to speech, it implies that we should be free to decide both whom we want to involve in discussion and whom we want to exclude. Our possession of this right enables us to discuss intimate matters which we do not want to be made public, for example, but also to engage in decision-making about issues which fall within the remit of collectives such as sports teams, businesses, or states, and where unrestricted disclosure would interfere with the success of legitimate endeavours.

Ethical Assessment – Preliminaries

Taking PSYOP as a form of speech then, as with free speech in general, we aim to find ways both to distinguish instances of protected PSYOP – which should not be prevented or punished – from unprotected ones, and to identify further moral and pragmatic considerations which may constrain the use of PSYOP. Moreover, there are ethical issues involved in possible responses to PSYOP.

Before addressing these matters, we note a number of cross-cutting distinctions which help structure our discussion. First, we can distinguish between what we will call positive PSYOP, which aims to produce a favourable attitude or opinion to the originating state in its target audience, and negative PSYOP, which aims to sow mistrust or doubt in the target state, especially, but not exclusively, about the integrity and competence of political authorities.[7]

Second, following convention, information used in PSYOP will be classified as white, grey, or black propaganda (Jowett and O 'Donnel 1986, 17–18).[8] There are two criteria for these classifications: veracity (is the information transmitted true) and transparency (can the audience for the PSYOP easily find its source). Accordingly, some PSYOP is pure white when it is true and its source is clear, and pure black when the information is false and its source deliberately misattributed.

Third, forms of PSYOP may be categorised as either strategic, tactical, or consolidatory.[9] Strategic PSYOP aim to generate support for its sponsor, or weaken the effectiveness of a target government, or in wartime undermine popular morale and support for the war. Tactical PSYOP have more narrowly circumscribed objectives, such as helping a preferred political party win an election, or encouraging local populations in enemy territory not to interfere with tactical operations during war. As is generally true, the distinction between strategy and tactics is not always sharp, and the same operation may serve both strategic and tactical goals. Consolidatory PSYOP occur only during or in the aftermath of war and facilitate cooperation with invading or occupying forces by, for example, providing information about the mutual duties and rights of occupier and occupied.

Finally, PSYOP are used at different stages of conflict between states. As discussed in Chapter 1, it has been held that there is a categorical distinction between the states of peace and war, with the change between them marked through devices such as declarations of war and signing of peace treaties. During war, an equally firm distinction is taken to hold between combatants and civilians, marked by organisational affiliation and dress. In practice, these distinctions have not always been clear-cut, or universally respected, particularly with sub-state conflicts, but they have underpinned official policy, legal regulation, and moral thought. As introduced in Chapter 1, and discussed in detail in Chapters 3 and 4, the just war tradition (JWT) provides the framework informing both ethical theory about war and its legal regulation, providing constraints on the resort to war (*jus ad bellum*) and the way it is waged (*jus in bello*). The purpose of the standard *jus in bello* constraints, such as proportionality, necessity, and discrimination, is to limit the damage done in war and protect civilians. That purpose also applies to PSYOP in war, though the relevant constraints need to take a somewhat different form, and ethical and legal understanding is less developed here than in respect of, say, military force.[10]

As discussed, while there is, at least in theory, a sharp line between peace and war, it is not always easy to decide on which side of the line particular PSYOP operations fall. Like other military capabilities, PSYOP capacities need to be maintained during peacetime. But unlike, say, the capacity to bombard enemy positions, efficacy in PSYOP against an enemy in wartime may depend on its use against them in peacetime. Whether the population of an antagonistic state has the attitudes which PSYOP is meant to generate during war, such as sympathy and support for its policy, and doubt or disapproval for the actions of their own state, is likely to depend on the extent to which those attitudes have been fostered during peace. Moreover, since PSYOP does not involve the use of violence, it can be used as a means for taking hostile action, short of military force. The increasing importance of PSYOP, together with other non-violent means for the projection of force, has led to the sorts of claims made by the US Defence Department[11] in recommending the replacement of what it calls "the institutional remnants of the obsolete peace/war binary conception" with "a new model of cooperation, competition below armed conflict, and armed conflict", in response to "revisionist states", such as China and Russia, which are supposedly already operating with the "new model". While it is obvious that states will have antagonistic relationships with each other, there are both practical and moral reasons why it is desirable that the categorical distinction between peace and war remain in place. Blurring that distinction makes it more likely that competition becomes conflict and that conflict becomes violent. Hence the importance of continued engagement with the difficulties in understanding, assessing, and regulating PSYOP and the like within the framework of the war/peace categorisation.

PSYOP and Peace

We turn now to a consideration of the ethical use of PSYOP, and responses to its misuse. Let us begin by considering PSYOP directed by one state towards another with which it is at peace. Taking PSYOP as a kind of speech, there is a defeasible presumption in favour of its exercise; one of our tasks is to determine the grounds on which that presumption is or isn't defeated. Since a defining feature of PSYOP is that it involves communication from, or on behalf of, one state towards members of another, our discussion must be informed by the rules governing inter-state relations. Fundamental to those rules is respect for state sovereignty, implying the right to govern without interference from outside bodies.[12] It doesn't follow that PSYOP is therefore illegitimate where it is opposed by the target state. Sovereignty does not entitle the ruling power to violate the rights of others, whether citizens or not. As noted earlier, one of the implications of the right to free speech is a right to hear. So if the content of PSYOP is within the category of protected speech, its authors have a right to promulgate it, and citizens have a right to hear it. Moreover, sovereignty is now typically seen as *popular* sovereignty – it is the people who are sovereign. The right to rule may be embodied in a political authority, but to be legitimate, it must have the right kind of relationship with the people, such as being given a mandate through a free and fair electoral process.

The ethical acceptability of a PSYOP operation during peacetime depends on its consistency with its respect for the people to whom it is directed, including their right to political self-determination. Here is an example of a PSYOP operation which was clearly unwelcome to the government of the state to which it was directed, but it was, in our view, ethically justified, indeed ethically good. In 1953, Joseph Swiatlo, a high-ranking official in Poland's secret police force, defected to the West (Puddington 2000, 33–60). Beginning in September 1954, he broadcast a series of over a hundred programmes transmitted into Poland by Radio Free Poland, a service supported by the US Government, with the mission of supporting the US in its ideological struggle against the USSR. Swiatlo's programmes, reaching a huge audience inside Poland, provided richly detailed accounts of Secret Police torture, rigging of elections, the subordination of the Catholic Church, and the means by which the USSR exerted control over the nominally independent state. His testimony further revealed the effective hierarchy in Polish political life: the Polish Communist Party ruled over the people, the Police controlled the Party, and the Soviet Union commanded the Police. The programmes had a large impact, both immediately in the organisation of the state apparatus, but more significantly in the long term, in popular attitudes towards the Communist system and the influence of the USSR in Polish life. As such, they were an effective example of strategic PSYOP, as well a paradigm example of "white propaganda" – their source was accurately identified and the contents were true. Of course, the US supported the broadcasts for their own reasons, but the people of Poland had a right to know the important information they contained, information which their own government did not want them to have. While that information appears to have contributed to changes in the political life of Poland, it did so by allowing Polish citizens to make better informed, more rationally justifiable decisions (Puddington, 2000).

Russian interference in the 2016 US presidential elections presents a more morally complex example of a peacetime PSYOP operation. As detailed in "The Mueller Report" (Mueller 2019), Russia aimed to discredit Hilary Clinton and promote other candidates, ultimately Donald Trump. It pursued these aims through two interrelated means: a social media campaign and the publication on Wikileaks of documents stolen from the Democratic National Committee and Clinton's campaign (Rid 2020, 377–409). Those documents indicated that Democratic Party officials had unfairly favoured Clinton over her main rival for party nomination, Bernie Sanders, and contained excerpts from speeches that Clinton had given to banks, for high fees, and had previously refused to release. The Russians engaged in so-called "narrative laundering" – planting the seeds of stories to be picked up and amplified by trusted media outlets, without readers knowing their source. Many of these stories, such as the allegation that Clinton's campaign CEO was a member of a bizarre secret cult (Jamieson 2020), were false, and only picked up by "fake news" sites and social media. The texts on Wikileaks, however, were genuine, and they did reflect poorly on Clinton's campaign and the upper echelons of the Democratic Party, providing ammunition for Trump's attack on arrogant elites (Wylie 2020, 207).

In the social media wing of its operation Russia successfully exploited a number of features of the social media "infosphere". In the mechanical age, the cost and complexity of producing and disseminating media content meant that it could generally only be undertaken by large, recognisable organisations. The identity of traditional media, such as newspapers and television stations, allows them to be held accountable for their output, giving them at least some incentive to winnow falsehoods and constrain the expression of extreme views. Social media content, on the other hand, can be produced, and reproduced, anonymously by anyone with access to a computer, with the potential to reach as many readers as the most established media outlets, and without disincentives for lying or deception. These features of social media alone empower irresponsible or malevolent actors to spread misinformation, and they were certainly useful for the Russian mission. But the Russians also exploited the business model of social media platforms such as Facebook, which exploit the so-called outrage economy, where

> [w]hat captures the most attention on social media isn't content that makes a profound argument or expands viewer's intellectual horizons. Instead it is content that stirs emotions. Amusement, shock, and outrage determine how quickly and how far a given piece of information will spread through a social network.
>
> (Singer and Brooking 2018, 161)

Russian hackers, with fake American names, created Facebook profiles and produced inflammatory advertisements on topical political issues. With the assistance of Facebook's own tools, they directed those advertisements first to specific demographics seen as likely to be sympathetic to the messages. They further targeted individuals who had accessed pages promoted by the advertisements (Rid 2020, 397–409). In turn, many of these people further circulated the pages they had visited and the information they contained. While the advertisements reached some 29 million Facebook users, the total number of users who viewed the circulated messages is estimated to be at least 126 million.

Research shows that the Facebook "friends" networks of users who identify with a partisan political position tend to be segregated along ideological lines, so unsurprisingly users are much more likely to read and share news articles that are aligned with their ideological positions than those opposed to them (Eytan, Messing, and Adamic 2015). Moreover, Facebook presented users with pages selected by Facebook's algorithm. That algorithm is designed to maximise "engagement", understood as use of the platform, in order to drive profit. Since users are more likely to engage with controversial and extreme content – exactly the kind the Russian hackers wanted to be circulated – irrespective of its veracity, the algorithm is set to present such content. Facebook's own research shows that maximising engagement in this way contributes to political polarisation, and conversely, reducing polarisation would also mean reducing engagement (and hence profit). Facebook's research also showed that it not only hosts many extremist groups but promotes them to users, with 64% of the "joins" to these groups coming as a result of Facebook's recommendation tools (Hao 2021). In brief, Facebook facilitated the transmission of false and misleading information planted by Russian hackers about the US Presidential election without identifying their source, and in doing so contributed to further hardening and widening of ideological differences in the American public, and growing mistrust of important institutions (and made money by so doing). Social media offers the perfect vehicle to push PSYOP and drive political polarization.

> The speed, emotional intensity and echo-chamber qualities of social media content make those exposed to it experience more extreme reactions. Social media is particularly suited to worsening political and social polarization because of its ability to spread violent images and frightening rumours quickly and intensely.
>
> (Aday, Freelon, and Lynch 2021)

The Russian actions were morally outrageous, both in their goals and the means used to achieve them. The social media campaigns used deep black propaganda, spreading falsehoods and disguising their source, with the aim of manipulating those they misled to act in ways which furthered Russia's political goals. Irrespective of who Russia's preferred candidate was, and the means they used to support them, they had no right to attempt to intervene in the US election. We noted earlier that the legitimacy of PSYOP depended on their respect for the rights of the people to whom they were directed, including their right to political self-determination. The Russian actions violated that right in two ways. Free and fair elections are fundamental to political self-determination in a democracy, and the ability of citizens to gain accurate information, on the basis of which they can decide how to vote, is a necessary condition of free and fair elections. The spread of disinformation by Russia was antithetical to that condition. Second, the right to political self-determination is a special case of the broad right to free association, as discussed earlier. It means that it is up to members of a polity jointly to determine the details of their common life through discussion and decision procedures such as elections. Others may be entitled to provide information to be used in those processes, but not to involve themselves in them.

The Russian attack on the US election exemplified both tactical and strategic PSYOP. Tactically, it was powerful. It remains a matter of debate as to whether it made the difference between Trump winning or losing,[13] but there is no doubt that its messages were widely shared.[14] As well as the specific aim of ensuring Trump's victory, the Russian operation can be understood as having broader, strategic, aims, in sowing social discord, and undermining trust in the fundamental institutions of electoral politics and the media. Again, it is impossible to be definitive about the extent to which Russia achieved these strategic goals. What is undeniable is that the trend in America is in the direction Russia wanted, with increasing political polarisation, and growing mistrust of the media and of the electoral system (Allcott and Gentzkow 2017, 215–216), to the point where the false claim that the result of the 2020 Presidential election was fraudulent is widely accepted.[15]

Whatever the actual impact of the Russian PSYOP assault on the integrity of the 2016 US Presidential elections, it showed the destructive potential of PSYOP. There are, we take it, two broad strategies to address the dangers posed by PSYOP. The first is to attempt to reduce the harm they might cause and the second is to respond to PSYOP, or the threat thereof, by putting in place effective deterrent measures or responding to them in ways which force their initiators to desist. We address first strategies of mitigation.

Mitigation

One strategy (or family of strategies) of harm reduction is regulation, of the kind France, for example, introduced following Russian interference in their 2017 presidential election (Couzigou 2021). The legal measures the French took recognise the need to protect freedom of speech, particularly during elections; indeed, French law allows for a more liberal interpretation of freedom of expression in electoral campaigns than in other circumstances. They aim to protect the integrity of the electoral process, not by forbidding the promulgation of false information *per se*, but rather by combatting the use of false information online to manipulate opinion. Judges are given wide discretionary power to halt the spread of such information, including requiring that internet access providers suspend or suppress content, close a user's account, or even block access to a website. Judicial exercise of these powers must be necessary and proportionate to their objective.

The kinds of measures adopted by the French involve officials making judgments about the veracity of information, and deciding what citizens are allowed to see and hear. To that extent, they constitute a restriction on freedom of speech. As with any policy which limits freedom, they require justification, both at the level of the laws and in the particular applications of those laws. Those justifications are consequentialist in nature – these restrictions are better than the risk of compromising the integrity of elections. The restrictions are justified only if they are *necessary* to achieve that goal. As argued in Chapter 4, necessity is not a feature of actions *per se.* An action is necessary only where there is no other feasible, less costly, way of achieving the desired outcome. There are, in fact, a range of possible measures to reduce the potential harm caused by PSYOP against civilian populations which do not involve restricting freedom of speech, at least if that is taken, as suggested earlier, as freedom of discussion.

First, there are possible regulatory actions to address the way in which social media platforms amplify harmful content. We noted in our discussion of Russian attacks on the integrity of the US election in 2016 that they exploited the capacity of the social media users to communicate anonymously, and the business model of the major social media platforms, particularly Facebook. While the social media platforms themselves have taken some steps to control content and flag material of dubious veracity, at least in part because of the negative publicity consequent on the events in 2016, they have not been prepared to make fundamental changes to the algorithms which select content to present to users. Unless Facebook and similar platforms are prepared to make the changes necessary to prevent the harms resulting from their algorithms (which they show no sign of doing), states have good reason to legislate to force them do so. Far from such legislation interfering with free speech, it would push social media platforms in the direction of providing a true "market place of ideas", where users are confronted with a range of contrasting claims, rather than herding them into isolated, self-reinforcing epistemic clusters, as they currently do.

The strategies of mitigation we have considered so far aim to make it less likely that people will be exposed to false and misleading messages transmitted from PSYOP. A different, though compatible, set of strategies aim to make it less likely that they will be affected by them even if exposed, by increasing their ability to discriminate between true and false claims and between reliable and unreliable sources of information – by developing social media literacy. As noted in our discussion of the Millian distinction between protected and unprotected speech, some speech act can fall into the unprotected category when it is uttered in a context where it is likely to incite non-rational behaviour with seriously harmful consequences, though in a different context it would fall into the protected category. Legislation of the kind introduced in France in effect is justified along these lines: authorities have the power to suppress material where – but only where – they judge it is likely to subvert the integrity of the electoral process. That judgment must take into account the effects of the material on those exposed to it. The less likely they are to believe it, the less need for its prohibition, and the more broadly the boundaries of protected speech can be drawn.

To some extent, social media literacy is likely to increase naturally, as it has with other novel media, such as cinema and television, where consumers have become more sophisticated and discerning over time. But there is much that can be done to hasten the process. Apart from regulation, the very techniques and technologies which have made social media so ripe for exploitation have the potential to help combat its misuse. Machine learning is capable of detecting “fake news” (Tacchini et al. 2017; Wang 2017), while “crowdsourcing” – using large numbers of people to reach judgments about the reliability of different information providers or the likely veracity of individual stories – has also been shown to be highly accurate (Pennycook and Rand 2019). Use of these techniques and promotion of their findings can make falsehoods on social media less likely to be believed and transmitted. And of course the education system can assist students to become more discerning users of social media. Again, development of social media literacy is desirable in itself, in fostering a more informed and discerning populace.

Deterrence and Response

As we have noted, PSYOP are not *per se* illegitimate. Just as there is a presumption that speech is protected, with the onus on those who wish to prevent or penalise it to show that it is unprotected, so there is a presumption that PSYOP is permissible, with the onus on those who want to repress it to show why they are justified in so doing. And just as resisting or punishing those who engage in the wrongful suppression of speech may be justified, so may resisting or penalising those who wrongfully suppress legitimate PSYOP. International human rights instruments, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), enunciate the right to free speech, including across national borders, while recognising (in the case of the ICCPR) limits to that right. The ICCPR prohibits “any propaganda for war”; and “[a]ny advocacy of national, racial, or religious hatred that constituted incitement to discrimination, hostility or violence”.[16]

It is necessary, then, to distinguish legitimate and illegitimate PSYOP. Illegitimate PSYOP justify proportionate countermeasures, as per the reciprocity principle introduced in Chapter 4. However, the nature of modern PSYOP often presents difficulties in knowing when such responses are justified, against whom, and in what measure, posing challenges for discrimination and proportionality. First, the relative cheapness and availability of the technology needed to undertake PSYOP means that they can be undertaken by non-state actors, albeit ones which may be acting on behalf of a state or at least with its support, making it hard definitively to identify a responsible state actor, if there is one. Even where there is evidence that makes this possible, the responsible state may deny involvement. Second, even where it is possible clearly to identify the agent responsible for PSYOP, it can be difficult, if not impossible, to calculate its impact, as we pointed out regarding the Russian actions in 2016.

Moreover, we are not suggesting that we can never know, or at least have good reason to believe, whether or not an attempt to influence someone to act in a certain way has succeeded. In the case of the Russian operation, however, the information they put into circulation was only one ingredient in a stew of influences, including prior ideology, conversations with peers, and the reach of mainstream media. Moreover, typically the messages circulated did not directly advocate voting one way or the other, so whatever causal impact they had was heavily mediated through the attitudes, beliefs, and actions of those they reached, and subsequently on the institutions of democracy. To calculate the impact of the Russian PSYOP operations, it would be necessary to establish a complex counterfactual: what would have happened if they did not exist? Given the range of influences on a personal decision to vote for a particular candidate in a particular election, such counterfactuals could only be highly speculative and approximate. For many PSYOP there will be similar problems in calculating their effect, and hence in deciding what would count as a proportionate response.

Even where it is clear that hostile PSYOP has occurred, where the responsibility for it lies, and what its impact was, it does not follow that it will have breached international law. The Russian actions in 2016, for example, violated a number of national laws, with charges being laid against individuals, but they may not have been of a kind or level which breached international law. The legal scholar Alison Denton denies that they were, on two grounds. First, "the harm resulting from the influence campaign was minimal" (Denton 2019, 200). Second, and more significantly for our purposes, the Russian actions were not, on her view, the sort of acts which are prohibited under international law; they did not constitute an armed attack or use of force; they did not violate the norm of non-intervention because they were "not sufficiently coercive"; and they did not infringe on US sovereignty as they "failed to interfere with or usurp an inherently governmental function". We do not intend – nor are we qualified – to engage in a discussion about international law. What we take to be significant about the picture of international law painted by theorists, such as Denton, is that it fails to accommodate the developments in the power and reach of PSYOP.[17] We elaborate on this point below.

Whatever the difficulties in determining whether or not PSYOP are illegitimate, and if so what sorts of responses are justified, none of these difficulties need apply, either in principle or as a matter of fact – there are cases where there it is clear where responsibility lies, and the aim of PSYOP so explicit, and the link between it and its desired effect so obvious, that there can be no doubt about its impact. The media campaign in Rwanda leading up to the massacre of hundreds of thousands of members of the Tutsis group by Hutus, largely undertaken through radio broadcast, is a paradigm case. Over a period of years, media outlets supporting the incumbent regime fostered an "us and them" mentality in a society where the two groups had long coexisted and cooperated, went on to describe alleged, unsubstantiated atrocities committed by Tutsis against Hutus, creating a "kill or be killed" atmosphere, and made explicit calls to hunt down and kill Tutsis, with directions as to where to go to do so.[18] The UN International Criminal Tribunal for Rwanda subsequently found three senior media operatives guilty of genocide, incitement to genocide, conspiracy, crimes against humanity, extermination, and persecution.

PSYOP as Just Cause for War?

Whether or not the harm of the Russian operations in 2016 was minimal, clearly there is potential for much more significant harms to be generated by well-planned and executed PSYOP operations. Apart from those we have already noted – attacks on the integrity of the electoral process, social polarisation, and diminishing of trust in the media – such potential harms include undermining of financial confidence leading to panic and collapse of stock markets, radicalising vulnerable youths, support for terrorist violence, and inciting hatred between ethnic groups, leading to civil war. So, it may be clear that PSYOP is creating a catastrophic state of affairs, which demands an immediate effective response. Imagine, for example, an ongoing, well-disguised attack on the electoral system, including widely circulated and believed allegations of massive fraud committed by partisan officials, leading to widespread rejection of the legitimacy of the elected regime and increasing civil unrest and violence.

Could such PSYOP count as *causus belli* – an act which justifies its target, and other states, in responding with a declaration of war[19] and engaging in military action against the offending state with the aim of forcing them to stop? To be clear, the question is not whether if such acts were part of a range of activities such as cyberattacks, armed incursions, etc., they could be counted as relevant to calculations regarding the seriousness of an attack, and whether these acts jointly counted as an act of war. The question is whether PSYOP by *themselves* could so count as an act of war. States are customarily recognised as having an inherent, sovereign right of self-defence. Since the end of the Second World War it has been accepted that the exercise of that right is triggered only by aggression from another state. While the kinds of acts which count as aggression have not been definitively defined in international law, it has been understood as kinetic, military force that poses a threat to a state's control over its territory and ultimately its political autonomy.[20]

In no standard sense of the term "force" could it be taken to apply to PSYOP and other non-violent hostile actions, though a lot of ink has been spilt trying to show that it should be.[21] Rather, we should look to the analogies between the features of military aggression which justify counting them as the kinds of acts which trigger the right to self-defence, and those of PSYOP. If those analogies are strong enough, some PSYOP may count as just causes for states going to war in self-defence. We list six features of an act of military aggression: the first three specify the conditions which are necessary for it to count as an act of war; the second three specify conditions which must be satisfied for the victim of aggression to be justified in believing that they have a just cause[22] for going to war against the agent of that aggression.[23] We then consider the strength of analogies between these features and those of PSYOP of the kind outlined in the previous paragraph.

1 *Severity*: this includes both the kind of harms (such as death and destruction, or breakdown in social order or political authority) caused by the aggressive act and their amount.

2 *Immediacy*: absent preventive action, these harms are unavoidable in the present or very near future.
3 *Invasiveness*: the aggressive act causing the harm reaches into the target state to produce its effect.
4 *Directness*: the harms caused are clearly both an effect of the actions of the aggressor and intended as such.
5 *Measurability*: there is an agreed metric concerning how relevant harms are measured, and it is in fact possible to (approximately) measure them using that metric.
6 *Presumptive illegitimacy*: The kind of act which causes the harms (e.g. military violence) is presumptively illegitimate. There is a standing prohibition against it, except in specified circumstances.

We take it that the kinds of PSYOP, we have outlined earlier, clearly exhibit features 1–3; they cause severe harms, which are unavoidable unless preventive measures are taken, and they cause those harms by actions which take effect within the target state. These features concern the effects and site of the aggressive act – it is happening (or is about to happen) within the borders of the victim state and will cause large amounts of serious harm unless resisted or prevented. Given the inherent rights of states to defend themselves, it follows that states have rights to take the necessary measures to resist such acts, whether they involve the use of military force or some other method.

Features 4–6 are concerned with the normative evaluation of the harmful acts and those responsible for them: (4) specifies necessary conditions for holding an agent to be morally responsible for an act, *viz* that they caused it and did so intentionally; (5) points to the need to be able to assess the extent of the harms caused in an objective and generally accepted way; (6) pertains to the onus of justification – does it rest on the agent responsible for an action, or those who claim that they are entitled to take it, or demand that they stop?

As a general rule, the analogies between the kind of military force which could justify defensive military action and PSYOP are much weaker in the case of features (4) and (5), which is not to say that they never hold. The Rwandan media case showed that it may be possible to see a direct causal link between particular PSYOP and the harm caused, and for it to be plain that this was the intention of those responsible for the PSYOP. Moreover, assuming that the relevant harmful effects of PSYOP in that case were primarily the resultant death and mutilation, they could be (roughly) quantified. But the mediated effects of PSYOP mean that this will often not be possible: while it may be plausible that the PSYOP had *some* impact, the multi-factorial causes of most important social phenomena make it impossible to separate out the effect of PSYOP from other causes with any exactness. And the intentions of those responsible for a PSYOP may only be vague and indeterminate. The Swiatlo broadcasts, for example, may ultimately have played some role in the rise of Solidarity in Poland and even to the shape of the post-communist regimes there, but the sponsors of the broadcasts could have intended such effects only in the most general terms.

In JWT, the just cause criterion is often considered to be the most important of the six *ad bellum* criteria. While in theory PSYOP could count as a *causus belli*, in practice it will be rare, since difficulties in demonstrating that PSYOP led to some particular social and political outcome make it impossible to satisfy conditions (4) and (5).

In respect of condition (6), unlike the use of military force, which is presumptively illegitimate, given the presumption against resort to violence, PSYOP are presumptively legitimate, given the presumption in favour of free speech. *Presumptively* legitimate doesn't mean *actually* legitimate, of course, and particular PSYOP may be, or judged to be, illegitimate. The problem is the contestability of such judgments in many cases, given the indeterminacy of the features of directness and measurability. The contrast with military aggression is illustrated by the differences in difficulty in judging the wrongness of Russian actions in 2016 and 2022, and the appropriateness of responses to it. While, as we've seen, well-qualified judges disagree about the effects and seriousness of the Russian attempts to promote Donald Trump's election in 2016, very few in liberal democratic states reasonably dispute that Russia's invasion of Ukraine was an illegitimate act of aggression and that the Ukrainians are justified in their military resistance.

The post Second World War prohibition against aggressive war looked to reconcile the right to self-defence with the maintenance of a peaceful international order. That reconciliation depends on the existence of bright lines demarcating aggression from non-aggression, which make it clear how states are and are not entitled to act, so that it is difficult, if not impossible, for a state to use the false or mistaken claim that is a victim of aggression as a pretext for war. In the case of military force, national borders function, literally, as those lines. In the case of PSYOP, national borders don't function as bright lines, since it is not in itself wrong to transmit information across them, even when that is unwelcome to the receiving state. Furthermore, the judgments as to whether PSYOP does, in fact, constitute an unjustified attack on sovereignty may depend on the point of view of the spectators. As PSYOP come to pose greater threats to states' political self-determination, there is increasing risk that what one state sees as justified recourse to war, its antagonist will see as unjustified aggression in response to legitimate communication, making it harder to reconcile respect for states' inherent right of self-defence with the maintenance of peace.

PSYOP in War

Once war has begun, PSYOP have two roles. As with other military functions, they operate to degrade enemy capacity. As well as its function in achieving military success, consolidatory PSYOP have an important role in communicating with enemy forces and civilians in order to limit harms in war.

Like any means used in war, PSYOP is subject to ethical constraints. However, since it does not make use of violence, the rationale for those constraints, which apply to the use of military force, say, may not apply, or apply in the same way. For example, the condition of necessity requires that the least harmful feasible means be used to achieve a military objective. This condition obviously restricts the use of military force (violence), which, by its nature, is harmful, to as much, but no more than, as is necessary to achieve the objective. That amount is influenced by the availability of (legitimate[24]) efficacious PSYOP, which, by its nature, is not harmful: the more effective they are, the smaller amount of violence necessary. So the condition of necessity requires the maximum efficacious use of PSYOP and the minimum efficacious use of violence. Furthermore, the greater the availability of effective PSYOP, the easier it will be to satisfy the criteria of proportionality. A war, which would be disproportionate if waged only by the use of armed force, may become proportionate through the use of PSYOP.

Much, though but by no means all, PSYOP in war involves the use of deception. The use of deception falls under the heading of "chivalry" in the law of war (International Committee of the Red Cross 1977). Despite the association of the term with outdated romantic notions, chivalry in this sense has an important ethical role, in supporting respect for rules which limit the damage done in war. A distinction is drawn in law between "ruses", which are permissible, and perfidy, or treachery, which is not (International Committee of the Red Cross 1977, article 37). PSYOP have made use of a wide range of ruses, such as "allowing" deliberately misleading but apparently authoritative operational plans to fall into enemy hands, issuing of bogus orders purporting to have come from the enemy commander, erection of dummy camps and airfields, and so on. Perfidy involves deceptively violating the protections given by the laws of war, in order to gain a military advantage, say. So it is an act of perfidy to pretend to accept surrender of troops, then kill them, just as it is an act of perfidy to pretend to surrender in order to lull enemy troops into a complacent position which makes them vulnerable to attack. If soldiers lose confidence that they will become immune to attack if they surrender, they have no incentive to stop fighting even when they judge their military situation is hopeless, perpetuating conflict and increasing casualties on both sides. We can explain these constraints by reference to the principle of reciprocity, motivated here by mutual self-interest.

Just as the ethical considerations restricting the use of deceptive PSYOP in wartime aim to limit the destructiveness of war, so do those governing the use of consolidatory PSYOP. Consolidatory PSYOP applies to both enemy forces and civilians. In the case of armed forces, it includes the provision of information about means and consequences of surrender. Giving false information about these matters, or not respecting the assurances given, counts as perfidious. Moreover, there is not simply a negative obligation not to promulgate false information but a positive obligation to provide true, accessible information, in order to allow orderly processes of surrender, transfer of power and administration by occupying powers, processes which benefit all involved.

In the case of consolidatory PSYOP directed to the civilian population, the principle of discrimination, forbidding the intentional harming of civilians, makes a wide range of PSYOP ethically unacceptable. These include PSYOP which degrade the efficacy of important infrastructure, particularly communications systems, by, for example, promulgating false information which purports to be issued by official sources, causing loss of confidence in the reliability of official channels, or interfering with the good functioning of civil society by, for example, promulgating misinformation about public health measures. As with consolidatory PSYOP directed at armed forces, there is also not simply a negative requirement to refrain from certain kinds of consolidatory PSYOP directed at civilians but a positive requirement to engage in it, through the provision of accurate information about civilian rights and duties in relation to invading or occupying forces, information which facilitates their acting in ways which does not endanger them and allows them to access assistance as needed. This requirement can be seen as a consequence of the principle of discrimination, assuming that the rationale of that principle is understood as the minimisation of the harm suffered by civilians in war. So understood, the principle is not satisfied simply by armed forces not intending to harm civilians in their actions, they must also intend not to harm them, consistent with military necessity and proportionality.[25]

Conclusion

PSYOP, as means for the promotion of state interests across international borders, need to conform to the ethical constraints governing international relations in both peace and war. The growth in the reach and power of PSYOP means that it has become increasingly important to decide whether they do so, and the kinds of responses appropriate when they do not. Taking PSYOP as a form of communication, we have pointed to two interacting implications relevant to such decisions. First, as with communication in general, 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. In some cases, PSYOP fall into the unprotected category simply in virtue of their content, such as propaganda for war, or advocacy of hatred of particular groups. In many cases, however, it is the effects rather than the content of PSYOP which determine which category they fall into. PSYOP, which have the (likely) effect of seriously undermining the capacity for self-determination of a state, for example, thereby fall into the unprotected category. If the harmful effects are serious and imminent enough, such PSYOP may count as *causus belli.*

Thus, whether a particular PSYOP should count as unprotected or not in virtue of its effects, and in particular whether it should count as an instance of aggression which justify exercise of the right to self-defence, requires a case-by-case judgment. Unlike typical cases of military aggression, the mediated nature of the effects of PSYOP means that such judgments are often difficult to make and contestable. If disagreements about the effects of PSYOP, and responses to them, are not themselves to become triggers for conflict, it will be necessary to put in place systems of regulation, adjudication, and enforcement of PSYOP.

Notes

[1] We follow the US practice of using the term PSYOP to refer both to particular national security psychological operations and to the general practice.

[2] A more recent, widely cited, definition is found in the document "JP 3-13.2, Psychological Operations", from the US Joint Chiefs of Staff (2010), which characterises PSYOP as *[p]lanned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organizations, groups, and individuals*. Both definitions are wide in scope, but the earlier definition has the advantage of making it clear that PSYOP are supposed to be in the service of "national objectives".

[3] Taylor (2007) sees dedicated military PSYOP organisations beginning in the First World War.

[4] The increasing importance of non-violent means in pursuing military goals is reflected, for example, in the claim by General Valery Gerasimov, Chief of the Russian General Staff, that the ratio between non-military (non-kinetic) and military (kinetic) operations should be 4:1. "Non-kinetic" operations are of course wider than PSYOP, but include them. Splidsboel Hansen (2017).

[5] A good discussion of these developments and their implications, as well as further references, is found in Tim Hwang and Lea Rosen (2017); cf. Wagner et al (2012).

[6] Not all PSYOP makes use of language, or even expression in any ordinary sense. For example, US military interrogators were reported to have repeatedly played heavy metal music to detainees – a form of torture – as a way of breaking their resistance and getting information from them. While this arguably fits the characterisation of PSYOP, we take it that it is a marginal form.

[7] It's possible that a successful PSYOP operation may have both a positive and a negative aspect, enhancing the standing of one state while diminishing that of its foe.

[8] The term "propaganda" generally has a pejorative connotation, with implications of manipulation and deception. In this context, it need not have those connotations, particularly in reference to "white" propaganda.

[9] US Joint Chiefs of Staff (2010, chapter 7).

[10] For a useful discussion of the legal situation, with implications for relevant ethical issues, see Hwang and Rosen (2017).

[11] US Joint Chiefs of Staff (2018).

[12] State sovereignty and its relation to privacy is discussed in Chapter 8.

[13] Jamieson (2020) argues that it is likely that Russian interference swung the election in Trump's favour. Denton (2019) is more sceptical. Jane Mayer (2018) outlines Jamieson's argument and discusses countervailing views. Likewise, Thomas Rid argues that the efforts by the Russian Internet Research Agency and others were "the least effective component of the overall Russian disinformation effort in 2016" (Rid 2020, 409).

[14] Jane Mayer (2018) says that, for example, 470 Facebook accounts are known to have been created by Russian agents: six of them alone generated content shared at least 340 million times. A Facebook page for a fake group, Blacktivist, inflamed racial tensions by posting militant slogans and videos of police violence against African-Americans: it received more hits than the Facebook page for Black Lives Matter. Cf. Denton (2019, 192).

[15] Around 65% of Republican voters believe this, and about 35% of the American public overall (Swann 2022).

[16] See International Covenant on Civil and Political Rights of 1966 (United Nations n.d., articles 19 and 20).

17 For a more developed argument to this conclusion, incorporating Information Operations more broadly, see Hollis (2008).

18 Kellow and Steeves (1998); transcripts of the inflammatory radio broadcasts can be found at http://migs.concordia.ca/links/RwandanRadioTrascripts_RTLM.htm

19 Assuming, of course, that the other *jus as bellum* conditions such as proportionality, probability of success, etc. are satisfied.

20 A 1974 resolution of the UN General Assembly (A/Res/29/3314) provides a non-exhaustive list of acts of aggression, including "invasion or attack by the armed forces of a State of the territory of another State", "bombardment by the armed forces of a State against the territory of another State", and the "blockade of the ports or coasts of a State by the armed forces of another State".

21 For an influential example, see Schmitt (1999). Schmitt distinguishes between what he calls instrument-based (e.g. use of armaments) and consequence-based approaches to defining force and recommends the consequence-based approach. Schmitt, along with others, is, in effect, trying to fit responses to novel methods of coercion into the prevailing conceptual structure of international law, but can only do so by bending the meaning of words such as "force" (in our view beyond their breaking point). His method involves a confusion between descriptive and normative criteria. His "consequence-based" approach conflates the meaning of different (sorts of) acts on the basis of the sameness of their outcomes. Poisoning may have the same effect as shooting, but poisoning is not the same as shooting, even though poisoning may be just as bad as shooting.

22 The kind of justification at issue here is subjective justification. If the first three conditions hold, then it is possible that there is in fact (objectively) justification for the target of PSYOP going to war. For them to be subjectively justified, they must know, and be able to demonstrate, that these conditions hold.

23 This is adapted from Schmitt ibid., p. 914.

24 The conditions of legitimacy are discussed further.

25 Walzer summarises this requirement as the "doctrine of double intention" (Walzer 2015, 151–56).

References

Aday, Sean, Deen Freelon, and Mark Lynch. 2021. 'How Social Media Undermined Egypt's Democratic Transition.' *Washington Post*. www.washingtonpost.com/news/monkey-cage/wp/2016/10/07/how-social-media-undermined-egypts-democratic-transition/

Allcott, Hunt and Gentzkow, Matthew. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31(2): 211–36. doi: 10.1257/jep.31.2.211

Bakshy, Eytan, Solomon Messing, and Lada A. Adamic. 2015. "Exposure to Ideologically Diverse News and Opinion on Facebook." *Science* 348(6239): 1130–32.

Couzigou, Irène. 2021. "The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression." *Election Law Journal: Rules, Politics, and Policy* 20(1): 98–115.

Denton, Allison. 2019. "Fake News: The Legality of the Russian 2016 Facebook Influence Campaign." *BU Int'l LJ* 37: 183.

Fish, Stanley. 1994. *There's No Such Thing as Free Speech: And It's a Good Thing, Too*. New York: Oxford University Press.

Hao, Karen. 2021. "The Facebook Whistleblower Says Its Algorithms Are Dangerous. Here's Why.' *MIT Technology Review*. www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms/

Hollis, Duncan B. 2008. “New Tools, New Rules: International Law and Information Operations.” In *The Message of War: Information, Influence and Perception in Armed Conflict*, edited by G. David and T. McKeldin. Temple University Legal Studies Research Paper No. 2007–15. https://ssrn.com/abstract=1009224

Hwang, Tim and Lea Rosen. 2017. *Harder, Better, Faster, Stronger: International Law and the Future of Online PsyOps*. ComProp Working Paper.

International Committee of the Red Cross. 1977. “Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I).” June 8. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/470-750046?OpenDocument

Jamieson, Kathleen Hall. 2020. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don’t, Can’t, and Do Know*. Oxford University Press.

Jowett, Garth and Victoria O ’Donnel. 1986. *Propaganda and Persuasion*. Thousand Oaks, California: Sage.

Kellow, Christine L. and H. Leslie Steeves. 1998. “The Role of Radio in the Rwandan Genocide.” *Journal of Communication* 48(3): 107–28.

Mayer, Jane. 2018. “How Russia Helped Swing the Election for Trump.” *The New Yorker*. September 24. www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump

Mill, David van. 2017. “Freedom of Speech.” The Stanford Encyclopedia of Philosophy. 2017. http://plato.stanford.edu/archives/win2013/entries/freedom-speech/

Mill, John Stuart. 1971. *Essential Works of John Stuart Mill*. London: Bantam Press.

Mill, John Stuart. 1971. “On Liberty.” In *Utilitarianism, On Liberty, Essay On Bentham*, edited by Mary Warnock. London: The Fontana Library, pp. 88–180.

Mueller, Robert P. 2019. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. www.justice.gov/archives/sco/file/1373816/download

Pennycook, Gordon and David G. Rand. 2019 “Fighting Misinformation on Social Media Using Crowdsourced Judgments of News Source Quality.” *Proceedings of the National Academy of Sciences* 116(7): 2521–26.

Puddington, Arch. 2000. *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty*. Lexington, University Press of Kentucky.

Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. London: Farrar, Straus and Giroux.

Sadurski, Wojciech. 1999. *Freedom of Speech and Its Limits*. Dordrecht, Boston: Kluwer Academic.

Schauer, Frederick. 1982. *Free Speech: A Philosophical Enquiry*. Cambridge: Cambridge University Press.

Schmitt, Michael N. 1999. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.” *Columbia Journal of Transnational Law* 37: 885.

Singer, Peter Warren and Emerson T. Brooking. 2018. *LikeWar: The Weaponization of Social Media*. Boston: Eamon Dolan Books.

Splidsboel Hansen, Flemming. 2017. *Russian Hybrid Warfare: A study of Disinformation*. DIIS Report, No. 2017:06, ISBN 978-87-7605-880-7. Copenhagen: Danish Institute for International Studies.

Sunstein, Cass R. 1993. *Democracy And The Problem Of Free Speech*. New York: The Free Press.

Swann, Sara. 2022. “No, Most Americans Don’t Believe the 2020 Election Was Fraudulent.” *Politifact*. February 2. www.politifact.com/factchecks/2022/feb/02/viral-image/no-most-americans-dont-believe-2020-election-was-f/

Tacchini, Eugenio, Ballarin, Gabriele, Vedova, Marco L. Della, Maréchal, François, and De Alfaro, Luca. 2017. "Some Like It Hoax: Automated Fake News Detection in Social Networks." *ArXiv (Cornell University)*, April. https://doi.org/10.48550/arxiv.1704.07506

Taylor, Philip M. 2007. " 'Munitions of the Mind': A Brief History of Military Psychological Operations." *Place Branding and Public Diplomacy* 3: 196–204.

United Nations. n.d. "International Covenant on Civil and Political Rights." OHCHR. www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

US Joint Chiefs of Staff. 2010. "JP 3-13.2–Psychological Operations." January 7. https://fas.org/irp/doddir/dod/jp3_13_2.pdf

US Joint Chiefs of Staff. 2018. "Joint Concept for Integrated Campaigning." March 16. www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257

Wagner, Claudia, Silvia Mitter, Christian Körner, and Markus Strohmaier. 2012. "When Social Bots Attack: Modeling Susceptibility of Users in Online Social Networks." *#MSM2012*.

Walzer, Michael. 2015. *Just and Unjust Wars*. New York: Basic Books.

Wang, William Yang. 2017. "Liar, Liar Pants on Fire": A New Benchmark Dataset for Fake News Detection." *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics*. https://doi.org/10.18653/v1/p17-2067

Wylie, Christopher. 2020. *Mindf* Ck: Cambridge Analytica and the Plot to Break America*. London: Profile Books.

Part III

The Future of Intelligence and the Evolution of Intelligence Institutions

In the final part of this book, we have four chapters that look at a range of ethical challenges in intelligence that force us to rethink certain concepts central to intelligence ethics; privacy and independence, and demand that our intelligence practices and institutions evolve in ways that are in line with current and future intelligence practices and national security challenges; emerging technologies, and intelligence for public health surveillance.

The point of these chapters is to show that if intelligence is to be responsive to new and developing national security threats, then intelligence ethics must also reflect and respond to those changes. What we suggest here is that principles like privacy and independence – which are core to good intelligence practice – must be updated to recognise the current national security environment. Likewise, we look to a set of new technologies that pose particular challenges that only intelligence institutions can respond to. Finally, in our concluding chapter, we look to the roles played by intelligence institutions in the recent COVID-19 pandemic to offer suggestions of how intelligence ethics needs to recognise and embrace the blurred lines between traditional intelligence and the modern reality of national security risks and threats faced by states.

DOI: 10.4324/9781003106449-10

8 Privacy as Digital Sovereignty

Rethinking Privacy for International Intelligence

Adam Henschke

This chapter looks at the ways that technology and intelligence practices change how we think of privacy. In the academic philosophy literature on privacy, it is typically discussed in two broad ways – descriptive accounts: what do we mean when privacy is violated and so on, and normative accounts: why does privacy matter at all? In much of this literature, privacy is understood as an interpersonal ethical issue – we understand privacy descriptively and normatively by reference to interpersonal relations. Parallel with these discussions, privacy is also frequently considered in a political sense – seen as a bulwark against state power intruding on citizens. Much discussion of privacy and security, for example, sees the relevant questions as what are the state's duties and responsibilities to its citizen's privacy in the face of the need to gather intelligence against things like terrorist threats? On this approach, rather than individuals, the relevant actors are the state and its citizens. In addition to these conceptions of privacy, I propose a third concept of privacy that arises largely due to technological disruptions – the idea of privacy as a species of international relations. Here, due to cyberspace's non-geographic nature, states as actors can violate the privacy of other state's citizens. Yet, on this species of privacy, neither the interpersonal nor the state-citizen accounts of privacy seem capable of dealing with such privacy violations. Instead, I suggest that the notion of digital sovereignty can go some way to dealing with privacy violations when the primary actors are states.

A Problem in Context and of Concepts

The basic issues that this chapter looks at are how privacy relates to intelligence, how new technologies and state behaviours are changing how we think of privacy, and the limits and responsibilities of intelligence institutions in liberal democracies. The chapter will present a plural concept of privacy in which we recognise different ways of conceptualising privacy. This plural concept first acknowledges that there are different ways to conceptualise privacy. Second, the plural concept offers a way to deal with the special issues that arise for privacy when considering it in a context of intelligence and counter-intelligence. That is, privacy is an essential concept for us to understand when considering the ethics of intelligence, but

DOI: 10.4324/9781003106449-11

in order for this concept to serve a practical purpose, we need to see privacy in at least three different ways – as interpersonal, as institutional, and, increasingly, as international.

To begin, consider the following events. First, in March 2019, an armed man attacked two mosques in Christchurch, New Zealand, wounding 40 and killing 51. The shooter took advantage of social media, broadcasting his attacks live. Prior to the attacks he had posted a 74-page manifesto that sought to explain the attacks as an effort to protect the white race from genocide (Moses 2019). After the Christchurch attacks, a number of white/nationalist terrorist plots have been foiled in range of countries, in which the would-be attackers explicitly stated that the Christchurch shooter's manifesto played a role in motivating their plans. A 24-year-old man from Oldham, Greater Manchester, UK was arrested on 16 March for sending Facebook posts in support of the shooting. On 20 March, an employee for Transguard, a company based in the United Arab Emirates, was fired by his company and deported for making comments supporting the shooting as well. In Canada, neo-Nazis Paul Fromm and Kevin Goudreau were put under investigation after the former shared the manifesto of the shooter on the website of his organisation Canadian Association for Free Expression. Founder of a Facebook group, known as Odin's Warriors, Thomas Alan Bolin and his cousin Austin Witkowski attempted to commit a copycat attack in Baltimore, Maryland. Under the aliases "Peter Vincent" and "Ragnar Odinson", the duo sent threatening messages on Facebook Messenger and planned to buy food, ammunition, and firearms in preparation for a similar attack. Bolin also praised the Christchurch shooter's live-stream and manifesto. Then, in April 2019, the terrorist group National Thawheed Jamaath carried out a terrorist attack on Easter Sunday targeting Christians in Sri Lanka. "In all, eight men and one woman belonging to local Islamist groups detonated bombs almost simultaneously in several parts of the country, killing themselves and more than 250 others" (Gunasingham 2019, 8). The Sri Lankan Defence Minister stated that the attacks were a response to the terrorist attack in Christchurch (Laxman and Kesslen 2019).

This example has been chosen to show the international challenges facing modern intelligence. We have a blurring of the lines between domestic and international terrorism where acts of domestic political extremism need not be just understood in an international context but also require intelligence and information sharing between countries about their own domestic national security risks. The Christchurch shooter was an Australian, who travelled to New Zealand, to engage in an act of terrorism. This act then played a role in motivating others around the world to plan and engage in acts of violence. In the case of those influenced by the manifesto, intelligence agencies required the capacity to engage in a traditional domestic intelligence operation, receiving intelligence about a potential domestic threat and crafting a response to that threat. This domestic response had to be conducted in a context in which the international aspects were understood.

In a second event, in 2019, the Australian National University (ANU) publicly stated that it was the victim of foreign intelligence attacks and named China as the source of these attacks. The ANU Vice Chancellor stated that "[w]e believe there was unauthorised access to significant amounts of personal staff, student and visitor data extending back 19 years" (Martin 2019). In this attack, the information said to have been accessed included staff and student "names, addresses, dates of birth, phone numbers, personal email addresses, emergency contact details, tax file numbers, payroll information, bank account details, passport details and student academic records" (Martin 2019).

While very different in scope, content, and outcome, both examples point to a set of common elements – that governments of liberal democracies need to act in complex informational spaces. On the one hand, as threats like terrorism evolve, governments must keep pace to ensure that their citizens are safe. This essentially means that intelligence institutions must keep up with changing nature of threats to national security, and governments grant them the powers that they need in order to keep their citizens safe.[1] A key element to this is the capacity to engage in technologically enabled surveillance. On the other hand, as the ANU example shows, private citizens, private companies, and public institutions are now the targets of foreign intelligence operations. So governments – through various intelligence and other national security agencies – need to be more involved in widespread counter-intelligence activities. Given that information is an evolving national security concern, national security practitioners need to be able to develop their responses in kind (Henschke 2021). In short, in order for intelligence agencies to do their job, they need to both use and protect personal information.

The ethical challenge, however, is how to do this in a way that is privacy-respecting. For liberal democracies, privacy is a cornerstone concept, something that sits at the very heart of what a liberal democracy is.[2] This is both a social and a political claim. It is a social claim in that liberal democratic societies take privacy to be important. Someone cannot peer into your bedroom window, access your medical information, place cameras in your home, without your knowledge or consent. Likewise, it is a political claim in that governments cannot do this either. There is a general prohibition on the government spying on you. In liberal democracies, government agents typically must go through some set of legal or related processes in order to gain permission to engage in activities that would typically violate a citizen's privacy. For instance, a warrant is needed in order for a surveillance camera to be place in your home, and in order for that warrant to be granted, the requesting agency typically must prove that the surveillance is necessary, discriminate, and proportionate (Michaelsen 2010). In liberal democracies, privacy matters.

Much like many of the problems that we have already discussed in this book, when thinking of privacy, intelligence sits in an ethically, socially, legally, and politically complicated space, where intelligence institutions will be criticised for not acting, as well as acting. For instance, former US President Trump criticised the Federal Bureau of Investigations (FBI) for not monitoring and responding to social media posts by the Stoneman Douglas High School shooter (Graham 2018). At the same time, Trump repeatedly criticised the FBI for placing him and his associates under surveillance and investigation.[3] Intelligence agencies are thus criticised for respecting privacy too much and not enough. Similar to other government institutions, as Genevieve Lester points out, intelligence typically operates in a pendulum cycle, where perceived intelligence failures lead to increased intelligence powers, which lead to concerns and criticisms of intelligence overreach, which lead to constraints and oversight of intelligence powers, and so on (Lester 2016, 206–208). Looked at in this way, the issues of privacy and intelligence are pretty standard issues for both intelligence and general political philosophy: what permissions and constraints do we place on intelligence agents and agencies? In order to better understand the privacy-related issues faced by the rapidly evolving spaces that modern intelligence practice and oversight find themselves in, we must look more closely at the notion of privacy.

Here, we find a second challenge, one centred on the very concept of privacy. The challenge here is that, like much ethical theory, the stories about ethics and privacy typically derive their narrative force from person–person relations.[4] For instance, imagine a situation where Tom is peeping in the window of Carly. A standard privacy analysis would look to Carly's interests, her rights, the harms that such violations privacy could entail, and so on, to say why what Tom is doing is ethically impermissible. I will call these problems ones of the sort "Interpersonal Privacy".

When thinking of intelligence and privacy, however, the stories about ethics and intelligence are about different actors. Instead of Tom peeping on Carly, we are concerned with a government agent Tim working under the authority of a given intelligence agency placing a camera in Carlo's house, such that Tim can gather intelligence and evidence on Carlo's criminal or, otherwise, illegal activities. The ethical questions here concern questions like the following: is this action legal, is Tim permitted to do this, did Tim and his agency seek the proper approvals, what moral authority grants permissions specifically and generally to the particular agency and intelligence agent, and so on. I suggest that these questions derive their narrative force from citizen-government relations. What matters is not so much the *interpersonal* moral relations like those between Tom and Carly, but the *institutional* and political relations between Tim and Carlo. These questions are still privacy-related questions, but the way we understand them will be different to Tom and Carly. I will call these problems ones relating to "Institutional Privacy A".

In the modern era, we have a similar set of intelligence concerns relating to private companies and customers.[5] As Soshana Zuboff has argued, given the immense informational power that private companies like Facebook, Google, and so on have, we are in an age of surveillance capitalism (Zuboff 2019). Now, rather than the privacy issues being about Tom and Carly (interpersonal), or Tim and Carlo (state-citizen), the issues are more likely to be of the sort where Karl has bought a smart TV, from the company Trams, and subsequently discovers that the Trams SmartTV has been recording and analysing his movements by remotely activating its camera and microphones.[6] This is a similar issue to Tim and Carlo, in which a particular issue concerns an institution and relevant institutional actors and particular person or set of people who stand in special relationship to that institution. Here, however, the particular actors and relations are ones of company and customer. As this is a variant on Institutional Privacy A, I will call this "Institutional Privacy B".

Finally, as I will discuss later in the chapter, we are also increasingly having to deal with a third sort of privacy issue. The relevant point of difference builds on how we recognise and conceptualise the morally relevant actors. Consider here that Trent and Karla are the specific individuals. Karla is an average private citizen. Trent has been spying on Karla, but he is a foreign intelligence agent, who is using Karla's Trams SmartTV to gather intelligence on her. So far, we have a mixture of Interpersonal Privacy (one individual violating the privacy of another), Institutional Privacy A (one government agent spying on a private citizen), and Institutional Privacy B (the spying is enabled by internet-connected technologies). In this variant, however, Trent is a spy in the employ of a foreign country and neither of our previous sorts of privacy problem quite fit. As I will argue, while Karla and Trent are the specific individuals involved, we cannot understand, much less offer an ethical criticism, of this scenario on an individual or even a state-citizen or company-consumer frame. Instead, the relevant moral relations here are between states. I will call this International Privacy. The overall point is that in order to understand privacy and intelligence, we must contextualise our analysis by reference to the sorts of actors involved.

The reason why differentiating the key actors matters is that we are looking not just at the ethics of privacy, simpliciter, but the ethics of privacy *and intelligence*. As per the social contract, citizens expect government agents and agencies to do things that people normally can't do. As was discussed in Chapters 1 and 3, this is a basic point of liberal democracy and national security. The basic notion of the social contract is that individuals forgo or forfeit certain rights in order to be part of a wider society.

In terms of the legitimacy or authority of the state, at least for modern liberal democratic states, the state is considered to gain its legitimacy from the support and endorsement of its citizens.

> One common way of explaining this is by reference to a hypothetical social contract that people enter into with the state… Put simply, it is in people's self-interest to collectivise certain aspects of their life, as there are particular goods that are either only achieved or secured collectively or are better achieved collectively.
>
> (Henschke 2021a, 78–79)

Moreover, the provision of national security is typically seen as one particularly important good that the state delivers as per the social contract.

> [T]he conduct of government is morally acceptable if and only if it serves to promote the safety and welfare of the person of the state, and in consequence the common good or public interests of the people as a whole… *Let the Safety of the People be the supreme Law*.
>
> (Skinner 2009, 362; emphasis original)

The idea here is not just that the state is generally given certain permissions in order to pursue legitimate national security ends but also that any sensible ethical analysis of particular state actions must take this social contract context into account. We cannot offer a sensible analysis of the notion of privacy with relation to intelligence without recognising the different frames of analysis – particularly Institutional Privacy A and International Privacy. This is not at all to say that Interpersonal Privacy is unimportant. Rather that, when engaging with issues of intelligence, we need to adapt the basic principles undergirding Interpersonal Privacy to the state-citizen and state–state contexts.

A second aspect that needs to be properly and effectively recognised is the way that new information and communication technologies are disrupting those relationships.[7] As we saw in the opening examples, the role of informational handling systems like social media are playing an increasingly central role in intelligence practice. Likewise, the ways that foreign intelligence services can use information and communication technologies to engage in surveillance operations is disrupting how we think of both intelligence and privacy. The point here is that we cannot offer a sensible analysis of the notion of privacy with relation to intelligence without recognising the ways that new technologies are disrupting intelligence practices – this is particularly relevant for Institutional Privacy A, Institutional Privacy B, and International Privacy. Here, the principles identified in Interpersonal Privacy can be useful to help identify and develop new ethical norms for intelligence practice.

In what follows, I will outline some general theories of privacy and then show how Interpersonal Privacy, Institutional Privacy A and B, and International Privacy not only differ but also offer useful ways to think about privacy and intelligence. That is, while discussions of Interpersonal Privacy are essential to understanding the general concepts and conceptions of privacy, they are largely lacking the institutional context that drive discussions of intelligence. It is a mistake to try to understand ethics of intelligence as it relates to privacy simply in terms of person–person relations. By adding the institutional context, we see a need to consider Institutional Privacy A/Institutional Privacy B and, increasingly, International Privacy.

On Privacies

In the following sections, I offer a pluralistic conception of privacy. This approach holds that "Privacy is too complicated a concept to be boiled down to a single essence. Attempts to find such an essence often end up being too broad and vague, with little usefulness in addressing concrete issues" (Solove 2008, 103). I suggest here that privacy is more than one single conception, reducing it to a right, or intimacy, or other foundation misses important elements that other conceptions add. Seeing privacy pluralistically

> allows the different elements to both explain and limit each other. The point here is that the problem with the different conceptions… is that, in seeking to reduce privacy to a single conception, they lose the utility of the other conceptions.
>
> (Henschke 2017b, 46)

Further to this, this approach suggests that when seeking to understand privacy for intelligence, we should analyse privacy in terms of layers of analysis – interpersonal, institutional, international, depending on the particular key actors we are concerned with. If we take too abstract a view of privacy, we lose much practical utility when considering it in relation to intelligence – when considering privacy and intelligence, the institutional context is essential.

The Simple Solution: Interpersonal Privacy and Intelligence

The simplest way of looking at the issues we are concerned with are to start with the reductive individualist account – When Tom is peeping on Carly, what is happening here, and why should we care? This tracks roughly to two complementary ways of looking at privacy: descriptively and normatively. On the descriptive account, there are

> five common ways that people have conceptualised privacy in privacy literature: as a right, as something secret, as a space, as control over information and as a realm free of government intrusion. These concepts cluster together as they track to ways in which people describe privacy; they seek to answer the question of "what counts as private?"
>
> (Henschke 2017b, 36)

If Tom is peeping on Carly, then he might be violating a privacy right that Carly has. He might be observing something secret or non-public. He might be accessing a particular space that Carly has claim over, or might be accessing some particular information that Carly has control over. I will discuss the government aspect later.

In contrast to these descriptive accounts, we can also understand privacy normatively. That is, rather than asking "what counts as private", we "seek to understand privacy by reference to some morally distinctive relevant feature" (Henschke 2017b, 40). For instance, we might seek to justify a right to privacy by arguing that such a right "protects the individual's interest in becoming, being, and remaining a person. It is thus a right which *all* human individuals possess – even those in solitary confinement" (Reiman 1976, 44; emphasis original). This account draws from the recognition that privacy is essential for the development of personal autonomy. "Without privacy, autonomy is threatened… It takes rare strength to swim against strong social currents… The richness of personal relations depends upon our emerging from our shells, but few of us would risk emerging without privacy" (Griffin 2008, 225–226). Another approach sees privacy drawn from what is intimate, the things that we like, love, and care about. This approach "holds that it is not the particular content of something that determines its privacy; rather it is the relation between the private thing and the person. As a way of making it distinct from individual development, intimacy is interpersonal" (Henschke 2017b, 42). As Daniel Solove describes it, "[t]his theory appropriately realises that privacy is essential not just for individual self-creation, but also for human relationships" (Solove 2008, 34).

The normative approaches are all similar in that they seek to tell a story of why privacy matters by looking for a core foundation in some moral principle. For instance, the personhood accounts will typically, implicitly or explicitly, say that we ought to care about privacy because respecting privacy is showing respect for the individual as an individual. Other accounts, like that of Daniel Solove, seek to explain why we ought to care about privacy by looking at the harms that might arise if privacy is not recognised (Solove 2008). A third approach might instead explain privacy's importance by reference to basic consistency – it looks at the golden rule, and asks if that person violating privacy would like it if their privacy was violated. Mark Zuckerberg, the Facebook CEO, who once declared that privacy was no longer a social norm (Johnson 2010), subsequently bought up all the property around his home and demolished the houses there to make smaller houses which had less chance of being able to look onto his personal property (Bayly 2016). The ethical principle here is one of justice, where we expect people to treat others equally to the way that treat themselves. All these approaches look for some core value or values to develop a principle for privacy, by understanding what it is and why it matters.

A More Practical Solution: Institutional Privacy A/B and Intelligence

The strength of the reductive individualist approach is that it allows us to explain why privacy matters by reference to a well-recognised principle or set of principles.[8] We can then seek to use these principles to guide the development of norms, or apply particular norms to new situations. These reductive individualist accounts are useful insofar as they point to foundational ideas or values that explain what privacy is (such as a rights violation), and why we should care (such as we have the right in order to personally develop). The problem is that in order for them to tell us something about intelligence, we need more detail; we cannot simply apply the interpersonal accounts of privacy to intelligence practice. As Nissenbaum argues, in order to properly engage with privacy as a set of concepts, we can look at privacy as being primarily concerned with "context relative informational norms" (CRINS). CRINS can "explain why people feel concerned about some privacy violation and how to respond to it" (Henschke 2017b, 49). While an individualist approach can tell us something about the problem with Tom peeping on Carly, when we consider intelligence practices, we need more. If we are going to understand these CRINs, intelligence and the wider national security landscape are contexts fundamental to understanding what is happening and why. That is, the ethical analysis of what is happening will change if Tom is peeping on Carly because of some personal sexual kink, versus Tim watching Carlo as part of a criminal investigation. Again, the point here is not to discard Interpersonal Privacy – the interpersonal analysis of privacy is important both to clarify the concept and locate some moral foundation to ground and guide our practice. Rather, the point is to say that where intelligence is concerned, we need to look at privacy in the context of intelligence institutions, and principles like the just cause for intelligence, right intention, logical resort, and so on.

This leads us to Institutional Privacy A. Recall that in this account, Tim and Carlo are understood not just as individuals but as a representative of the state and a citizen of the state, respectively. As such, Institutional Privacy A is an explicitly *political* account of privacy.

> [R]ather than being centred on the notion of personal information and interpersonal relations, this conception of privacy frames the concept in relation to state–citizen relations. Rather than simply being between two people, the relevant relation in this conception is between the state and its citizens, or some variant thereof. And, rather than being about personal information per se, the relevant aspect is how that personal information plays a role in the use of state power against its citizens.
>
> (Henschke 2020, 15)

Importantly, this political conception expands the notion of privacy to be not just about information or even access to individuals, but about the relations between the state and the citizen. "By describing privacy as political, this conception takes it that privacy is the realm where one specific actor, the 'state', cannot enter. In this explicitly political sense, privacy is seen as opposed to government intrusion" (Henschke 2020, 15). While such an account coheres with the idea of privacy as a zone free of oversight or intrusion, what matters are the agents involved. When casting privacy as political,

> Private describes that zone that the government is not permitted to interfere in… A person's home, for example, is private. And whatever happens there is none of the government's business–'abnormal' sexual activity, drug use, religious or political gatherings. Insofar as they occur behind closed doors, they occur in a zone or space that is sheltered from government scrutiny.
>
> (Henschke 2017a, 39f)

So, on this political layer of analysis, the key recognition is that "the relevant actors are different [from the interpersonal conception of privacy]. Now, rather than simply being about interpersonal relations between two moral agents, the relevant actors are now 'the state' and its citizens" (Henschke 2020, 15).

This institutional conception of privacy is essential when seeking to understand and criticise intelligence practice and institutions. For instance, we can look at what legal rights Carlo has not to be spied on by their government. We can ask if Tim went through the appropriate warranting processes to place Carlo under surveillance, is Tim still adhering to these processes. Moreover, by placing privacy in a context of how intelligence institutions operate, we are able to question how those warranting processes have developed, what oversight and restrictions exist on what other intelligence actors can and should do with Carlo's personal information, and indeed, upon what authority is Tim operating, is the intelligence agency operating, are the warranting and oversight systems operating.

As discussed earlier in this book, intelligence practice must adhere to principles of discrimination, necessity, proportionality, and reciprocity. Importantly, however, for this political conception of privacy, we recognise that citizens like Carlo have a *pro tanto* privacy right. That is, in liberal democracies at least, the default setting is that the state must stay out of Carlo's affairs and cannot gather or use personal information about Carlo or other citizens. It is only when particular events or situations arise that permit that right of privacy to be abrogated (or perhaps violated). We see here the role of the just cause for intelligence and logical resort for intelligence in operation. For instance, if Carlo is engaged in some activity that threatens the security and safety of other citizens, or national security more broadly construed, then there might be a case for Tim to engage in surveillance of Carlo. However, in a functioning liberal democracy that adheres to the social contract, Tim typically cannot make this decision arbitrarily. He must have good reasons to proceed, and depending on the levels of privacy that are being abrogated, any such activity must be determined to be warranted. As is found in standard legal practices, Tim may literally need a warrant, and that would involve meeting conditions of discrimination, necessity, and proportionality.

The notion of privacy as institutional, rather than moral, is not without problems, however. On this institutional account, what matters are state-citizen relations. This is all well and good for Tim and Carlo if Carlo is a citizen of the country that Tim is working for. But what happens if Carlo is not a citizen? Here, if we see that privacy is at its core a moral notion, then Carlo's citizenship should not matter. Instead, many countries around the world treat surveillance of their own citizens quite differently from surveillance of foreigners. The point here is that viewing the limits that privacy can place on intelligence practices in a political sense by reference to state-citizen relations faces challenges when considering non-citizens. I will return to this point again when discussing International Privacy.

Institutional Privacy B follows a similar path to Institutional Privacy A, in that it is concerned with the relations between a particular set of institutions and individuals. For Institutional Privacy B, we are looking at the relations between a company that provides some particular good or service and their customers (broadly construed). In an age where people buy and use products and services that allow for unprecedented amounts of personal information to be gathered on these people, we cannot overlook the role of non-state institutions in modern intelligence practice. Adding further detail to this, we must also recognise that many of the products and services of interest here are willingly bought, used, and literally introduced into people's private spaces. It is no exaggeration to say that smart phones, social media, and smart homes permit intelligence gathering on people at a level unlike any in human history.

> Combine the near invisible presence of ICTs in our lives with their informational capacities and we have the age of surveillance: a social epoch marked by informational technologies which endorse, encourage and enable us to live lives under constant surveillance… What marks this age as one of surveillance is our own role in this – it is not simply that there are these new information technologies that target us for observation. We are complicit in this observation– we are often the willing sources of this information, happily uploading selfies, buying wearable surveillance technologies, actively publicising vast amounts of Personal Information like no other time in history.
>
> (Henschke 2017b, 4)

If we are to talk meaningfully about privacy and intelligence, we have to recognise the role of non-state intelligence institutions. Moreover, we have to recognise that the ethical issues of Institutional Privacy B are different from Institutional Privacy A.

The reason for clustering Institutional Privacy A and Institutional Privacy B together is that the ethical questions that underpin them are the same – what grants an institutional actor, such as the state or a private company, moral authority to access personal information and/or a person's intimate spaces? Where they differ is that when looking at state-citizen relations of Institutional Privacy A, the moral authority comes from the social contract (or some other set of mechanisms essential to liberal democracy). When looking at the company-customer relations of Institutional Privacy B, the moral authority comes instead from a social licence. Companies have this social licence "as a means of pursuing new relationships between industry and communities to reflect public values and ensure community support for projects" (Aitken et al. 2020, 3). This is a similar process to the social contract where "an operation's social licence is theorised as comprising ongoing acceptance or approval from the local community" (Parsons and Moffat 2014, 344). Here though, the relevant targets of moral analysis are different. However, given the increased rise, and role, of the intelligence capacities of information companies, Institutional Privacy B is an important part of the analysis of relations between institutions and individuals.

The implications of recognising a difference between Interpersonal Privacy and Institutional Privacy A and B are that adding this institutional layer of analysis allows us to better update and amend our analysis of the ethics of intelligence when the specific facts around privacy change. For instance, as a threat to national security, the lives of citizens and the quality of life of customers change, and so too should the intelligence activity. Otherwise, the state or company may be forfeiting their commitments under the social contract and social licence. This is, again, the point of just cause for intelligence and logical resort of intelligence principles. By adding this Institutional Privacy layer of analysis, and recognising the important role of social contract and licence, the discussion about ethics and privacy is not just about what information is revealed, the impacts that information might have on people, and/or the specific semantic factors around information. The Institutional Privacy layer of analysis allows us to include principles like those described in Chapters 3 and 4 for the *jus ad intelligentium* and *jus in intelligentia*.

The institutional layer also means that we can better engage with related ethical issues like free speech, free public communication, and the chilling effects that intelligence and widespread surveillance programmes can have on citizens, consumers, and communities.[9] Moreover, the institutional layer also recognises that, even if there are legitimate national security concerns that a state may have, these concerns must be balanced against the need for legitimate media to investigate and report on government practices. If we grant too much power to state intelligence agencies, this can have pernicious effects on the media, which can undermine core liberal democratic institutions. Finally, recognising the distinction between Institutional Privacy A and Institutional Privacy B means that we can grant more attention to companies and the threat to democracy posed by surveillance capitalism.

The broader point here is that it is a mistake to try to simply apply the principles identified in Interpersonal Privacy to Institutional Privacy. And, indeed, it is a mistake to do the reverse and take what we know about state-citizen relations and apply them simply to the interpersonal context. Any story that does that misses the context and will be too general to be useful. The obvious counterargument is that adding the Institutional Privacy layer of analysis is unnecessary. This counterargument would suggest that we already have the foundational values of Interpersonal Privacy, and we already do adapt them when considering intelligence. The response here is that an approach which does this and seeks to understand privacy and intelligence in the context of states or companies is doing what we are suggesting, they are engaging in an institutional analysis. They are in agreement with the position advocated here; it is simply a matter of semantics, and whether the re-contextualised, nuanced account of privacy is in fact simply Interpersonal Privacy adapted or Institutional Privacy A/B. As long as these practical accounts add in the relevant context, then they are engaging with our institutional approach in everything but name.

On Privacy and Intelligence in the International Context

All that said, with the rise of modern information and communication technologies, we face an emerging challenge for privacy and intelligence – how does privacy work when considering state–state relations? Recall from the opening examples, where staff and students of ANU were being spied upon by a foreign nation. This is a sort of privacy problem like that involving Trent and Karl. Karl is a private citizen, and his personal information and larger private space is being violated by Trent. However, unlike Institutional Privacy A/B, the agent violating his privacy is not an agent of Karl's government nor is that agent an employee of a company. Trent is an agent of a foreign state, and any ethical analysis of the intelligence activity here must take that into account. Moreover, Karl's relationship to Trent is fundamentally different than Institutional Privacy A or Institutional Privacy B. Karl does not have a social contract or social licence with Trent, and so cannot withdraw Trent's moral authority in protest for what is happening. Moreover, Karl essentially has very little power to do anything against Trent. The most Karl can do is employ better cybersecurity practices and hope that this does not happen again. Consider the ANU example – if, as a member of ANU's staff or a student, I find out that my personal information has been accessed and used by an agent of the foreign power, what can I as an individual do? As an individual person, I cannot do anything but hope that ANU improves its security. I personally cannot go out and punish the foreign power. In fact, in many jurisdictions, if I was to actively pursue some retributive action through hacking the foreign power myself, I would be in violation of my own country's laws. What I suggest here is that there is a further layer of analysis that is required in our information age, that looks at privacy in the context of state–state relations – International Privacy.

Adding a new layer of analysis might seem a bit too fast, however. For instance, Article 12 of the United Nations' Universal Declaration on Human Rights (UNDHR) states "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations 1948). If Trent is accessing Karl's personal information, invading a personal space, and so on, then this is simply a violation of Karl's privacy. We do not need International Privacy to criticise what is happening here. However, this approach returns us back to Interpersonal Privacy. While we might agree that Karl's privacy has been violated, we have reduced the privacy discussion back to person–person relations. However, recall that in the scenario, Trent is an intelligence agent acting on behalf of his country, against Karl, who is the citizen of another country. Simply saying that Karl has a right to privacy, as recognised by things like the UNDHR, does not tell us anything helpful about *intelligence*. If, instead, we look to the political conception, and say that we should understand Trent and Karl's relationship as like that of the state and citizen, we fall short again. The problem here is that, first, we are potentially talking about different political cultures. Second, Karl has no social contract with Trent's government or people more generally. Again, looking at this in the same way as Institutional Privacy A, we are not able to tell a full story that is relevant to intelligence.

In the past, International Privacy would not be a significant challenge. While some people might be placed under surveillance by a foreign power, this was quite limited. But the rise of information and communication technologies that span nations and jurisdictions means that cyberspace is an international concept, filled with agents from all over the world. Recall also that, as with the Christchurch shooting leading to similar attempts around the world, and perhaps playing a role in the Sri Lanka Easter attacks, even domestic intelligence agencies must be ever more engaged in international events. Moreover, as the ANU example shows, non-government people like the staff and students of a university are now the targets of sophisticated intelligence operations. The point that International Privacy seeks to recognise that new information and communication technologies are changing the scope and reach of intelligence practice. In the past, an employee or student of an Australian university would not have had to even think about a foreign nation as a risk to their privacy, either Interpersonal Privacy or Institutional Privacy A/B would have sufficed.

Much of these changes have been spurred by the development of new technologies. This may lead us to believe that we are in a post-privacy age.

> Facebook shows us that we don't really care about privacy, and Google tells us we can't do anything even if we did care. And, lest we forget, Snowden has shown us that governments are using information technologies, exploiting our behaviours, to engage in surveillance at a level unprecedented in human history. Has technology killed privacy?
>
> (Henschke 2017b, 35)

However, before we declare that privacy is dead, we need to recognise that new technologies have spurred development of new concepts of privacy.

> The seminal paper *The Right to Privacy*, written by Samuel Warren and Louis Brandeis in 1890, was written *in response* to new technologies: in the late nineteenth century, cameras had become portable, could take photographs practically in an instant and could be used by almost anyone who could afford one.
> (Henschke 2017b, 35; emphasis original)

This "new technology made it important to explicitly and separately recognize this protection under the name of privacy" (DeCew 2006).

There are two related points being made here. First, that new technologies and their uses hardly mean the end of privacy. Warren and Brandeis' article is largely seen as the conceptual and normative foundation for privacy in the US, UK, and other English-speaking countries. Second, that privacy is not only a pluralistic idea but one that evolves and changes. While the simple foundational premises might remain unchanged, how we care about privacy, how we protect it, and what constitutes a privacy violation may change. In short, I suggest here that we need to add a new concept to the privacy bundle.

When thinking of the problems posed by International Privacy, we can perhaps start to think of privacy including digital sovereignty. Returning to the ANU example, as a staff member or student of ANU, individuals are largely unable to do anything against a foreign country's intelligence activities. The reason for this is that such events are the proper province of state–state relations. States have a long history of diplomacy and international relations around sovereignty, and how this relates to the protection of their citizens. We have established norms of behaviour by states in relation to citizens and sovereignty.

I suggest here that a principle of reciprocity would be fundamental to understand and guide intelligence practices and institutions. How exactly this ought to play out in relation to the ethics of intelligence qua privacy is an ongoing question, and one that I do not expect to answer here. Rather, my point is a more general one about privacy and intelligence: that a sensible discussion needs to recognise the different moral actors involved in the analysis of the concepts and the application of particular principles. Just as we cannot understand ethical issues in domestic intelligence without recognising that the key moral agents are the state and its citizens, when thinking of international intelligence, we must recognise that the key moral agents are states interacting with other states. If an Australian citizen has had their privacy violated by a foreign actor, then it is the proper and legitimate role of the Australian government to engage with that country on this. It is not the responsibility or even province of the staff members or students.

Another feature of International Privacy is that it places a stronger responsibility on states to both engage in and support good counter-intelligence practice. This is typically covered in discussions of cybersecurity, and most governments around the world are actively engaged in developing the cybersecurity practices of their institutions and citizens. The argument here is that states must engage in effective counter-intelligence that covers the

> resources and support for effective and integrated [Cyber Emergency Response Teams] that actively work with civilian and private cyber-actors as well as key international players and foreign allies to ensure that the relevant information about cyber-risks and cyber-threats is distributed… [the] provision of basic education for the populace at large. Typically, most breaches in cyber-security involve human failure at some stage in the process. Basic cyber-literacy with a component in cyber-security is an essential element to reduce the risk and impact of the human element in cyber-security failings… there might [also] be a requirement for government oversight and possibly provision of technical support, including anti-virus software.
>
> (Henschke 2017a, 219)

My point here is not so much about the responsibility of governments to provide the resources and support for good cybersecurity, this is a well discussed and unoriginal point. Instead, my point is that we need to see such activities as part of an effective counter-intelligence programme. A further point is that advancing the case for International Privacy, we can now recognise that such cybersecurity and counter-intelligence practices are in fact part of a discussion about privacy.

Conclusion

The point of this chapter has been to explore privacy and its relation to intelligence practices and institutions. I developed an argument that privacy needs to be understood as a range of related concepts. In particular, in order for us to have a practical and useful set of notions around privacy, we need to see that the context matters. To detail this, I presented three different layers of analysis for privacy. First was Interpersonal Privacy. Here, our conceptual and ethical analysis uses the interactions and relations between two people to give an understanding what privacy is, and why it matters. Second was Institutional Privacy. Rather than understanding privacy as the relationship between two people, when considering intelligence, we need to see that government and citizens may be the key actors shaping our analysis. Similarly, with the rise of information technologies, the key actors framing our analysis will be companies and customers. At this layer of analysis, the moral authority and legitimacy of the institution, born, in part at least, through the relations between that institution and its citizens/customers, shape the ethical analysis of privacy. Finally, we have a final layer of analysis, in which the key actors are states. I called this International Privacy. The point here was that with changing information technologies and practices, individuals in one state are now potential targets of intelligence actors and institutions of another state, perhaps one that is geographically distant. Given that the individual here cannot do much except improve their cybersecurity habits, and may in fact be legally prohibited from doing anything more, an effective ethical and political analysis of privacy and intelligence needs to be conducted at the layer of state–state interactions.

Notes

[1] See Henschke, Robbins, Reed for more on related issues (Henschke, Reed, and Robbins 2021).

[2] For more on general privacy discussions, see Koops et al. (2016); Solove (2008); Inness (1992); Nissenbaum (2009); Henschke (2017b); van den Hoven (2007); Westin (1967).

[3] See Chapter 9 for more on these issues.

[4] This approach of "reductive individualism", in which ethical analyses involve a reduction of an ethical issue to individual interpersonal relationships, has been particularly popular and influential in just war discussions. Jeff McMahan's work has been particularly influential here (McMahan 2009).

[5] Or users, consumers, etc. For the purposes of this chapter, however, I will refer to the individuals as customers.

[6] The cameras and microphones of various smart TVs and smart home assistants have been shown to be active without explicit customer knowledge or consent (Matyszczyk 2015; AAP 2019).

[7] Chapter 10 discusses other implications of new information and surveillance technologies.

[8] I say set of principles here, as a number of privacy theorists promote a pluralistic account of the normative foundations of privacy, where it not just rights, or harms, or justice that matter, but some combination of them and/or other principles. See van den Hoven (2007); Nissenbaum (2009); Henschke (2017b) for more on these pluralistic approaches.

[9] See, for instance, Reed and Henschke (2021); Henschke and Reed (2021); Henschke (2021b).

References

AAP. 2019. "Google Listens to User Speaker Recordings". *SBS News*. www.sbs.com.au/news/google-listens-to-user-speaker-recordings

Aitken, Mhairi, Ehsan Toreini, Peter Carmichael, Kovila Coopamootoo, Karen Elliott, and Aad van Moorsel. 2020. "Establishing a Social Licence for Financial Technology: Reflections on the Role of the Private Sector in Pursuing Ethical Data Practices". *Big Data & Society* 7(1): 2053951720908892. https://doi.org/10.1177/2053951720908892

Bayly, Lucy. 2016. "Zuckerberg to Bulldoze Homes Worth $30M Just to Keep His Privacy". *NBC News*, May 26. www.nbcnews.com/tech/tech-news/zuckerberg-demolish-30m-real-estate-keep-things-private-n580216

DeCew, Judith. 2006. "Privacy". The Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/archives/fall2006/entries/privacy/

Graham, Chris. 2018. "Florida Shooting: Donald Trump Blames FBI's Russia Probe for Failure to Spot Suspect's Warning Signs". *Telegraph*, February 18. www.telegraph.co.uk/news/2018/02/18/florida-shooting-donald-trump-blames-fbis-russia-probe-failure/

Griffin, James. 2008. *On Human Rights*. Oxford: Oxford University Press.

Gunasingham, Amresh. 2019. "Sri Lanka Attacks: An Analysis of the Aftermath". *Counter Terrorist Trends and Analyses* 11(6): 8–13.

Henschke, Adam. 2017a. "Duties to Defend: Ethical Challenges of Cyberspace". In *Rethinking Security in the Twenty-First Century: A Reader*, edited by Edwin Daniel Jacob. 209–221. Somerset: Palgrave Macmillan. https://doi.org/10.1057/978-1-137-52542-0_15

Henschke, Adam. 2017b. *Ethics in an Age of Surveillance: Virtual Identities and Personal Information*. New York: Cambridge University Press.

Henschke, Adam. 2020. "Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System". *Moral Philosophy and Politics* 7(1): 123. https://doi.org/10.1515/mopp-2019-0056

Henschke, Adam. 2021. "Information as an Evolving National Security Concern". In *The Palgrave Handbook of National Security*, edited by Michael Clarke, Adam Henschke, Matthew Sussex, and Tim Legrand. 389–408. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-53494-3.

Henschke, Adam. 2021a. "Ethics and National Security: A Case for Reasons in Decision-Making". In *The Palgrave Handbook of National Security*, edited by Michael Clarke, Adam Henschke, Matthew Sussex, and Tim Legrand. 73–92. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-53494-3Henschke, Adam. 2021b. "On Free Public Communication and Terrorism Online". *Counter-Terrorism*, July. www.elgaronline.com/view/edcoll/9781800373068/9781800373068.00017.xml

Henschke, Adam and Alastair Reed. 2021. "Toward an Ethical Framework for Countering Extremist Propaganda Online". *Studies in Conflict & Terrorism* 1–18. https://doi.org/10.1080/1057610X.2020.1866744

Henschke, Adam, Alastair Reed, and Scott Robbins, eds. 2021. *Counter-Terrorism, Ethics, and Technology*. New York: Springer.

Hoven, Jeroen van den. 2007. "Privacy and the Varieties of Informational Wrongdoing". In *Computer Ethics*, edited by John Weckert, 317–330. Aldershot: Ashgate Publishing.

Inness, Julie C. 1992. *Privacy, Intimacy, and Isolation*. New York: Oxford University Press.

Johnson, Bobbie. 2010. "Privacy No Longer a Social Norm, Says Facebook Founder". *Guardian UK*, January 11. www.theguardian.com/technology/2010/jan/11/facebook-privacy

Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Ivan Skorvanek, Tomislav Chokrevski, and Masa Galic. 2016. "A Typology of Privacy". *University of Pennsylvania Journal of International Law* 38: 483.

Laxman, Sanjeev, and Ben Kesslen. 2019. "Sri Lanka bombings were retaliation for Christchurch shooting, defense minister says". NBC News, April 23. www.nbcnews.com/news/world/sri-lanka-bombing-was-retaliation-christchurch-shooting-defense-minister-says-n997391

Lester, Geneveive. 2016. *When Should State Secrets Stay Secret?* Cambridge: Cambridge University Press.

Martin, Lisa. 2019. "Australian National University Hit by Huge Data Breach". *The Guardian*, June 4. www.theguardian.com/australia-news/2019/jun/04/australian-national-university-hit-by-huge-data-breach

Matyszczyk, Chris. 2015. "Samsung's Warning: Our Smart TVs Record Your Living Room Chatter". *CNet*, February 8. www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/

McMahan, Jeff. 2009. *Killing in War*. Oxford: Clarendon Press.

Michaelsen, Christopher. 2010. "The Proportionality Principle, Counterterrorism and Human Rights: A German-Australian Comparison". *City University of Hong Kong Law Review* 21(1). http://heinonline.org.virtual.anu.edu.au/HOL/Page?handle=hein.journals/ciunhok2&id=21&collection=journals&index=journals/ciunhok

Moses, A. Dirk. 2019. "'White Genocide' and the Ethics of Public Analysis". *Journal of Genocide Research* 21(2): 201–213. https://doi.org/10.1080/14623528.2019.1599493

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

Parsons, Richard and Kieren Moffat. 2014. “Constructing the Meaning of Social Licence”. *Social Epistemology* 28(3–4): 340–363. https://doi.org/10.1080/02691728.2014.922645

Reed, Alastair and Adam Henschke. 2021. “Who Should Regulate Extremist Content Online?” In *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*, edited by Adam Henschke, Alastair Reed, Scott Robbins, and Seumas Miller, 175–198. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-90221-6_11

Reiman, Jeffrey H. 1976. “Privacy, Intimacy, and Personhood”. *Philosophy and Public Affairs* 6(1): 26–44.

Skinner, Quentin. 2009. “A Genealogy of the Modern State”. *Proceedings of the British Academy* 162(325): 34.

Solove, Daniel. 2008. *Understanding Privacy*. Harvard: Harvard University Press.

United Nations. 1948. “Universal Declaration of Human Rights”. www.un.org/en/documents/udhr/

Westin, Alan F. 1967. *Privacy and Freedom*. London: Bodley Head.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Fronteir of Power*. London: Public Affairs.

9 Beyond Independence

The Ethics of Trustworthy Intelligence Institutions

Adam Henschke

An oft stated view about intelligence is that intelligence should be independent of politics, and that politics should be independent of intelligence.

> There is a natural tension between intelligence and policy, and the task of the former is to present as a basis for the decisions of policymakers as realistic as possible a view of forces and conditions in the external environment. Political leaders often find the picture presented less than congenial…When intelligence people are told, as happened in recent years, that they were expected to get on the team, then a sound intelligence-policy relationship has in effect broken down.
>
> (John Huizenga, quoted in Church 1976a, 75)

This need for independence takes on a special relevance when considering intelligence agencies. This is in part because intelligence agencies are a core part of a nation's national security apparatus, and as conventional wisdom has it, national security is too important to play politics.

The independence of intelligence agencies is also of particular importance because if political decisions interfere with intelligence, then it undermines the capacity and effectiveness of intelligence agencies to inform political decision-makers. Similarly, given the ways that intelligence products can influence politics, politics ought to be protected from intelligence. In liberal democratic nations, the influence of non-elected officials can degrade the very notion of representative democracy.

In short, intelligence should be independent of politics, and politics should be independent of intelligence. This is a "bidirectional" independence thesis, where each institution should be independent from the other. This chapter, however, will argue that this bidirectional independence thesis is a myth, albeit one that has a good set of reasons to propagate and aim at. There is ample evidence supporting that key stakeholders hold this bidirectional independence view. However, intelligence agencies in many liberal democracies are indeed directly and indirectly influenced by politics, and political actors are equally able to be influenced by

DOI: 10.4324/9781003106449-12

intelligence agencies. The argument put forward here is that we should not be aiming at independence, rather, we need trustworthy intelligence.

Nowhere is the importance of, and complexity of, the relationship between intelligence and politics more clear than the relationship between various intelligence institutions and former United States President Donald Trump. As this chapter was written, Trump had been indicted in four separate cases (Geoghegan 2023). Throughout this process, Trump has continually and vociferously claimed that these charges are politically motivated. He has specifically argued that such investigations and charges are election interference. For instance, in July 2023, he stated that the investigation by Jack Smith is "interference with the election. It's election interference, never been done like this in the history of our country and it's a disgrace" (Trump 2023). Trump was booked in Georgia at the Fulton County jail in late August 2023 (Mangan and Breuninger 2023). Following his arrest, which included production of a booking photograph, Trump returned to Twitter/X, posting his booking photograph with the text "ELECTION INTERFERENCE NEVER SURRENDER!" (Lepore 2023). It is important to note that this was Trump's first tweet since the insurrection on 6 January 2021. On the view of Trump and many of his supporters, the fact that he is being investigated is – in and of itself – election interference, intelligence seeking to influence politics. At the same time, Trump and his supporters have called for the investigations to end. Following his indictment on charges of interfering with the 2020 election outcome in Georgia, Republican Senator Colton Moore sought to pursue a path to impeach the Fulton County District Attorney Fani Wills, who charged the former President (Bickerton 2023).

Regardless of where one stands on the guilt or innocence of the former President, the inflamed commentary and tension around his investigations show the importance and precariousness of intelligence and politics. Intelligence – whether through the act of investigations or the discovery of pertinent information – can have significant political impacts. Likewise, political actors and politically astute members of intelligence institutions may have, or seek to use, political power to influence intelligence processes. Furthermore, as this ongoing Trump example shows, the relationships between intelligence and politics, and the positions that one might take on them, are likely to shift depending on the case at hand. In liberal democracies, we generally want intelligence and politics to be independent of each other.

As with the book's overall focus, I will be talking about typical liberal democracies. This is partly because of the public accountability measures that are central to liberal democracies and partly because of the constraints that liberal democracies place upon intelligence agencies.

> Here we think of democracy as a set of institutional arrangements that involve the active participation of ordinary citizens, sometimes directly in making policy, but more often in holding accountable officials and representatives who are more proximately involved in policy-making.
>
> (Orr and Johnson 2018, 62)

While many of the practical issues raised in this chapter likely apply to non-liberal democracies, it is unlikely that many of the values referred to here will simply apply to non-liberal democracies, much less to authoritarian states. I cover this point in part three of the chapter.

This chapter proceeds as follows. It sets up the bidirectional independence thesis. It shows next that this independence thesis is largely a myth. It then suggests some reasons why we might want to keep this myth alive. As I will show, there is a normative basis for this independence myth. Moreover, if we look at the intelligence and political relations through the frame of trust, rather than independence, we can find ways to achieve the values that the independence myth aims at. I present a three-layered account of trust to show how we gain the values that the independence myth takes to be important, while not falling into the trap of holding the independence thesis to be accurate.

On the Independence Thesis

Many in the intelligence world publicly hold that intelligence ought to be independent from politics. For instance, former Director of US Central Intelligence George Tenet

> had liked to tell his bosses at the White House that CIA officers should stay removed from the process of making policy. He evoked an almost monastic image of the spies at Langley producing intelligence assessments, while those "across the river", at the White House and in Congress, made decisions based on these assessments.
>
> (Mazzetti 2014, 13)

The basic idea here is that intelligence and policymaking serve two very different purposes. Michael Hayden, the former director of the United States' National Security Agency (NSA) and Central Intelligence Agency (CIA), describes these different purposes in this way: "Intelligence is fixated on the world as it is. The president and his policy team dream of the world as they want it to be" (Hayden 2019, 78). On this view, intelligence is at its core an epistemic enterprise. In seeking to describe the world as it is, it is an exercise in truth seeking, whether it is to uncover secrets, to understand the world, or to explain the context in which events are occurring. Politics and policymaking, however, are about changing the world. The relevance of this distinction is that, on the independence thesis, intelligence institutions, officers, agents, and leaders should not make political decisions nor engage in politics. Their role is to describe the world. In liberal democracies, politically relevant decision-making is the role of policymakers and ultimately the elected representatives. To clarify, of course, intelligence officers and the like do make decisions and seek to change the world in some way, but on the independence thesis, they should not be making *political* or *policy decisions*.

This view is not simply common, it is central to the self-understanding of many intelligence agents and actors. Former Federal Bureau of Investigations (FBI) leader James Comey states that "[t]hough it is a part of the Executive Branch, the FBI is meant to stand apart from politics in American life. Its mission is to find the truth" (Comey 2018, 2). He later writes that "[t]here had always been a line. The intelligence community does facts; the White House does politics and spin… The searing lesson of the Iraq war – based on bad intelligence about weapons of mass destruction – was 'never mix the two'…" (Comey 2018, 221). Again, we see this idea that intelligence agencies serve a particular purpose, and that veering from this purpose is antithetical to the very core of the institution of intelligence. Moreover, should such agencies step aside from their core role, they are causing trouble for representative democracy.

Drilling down into the purpose of intelligence, former director of the GCHQ in the UK, David Omand states that "*the most basic purpose of intelligence is to improve the quality of decision-making by reducing ignorance*" (Omand 2010, 22; emphasis original). This goes deeper to the purpose of intelligence as providing information to support decision-making. Omand further breaks intelligence down into three key roles.

> The first use, and by far the greatest in terms of volume of effort involved, is… *building situational awareness*… The second use of intelligence in supporting decision-making can best be described as *explanatory*… The third use of intelligence is both potentially the most valuable, and the most fraught, and that is for *prediction*.
>
> (Omand 2010, 24–25; emphasis original)

This is the epistemic enterprise of intelligence in a nutshell – in each of these three roles, the purpose of intelligence is to assist decision-makers in their role. In a later book Omand co-authored with Mark Pythian, they argue that the purpose intelligence is to improve decision-making (Omand and Phythian 2018).

Underpinning this is the purpose of intelligence as an institution. The intelligence is gathered for a reason. While this purpose is contested, one prevalent view holds that the point of intelligence institutions is to aid in political decision-making.

> Why do governments spy on each other and on members of their own populations? The reasonable justification for any intelligence activity is to acquire information that one believes will improve the quality of decision-making by statesmen, policy makers, military commanders, or police officers by reducing their ignorance about their operating environment. Better-informed decisions lead to better government and a safer more secure society.
>
> (Omand and Phythian 2018, 1)

While gathering and using accurate information is arguably essential for typical government decision-making, *intelligence* marks itself out as being distinct, as "the environments in which intelligence is required are fundamentally competitive ones" (Omand and Phythian 2018, 10). Essentially, intelligence involves gathering information on competitors that they do not want you to have, while at the same time, protecting your own information from those competitors. As was noted earlier in the book, it bears repeating that this competitive aspect marks intelligence out from other collective epistemic enterprises. Moreover, the justificatory purpose of the sort of intelligence that we are concerned with here marks it out as distinct from, say, corporate intelligence which may also occur in other competitive environments.[1] As David Omand and Mark Pythian noted earlier, the purpose of this intelligence is not simply to aid decision-making, nor even to aid government decision-making, but to bring about a safer and more secure society. We are thus concerned with *national security* intelligence, "information provided to a nation's leaders by secretive government agencies to protect citizens against threats posed by domestic or foreign sources" (Johnson 2017, 4). This is born out in a definition offered by Peter Gill and Mark Pythian, where "*Intelligence comprises 'the mainly secret activities – targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities*" (Gill and Phythian 2018, 5; emphasis original). As with this book's general argument, intelligence is understood as an epistemic enterprise, conducted in a competitive environment, that seeks to aid in national security.

The point of these references is to show that high-profile and high-level leaders of intelligence institutions hold the view that intelligence agencies and their members ought to be independent of political decision-making. This is because intelligence and politics are fundamentally different practices, serving different purposes. Intelligence exists to support decision-making, national security intelligence exists to support political decision-makers secure a nation and its people.

As much as we want intelligence to be independent of politics, we also want politics to be independent from intelligence. We frequently see significant criticism when intelligence actors step into the political sphere. This is perhaps most clearly demonstrated by the tense and combative relationship between intelligence actors and political actors in the lead up to, and during, Donald Trump's tenure as US President. Comey, for instance, was the focus of significant and sustained criticism for the roles he played during the 2016 US presidential elections and subsequently was removed from the FBI by US President Donald Trump. Two weeks before the 2016 US election, Comey decided to publicly announce that the FBI was reopening an investigation into Secretary Hillary Clinton's use of an email server. This added fuel to a long burning distrust of Clinton by a significant proportion of the US public. Following Trump's win, Hillary Clinton blamed the decision by Comey, in part, for her loss. "[O]ur analysis is that Comey's letter raising doubts that were groundless, baseless, proven to be, stopped our momentum" (Chozick 2016). Comey was later controversially fired by Trump, with Trump complaining to advisors that Comey was a showboater and a grandstander (Tucker 2021). The point here is that Trump stated that Comey was too publicly visible and too politically active to remain in the role as FBI director.

However, the fractured relationship between Trump and the intelligence community is best captured by the constant reference by Trump and others to a nefarious "deep state" that was seeking to undermine him and his administration.

> [The deep state] is said to be a system composed of high-level elements within intelligence services, military, security, judiciary, and organized crime. [It can be meant as] a hybrid association of key elements of government and parts of top-level finance and industry that is effectively able to govern the United States with only limited reference to the consent of the governed as normally expressed through elections.
>
> (Lofgren 2016, 5)

Sean Hannity, a media commentator and well-known Trump supporter, said this in June 2017:

> This deep state, this fourth branch of government, as we're calling it, doesn't care about getting the truth to you, the American people. And of course, the media – they're the willing accomplices. Their goal is the exact opposite here. They are selectively leaking information, intelligence information that is meant to damage, in this case, the president of United States of America, which is exactly what we have been seeing now almost on a nightly basis.
>
> (Schwartz 2017)

This public criticism of intelligence leaders and the wider intelligence community by Trump and his surrogates has likely had a significant effect on the trust of intelligence agencies in the US. In a 2018 poll, 73% of Republicans agreed with the statement that "members of the FBI and Department of Justice are working to delegitimize Trump through politically motivated investigations" (Rohde 2020).

Perhaps the strongest example of Trump's animosity towards the intelligence community can be found in his response to the Robert Muller enquiry into his 2016 campaign's dealings with Russia. Trump was a prolific user of Twitter, and the Muller enquiry was one of his most tweeted about topics.

> A search of the Trump Twitter Archive … between January 2017 and August 2019 shows 452 tweets about the investigation. The next closest topics are Fake News (with 362), FOX News/Sean Hannity (315), Hillary Clinton (202), and Barack Obama (171). Half of the tweets (224) use the term "witch hunt" to refer to the Russia investigation, a term Trump began using months before special counsel Mueller was appointed.
>
> (Harriger 2020)

The use of the term "witch hunt" is especially pertinent here – through use of this term, Trump was not just casting doubt about the motivation of the special investigator and his team, but drawing from the principle that the use of intelligence means and methods to investigate a domestic political actor, especially a president, was illegitimate. This sense of animosity and competition continues in the ways that the US House Committee on the Judiciary has responded to various state-level Attorneys General's investigations into Trump (Zhou 2023), and the establishment of a House Committee into the "weaponization" of government (Broadwater and Edmondson 2023).

Of course, we can be quite sceptical about the actual reasons for Trump's animosity towards the Muller investigation, and whether it was due to him consciously holding a belief that intelligence and politics should be kept apart.

> When former Attorney General Jeff Sessions told President Donald Trump that a special counsel had been appointed to conduct the Russia investigation, the president responded: "Oh my God. This is terrible. This is the end of my presidency. I'm fucked"…
>
> (Newburger 2019)

However, the underpinning concern has force – a key part of intelligence is having secret information on people, and that information can be not just powerful, but used to subvert and undermine political processes.

Beyond any criticism of Trump's character, the political power that can come from intelligence actors having secret knowledge about political actors is of significant concern. Comey, writing of his predecessor J. Edgar Hoover, points out how intelligence actors can use their position and epistemic tools to influence the political processes.

> For decades, Hoover used an iron hand to drive the agency and strike fear into the hearts of political leaders. He had "personal files" on many of them, something he let them know. He dined and drank with presidents and senators, letting them use the FBI when it suited him, and frightening them with the FBI when that suited him
>
> (Comey 2018, 121)

Hoover's willingness to use the FBI to not just collect information on political actors, but to use it in order to gain political power is a paradigm example of how intelligence actors use their privileged epistemic status to impact political spheres.

The Russian term "kompromat", from the Russian компрометирующий материал, translates as "compromising material". An adversary or competitor gains some damaging or embarrassing information on you, and then uses the threat of going public with it as leverage in your decision-making. One of the features of kompromat is it is frequently associated with, or used by, government actors. Hoover's use of intelligence to gain political power and leverage was essentially kompromat. Trump's response to the Muller enquiry was not just about self-preservation, but a recognition of how intelligence gathered on, and used against, political actors can be powerful, dangerous, and perhaps politically destabilising.

The point here is not to endorse those criticisms of special investigator Muller's actions, nor indeed to give any credence to the deep state conspiracies. Rather, it is to draw attention to the notion that people, including but not limited to political leaders, fear and are opposed to, intelligence playing a role in politics. That is, politics ought to be protected from intelligence. The independence thesis is thus bidirectional. Intelligence not only needs to be independent of politics, but politics needs to be independent of intelligence.

On the Independence Myth

This independence thesis is, however, largely a myth. I mean myth here in two ways. First, this myth is descriptive in that it does not describe the world as it is. Second, this myth is aspirational, in that it is something worth aiming at. In this section, I set out the reasons for this why we should see this myth as both descriptive and aspirational.

The Myth as Descriptive

To begin, "consider the fact that all intelligence analysis occurs within a political system" (Lowenthal 2017, 60). Intelligence, as described earlier, is about guiding political decision-making. It is, in this most fundamental way, a political enterprise.

> One must always be mindful of the fact that intelligence analysis exists in a political arena and not in some abstract intellectual salon. Intelligence analysts strive and usually succeed at remaining politically neutral, but their work is part of a process that has political implications… [I]ntelligence is always a part of the larger political and policy process, and will be judged not just by accuracy, objectivity, and transparency [but] also by the political milieu.
>
> (Lowenthal 2017, 60–61, 89)

Former Director of Central Intelligence Robert Gates states it bluntly: "The CIA is a uniquely presidential organization. Virtually every time it has gotten into trouble, it has been for carrying out some action ordered by the president" (Robert Gates, quoted in Lester 2016, 129).

This relationship between intelligence and politics applies to all aspects of intelligence. In the US, for instance, congressional oversight is "responsible for authorizing programs and activities and appropriating funds for them" (Lester 2016, 76). In all liberal democracies, intelligence agencies are not simply accountable to political leaders, but dependent upon them. This is the power of the purse.[2] "What can the committees do if they disagree with a proposed program? The most strenuous measure would be to curtail funding. Programs are reviewed every year, and budgets for them can be cut, amended, or extended" (Lester 2016, 104). Political actors thus have the capacity to influence intelligence operations and practices through funding decisions.

Moreover, in some liberal democracies, the hiring and firing of leaders and staff of intelligence agencies is made by politicians, in a political context. For example, John Brennan withdrew himself from consideration as CIA Director in the first Obama administration due, in part, to concerns about his earlier support of enhanced interrogation and torture (G. Miller 2008). And political decision-makers have significant agency over the hiring and vetting of new staff.

> [T]he government is heavily influencing the staffing of all agencies by pressuring them to tighten up their selection processes and security clearances… the effect is to make agencies increasingly conservative in their outlook and less inclined to challenge the Government when its public statements and policy settings deviate from the information and expertise in the agencies' possession.
>
> (Wilkie 2006, vii)

And, as we have seen with former US President Trump and Comey, if an intelligence actor is either not deemed sufficiently loyal, or might contravene the political narrative on a given topic, their own job may be at risk. The point here is that whether it is the political implications of particular intelligence analysis, the selection and funding of particular programmes, or who leads an intelligence agency, involves political decisions. In short, intelligence is political.

Further to this point about independence being a myth, consider this description of the CIA: "For an agency that is remarkably insulated, the Central Intelligence Agency's vulnerability to the exigencies of a changing political environment has had an inordinate impact on the development of its internal institutional culture" (Lester 2016, 33). Like all intelligence agencies in liberal democracies, the evolution of the CIA was shaped by the political environment that it found itself in. We can perhaps best demonstrate this by reference to the creation of the Director of National Intelligence (DNI) in the US. The role of the DNI was created in response to the 9/11 attacks, and subsequent enquiries which found that the lack of coordination across intelligence agencies in the US was a contributing factor in the 9/11 attacks. A more cynical take might be that various institutional actors saw an opportunity to reduce the influence of the CIA on US policymaking, in order to support and promote the institutions that they worked in. The point here is that the evolution of intelligence is typically directly related to the political, social, and security needs of the given time and place.

Moreover, in liberal democracies, intelligence institutions must be subject to oversight and accountability. As Lowenthal argues, "proper governance of intelligence is essential" (Lowenthal 2017, 81). This good governance can refer to *control*, where political leaders and citizens have "certainty that intelligence agencies are under the firm control of the policy makers", *responsiveness* where intelligence actors and operations are carried out "in the manner prescribed by policy makers", coupled to meaningful *oversight*, such that "policy makers will be able to have knowledge about what the intelligence agencies are doing and that intelligence agencies will cooperate in these efforts", necessarily underpinned by *public support*, in liberal democracies, the public must accept "intelligence activities that are conducted by people who have been elected to office or by their duly appointed designees" (Lowenthal 2017, 82–83). The overall point made by Lowenthal is one about the relation between intelligence agencies and political decision-makers and policymakers – that intelligence cannot be independent from politics, policymaking, or the wider community. In fact, one of the hallmarks that distinguishes authoritarian states from liberal democracies is the lack of control, oversight, and public support for intelligence agencies.

This notion of accountability is essential to liberal democratic states and intelligence institutions. "Most important in terms of the actual autonomy of the mechanism is recourse, that is, the ability of the supervisor to exact consequences and require change in behavior through these consequences" (Lester 2016, 16). On Genevieve Lester's view, intelligence needs more than simply oversight. In order for intelligence agencies to be *accountable*; those bodies tasked with supervising intelligence agencies must be able to actually affect the actions and behaviours of those agencies and agents in some meaningful way. That is, the intelligence agencies need to be held accountable. Which, again, goes against the simple independence thesis. If intelligence agencies were to be properly independent, no external body should have the capacity to cause them to change to their behaviours or be held accountable for their actions. Yet, this is something that we do not want for intelligence agencies; they must be accountable. Thus, we can see that claims about intelligence and politics being independent are a myth as they are descriptively inaccurate.

Similarly, politics is simply not independent of intelligence, or, at least, particular aspects of intelligence. Clear evidence of this can be seen in the impact of intelligence on recent US politics. On the issue of going public about the reopened investigation into Clinton in the late stages of the 2016 election, Comey saw that the FBI had but two options – speak or conceal. If they went public with the reopened investigation, to "speak" "would be really, really bad. It would put the Bureau and me in a place where we might have an impact on an election. Really bad, nauseating even. To be avoided if humanly possible" (Comey 2018, 194). The other option was to "conceal", to keep secret from the public that the FBI was again investigating one of the political candidates. Comey asked "[w]hat if, after the election, we actually found information that demonstrated prosecutable criminal activity? No matter what we found, that act of concealment would be catastrophic to the integrity of the FBI, and the Department of Justice" (Comey 2018, 195–196). Similarly, it is plausible to suggest that the repeated investigations of Trump, his campaign team, his administration, and associates, no doubt, played a significant role in him losing the 2020 election. Looking at independent voters, Joe Biden won

> a 54 percent majority of independents, a 12-point rise from Clinton's 42 percent showing in 2016. The pattern was seen across key battleground states, including Wisconsin, where independents flipped from backing Trump by a 10-point margin in 2016 to supporting Biden by a 14-point margin. In Arizona, Biden won independents by 11 points four years after Trump won the group by a narrower three points.
>
> (Alcantara et al. 2020)

The point here is that the information gathered from intelligence investigations of political actors, even the fact that there is an investigation going on, has deep political significance. We see that the independence of politics from intelligence is a myth.

The Myth as Aspirational

Here, I want to argue that there is value in the independence myth – independence is something we ought to aim at, it is worth aspiring to. To establish this idea that particular institutions ought to be held apart from each other, we can look at Michael Walzer's *Spheres of Justice*. In this book, Walzer presented an argument that different institutions should be independent from each other. If and when they concern themselves with the distribution of different social goods, they commit an injustice. "To convert one good into another, when there is no intrinsic connection between the two, is to invade the sphere where another company of men and women properly rules" (Walzer 1983, 19). His basic point is that what occurs in one area or "sphere" of influence ought not influence what occurs in another sphere. He marks politics out as one sphere of influence that is particularly powerful. "Politics is always the most direct path to dominance, and political power… is probably the most important, and certainly the most dangerous, good in human history" (Walzer 1983, 15). I draw on this as it gets to the basic intuitive pull of the independence thesis; first, that intelligence and politics are different spheres, and second that neither should seek to, nor have the capacity to, influence the other.

We find a clear expression that politics and intelligence are different in some of the quotes, discussed earlier, from senior intelligence actors like Hayden, Omand, and Comey. Intelligence is, at its core, an epistemic institution that describes the world as it is. Politics is, in contrast, normative or prescriptive; it seeks to change the world. So, on the spheres view, we can see that they are different institutions, with different purposes. But that leaves us with the question *why* we would want them kept apart? On what ethical basis could we argue that they ought not influence each other? In this section, I set out three related values as to why intelligence and politics ought not influence each other and present them in such a way as to mark out why intelligence as an institution is perhaps different from other institutions. First goes to the notion of intelligence as epistemic enterprise, and that intelligence must be reliable. Second goes to a separation of powers, that intelligence is predictably constrained. Third is about representative democracy, that intelligence and politics are used for their intended purposes. That is, I show what makes intelligence warrant special or unique concerns to make it independent from politics, and politics from intelligence; that independence is something worth aiming it.

As has been stated throughout this book, we ought to think of intelligence as an epistemic enterprise. By that I mean that intelligence institution's fundamental role is related to information, more specifically about knowledge. It is "the effort to obtain and analyze information required by national leaders" (Lowenthal 2017, 1). Traditional intelligence practices involve collection, analysis, and communication/explanation of that information to the customer.[3] Further, these epistemic actions are not simply information collection and analysis for their own sake but conducted in order to improve the decision-making by national leaders in a national security context. "Intelligence agencies are meant to serve policymakers, providing them with relevant, timely and objective information related to national security.

Intelligence agencies don't take sides in the domestic political struggle, they don't formulate policy, nor… do they recommend policy" (Faini 2020, 4–5).

The connection between intelligence as an epistemic enterprise for good decision-making and independence can be seen in the contrast with the relation between intelligence and politics in authoritarian states. Lowenthal states that "[a]nother constraint for intelligence in authoritarian states is the likely limit on being able to report 'bad news', or intelligence that conflicts with the official line" (Lowenthal 2017, 5). Moreover, there is a risk that threats will be underplayed. "[T]rue dissent or political disinterest may be under-reported to avoid having the intelligence services appear incompetent" (Lowenthal 2017, 5). If intelligence collection, analysis, and reporting are driven by political ideologies, not independent from politics, then the quality of the intelligence is going to suffer.

The importance of this is that the political decision-makers require that information to be accurate and reliable. If the information is inaccurate, then that will likely result in poor decision-making. The decision by the US and UK to invade Iraq based on faulty intelligence about weapons of mass destruction (WMD) show how dangerous it is to have bad information.[4] The accuracy of the information received, and the confidence that decision-makers have in that information is essential to the task of intelligence supporting good decision-making. Not only will politically tainted intelligence lead to poorer decision-making, but it may also undermine the purpose that intelligence is there to guard against threats to national security. Thus, we want intelligence to be independent from politics such that those political decision-makers can actually make the best decisions possible.

There is further concern about the need to remain committed to intelligence as an epistemic enterprise. "To abandon facts… is to abandon freedom. If nothing is true, then no one can criticize power because there is no basis to do so… Post-truth is pre-fascism" (Timothy Snyder, quoted in Hayden 2019, 250). The point here is one about authority – If we lose objective reality as an authority, then it is those in power who define the world. This is an essential feature of authoritarianism. If those in intelligence agencies are beholden to those in power, rather than truth, they become a powerful authoritarian tool. Hayden, former director of the NSA and CIA, puts it this way: "Rejecting a fact based intelligence assessment – not because of compelling contrarian data, but because it was inconsistent with a preexisting worldview or because it was politically inconvenient – is the stuff of ideological authoritarianism, not pragmatic democracy" (Hayden 2019, 72). Insofar as we want and need the *truth* to be authoritative, rather than a particular political actor or ideology to be authoritative, then we need to both protect, and listen to, our epistemic institutions. If intelligence becomes an arm of political actors, then we lose this connection with reality and are on a slide into authoritarianism.

This leads us to the second point that blurring intelligence and politics undermines effective control over the intelligence process. These two institutions are separately quite powerful, and those powers need to be kept separate. Intelligence institutions, like any public institution, must be accountable. This is not only true, but given the power and unique nature of intelligence work, we ought to also be particularly concerned with how accountable intelligence actors are. However, "the mechanisms

[must] have an independent and autonomous role from the overseen… they [must] have a separate statutory basis for their operations, and thus, that their activities and decisions cannot be influenced by pressure from the overseen" (Lester 2016, 16). The issue here, as Lester notes, is that this accountability needs to be insulated from political influence. If intelligence and politics are not independent from each other, it raises the risk of intelligence actors being granted political cover to engage in a range of actions that may not only benefit those political actors, but are unethical, illegal, and lacking in justification. In short, while we can see that the independence thesis is a myth, it is perhaps one worth aspiring to.

A further reason for pursuing the independence myth is that granting political power to intelligence actors subverts the very core of representative democracy. "[I]ntelligence officers do not make policy recommendations. That is the exclusive sphere of elected officials and their appointees in the policy departments" (Lowenthal 2017, 4–5). The basic point here is that if we allow intelligence actors to decide policy, we are no longer representative democracies. The criticisms of J. Edgar Hoover's use of intelligence to wield power are based, in part, on the recognition that he was neither elected to represent people, moreover, that he was not subject to the same oversight and accountability of elected leaders.

At its core, the worry is that the privileged epistemic position of intelligence actors grants them the power of manipulation.

> Manipulation is a form of power that employs deception of those over whom power is exercised. It is a way of getting what you want despite the possible resistance of others. Manipulation occurs when someone exercises power over other people, inducing them to behave as the exerciser of power wishes, without their awareness that power has been exercised.
>
> (Beitz 1989, 54)

This capacity for manipulation is inimical to liberal democracies.

> The offense to individual autonomy is compounded at the social level by an offense to democracy, whose integrity depends on the capacity of its people to participate knowledgeably and rationally in political deliberation. This, of course, is precisely what manipulation subverts.
>
> (Beitz 1989, 56)

Not only are unelected people using intelligence to direct political outcomes, when it is done covertly, it severs the necessary connection between citizens and their capacity to understand and participate in policy decisions. "[D]emocracy involves argument, discussion, debate. On the other hand it relies on voting or some other means of aggregation. In order to be democratic, argument and aggregation presuppose conditions of freedom and equality" (Orr and Johnson 2018, 62). Insofar as relevant information is kept from the voting public, and/or information is used in an effort to manipulate that debate and/or the voting processes, we have a significant failure in the democratic model. And intelligence institutions and actors, expert in the use of information, misinformation, and disinformation, can play a fundamental role in influencing, interfering in, and even subverting democracy.[5] So, we see here reasons why we want to keep politics independent from intelligence.

Trust in Intelligence

So, having shown that the independence thesis is a myth, yet holding that there are important ethical and political reasons for aspiring to this myth, we are left with a challenge – on the one hand, we want intelligence and politics to be independent from each other. But on the other hand, we do not want this. Moreover, "[i]ntelligence needs to be close enough to policy makers to be relevant, but not so close that it stops being objective" (Faini 2020, 5). This a common challenge in public policy for liberal democratic societies.

> To what extent should the public service be independent of the government of the day? The public service exists to serve the public interest by implementing the policies of the government. So, on the one hand, the public service must be responsive to the elected government of the day. Yet on the other hand, the public service must have a degree of independence in order to ensure that proposed policies are lawful, accurately costed, and that presidents, prime ministers, cabinet ministers, and the like are provided with "frank and fearless" advice in relation to their policies.
>
> (S. Miller and Gordon 2014)

The solution to this challenge, I suggest, is to aim at trust. The features of intelligence, its "secrecy, objectivity and an apolitical image – makes intelligence's judgment valuable for policymakers engaged in a public dispute… intelligence is generally trusted by the public opinion and its estimates play an important role in resolving public debates" (Faini 2020, 6). My suggestion here is that the reasons why we want intelligence and politics to be independent from each other is not independence for the sake of independence. Instead, we want this separation because we need to trust both institutions – the aspiration of independence is ultimately to have institutions that are worthy of our trust.

Trust is valued as a form of social capital (Fukuyama 1995). It serves a purpose in public policy "because it cuts transaction costs" (Norton 1996, 351). When institutions and political processes are trusted, people and agencies can get on with their work, rather than having to convince people that they are working. For instance, "[w]hen politicians win elections in societies where trust works, they can get on with the job of governing without distracting their energies into ensuring that the military does not reverse the election result" (Braithwaite 1998, 350). And given the need for secrecy in the intelligence and wider national security sector, trust is an especially important feature. Important elements of intelligence occur in the shadows, outside of the view of normal political and social activities. Moreover, as particular aspects of intelligence occur outside normal ethical and legal norms, we must trust that these events are limited, constrained, and accountable. A loss of trust in intelligence can be quite problematic. Comey, for instance, talks about the FBI having a "reservoir of trust", and if it gets too low, the wider institutions of justice will soon fail to work (Comey 2018, 54, 179).

While we might agree that trust is valuable, especially in intelligence, trust itself is a relatively complicated and complex notion. Here, I want to focus on three related features of trust as they apply to intelligence and politics. We must first ensure that the intelligence practice and product are reliable Second, we want to know that intelligence practices are predictable. And third, we must check if the intelligence practice and use of product track to their institutional ends. This builds from a three-part conceptualisation of trust, in which trust can be about reliability, whether an actor or institution will act predictably, and if that actor or institution has an attitude of goodwill to those who must trust them.[6] These three features track to the aspirational elements of independence discussed earlier – we want intelligence itself to be reliable, we need it to be constrained, and intelligence ultimately needs to stay out of politics.

On the first point, when thinking of reliability as form of trust, it is considered "a technical concept, and relates to the correct operation of a component or system under specific circumstances" (Clark and Blumenthal 2011, 365). In the simplest terms, the issue is that a customer or user of intelligence must have confidence that the intelligence that they are receiving is accurate, that that intelligence can be trusted to inform them properly. If we want intelligence actors and processes to give meaningful advice to political actors, then that intelligence must be *reliable*.

This builds from the conceptualisation of intelligence being an epistemic enterprise.

> One of the central questions when dealing with any intelligence is its reliability. Is the human source truthful, a fabricator, or a double agent, sent to deceive? Has the collected image or signal been subject to description of some sort?
>
> (Lowenthal 2017, 28)

This is not just about the sources of intelligence, but also to do with analysis and the need for consumers of intelligence to know that intelligence is reliable.

> [W]hile the right information will be provided only if the producers know what the consumers need, the process of assessment must be objective and seen and believed by all consumers to be objective, if the consumers are to rely on it. To achieve these things, intelligence producer and the intelligence assessment process must be independent and be seen to be independent.
>
> (Australian Government 1976, Section 47)

In short, if the intelligence gathered and presented to a consumer lacks independence, it cannot fulfil its role as properly informing decision-makers.

We can see here why it is fundamental to keep intelligence and politics apart from each other – if political actors influence intelligence reports, seeking to frame findings in a particular way, to present confidence in particular assessments that favour one political view over another, then the reliability of that intelligence is reduced. To be clear, this influence need not just be explicit, where a political actor demands that the intelligence support a decision that they want to make. Institutions that become heavily politicised will often implicitly encourage particular advice – those people who give advice that the political actor wants to hear will receive support and promotions, those who give unwanted advice will lose support, and their careers suffer. The development of, and manner in which, the CIA produced a report on potential WMD that underpinned the invasion of Iraq in 2003 shows how political influence can reduce the reliability of intelligence reports, and degrade the trust in intelligence institutions more generally.

> In [Senator Bob] Graham's opinion, Tenet had diluted the original document to keep in step with the opinion of the White House that Saddam was a great menace to the United States… Republican Senator Chuck Hagel… concluded that the condensed [National Intelligence Estimate] was "doctored" to suit the political needs of the White House.
>
> (Johnson 2017, 70)

If political actors are able to influence the production of an intelligence product, that product becomes unreliable. Trust in the intelligence agencies degrades, which ultimately leads to a reduced capacity for intelligence actors to effectively inform political actors' decision-making. The point here is that we want separation between intelligence and politics in order to ensure that intelligence is reliable, that is, it is trustworthy. Independence is not be valued for its own sake, but because it effectively increases the reliability of the intelligence product, and ultimately builds and maintains trust in the intelligence institutions.

The second point is concerned with whether we can expect an actor or institution to act in particular ways; can we *predict* how they will act? According to Peter Uslaner, "[t]rust on this account is an estimation of the probability that you will keep your promises, that you are trustworthy" (Uslaner 2002, 3). We are now concerned not so much with the quality or accuracy of the intelligence, but with the means by which that intelligence is gathered. For instance, if an agent is tasked with gathering intelligence on a particular target, we want to know first if they will actually get the intelligence that is needed. Second, and perhaps more importantly here, we need to know if they will get that intelligence in ways that are within the limits of the law.

The special nature of intelligence practices becomes particularly important here. While much intelligence activity is mundane, many of the defining activities of intelligence sit outside the margins of ethical and legal norms. John Magruder, the director of the Strategic Services Unit, which was later rolled into the CIA, "put it baldly, such operations are necessarily extra legal, and sometimes illegal" (John Magruder, quoted in Weiner 2008, 13). Tenet stated "[l]et's be blunt about what we do. There is no dishonor in it. We steal secrets for a living. If we do not steal secrets for a living, then we ought to shut the doors and do something else for a living" (George Tenet, quoted in Omand and Phythian 2018, 9). The pointy end of intelligence involves manipulation of individuals, violations of their privacy, interference in the political and social affairs of other states, and even lying to friends and family to protect the covert and secret nature of one's work. The point is not to discuss these ethical issues here, rather it is to draw from one of the key points in Chapter 3 that particular aspects of intelligence involve behaviours that would normally be ethically criticised because they are outside standard ethical and legal norms. Though such actions might be normally ethically or legally impermissible, when these actions are conducted as part of intelligence institution, they may have some justification. For instance, while it would normally be impermissible for me to lie to someone in order to steal personal information from them, if I was doing this in order to gain vital information to protect my country from an impending military attack, such behaviours may become permissible, even obligatory.

As Ross Bellaby notes, however, just because intelligence actions can be justified, it "does not mean that intelligence agencies should be allowed free reign" (Bellaby 2014, 2). Intelligence agencies must have constraints on what they do. As Lester discusses at length throughout *When Should State Secrets Stay Secret* (Lester 2016), in the US there is significant legal oversight and ultimately constraint on what intelligence actors can do. "Internal accountability of the CIA is strong and breaches of it are noticeable and quickly punished" (Lester 2016, 30). The point here is that while intelligence actors and actions might frequently exist outside of standard norms of acceptable behaviour, in liberal democratic nations, there are significant systems of oversight and accountability to both keep tabs on and control those behaviours.

This goes to seeing trust as *predictability*. Given the nature of what intelligence involves, the secrecy that often comes as part of that work, and occasion where one acts outside of standard ethical and legal norms, intelligence requires effective constraints. We need confidence that the intelligence practices are being conducted within constraints. That is, we want to know that intelligence, despite its exceptional nature, is predictable. The underpinning point is that, by knowing that there is oversight and accountability of intelligence, we can still say that it is acting predictably. Consider that there is a prohibition on torture – if particular intelligence is gathered from a captured enemy, the prohibition on torture tells us that intelligence was produced without torture. That is, the prohibition on torture tells us that we can predict that our intelligence agents will not use torture, not only is the intelligence itself reliable but also those engaged in its production are trustworthy.

Bringing this back to the relations between intelligence and politics, we see how trust as predictability becomes operational. By keeping intelligence distant from politics, we limit the potential for misuse of intelligence. The issue here is that intelligence operations, particularly things like covert operations, are seen as a "*tertia optio*", (Jacobsen 2019, 3). When comparing an intelligence operation against a decision to go to war, intelligence is not only preferable in terms of a proportionality calculation, but it is also likely to be far more attractive politically. The problem, however, is that intelligence might be a far less feasible option than diplomatic efforts. And if an intelligence operation goes wrong, it can be incredibly damaging – the Covert Action the Bay of Pigs invasion, for instance, caused considerable problems for the Kennedy administration (Weiner 2008, 197–206).[7]

The issue here is that, when comparing against other options like open warfare, the use of intelligence might seem not just better, but easier politically. So, we need constraints on what intelligence can do, as well as constraints on how political decisions are made. Maintaining operational independence between intelligence and politics means that those intelligence operations are not simply bounded, preventing impermissible actions like torture, but also ensuring that political actors do not seek to use intelligence when options like diplomatic efforts would be more appropriate.

Second to this, given the power that intelligence can have over political actors, we want to ensure that intelligence is not used for domestic political purposes. As part of the COINTELPRO operations, the FBI gathered intelligence on Martin Luther King's infidelities. The Church Committee, for instance, stated that

> The FBI mailed Dr. King a tape recording made from microphones hidden in his hotel rooms which one agent testified was an attempt to destroy Dr. King's marriage… The tape recording was accompanied by a note which Dr. King and his advisors interpreted as threatening…to release the tape recording unless Dr. King committed suicide.
>
> (Church 1976b, 11)

The issue here is that we need to have confidence that intelligence actors are not seeking to involve themselves in political affairs. Effective constraints and oversight are needed such that we know that intelligence actors and institutions are acting in ways that are predictable, that is, that they are trustworthy. Again, we want independence not for its own sake, but because we need intelligence institutions to be trustworthy.

The final concept of trust goes to the *motivations* of particular actors. "On this view, trust is more than a form of risk analysis; it is not simply a matter of what we might reasonably expect from others given their past behavior, it goes to people's motivations towards others" (Henschke 2020, 86). The basic idea here is that trust can also be understood as what one's motivations are for acting. In a more traditional context, we trust those who have good motivations towards us, who care for us and have our best interests at heart. On the face of it, this does not seem applicable to intelligence – as discussed, intelligence may involve deception, violation of privacy, even manipulating or killing an enemy target. However, what I offer here is the notion that the motivations for acting can be tracked back to the institutional ends. If an intelligence agent is engaged in some epistemic activity for the sake of national security, then they meet the motivational element.

We can then see how trust and the independence claims relate to each other – what we are looking for in a trustworthy institution is one where the proximate intentions of the individual actors are about gathering, analysing, and communicating information to aid in decision-making. To return to Omand and Pythian, "[t]he reasonable justification for any intelligence activity is to acquire information that one believes will improve the quality of decision-making by statesmen, policy makers, military commanders, or police officers by reducing their ignorance about their operating environment" (Omand and Phythian 2018, 1). On the account of intelligence offered here, the ultimate intentions are to support an institution whose telos is to promote national security. An intelligence agency and its actions are worthy of trust when they conform to that end.

As discussed, following Walzer's account of injustice, when intelligence starts doing politics, those actions and the institution have shifted their proper intention. Likewise, if political actors start using intelligence for political ends, they are shifting their proper intention. By identifying and sticking to the correct intention for each institution, we have trustworthy institutions. Again, independence is not valued for its own sake, but because of the ways that independence between the two institutions means that these institutions are trustworthy.

Conclusion

This chapter has looked at intelligence and politics, and interrogated the notion that they should be independent from each other. We have seen that many hold a view of bidirectional independence – intelligence institutions should be independent of politics, and political institutions should be independent of intelligence. We then saw that this bidirectional thesis is largely a myth. It is, however, a myth that we ought to aspire to – there are important aspects of independence that we ought to aim at. Instead of pursuing independence for independence sake, I have instead suggested that the reason we want these two institutions to be independent from each other is because we want intelligence to be trustworthy. To explain this point, I have offered 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 institutions. There is, of course, a further discussion to be had about how reliability, predictability, and correct intention can be ensured and the public assured that they are being met, but those discussions are beyond the scope of this chapter.

The final note to finish on is to show how important trustworthy intelligence is. In a sustained criticism of former US President Trump, Hayden points out the cost to both individuals and institutions when politics and intelligence become blurred.

> The president was doing more than just harming institutions. He was harming people, good people, American heroes, who deserve our gratitude… that was the very essence of the Trump accusation: that American intelligence agencies had been used by one political entity to spy on another… The president had used the American intelligence community as a handy political prop, and an ugly one at that.
>
> (Hayden 2019, 217, 139)

If we want to protect intelligence, we must ensure that it is worthy of our trust. Rather than aiming at independence, we should instead be concerned with trust.

Notes

[1] See, for example, Gill and Pythian's discussion of corporate and non-state sovereignty intelligence actors (Gill and Phythian 2018, 58–61).

[2] Lester covers the power of the purse in detail (Lester 2016, 151–157).

[3] I note here that intelligence frequently also involves "covert actions", which may be kinetic actions such as assassinations, targeted killings, or similar (see Chapter 6 for more on covert actions). I think it is an open question if such actions *should* be part of intelligence activities. However, we can include these kinetic actions under the umbrella of epistemic actions as such covert actions involve secrecy, counter-intelligence as an effort to *suppress* information. The secrecy that is required for such actions to be covert is part of the epistemic enterprise of intelligence. Again, the ethical arguments around covert actions, and intelligence's role in them, are beyond the scope of this chapter, and are covered in Chapter 6 and other sections of this book.

[4] I recognise here that it is still contested whether the National Intelligence Estimate (NIE) prepared in advance of the US decision to invade Iraq led to that outcome (Lowenthal 2017, 9). However, as will be discussed in the next section, the role of the intelligence in the decision to go to war in Iraq has led to an undermining of the trust in intelligence.

[5] See, for instance, Thomas Rid's description of intelligence as part of interstate political conflict (Rid 2020).

[6] I have discussed these components of trust elsewhere (Henschke and Ford 2017; Henschke 2020).

[7] I note here that the Bay of Pigs is a covert action, as described by Alexandra in an earlier chapter. It was undertaken by the CIA 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. It likely sits closer to the military end of covert action than the epistemic actions of intelligence institutions described throughout this book. However, the basic point holds.

References

Alcantara, Chris, Leslie Shapiro, Emily Guskin, Scott Clement, and Brittany Renee Mayes. 2020. "How Independents, Latino Voters and Catholics Shifted from 2016 and Swung States for Biden and Trump". *Washington Post*, 12 November. www.washingtonpost.com/graphics/2020/elections/exit-polls-changes-2016-2020/

Australian Government. 1976. "Royal Commission on Intelligence and Security Third Report on Intelligence Co-Ordination Machinery – Abridged Findings and Recommendations". 4727805. www.naa.gov.au/explore-collection/intelligence-and-security/history-australian-intelligence-and-security/royal-commission-intelligence-and-security-1974-77

Beitz, Charles R. 1989. "Covert Intervention as a Moral Problem". *Ethics & International Affairs* 3 (March): 45–60. https://doi.org/10.1111/j.1747-7093.1989.tb00211.x

Bellaby, Ross. 2014. The Ethics of Intelligence. Abingdon: Routledge. https://doi.org/10.4324/9780203383575

Bickerton, James. 2023. "Will Fani Willis Be Impeached? Georgia Republican's Plan Explained". *Newsweek*, 18 August. www.newsweek.com/will-fani-willis-impeached-georgia-republican-plan-explained-1820733

Braithwaite, John. 1998. "Institutionalizing Distrust, Enculturating Trust". *Trust and Governance* 343: 356.

Broadwater, Luke and Catie Edmondson. 2023. "Divided House Approves G.O.P. Inquiry Into 'Weaponization' of Government". *The New York Times*, 10 January. www.nytimes.com/2023/01/10/us/politics/house-republican-committee-weaponization-government.html

Chozick, Amy. 2016. "Hillary Clinton Blames F.B.I. Director for Election Loss". *The New York Times*, 12 November. www.nytimes.com/2016/11/13/us/politics/hillary-clinton-james-comey.html

Church, Frank. 1976a. *Foreign and Military Intelligence Book 1: Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate Together with Additional, Supplemental, and Seperate Views*. Washington DC: U.S. Government Printing Office.

Church, Frank. 1976b. *Foreign and Military Intelligence Book 2: Intelligence Activities and the Rights of Americans. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate Together with Additional, Supplemental, and Seperate Views*. Washington, DC: U.S. Government Printing Office.

Clark, David D. and Marjory S. Blumenthal. 2011. "The End-to-End Argument and Application Design: The Role of Trust". *Federal Communications Law Journal* 63(2): 357.

Comey, James. 2018. *A Higher Loyalty: Truth, Lies, and Leadership*. New York: Pan Macmillan.

Faini, Matteo. 2020. *Spies and Their Masters: Intelligence – Policy Relations in Democratic Countries*. Abingdon: Routledge.

Fukuyama, Francis. 1995. *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free Press.

Geoghegan, Tom. 2023. "Trump Indictments: A Very Simple Guide to His Four Big Legal Cases". *BBC News*, 15 August. www.bbc.com/news/world-us-canada-66508259

Harriger, Katy J. 2020. "The Law: "Witch Hunts" and the Rule of Law: Trump, the Special Counsel, and the Department of Justice". *Presidential Studies Quarterly* 50(1): 176–192.

Hayden, Michael V. 2019. *The Assault on Intelligence: American National Security in an Age of Lies*. New York: Penguin Books.

Henschke, Adam. 2020. "Trust and Resilient Autonomous Driving Systems". *Ethics and Information Technology* 22: 81–92. https://doi.org/10.1007/s10676-019-09517-y

Henschke, Adam and Shannon Brandt Ford. 2017. "Cybersecurity, Trustworthiness and Resilient Systems: Guiding Values for Policy". *Journal of Cyber Policy* 2(1): 82–95.

Jacobsen, Annie. 2019. *Surprise, Kill, Vanish: The Secret History of CIA Paramilitary Armies, Operators, and Assassins*. New York: Little Brown.

Johnson, Loch. 2017. *National Security Intelligence*. 2nd ed. Cambridge: Polity Press.

Lepore, Stephen M. 2023. "Trump Tweets Photo of Mugshot in First Post since January 6 Riots". *Mail Online*, 25 August. www.dailymail.co.uk/news/article-12443847/trump-tweets-mugshot-post-jan-6.html

Lester, Geneveive. 2016. *When Should State Secrets Stay Secret?* Cambridge: Cambridge University Press.

Lofgren, Mike. 2016. *The Deep State: The Fall of the Constitution and the Rise of a Shadow Government*. London: Penguin.

Lowenthal, Mark M. 2017. *The Future of Intelligence*. Cambridge: Polity Press.

Mangan, Dan and Kevin Breuninger. 2023. "Trump Arrest Full Recap: Mugshot, Surrender, What's Next in Georgia Election Case". *CNBC*, 25 August. www.cnbc.com/2023/08/24/donald-trump-to-be-arrested-in-georgia-live-updates.html

Mazzetti, Mark. 2014. *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth*. New York: Penguin.

Miller, Greg. 2008. "Would-Be CIA Chief Withdraws". *Los Angeles Times*, 26 November. www.latimes.com/archives/la-xpm-2008-nov-26-na-cia26-story.html

Miller, Seumas and Ian A. Gordon. 2014. *Investigative Ethics: Ethics for Police Detectives and Criminal Investigators*. Malden: Blackwell Publishing.

Newburger, Emma. 2019. "Donald Trump on Mueller's Appointment: 'This Is the End of My Presidency. I'm f----d' ". *CNBC*, 18 April. www.cnbc.com/2019/04/18/donald-trump-on-muellers-appointment-this-is-the-end-of-my-presidency-im-f-----d.html

Norton, Andrew. 1996. "Filling the 20 Per Cent Gap: Francis Fukuyama on Trust and Social Capital". *Agenda: A Journal of Policy Analysis and Reform* 3(3): 351–358.

Omand, David. 2010. *Securing the State*. Oxford: Oxford University Press.

Omand, David and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Oxford: Oxford University Press.

Orr, Susan and James Johnson. 2018. "Models, Mechanisms, Metrics: The Entanglement of Methods of Policy Inquiry with Democratic Possibilities". *The Routledge Handbook of Ethics and Public Policy*. Annable Lever and Andrei Poama (eds). 62–75. Abingdon: Routledge.

Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. London: Farrar, Straus and Giroux.

Rohde, David. 2020. *In Deep: The FBI, the CIA, and the Truth about America's* "*Deep State*". New York: W. W. Norton.

Schwartz, Ian. 2017. "Hannity Rips 'Deep State': 'Unelected Fourth Branch of Government Looking for Retribution'". *Real Clear Politics*, 17 June. www.realclearpolitics.com/video/2017/06/17/hannity_rips_deep_state_unelected_fourth_branch_of_government_looking_for_retribution.html

Trump, Donald. 2023. "CNN.Com – Transcripts'. 19 July. https://transcripts.cnn.com/show/es/date/2023-07-19/segment/01

Tucker, Eric. 2021. "The Comey Firing, as Retold by the Mueller Report'. *AP NEWS*, 20 April. https://apnews.com/article/north-america-donald-trump-ap-top-news-criminal-investigations-james-comey-4ff1ecb621884a728b25e62661257ef0

Uslaner, Eric. 2002. *The Moral Foundations of Trust*. Cambridge: Cambridge University Press.

Walzer, Michael. 1983. *Spheres of Justice: A Defense of Pluralism and Equality*. New York: Basic Books.

Weiner, Tim. 2008. *Legacy of Ashes: The History of the CIA*. New York: Anchor.

Wilkie, Andrew. 2006. "All Quiet in the Ranks: An Exploration of Dissent in Australia's Security Agencies". Canberra: The Australia Institute.

Zhou, Li. 2023. "The Trump Indictment Pits the Manhattan DA against House Republicans". *Vox*, 12 April. www.vox.com/politics/2023/4/12/23680531/jim-jordan-alvin-bragg-trump-indictment

10 Changing Practices, Disruptive Technologies, and the Evolution of Intelligence Institutions

Adam Henschke, Patrick F. Walsh, and Roger Bradbury

One of the main themes of this book is that a just intelligence theory (JIT) needs to be significantly different from the principles and applications of the just war tradition (JWT). The second main theme is that intelligence is not simply about practice, but institutions. A JIT, then, must include intelligence institutions in its principles, and how they are applied. In this chapter, we will discuss the ways that intelligence practices are currently changing, driven significantly by a range of disruptive technologies, and how this relates to intelligence institutions.

Any ethical analysis and guidance of intelligence practices and institutions must draw from, be reflective of, and responsive to the reality of those practices and institutions. This is not to say that practice should determine the principles; it is instead saying that principles and practice must engage in a process of reflective equilibrium. As Fritz Allhoff describes it: "we have various moral principles and various judgments regarding particular cases. Neither the principles nor the judgments enjoy any sort of privileged role. Rather, they engage each other in a process of mutual revision" (Allhoff 2011, 4). Following this, the approach taken in this chapter is to look at both principles and practice involved in intelligence, and to revise both in the light of current intelligence challenges. In this chapter, we look at a range of intelligence practices that are changing, with a particular focus on new and emerging technologies, to show intelligence institutions are evolving, and how they need to evolve.

Chapter 8 looked at privacy as a particularly important ethical issue for intelligence. Given that intelligence is an epistemic action – a complex group action that needs to be understood in relation to different institutional contexts – privacy is essential for any sensible discussion of intelligence and ethics. The focus of that chapter was on information: the rights, responsibilities, constraints, and competition around information relevant to national security. In this chapter, we maintain a focus on information, but instead of privacy-related concerns we take a different tack. The practices and institutions of intelligence are facing significant challenges due to changing technologies and changing social behaviours around the collection, use, and distribution of information.

This chapter will look a range of modern technologies that are causing disruptions to intelligence practice and institutions and require ethical analysis. We will show

DOI: 10.4324/9781003106449-13

throughout that the context of intelligence institutions is necessary to understand good intelligence practice. That is, we cannot reduce intelligence simply to practice; institutions are essential to an ethical analysis of intelligence. The first set of technologies that we are concerned with is biometric technologies, in particular, facial recognition technologies (FRTs). The second set is encryption technologies, in particular, the capacity for individuals with limited technological sophistication to access and use these encryption technologies effortlessly. The final example is the rise of open-source intelligence (OSINT). Here, this is enabled by a range of different technologies. What is common is the changing relationship between intelligence professionals and the public. 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 in order for them to be considered just. These technologies also interact to create further ethical complexities, which we will discuss later.

Facial Recognition Technologies, Biographies, and Institutional Risk

In Australia in 2022, community backlash and an investigation of the Office of the Australian Information Commissioner drove a number of major retail chains to reverse the roll-out and application of FRTs in their stores (Taylor 2022). This example is interesting for two reasons. First, the justification and limits of FRTs in this case go to core principles in the ethics of intelligence. The FRT in these occasions was being used or trialled in order to identify people who were known safety risks to staff and other customers. The managing director Mike Schneider of Bunnings, Australia's major hardware and home supplies chain, explained their reasoning like this:

> When we have customers berate our team, pull weapons, spit, or throw punches – we ban them from our stores. But a ban isn't effective if it's hard to enforce… Facial recognition gives us a chance to identify when a banned person enters a store so we can support our team to handle the situation before it escalates.
>
> (Taylor 2022)

In the same article, they report that there were limited risks to the average customer. "Schneider said regular customers did not have their images retained in the system. The technology, however, needs to scan the face of every customer entering the store to check against the database of banned customers" (Taylor 2022). What we see here is an example of the classic dilemma that intelligence institutions face in liberal democracies – how do you pursue security or safety, while ensuring that the basic rights of your citizens are respected?

While the privacy issues with FRT and related biometric identification technologies are significant issues in intelligence (privacy issues were discussed in Chapter 8), this Australian example draws out a distinct ethical challenge for intelligence institutions that is not covered by reference to the ethical principles developed in the JWT. To help motivate this claim, consider that Facebook was ordered to pay a US$650 million settlement to users in early 2021. This case was motivated by Facebook's use of FRT.

> The class-action suit, filed in Illinois in 2015, involved Facebook's use of facial recognition technology in its photo-tagging feature. With that feature, users can tag friends in photos uploaded to Facebook, creating links to the friends' profiles… The site's Tag Suggestions program generated automatic suggestions by using scans of previously uploaded images to identify people in newly uploaded shots. The lawsuit alleged that the scans were created without user consent and violated Illinois' Biometric Information Privacy Act, which regulates facial recognition, fingerprinting and other biometric technologies in the state.
>
> (Moyer 2021)

Like the Bunnings case, this example clearly relates to a range of privacy issues, but there is a different ethical issue here. Put simply, the issue is the *ease* with which modern technologies allow for identification of individuals by reference to biometric identifiers. In the Bunnings case, the FRT was being trialled and applied in physical locations, using physical infrastructure (cameras, etc.), in order to identify people in the world. In the Facebook case, the FRT was being used in virtual locations, using images posted to social media, in order to identify people in the world.

Moreover, claims are made about FRT that suggest a range of capacities beyond simple identification of an individual. Recent research claims that FRT can potentially predict race, gender, occupation, political orientation, sexual orientation, clinical conditions (depression, anxiety), and key neuropsychological traits (Wang and Kosinski 2018; Kosinski 2021).

There are two elements to FRT that pose ethical challenges to intelligence institutions. First is whether they should use FRT themselves. This is definitely an important ethical and indeed political issue. For instance, the use of Amazon's public facing doorbell camera, Ring, has been the subject of a number of discussions about whether domestic law enforcement should have access to the data gathered by the Ring cameras (Burgess 2022). There are significant concerns here about privacy and intelligence accountability. However, given that we have already discussed privacy issues previously, and through the book have shown that intelligence accountability is an ongoing discussion, there is a more interesting discussion to be had in this chapter. In particular, we aim to explore how cheap and easy-to-use FRT poses a major challenge to intelligence institutions – how can intelligence institutions keep the identity of their employees safe when FRT and related biometric technologies allow for easier and easier identification of people?

To place these commercial applications in a national security and intelligence context, consider this scenario: Alexei is a diplomat/intelligence agent of the country Anxietous and is meeting an employee of a nuclear power facility of Belligerence in the hope that they might pass him information on their nuclear power programme. They meet in a public space, walk around to ensure that they are not followed, and discuss the potential of this contact giving Alexei some relevant information. While they are both careful to ensure that they are not followed, unfortunately they are in a commercial area in which a number of stores have cameras that not only allow for FRT to be used to identify people, but those stores are forced to share that information with Belligerence's intelligence institutions. Like our Bunnings example, both Alexei and his contact are automatically placed on watch lists for FRT to pick up their faces. The fact that they are both seen together at very least means that Alexei's operation has very little chance of success and could have serious ramifications for him and his contact.

Now, consider a variation on this. Like Alexei, Alexandra is an intelligence officer of Anxietous, and she is trying to infiltrate Belligerence's nuclear power programme. She has a fake identity, alias, fabricated biography, and so on. However, Belligerence is attuned to the national security importance of their nuclear power programme, and so they use FRT to compare Alexandra's alias and biography with any people that match her on social media. Unfortunately for Alexandra, she had been posting regularly to social media for years, and only stopped when she started working for Anxietous' foreign intelligence agency. It is obvious that her stated name and biography don't match with that information online. Belligerence is not only able to very quickly expose her, rendering her operation a failure from the start, it could place her in danger. What matters here is not just the FRT but its use in combination with social media. As the Facebook example has shown, this combination of FRT and social media has been in operation since at least 2015 and poses major challenges to modern intelligence practice.

Consider now that both she and her home agency recognise this risk, and so they use a set of technologies and connections to social media companies to scrub her history from social media. She is now simply "Alexa", and there is no trace of her life prior to this mission. However, again, this would raise significant red flags for any of Belligerence's barely decent counter-intelligence officers. While they may not be able to identify who she really is, having no online history whatsoever strongly signals that Alex may not who she says she is.

Consider instead that she and her home agency recognise this "black hole" risk of no history, and so they now use a set of technologies and connections to social media to fabricate her fake identity. "Alexa" now has an online name and biography that matches that of her cover story. While this might solve the identifiability and black hole problems, it raises significant ethical issues about the relationships between government actors and private actors. For instance, do these private companies have a right or even a responsibility to accede to the intelligence agency's demands? One of the main controversies arising from the revelations from Edward Snowden was how the National Security Agency (NSA) in the US, the Government Communication Headquarters (GCHQ) in the UK, and other state intelligence agencies worked with and/or compelled private telecommunications and information and communication companies like Google, etc. to provide them with information (Greenwald 2014; Harding 2014). Similarly, in the US the Federal Bureau of Information (FBI) ultimately lost a court case seeking access to encrypted files on an Apple device used by a domestic terrorist (Etzioni 2018). We return to encryption later. The point here is that there is a strong presumption *against* private companies, particularly ones that have so much informational power like modern social media companies, working with national security actors like intelligence institutions.

Returning to our example, consider now that Alessandro is not an undercover agent seeking to infiltrate an adversary's nuclear power programme. Instead, she is a desk analyst working for Anxietous' domestic intelligence agency. She was a colleague of Alexandra's when they entered the graduate programme of the intelligence agency, and like almost everyone of her generation, took a number of photos with her friends, including Alexandra, and posted them online. Alexandra, anticipating that she might end up in HUMINT or related, was careful with her social media profile, but Alessandro had no such aspirations and so could afford to be less concerned about what she posted online. The problem is that FRT is increasingly easy and cheap to use; again, any barely decent counter-intelligence practice by Belligerence ought to be able to use FRT to find photos with Alexandra and Alessandro from their time together. Moreover, while Alessandro's role as an analyst would no doubt result in her not declaring her role publicly, it would not be hard for Belligerence to use FRT to connect Alexandra and Alessandra, to induce that Alessandro might be working for a government agency (again, the more careful she is with social media, the more this would act as a flag of her potential national security role), and so to put Alexandra's identity, operation, and ultimately her safety at risk.

The point in this section is twofold. First, it is to make the obvious point that technologies like FRT, whether in the physical or virtual worlds, pose significant practical challenges to intelligence. Insofar as having control over the biography, real or otherwise, of agents is necessary for intelligence institutions, then FRT significantly disrupts that. Second, there are a range of ethical issues associated with the use and protection against FRT. Privacy is one, but there is also the issue of responsibility that the intelligence *institution* has towards its own agents and its sources. What we suggest here is that one way to think of this responsibility is in terms of institutional responsibility.

Consider that in all cases described, the individual actors have limited capacity to do anything about FRT exposing important details about their identity. While Alexei might be able to engage in behaviours to limit his face being captured and recognised by physical FRT, given that there is so much physical infrastructure being developed that will allow for FRT to be applied in many public and semi-public places, it is unlikely that an intelligence operator like Alexei will have much capacity to avoid the risk of identification in the future. Similarly, Alexandra, Alessandra, and Alessandro have little to no capacity to personally wipe their online histories. And, if they do, an informational black hole like Alexa may open up. The point here is that FRT shows that the individual intelligence operative has very limited capacity to protect against the intelligence risks from FRT.

Importantly, there are things that the intelligence *institution* can do that these individuals cannot. First and foremost, the institutions have a responsibility to know what these risks are, and to alert any and all relevant intelligence operatives to the risk that FRT poses. Second, the institutions have a responsibility to develop and provide training and skills to intelligence operatives in relevant counter-intelligence to reduce the risk from FRTs. The future of intelligence may require *all* potential intelligence employees to learn techniques like "presentation attacks" that either impersonate or obfuscate the person's identity exist to varying degrees of success (Ming et al. 2020). Similarly, with regard to online biographies, etc., intelligence institutions have the capacity to check for risks posed by various operative's online profiles, and to reduce those risks. Obviously, the particular ways in which those risks are identified and reduced will vary depending on the particular person, their role, the state of the art in the technology, and the relations – including legal authority – between the intelligence institution and the particular private company. The point here is more general – the risk posed by FRT is one that must be met and discharged by the intelligence institutions.

Encryption Technologies, Secrecy, Freedom, and Accepted Risk

Another set of technologies that pose opportunities and risks to intelligence are encryption technologies. The history of encryption is tightly linked to intelligence – encryption and deciphering messages have been a key part of geopolitics and intelligence since at least the Renaissance (Andrew 2019, 139).[1] Intelligence, as has been argued throughout this book, is a competitive epistemic activity, with adversaries simultaneously seeking information on their adversaries and seeking to protect their own information from those adversaries. Encryption is a fundamental tool in this competition. Again, as argued earlier, national security intelligence is not simply gathering information on the world for the sake of information gathering, but to improve understanding and ultimately to guide better national security decision-making. However, this fundamentally requires communication of that information between a range of different parties. And those communications pose significant national security risks and opportunities. Encryption of communications is essential to any informational security.

In perhaps the most well-known example of this, during the Second World War, the German military used the Enigma cypher machine to communicate important information. The rotating cypher principle driving the Enigma machines was first developed by Dutch engineers in the Navy during the First World War. This rotating cipher machine was patented in 1919; the company was subsequently bought by a German company in 1927. These machines were small, portable, easy to use, and thought to be almost uncrackable.

> When World War II started, all German radio communications were enciphered on various models of Enigma machines having varying levels of sophistication. Thousands of enciphered messages were sent every day, from orders signed by Hitler and troop movements to weather reports and inventories for supplies of

> troops and boats. By the end of the war, between 50 000 and 120 000 Enigma machines had been manufactured…
>
> (Durand-Richard 2019)

According to one account, the use of Enigma was utterly essential to the early German military successes. The *Blitzkreig* was a "speed of attack through speed of communications, [achieving] one of the greatest revolutionary changes in military history" (Welchman, quoted in Durand-Richard 2019) The story of the Enigma machines involves the Polish Cypher Bureau cracking earlier versions of Enigma before the start of the Second World War, and then the GCHQ famously cracked Enigma towards the end of the Second World War. The point here is twofold – first is to demonstrate how important encryption and cracked encryption are to intelligence and national security more generally. Second is to draw out the fact that Enigma was so important to the German war effort, not simply because it provided (for a time) a high level of information security but because the machines themselves were small, portable, and easy to use. The technology that enabled the encryption was vital to the German war effort.

These two principles – the centrality of encryption to military success and the ways that portability and ease of use of encryption technologies impact information security – are borne out in an example from the 2022 Ukraine conflict. Knowing the importance of encrypted technologies to military communications, Russian forces brought with them mobile phones that ensured encrypted communications.

> Several Russian soldiers' mobile phones have reportedly been hacked after their secure encrypted phone system was destroyed during the ongoing "special military operation" in Ukraine. Investigative journalism organization Bellingcat revealed that Russian troops have switched off their encrypted phone system and used normal phones with local sim cards during the invasion. The Russian military had been using an encrypted communication system called "Era" to communicate with commanders and fellow soldiers to prevent eavesdropping. However, since the 3G/4G towers needed for Era to operate have been destroyed, Ukrainian intelligence has intercepted phone calls, including one made by a Federal Security Service (FSB) field officer informing officials in Russia of the death of Major General Vitaly Gerasimov.
>
> (Saballa 2022)[2]

Due to the fact that their military had destroyed Ukrainian telecommunications physical infrastructure in the early days of the invasion, these encrypted mobile phones no longer worked. Instead, Russian soldiers in Ukraine resorted to using Ukrainian SIM cards for military communications. These SIM cards lacked any relevant encryption and so Ukrainian and allied forces were able to monitor military communications. This was a major operational security failure on behalf of the Russian forces.

These issues of encryption and security extend far beyond military concerns. Given the reliance of private individuals and the modern world on so many information and communication technologies, there has been an unsurprising rise in private companies offering easy-to-use encryption technologies. Private communication services like Signal and WhatsApp market themselves on their encrypted communications. Telegram started out as an end-to-end encrypted communication service and added a "channel" function in 2015 in which a user can effectively broadcast to a wide audience. Perhaps driven by the Snowden revelations that intelligence agencies in liberal democracies were engaged in global surveillance operations, many civilians moved to these private encrypted communications services. We have seen a "trend, post-Snowden, of consumer technology companies designing their encrypted products and services such that the decryption keys are only available to the end-user(s)" (Davis 2022, 2–3).

In another recent example, a large number of people around the world bought a phone handset called "An0m" to enable potential criminal activity.

> The people selling the phone claimed that An0m was the most secure messaging service in the world. Not only was every message encrypted so that it could not be read by a digital eavesdropper, it could be received only by another An0m phone user, forming a closed loop system entirely separate from the information speedways along which most text messages travel. Moreover, An0m could not be downloaded from any of the usual app stores. The only way to access it was to buy a phone with the software preinstalled.
>
> (Parkin 2021)

Unfortunately for its users, the An0m phone was in fact a gigantic sting operation. The handset and associated communications were developed by law enforcement officers in the US FBI and the Australian Federal Police (AFP). Here, a

> confidential source was paid $180,000 by the FBI in salary and expenses, and built "a master key" that, the FBI explained in court documents, "surreptitiously attaches to each message and enables law enforcement to decrypt and store the message as it is transmitted". Every message sent via An0m was effectively BCC'd to the police.
>
> (Parkin 2021)

The AFP then slowly supplied the An0m phone to distributors who would then sell it onto people in Australia's criminal networks. This allowed them to build up trust in the phone, which was sold around the world to around 12,000 people in 90 countries, including many people involved in organised crime. This ultimately led to a worldwide operation and "as of 25 July [2021], 693 search warrants have been issued, 289 alleged offenders charged, and A$49m in cash, 4,788kg of drugs and 138 firearms and weapons seized in Australia alone. Six illegal drug labs have been dismantled" (Parkin 2021). This is an example of how a particular technology can operated as a honey pot in an intelligence sting – the simple belief that one's communications are encrypted can result in a change in people's communications. AFP assistant commissioner Nigel Ryan stated that "[i]f they were talking about money, they'd describe the exact amounts. These were not coded conversations, they were black and white" (Nigel Ryan, quoted in Parkin 2021).

The ease with which private actors can access and use encryption technologies is a two-edged sword for intelligence institutions in liberal democracies. On the one hand, principles like free speech, and particularly free association, are significantly important principles in liberal democracies. Confidence borne of encryption is a way of securing those principles. On the other hand, however, encryption is a tool that is used by malicious actors. Whether it is domestic criminals, international terrorists, or enemies of the state, encryption can enable and even afford behaviours that the liberal democratic state *may* have a responsibility to monitor and respond to. As the Enigma example shows, in extreme circumstances like war, not only do they have a responsibility to break encryption, but this can be of major national security importance.

Given this latter aspect, it is no surprise that many states engage in a range of practices seeking to overcome encryption technologies. But these efforts are not without significant criticism. In one case,

> Amnesty International, Forbidden Stories, and more than a dozen other organizations published forensic evidence that a number of governments worldwide – including Hungary, India, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates – may be customers of the notorious Israeli spyware vendor NSO Group.
>
> (Newman 2021)

This private company is the producer and vendor of the "Pegasus" software that can

> copy messages you send or receive, harvest your photos and record your calls. It might secretly film you through your phone's camera, or activate the microphone to record your conversations. It can potentially pinpoint where you are, where you've been, and who you've met.
>
> (Pegg and Cutler 2021)

It bypasses many encryption tools by exploiting vulnerabilities in the phone's software.

> Simply by placing a WhatsApp call to a target device, malicious Pegasus code could be installed on the phone, even if the target never answered the call. More recently NSO has begun exploiting vulnerabilities in Apple's iMessage software, giving it backdoor access to hundreds of millions of iPhones.
>
> (Pegg and Cutler 2021)

Pegasus has subsequently been found on the phones of political actors (Henley and Kirchgaessner 2021), diplomats ("Takeaways from the Pegasus Project" 2021), journalists (Kirchgaessner 2021a), human rights activists (*Washington Post* 2022;

Kirchgaessner 2021b), and so on. These revelations have led to widespread condemnation of the NSO Group, resulting in it being placed on a blacklist by the US Government, as they determined that its actions were "contrary to the foreign policy and national security interests of the US" (Kirchgaessner 2021c). This is quite revealing as the US engages in widespread surveillance and fought a high-profile battle with Apple to gain access to a terrorist's encrypted communications. We will return to this point later.

Finally, in another highly controversial case involving encryption technologies, in late 2018 the Australian government passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TAA) that meant "that Australian authorities will be able to compel tech companies like Facebook and Apple to make backdoors in their secure messaging platforms, including WhatsApp and iMessage" (Newman n.d.). This raised significant concerns around the world, as these backdoors would create significant vulnerability to any information communications services that relied on the encryption.

> [I]f Australia compels a company to weaken its product security for law enforcement, that backdoor will exist universally, vulnerable to exploitation by criminals and governments far beyond Australia. Additionally, if a company makes an access tool for Australian law enforcement, other countries will inevitably demand the same capability.
>
> (Newman n.d.)

The overwhelming concern with the Australian legislation was not just about the potential power and overreach of the Australian government, but that in requiring these backdoors, the Australian government could significantly damage confidence in encryption technologies around the world.

The ethics question then is what ought intelligence agencies do about encryption? Is it a universal good, an enabler of malicious behaviour, or something else? The range of examples that we have shown here suggest that there is a range of answers to this question. Moreover, the applications of encryption range from military intelligence, to criminal activity, to terrorism command and control, to private citizens seeking to keep certain communicative spaces free of government surveillance. In short, any simple answer to encryption is going to lack any nuance or credibility.

Instead, our suggestion here is that encryption technologies are diverse, their applications are diverse, and the users and their motivations are diverse. As we saw with Enigma and An0m cases, there are many instances in which intelligence agencies cracking of encryption is warranted and may even be necessary. But as we saw with the Pegasus and Australian government cases, weakening encryption can be significantly dangerous to democracy and the global internet. Given the diversity in technologies, applications, users, and risks, intelligence agencies need a certain amount of discretion in how they approach encryption. That is, they are typically the ones who make the decision to use their tools to break encryption. In the TAA,

> The chief officer of the agency in question must simply satisfy *themselves* that the assistance would be "reasonable and proportionate", that compliance would be "practicable" and "technically feasible", and a range of other considerations. Any independent oversight happens after the fact, conducted for intelligence agencies by the Inspector-General of Intelligence and Security (IGIS), and for law enforcement by the commonwealth ombudsman and their state and territory equivalent.
>
> (Stilgherrian 2021; emphasis ours)

Putting aside concerns about the global vulnerability that the TAA may have created, this discretion on behalf of the chief officer is perhaps one of the bigger concerns with the TAA. Not so much that there is discretion, but that it seems to lack oversight and some form of external forward-looking accountability.

As the US blacklisting of NSO Group showed, any uses of tools that can undermine encryption must be in line with core liberal democratic values. But making such statements is at risk of being an empty platitude if those values are not specified, and if there is not some way of ensuring before and after that any such applications are consonant with those values. In short, accountability requires the intelligence agencies to have the institutional resources and infrastructure that can actually give an account of how a particular use of encryption technologies or their hacking actually fits with and meets the core values.

To be clear, such an account-giving exercise is not simple or easy. Like many other areas in intelligence and national security, more generally, there are going to be situations and circumstances where no good answer can be given. That is, no matter what happens, some less-than-ideal outcome will come to pass and/or some set of rights will be violated in favour of some other set of rights. But account-giving is central here again. For instance, if it turns out that an Australian intelligence agency did not break the communications of a suspected terrorist group, and that resulted in a successful terror attack, Australian citizens and people, more generally, would justifiably demand an explanation. In this case, if it turned out that the breaking of their communications would result in effectively undermining encryption at a global level, it would be possible to argue that the need to protect encryption outweighed that of the need to stop the terrorist attack.

We recognise that this is quite a controversial position – terrorism in particular is typically treated with a zero tolerance policy. And any decision-making that veers away from that is politically and socially fraught.

> [W]e have a political class that feels it must inoculate itself against allegations of weakness. Our politicians are more fearful of the politics of terrorism – of the charge that they do not take terrorism seriously – than they are of the crime itself.
>
> (Snowden 2016)

To be clear here, we are not necessarily advocating this position, and not saying in all circumstances that national security considerations can be outweighed by other concerns. Our point is rather that it is an open question about the trade-off between national security and individual human rights. And when considering intelligence ethics, it is equally an open question about encryption and building back doors into the infrastructure of the internet. However, it does not follow that labelling something an open question means that any decision is justified. What is needed here is effective, ongoing, and robust institutional accountability mechanisms that both ensure and assure[3] the public that the reasons given for a particular decision around encryption, and intelligence more generally, are not simply justifiable but have justification in the particular case.

One further point we do want to make here is that citizens of liberal democratic states must also bear some risk that their individual rights generate. For instance, if a nation's citizens deem it that the individual rights protected by encryption and threatened by backdoors are too important to risk, then these same citizens must equally accept that these rights protections put them at some risk of malicious actors. That is, they must accept that there is some risk that encryption will enable malicious actors to communicate and organise dangerous activities. Given that liberal democratic communities tacitly accept these costs with regard to privacy, it seems reasonable that the same ought to hold with regard to encryption.

This brings us back to accountability. If an intelligence institution takes certain liberal democratic principles to be ethically weighty, then there is an accepted risk arising from the limits on what the intelligence institution can do. Accountability here requires some explicit story around what the value trade-offs were, how the ultimate trade-off was made, and what the costs of that trade-off are. Moreover, it is good public policy for intelligence institutions, and the governments that they serve more generally, to actively, clearly, and truthfully explain this to the public. This goes back to the issue of trustworthiness, discussed in an earlier chapter. Not only do these trade-offs need to be explained publicly to engender public trust in intelligence decision-making but also that decision-making must be worthy of that trust. Accountability regarding the explicit ethical reasoning that led to a particular decision is essential.

OSINT and Institutional Accountability to and for the Public

As the 2022 Ukraine conflict developed, one of the interesting features was the evolution of OSINT. OSINT is more of a practice than the previous two technology-focused discussions, but evolving technologies and social behaviours around new social information technologies are driving an evolution in OSINT. Some of these changes in OSINT are driven by the rise in computational power and analysis. For instance, some claim that it is possible to use someone's online social media commentary to identify the author of that material (Kernot D., Bossomaier T., and Bradbury R. 2018; Kernot D., Bossomaier T., and Bradbury R. 2017a, 2017b).

Historically, OSINT could be thought of as the work that analysts do with publicly available information. "Open source intelligence is developed from publicly available electronic and print information" (Delmar P. Wright in Arrigo 2016, 516). The sources here differ from that of other intelligence gathering like HUMINT, SIGINT, GEOINT, etc., in that in those forms of intelligence, the people doing the collection are either an intelligence officer or technical specialist using, or with access to, privileged information. Drawing from the idea of intelligence being epistemic actions in a competitive environment, the more traditional modes of intelligence relied on, or used, information that was gathered in a way that was hard to get, and/or the sources of that information did not know that information was being collected on them. OSINT, traditionally, took a different tack. The paradigm example would be an analyst looking at and using publicly available information to offer an analysis on a particular source or topic. This could be considered research similar in form to academic research, but it still is intelligence in our definition as the derived information, the product that the analyst produces, is something that is privileged. It may not be classified as secret or top secret, etc., but it is still protected information.

The 2022 Ukraine conflict saw an increasing expansion of OSINT, supported in a significant way by a range of information and communication technologies. First, many Ukrainian civilians have been using cameras and microphones in attempts to document potential war crimes. "Images posted online will be crucial in prosecuting war crimes in Ukraine, according to UK legal experts… One online investigator said there was 'so much' useful and verifiable information in warzone footage" (Pigott 2022). While these actions likely do not meet the standard of intelligence that would be expected of professional HUMINT and SIGINT operations, the ways that new technologies are affording civilians greater roles in providing information for intelligence collection need to be recognised.

Another fascinating development in the Ukraine conflict relevant to OSINT is the rise of OSINT analysis. For instance, one university student in the US operates under the pseudonym Intel Crab, and "[f]rom his dorm room, the 20-year-old sifts through satellite images, TikTok videos, and security feeds, sharing findings like troop movements and aircraft models with more than 220,000 followers on Twitter" (Schwartz 2022). Note that in contrast to the more traditional description of OSINT given by Delmar P. Wright, earlier, we are now looking at open-source analysis, not collection. These OSINT analysts effectively engage in crowdsourced intelligence, with many online civilians looking at information posted online, analysing it, and producing an intelligence product for Ukrainian and allied militaries to use as they see fit. This trend developed prior to the Ukrainian conflict, "since at least 2014, [civilians have been] working collaboratively across the world to comb through freely available resources like Google Maps and the satellite imagery service Maxar Technologies" (Schwartz 2022). In a further example of just how this OSINT differs from traditional intelligence analysis, much of this analysis is made public, both for intelligence or national security actors to access, but also for wider public consumption. One OSINT analyst's Twitter "account lays out findings in tweet threads breaking down their research and deleting any tweets that they later find to include false information" (Schwartz 2022).

One fundamental problem and challenge of relying on civilian-sourced and analysed intelligence is how to treat that information. This is a part of the evaluation phase,[4] but information about OSINT must be included at the collection and collation phase.

> In the midst of a very active conflict, there's also an informational tussle that's going on online as well… For accounts that wield enormous followings, if they post and get it wrong, there's a good chance that it spreads very quickly.
>
> (Schwartz 2022)

This exposes the significant national security and ethical concerns with OSINT, in that relying on and responding to incorrect intelligence can lead to significant problems when it comes to decision-making.

The case of Curveball, the main source of faulty intelligence of evidence of weapons of mass destruction (WMD) in Iraq in the early 2000s mid 00s, is a stunning cautionary tale about the need to vet sources and properly and comprehensively evaluate intelligence (Drogin 2008). The problem with OSINT collection is that it may be incredibly hard to engage in the normal assessment of the source and the content of the intelligence that they provide. For instance, it is quite possible that the intelligence received through OSINT is counter-intelligence provided by the adversary in order to effectively poison the intelligence.

The basic principle here – both in terms of operations and ethical responsibility – is not to rely on OSINT collection alone for decision-making. In the Ukraine case, the use of civilian-collected intelligence for use in war crimes investigation carries less risk than that of operational intelligence. But as handheld surveillance technologies, like mobile phones, and internet-enabled platforms allow for increased OSINT collection and communication, significant care must be taken both in terms of how that information is treated, but also, in making explicitly clear if any professional intelligence analysis involves such OSINT. Further, this needs to be made clear throughout the intelligence cycle. As Curveball effectively demonstrated, there needs to be a clear and ongoing inclusion of the relevant information about the sources and confidence of intelligence.

A third feature of the Ukrainian conflict that makes it particularly interesting for the ethics of intelligence is the way in which civilian actors have been actively encouraged to engage in aggressive cyber operations. As the conflict developed, the Ukrainian government has actively asked for civilians to conduct aggressive cyberattacks on Russian targets. This is ethically complicated for at least two reasons. First, drawing from the JWT, while it is possible to argue that individual fighters might have the legitimate authority to engage in conflict that meets other just war criteria (Schwenkenbecher 2013), there is a very complicated debate about whether the Ukrainian political leadership ought to be actively encouraging this. Second, bringing us back to the institutional ethics concerns, what is the status of these vigilante civilian cyber-warriors, and what moral responsibility does a government or military bear when those civilian cyber-warriors are targeted by the adversary military and intelligence institutions?

At an early phase in the war, a Kyiv-based cybersecurity company wrote the following post at the request of a senior Ukrainian defence official. "Ukrainian cybercommunity! It's time to get involved in the cyber defense of our country", with the post asking for "hackers and cybersecurity experts to submit an application via Google docs, listing their specialties, such as malware development, and professional references" (Schectman and Bing 2022). While calls for civilian participation in conflict is nothing new, the technological shifts brought about by cyberspace change the assessment of this somewhat. Arguably, in the case of traditional conflict, if a person volunteers to fight, they know that they are putting their lives at risk. War, by definition, involves the risk of death for those who participate in conflict. In cyberconflict, however, it is perhaps harder to be assured that those participating in the conflict understand the risks that they are taking on. And here we need to ask if the government who is asking for volunteers can be certain that those participating in the conflict understand the risks that they are taking on.

Part of the reason why this is a hard question to answer is because cyberconflict is still relatively new. Given that, it is hard for individuals and institutions to know just what risks are posed by participating in cyberconflict. In 2013, Mojtaba Ahmadi, the commander of the Iranian Cyber War headquarters was shot and killed (McElroy 2013). This case is relevant because it was perhaps the first example of a cyber-actor being killed for their role in cyberconflict. It suggests that – for some actors, and in some contexts at least – participation in cyberconflict makes one liable for lethal force. While it is highly unlikely that Russia would have the resources or indeed the will to use lethal force against those cyber-volunteers engaged in hostilities against them, it is much more likely that cyber-volunteers would be at risk of being targeted for cyberattacks themselves.

On the one hand, considering the principle of reciprocity introduced in Chapter 4, international law may permit this under the principle of countermeasures. Rule 9 of the Tallinn Manual states that a "State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State" (Schmitt 2013, 40). While the Tallin Manual is not definitive, and ethics and international law do not necessarily align, this principle suggests that those cyber-volunteers open themselves up to a *potentially* justifiable set of countermeasures in response to their aggressive cyber actions. To be clear, we emphasise "potentially" here as this is an open area of debate but want to show that the principle of countermeasures might be seen by a country subject to cyberattacks as offering a justification for responses.

Of course, any such response would also need to be discriminate, necessary, and proportionate. However, on proportionality, it is very hard to clarify what that would mean (Henschke 2018). If a cyber-volunteer engages in an activity that shuts down the public transport in the target state's capital, what is a proportionate response to that individual? Would a proportionate countermeasure be a targeted attack on their car? If that is not possible, would freezing their assets, hacking their email, doxing them be proportionate? While the mode and target of the attack are still within cyberspace, so broadly proportionate, it is very hard to state whether such countermeasures are proportionate. Further to this, Rule 9 explicitly states that the countermeasures are permitted against the *responsible state*. Here we have a problem of discrimination. Just who is a legitimate target of attack here? In traditional conflict, it is perhaps easy to see how a volunteer fighter is part of a military force. But when we have volunteer cyberwarriors drawn, perhaps from around the world, and indeed, potentially not citizens of, or living in, any of the countries engaged in the conflict, it is very hard to know whether these citizens are legitimate targets or not, even if we grant the principle of countermeasures.

On this, again, we have no easy answers. However, we return to the point of institutional accountability. In this case, there is a significant and ongoing responsibility for a government – and the relevant military and intelligence institutions – who call for and encourage cyber-volunteers to both understand what risk those volunteers may face and to take special pains to ensure that those volunteers can understand what those risks are. Moreover, it seems incumbent on that government to have the capability to protect those cyber-volunteers. Given that the cyber-volunteers are taking on the risk on behalf of and deriving their ethical justifiability in the name of the particular state and its people, the state and its institutions – particularly SIGINT institutions – must take special care of their cyber-volunteers. They ought to be afforded a set of protections equivalent to the risk that they are taking on. And if that risk rises – for instance, if the intelligence agency of the given state determines that the adversary state is likely to hack and steal any money from cyber-volunteers – then they need to minimise that risk, alert the cyber-volunteer to that new risk, and perhaps even guarantee compensation equivalent to the lost money. This is of course controversial and needs much more discussion than can be covered here. The point here is that it is not enough to simply state that the cyber-volunteers take on all the risk themselves; the state has a special set of responsibilities to those cyber-volunteers, equivalent to the responsibilities that it has for volunteers in a physical fighting force.

Conclusion

The overall point of this chapter is twofold. First, that intelligence is changing as information and communication technologies change. Second, that these changes generate new and particular ethical responsibilities in the institutions of intelligence that cannot effectively be discharged by individuals alone. On the first point, this is a general and unsurprising observation. Information and communication technologies have been causing significant disruptions and driving change in most facets of human life for the past decades. Given that intelligence is an epistemic activity, we would expect that this would have an effect on intelligence practices too.

The second point is of greater interest to us here. We have shown how FRTs generate ethical responsibilities in intelligence institutions due to the fact that individuals have very little capacity to protect themselves against malicious or competitive use of FRT. We also argued that encryption technologies can be used in a host of ways by a host of intelligence actors for a host of purposes. Instead of offering any particular recommendation for the use of, and protection against, encrypted technologies, our conclusion was that intelligence actors need discretion when it comes to encryption technologies. However, such discretion is potentially problematic, and so effective accountability is needed here to ensure that the particular decisions around encryption are justifiable and justified. Again, this draws out the importance of the institution. It is not enough to simply say "we need accountability for encryption technologies"; this claim needs to be understood in reference to, and discharged by, the relevant intelligence institutions in question. Finally, we looked at the rise and evolution of OSINT. Again, the conclusion here is that the calls for, and the use of, OSINT generate particular institutional responsibilities. This might be to ensure that any intelligence product that involves OSINT is clearly communicating to the customer as involving OSINT and having some assessment on what risks that OSINT source and analysis pose to the quality, credence, and viability of the end product. We also argued that the intelligence institutions that use and encourage civilians to engage in OSINT have a duty of care to those volunteers. Just what this duty of care entails will vary from case to case, but the institutions must ensure that the risks to volunteer intelligence actors are known and mitigated to some degree.

We can also see here how the previous chapters and discussions both inform and drive the ideas of institutional ethics presented in this chapter. The basic principles of *jus ad intelligentium* and *jus in intelligentia* give the substance to the institutional responsibilities. Not only do these principles suggest how individuals ought to act, they also provide guidance on how to design intelligence institutions. Just as an intelligence institution that has no capacity to ensure that their actions are necessary, discriminate, and proportionate will not be a just institution, so too must these institutions recognise their special and evolving responsibilities in response to emerging technologies, such as FRT, encryption, and OSINT. Moreover, as argued in Chapter 9, just intelligence institutions must also attend to principles like being trustworthy. Our point in this chapter has been to extend the argument about institutional responsibility based upon the challenges posed by emerging technologies. That institutional responsibility is based in and drawn from the principles and their application, discussed in the earlier chapters.

Notes

[1] For a more recent history of the role of encryption and deciphering in modern computer development, see Greenberg (2012).

[2] I note that General Gerasimov was subsequently found to be alive.

[3] As has been argued elsewhere, where governmental surveillance is involved, in liberal democracies, any such decisions must ensure that they meet the relevant ethical and legal norms, as well as assure the public that any decisions have met the relevant justifications (Robbins and Henschke 2017).

[4] We draw here from the intelligence cycle, particularly Paul Burke's six-stage cycle, involving Direction, Collection, Collation, Evaluation, Analysis, Dissemination, returning to Direction (Burke 2022, 353).

References

Allhoff, Fritz. 2011. "What Are Applied Ethics". *Science and Engineering Ethics* 17: 1–19.

Andrew, Christopher. 2019. *The Secret World*. London: Penguin Random House.

Arrigo, Bruce A. 2016. *The SAGE Encyclopedia of Surveillance, Security, and Privacy*. London: Sage.

Burgess, Matt. 2022. "Amazon Handed Ring Videos to Cops without Warrants". *Wired*, September 1. www.wired.com/story/amazon-ring-police-videos-security-roundup/

Burke, Paul. 2022. "Intelligence and National Security: The National Security Problematique". In *The Palgrave Handbook of National Security*, edited by Adam Henschke, Matthew Sussex, Michael Clarke, and Tim Legrand. Cham: Palgrave Macmillan. pp 351–70. www.springerprofessional.de/en/intelligence-and-national-security-the-national-security-problem/19706514

Davis, Peter Alexander Earls. 2022. "Decrypting Australia's 'Anti-Encryption' Legislation: The Meaning and Effect of the 'Systemic Weakness' Limitation". *Computer Law & Security Review* 44 (April): 105659. https://doi.org/10.1016/j.clsr.2022.105659

Drogin, Bob. 2008. *Curveball: Spies, Lies and the Man behind Them: The Real Reason America Went to War in Iraq*. London: Random House.

Durand-Richard, Marie-José. 2019. "From Poznań to Bletchley Park: The History of Cracking the ENIGMA Machine". *CIIT Lab Workshop on History of Cryptograph*, January. www.academia.edu/41287162/From_Pozna%C5%84_to_Bletchley_Park_the_history_of_cracking_the_ENIGMA_machine

Etzioni, Amitai. 2018. "Apple: Good Business, Poor Citizen?" *Journal of Business Ethics* 151(1): 1–11. https://doi.org/10.1007/s10551-016-3233-4

Greenberg, Andy. 2012. *This Machine Kills Secrets: How Wikileaks, Cypherpunks and Hacktivists Aim to Free the World's Information*. New York: Penguin.

Greenwald, Glen. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

Harding, Luke. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted Man*. New York: Vintage Books.

Henley, Jon and Stephanie Kirchgaessner. 2021. "Spyware 'Found on Phones of Five French Cabinet Members'". *The Guardian*, September 23. www.theguardian.com/news/2021/sep/23/spyware-found-on-phones-of-five-french-cabinet-members

Henschke, Adam. 2018. "Conceptualising Proportionality and Its Relation to Metadata". In *Intelligence and the Function of Government*, edited by Daniel Baldino and Rhys Crawley. Melbourne: Melbourne University Press. pp 177–93.

Kernot David, Bossomaier Terry, and Bradbury Roger. 2017a. "Novel Text Analysis for Investigating Personality: Identifying the Dark Lady in Shakespeare's Sonnets". *Journal of Quantitative Linguistics* 24: 255–72.

Kernot David, Bossomaier Terry, and Bradbury Roger. 2017b. "The Impact of Depression and Apathy on Sensory Language". *Open Journal of Modern Linguistics* 7: 8–32.

Kernot David, Bossomaier Terry, and Bradbury Roger. 2018. "Using Shakespeare's Sotto Voce to Determine True Identity from Text". *Frontiers in Psychology* 9: 289.

Kirchgaessner, Stephanie. 2021a. "Phones of Journalist Who Tracked Viktor Orban's Childhood Friend Infected with Spyware". *The Guardian*, September 21. www.theguardian.com/news/2021/sep/21/hungary-journalist-daniel-nemeth-phones-infected-with-nso-pegasus-spyware

Kirchgaessner, Stephanie. 2021b. "New Evidence Suggests Spyware Used to Surveil Emirati Activist Alaa Al-Siddiq". *The Guardian*, September 24. www.theguardian.com/world/2021/sep/24/new-evidence-suggests-spyware-used-to-surveil-emirati-activist-alaa-al-siddiq

Kirchgaessner, Stephanie. 2021c. "Israeli Spyware Company NSO Group Placed on US Blacklist". *The Guardian*, November 3. www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist

Kosinski, M. 2021. "Facial Recognition Technology Can Expose Political Orientation from Naturalistic Facial Images". *Scientific Reports* 11: 100.

McElroy, Damian. 2013. "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination". *The Telegraph*, October 3. www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html

Ming, Zuheng, Muriel Visani, Muhammad Muzzamil Luqman, and Jean-Christophe Burie. 2020. "A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices". *Journal of Imaging* 6(12): 139. https://doi.org/10.3390/jimaging6120139

Moyer, Edward. 2021. "Facebook Privacy Lawsuit over Facial Recognition Leads to $650M Settlement". *CNET*, February 21. www.cnet.com/tech/services-and-software/facebook-privacy-lawsuit-over-facial-recognition-leads-to-650m-settlement/

Newman, Lily Hay. 2021. "An Explosive Spyware Report Shows the Limits of IOS Security." *Wired*, July 22. www.wired.com/story/nso-group-hacks-ios-android-observability/

Newman, Lily Hay. n.d. "Australia's Encryption-Busting Law Could Impact Global Privacy". *Wired*. Accessed August 3, 2022. www.wired.com/story/australia-encryption-law-global-impact/

Parkin, Simon. 2021. " 'Every Message Was Copied to the Police': The inside Story of the Most Daring Surveillance Sting in History". *The Guardian*, September 11. www.theguardian.com/australia-news/2021/sep/11/inside-story-most-daring-surveillance-sting-in-history

Pegg, David and Sam Cutler. 2021. "What Is Pegasus Spyware and How Does It Hack Phones?" *The Guardian*, July 18. www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

Pigott, Pual. 2022. "Ukraine: Online Posts 'Transform' War Crimes Documentation". *BBC News*, April 16. www.bbc.com/news/uk-wales-61011855

Robbins, Scott and Adam Henschke. 2017. "Designing for Democracy: Bulk Data and Authoritarianism". *Surveillance and Society* 15(3): 582–89.

Saballa, Joe. 2022. "Russian Military Phones Hacked: Report". *The Defense Post* (blog). March 9. www.thedefensepost.com/2022/03/09/russian-phones-hacked/

Schectman, Joel and Christopher Bing. 2022. "Ukraine Calls on Hacker Underground to Defend against Russia". *Reuters*. www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/

Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schwartz, Leo. 2022. "Amateur Open-Source Researchers Went Viral Unpacking the War in Ukraine". *Rest of World*. March 7. https://restofworld.org/2022/osint-viral-ukraine/

Schwenkenbecher, Anne. 2013. "Rethinking Legitimate Authority". In *Routledge Handbook of Ethics and War: Just War in the 21st Century*, edited by Fritz Allhoff, Nicholas G. Evans, and Adam Henschke. London: Routledge. pp 161–70.

Snowden, Edward. 2016. "Forward". In *The Assassination Complex: Inside the Government's Secret Drone Warfare Programme*, edited by Jeremy Schahill and Intercept. Simon & Schuster. www.theguardian.com/us-news/2016/may/03/edward-snowden-assassination-complex-governments-tagged-animals-drone-warfare-whistleblower

Stilgherrian. 2021. “The Encryption Debate in Australia: 2021 Update”. *Carnegie Endowment for International Peace*. March 31. https://carnegieendowment.org/2021/03/31/encryption-debate-in-australia-2021-update-pub-84237

“Takeaways from the Pegasus Project”. 2021. *Washington Post*, July 18. www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/

Taylor, Josh. 2022. “Bunnings and Kmart Halt Use of Facial Recognition Technology in Stores as Privacy Watchdog Investigates”. *The Guardian*, July 25. www.theguardian.com/technology/2022/jul/25/bunnings-and-kmart-halt-use-of-facial-recognition-in-stores-as-australian-privacy-watchdog-investigates

Wang, Y. and Kosinski, M. 2018. “Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images”. *Journal of Personality and Social Psychology* 114: 246–57.

Washington Post. 2022. “Dozens of Thai Activists and Supporters Hacked by NSO Group’s Pegasus”. Accessed August 3, 2022. www.washingtonpost.com/technology/2022/07/17/pegasus-nso-thailand-apple/

11 The Future of Intelligence Practice

Concluding Lessons for Just Intelligence Institutions

Patrick F. Walsh and Adam Henschke

This book has been advancing two interrelated theses. First, if we are to apply the general principles of just war to intelligence, these principles need to be significantly adapted to meet the particularities of intelligence. That is, we cannot simply take the just war principles from the context of warfare and use them in the same way in the context of intelligence. Second, in developing a comprehensive ethics of intelligence, we cannot simply look at intelligence as a practice. We need to also view the institutions of intelligence. The institutional focus enables us to both make sense of intelligence as a practice – the practice and institutions are tightly linked – and to better appreciate the moral purposes of intelligence. In this chapter, we look to health security to show how intelligence is evolving, and we speculate on what the future holds for intelligence practice and institutions, and for the ethics of intelligence more generally.

The basic argument of this chapter is that intelligence continues to evolve. The practices of intelligence change not just as technologies of intelligence and counter-intelligence change, as was discussed in Chapter 10, but as the context and needs for intelligence change. We use this idea of development of intelligence practices and institutions to conclude the book. This chapter serves to consolidate the preceding discussions and suggests that intelligence will continue to evolve. Fundamental to this evolution is the changing environment and roles of intelligence actors and institutions.

Nowhere is that more obvious than in the increased interactions and overlaps between intelligence and health security. In particular, as the COVID-19 pandemic spread around the world in 2020, intelligence actors and agencies were involved in the efforts to understand and limit the impacts of the pandemic. In this chapter, we will look at the ways that intelligence has been used during the pandemic to open up a discussion about the emerging role of health security in both national security and in intelligence. We suggest that many of practical and ethical challenges that intelligence actors and institutions faced during the COVID-19 pandemic indicate future areas in which the ethics of intelligence will become more important.

We hope to show that the future of intelligence requires intelligence practitioners and those engaged in intelligence studies to think about how to adapt ethical principles like discrimination, necessity, proportionality, and reciprocity to

DOI: 10.4324/9781003106449-14

intelligence. Moreover, we hope to show that the practices and institutions of intelligence stand in a unique relationship with people, private actors, and political institutions – embracing this institutional and social interaction means that the just intelligence theory (JIT) model is uniquely different from the just war tradition (JWT) model. Not only does this institutional focus mean that the principles underpinning the JWT and JIT models significantly differ in their application, as we saw in Chapters 3 and 4, but, as will be discussed later in this chapter, recognising the institutional and social context means that the JIT approach includes values like reciprocity and trust alongside the more traditional values found in the JWT.

To motivate and give substance to our points, we look at the ways that new surveillance technologies and practices have been used to understand and respond to the COVID-19 pandemic. We recognise that it is difficult to address these issues comprehensively, given their complexity, and the fact that we are still trying to understand the widespread impacts that the pandemic had on different people and different communities around the world. Nonetheless, given the loss of life due to COVID-19, now according to the WHO to be around 765 million cases and 7 million deaths (World Health Organization n.d.), and the ensuing and long-lasting economic, social, and security instability in many parts of the world suggest, there is a need to better understand how nations can best improve health security surveillance to more effectively detect, warn, and manage pandemic diseases. Moreover, by looking at the ways that intelligence practices and institutions were used during COVID-19, we hope to identify future ethical challenges in intelligence.

Drawing on the discussion in Chapter 10, but also the national security and ethical principles underscored in Chapters 2, 3, and 4, this chapter examines how surveillance technologies usually applied to more traditional national security threats and risks contexts (state-based threats, terrorism and organised crime) are now being used alongside public health surveillance measures against COVID-19. The chapter also addresses the question of efficacy – what is the efficacy of some of the surveillance technologies and wider intelligence approaches to prevent, disrupt, and or provide early warning of pandemics? We use this discussion to close out the book, introducing one final principle, the risk of transparency (ROT), as a final part of the JIT.

COVID-19 and Intelligence: Health Security, Health Surveillance, and National Security Surveillance

A key feature of public health responses to COVID-19 was the range of surveillance tools and methods that were rolled out to increase our understanding of the pandemic, and to try to minimise its impacts (Macnish and Henschke 2023). There was an understandable rush by many governments, including those in liberal democracies, to implement various data-driven public health and national security surveillance techniques and technologies. These were used to help augment the traditional public health epidemiological contact tracing approaches, given the rising case numbers, particularly in the first year of the pandemic where no vaccines were available. However, with improved public health knowledge and practice to counter the various variants of COVID-19 (particularly Alpha, Beta, Delta, and Omicron), including a largely effective suite of vaccines, better medical treatment, and enhanced infectious disease control measures (at least in some countries), it is timely for researchers to evaluate whether surveillance techniques and technologies introduced during the pandemic have been effective in their broadest sense. Additionally, in order to improve the effectiveness of various surveillance technologies and techniques used during COVID-19 for their use to counter likely future pandemics (whether they are accidental or intentional in origin), there is also a clear need to assess their efficacy in the broader context of how to navigate the inevitable ethical dilemmas arising from their use in liberal democracies.

This discussion requires us to offer descriptions of three key terms: "health security", "health surveillance", and "national security surveillance". Understanding "health security" helps frame how we understand threats and risks in the health context such as pandemics from a public health and national security perspective. Additionally, clarifying our use of "health surveillance" and "national security surveillance" is critical in framing the remaining discussion in this chapter about the depth and breadth of surveillance in the public health and national security context as they relate to COVID-19 and other pandemics.

Starting with health security, there are several perspectives on how to describe what is meant by "health security" (Walsh 2018,10). Such perspectives have been influenced by public health scholars, sociologists, IR/security (particularly those working in human and critical security areas), and intelligence studies scholars (Walsh 2018, 2020). Limited space does not allow an extended review of theorising around "health security", but suffice it to say, from the 1990s, many global health specialists begun to characterise global infectious diseases, such as HIV/AIDS, SARs, and EBOLA, as not just public health crises but as causes of instability in both strong economies and vulnerable countries. This demonstrates that they also have security dimensions.[1] Similarly, biosecurity and biodefence experts have long seen the national security implications of health crises such as pandemics, particularly the possibility that they may, in very rare cases, result from an intentional weaponisation of an infectious disease (Battin et al. 2008; Selgelid and Enemark 2008; Selgelid 2006, 2013). Whether a global pandemic is natural or weaponised in origin, the outcome, either way responding to it clearly, has public health and national security implications – hence neither public health authorities or those in national security exclusively "own the problem".[2] We use health security here to mean the

> security from health related threats and risks – whether they be from naturally occurring or emerging infectious diseases, or those that are intentional (from weaponizing dangerous biological materials), the deliberate misuse of dual use biotechnologies, and other threats that are unintentional from diverse range of pathogens that threaten the food supply and the environment.
>
> (Walsh 2018, 13, 2020)

In short, the term "health security" provides a theoretical anchoring under which studies about particular threats (biosecurity, biosafety, bioterrorism), pandemics, and others can be discussed together – given all health threats have an individual (human health) dimension and likely a broader global (biosecurity, biodefence) component to them (Albert, Baez, and Rutland 2021, 83–103).

The second term requiring clarification is health surveillance, and its distinction from national security surveillance. Similar to the case with "health security", several distinctions can be made on what surveillance is in either the national security or health context. Surveillance can generally mean

> to "watch over" and as such it is an everyday practice in which human beings engage routinely, often unthinkingly… In most instances, however, surveillance has a more specific usage, referring to some focused and purposive attention to objects, data, or persons.
>
> (Lyon 2009)[3]

This focused and purposive attention allows for a rough distinction to be made between health surveillance and national security surveillance. In line with the teleological approach described in Chapter 2, Davis recognises that national security surveillance and health surveillance have different purposes and applications (Davis 2021, 151). Broadly, this is true enough, given health surveillance techniques and technologies are about tracking disease, not an individual or group who actively and deliberately pose a national security threat. Additionally, Davis suggests that health surveillance's "use of personal technologies like apps on smart phones for pandemic surveillance monitoring and alerts as being more limited in scope and have privacy protections" (ibid. 157), when compared to a broader surveillance technology deployed by national security agencies, which are aimed at intercepting a range of personal and public communications technologies. Health surveillance is therefore concerned with a *focused and purposive attention to people, behaviours, and clinical information in order to gain an understanding of health-relevant phenomena*.

As COVID-19 has demonstrated, the use of surveillance systems traditionally used in tracking the movement of suspected national security threats is also useful in tracking the movement of people and determining if they may have an infectious disease. Israel, for instance, adopted a system from its internal security service, Shin Bet, which normally uses the anti-terrorism technology to tap into cellular data to retrace the movements of people infected by COVID-19 (Davis 2021, 158; Hickok 2020). As we will see, given how some national security surveillance techniques have been used during COVID to help contact tracing and for enforcement/compliance, and that surveillance of a broad range of health-related phenomena is increasingly important for national security concerns, the use of health and national security surveillance techniques and purposes have been blurred. Hence it will become more difficult in some contexts to distinguish between the two. This blurring, as we will argue later, is perhaps indicative of the future of intelligence and poses a series of ethical challenges for intelligence.

Efficacy of Health Surveillance Technologies: Fit for Purpose Criterion in Practice

In this section, we focus on addressing the first question in the chapter, what is the efficacy of some of the surveillance technologies used to identify and contain COVID-19, as well as those that are being used to prevent, disrupt, and/or provide early warning of pandemics. It is clear that some innovations in surveillance adopted during COVID-19 have relied on familiar technologies and others are newer applications. For example, some efforts involve building on "existing techniques of digital epidemiology – such as using cellphone signals and social media data to map the spread of the virus – whereas other, more innovative initiatives focus on implementing public health measures such as isolation and quarantine" (Mello and Wang 2020, 951). The ethical implications of using various surveillance techniques, technologies, and applications will then be discussed further. We also note that there was significant concern and panic in governments around the world, with many existing pandemic response plans either being ignored or only loosely followed. The COVID-19 pandemic significantly demonstrated that not only were many decision-makers caught unprepared, many decision-makers did not properly follow the plans that they had in place. This is evident in the trialling and roll-out of surveillance technologies and practices as the pandemic unfolded.

Several surveillance technologies and applications commonly used by national security agencies have been used during COVID-19 including CCTV, facial recognition software, data from mobile phones, financial transactions, and social media intelligence (Davis 2021, 156–166).[4] For example, we saw in China widespread use of facial recognition to detect elevated temperatures in a crowd, risk assessment, and monitoring compliance with lockdown measures (Hickok 2020). Similarly, China, Russia, and some more liberal democratic states, such as France, have used CCTV to monitor compliance with mask wearing. This section will focus on the use of mobile phone tracking data and early warning systems as there has been more extensive documentation of their application during COVID-19. These two areas will be examined in terms of how they have been applied in the initial acute phase of COVID-19 (2020–2021). The section will end with a brief discussion of other more advanced surveillance technologies and applications being developed which are likely to have potential use in the post-acute phase of COVID (i.e. 2022 onwards).

Intelligence practices in service of significant public health security challenges demonstrate the importance of the *jus ad intelligentium* fit for purpose criterion. Here, we need to ask if the intelligence operation and/or institution reliably assists in national security decision-making? When considering something like a public health emergency, such as a pandemic, we suggest that the just cause for intelligence criterion is met; public health information is needed to assist in and support decision-making for something that directly and indirectly poses risks for national security. On this, it would seem that the use of public health surveillance would be justified. However, given that people have a right to privacy, and that states ought to be limited in what information they gather on their citizens and the citizens of other countries, we must ensure that the information being gathered and the intelligence being produced are used for, and well suited *for that purpose.* That is, do the widespread public surveillance programmes actually help in *public health* decision-making?

This point is essential to recognise and clarify. First, if a particular technology, surveillance practice, or wider intelligence operation do not actually help in improving decision-making, then they lack the justification to go ahead. Recalling here that individuals and citizens have a presumption of a right to privacy, then any practices that override that right need to be justified. Second, and equally importantly, the justification in this situation is tied specifically to *public health* decision-making. Throughout this book, we have advanced a teleological approach to national security intelligence in which the joint epistemic actions that form intelligence are justified by reference to how they assist in national security decision-making. However, the use of intelligence practices and institutions for things like pandemics needs to be narrowly restricted. That is, we agree that pandemics pose national security risks, and that national security intelligence practices and institutions can and should be used to protect against risks like pandemics. However, the particular practices and institutions involved must be limited to how they contribute to public health decision-making. The national security connection is indirect and/or implicit.

This means that the surveillance programmes, and wider intelligence practices, must actually be useful for *public health decision-making*. So far, throughout the book, we have argued that intelligence be understood as national security intelligence, whereby the practices and institutions of intelligence are not simply explained by, but justified by, national security. Here, however, the surveillance and wider intelligence efforts are conducted in service of a different telos: the information is used to support and improve public health decision-making. On this, if a particular surveillance system does not actually provide information that is useful for the public health efforts, then it loses its justification. Basically, if the public health surveillance system lacks efficacy, it is not fit for purpose and should not be used. Or, at least, its scope of use should be significantly constrained to contexts and situations that are far less invasive of individual privacy. We return to this point of efficacy later.

Second, the surveillance programmes, and wider intelligence practices, are only justified for use for public health security. Given the explicit connections to national security, it is easy to imagine mission creep and to use that information in service of other more traditional national security needs. We suggest here that information gathered for the purposes of aiding public health decision-making requires a new justificatory reason if it was to be used for some non-public health purpose. As van den Hoven has argued, informational injustices occur when information gathered in one context and for one purpose is then used in a different context or different purpose (van den Hoven 2007). For instance, surveillance information gathered for contact tracing cannot *immediately* be used to identify terrorists. This is not to say that information cannot be used at all. Rather, we are saying that use of that information for non-public health purposes requires a stand-alone justification. Moreover, in line with some of the points made in Chapter 9, any such re-justification must be trustworthy. That is, there must be institutional policies in place that ensure that the reuse meets a new justification, and that the public can be assured that such reuse has gone through the necessary oversight and accountability processes.

Mobile Phone Facilitated Surveillance Systems[5]

To explore the issue of whether COVID-19 surveillance practices were efficacious, we look at various mobile phone-facilitated surveillance technologies and apps that were rolled out globally in nearly 30 countries starting in the first few months of the acute phase of the COVID-19 pandemic (Gerke et al. 2020, 1176; Davis 2021; Mello and Wang 2020). Apple and Google also launched their Exposure Notifications System, which enables local public health authorities to identify, with the help of Bluetooth technology, potential exposures to COVID-19 and alert the exposed users to further instructions (Gerke et al. 2020, 1176; Mello and Wang 2020, 952). Apps were used for a range of reasons, but generally to augment epidemiological contact tracing efforts, implement quarantine, and check compliance with public health orders. The extent of data collected, storage, and access arrangements also have varied between mobile phone-facilitated surveillance technologies and apps across countries. Israel adopted a system from Shin Bet used in counterterrorism to tap into cellular data to retrace the movements of people infected by COVID-19 (Davis 2021, 158; Hickok 2020). The Israeli approach made use of infected persons' cellphone location data on an involuntary basis. They then sent texts to persons who come into contact with known COVID-19 cases to inform them that they must immediately quarantine themselves for 14 days (Mello and Wang 2020, 951). In contrast, Singapore's mobile phone application, TraceTogether, was used to support the work of contact tracing, was a less restrictive approach than Israel's by transmitting users' data to officials only if an individual becomes infected, and then only in more restrictive ways (Mello and Wang 2020, 951). Australia's COVIDSafe app was based on similar technology to Singapore's TraceTogether in being primarily a data collection tool, which does not involve artificial intelligence (AI) using complex machine learning (Lodders and Paterson 2020, 154; Miller and Smith 2021).

Like Israel, South Korea, Taiwan, and China adopted contact tracing apps that use geolocation data without seeking an individual's consent. For example, during the initial wave of COVID-19, Taiwan used itineraries of passengers, who disembarked the Diamond Princess cruise ship to send text alerts to people residing in areas the passengers visited, asking them to self-monitor and notify officials of any symptoms. The recipient list was compiled by using mobile phone base station positioning (Mello and Wang 2020, 951). Taiwan's app was also used to ensure citizens comply with quarantine orders. However, perhaps an even more restrictive app used by China during the COVID-19 outbreak required that citizens in more than 200 cities install an Alipay app on their smartphones. As Mello and Wang suggest,

> the App assigns a risk code to each person indicating the extent to which they are permitted to move around the community. The coding algorithm reportedly incorporates information on time spent at risky locations and frequency of contact with other people. Public dissatisfaction with the app arose from lack of transparency about the reasons people were classified into groups and mismatched with individuals' own beliefs about their risk level.
>
> (Mello and Wang, 2020, 951)

Some earlier research using simulations suggested that using contact tracing apps was less effective at suppressing the spread than was previously thought in the early stages of the pandemic (Vayena cited in Sweeney 2020, 303). As Sahar Latheef points out, these concerns were sustained in a number of cases (Latheef 2023).

The effectiveness of a particular mobile phone surveillance system comes down to evaluating several variables. These include obviously whether the technological solution considered by governments are fit for purpose and if there are no other solutions for tracking and reducing infection. In other words, have technical and policy deliberations been extensive, and does the accumulated evidence suggest that there are no other options likely to be as efficient in assisting with either or all three public health functions: contact tracing, social distancing, and quarantine during a pandemic? Can the one app function efficiently to allow all three key public health functions, or if not, what is the most optimal way to ensure public understanding, confidence, and compliance?

Effectiveness is also a product of implementing the least restrictive surveillance system that relies on the most minimal access to data (particularly identifiable data), but one that still provides optimal management of a pandemic. Other considerations to effectiveness include how people are responding to the pandemic, the transmissibility of the pathogen, and what stage of the pandemic is the population currently in. A surveillance system, to provide early warning of a future pandemic, may be different in design to the one deployed to help with contact tracing once a disease is rapidly increasing in a population. For an example of the latter, the design and roll-out of Australia's COVIDSafe app suggest that the technology was not fit for purpose. Despite the modest public download of the app (around 6 million), there were a number of technical flaws (e.g. its ability to operate on certain phones, unreliability of Bluetooth, risks of false positives, anonymity and third-party tracking). Further investigation of the overall technical performance of COVIDSafe is warranted, given as, Lodders and Paterson point out, there also "remains uncertainty about the useful number of cases the app has found with initially only six unique connections found in New South Wales and none in Victoria that were not already known to contact tracers" (Lodders and Paterson 2020, 158–159). In other countries mobile phone surveillance systems seemed to have performed better. For example, in Taiwan,

> the government linked immigration and customs data on travellers (after deleting irrelevant travel history) to National Health Insurance data on hospital and clinic visits to identify individuals whose symptoms could be due to

> contracting the novel coronavirus during travel to an affected area. That information was shared with health care providers so that they could use it to make decisions during patient visits, such as asking for additional history of present illness and ordering a COVID-19 test. Travelers scan a QR code using their smartphone, which leads to an online travel declaration form that asks for travel history and flight information, symptoms of fever or respiratory infection, and contact information in Taiwan. On the basis of their health and travel information, travellers are either sent a pass by text, asked to do home quarantine for 14 days, or instructed to self-isolate at home for 14 days.
>
> (Mello and Wang 2020, 951)

Leaving aside examples of good practice during the early phase of the COVID-19 pandemic, part of the analysis of surveillance systems' effectiveness must also include extensive testing of both algorithms that guide data collection, and the data sets used for bias, so that there is confidence that they can identify public health risk as accurately as possible close to real time during a dynamic pandemic where the behaviour of people and pathogen can be difficult to assess. The capacity of governments and the private sector to process and store the data, and for how long, are also variables that will influence overall effectiveness. Are there appropriate legal, policy, and governance arrangements in place to support the effective and transparent implementation of the mobile phone-facilitated and other health surveillance systems? Robust governance of newly implemented mobile phone and other technical surveillance systems also relies on having streamlined well-understood policies and procedures by all relevant stakeholders in place that ensure efficient, timely, and transparent collection and analysis of data. The acute phase of COVID-19 demonstrated examples where poor governance of newly implemented surveillance systems that reported new infections and hospital carrying capacity could cause vulnerabilities and a lack of transparency in the technical surveillance solution adopted.

For example, Subbian et al. reported on several systemic vulnerabilities in the US national public health reporting system where the initial approach taken from state to federal agencies were ad hoc and non-standardised, perhaps in part as a result of panic and the discarding of existing pandemic preparedness plans. Further,

> the Department of Health and Human Services (HHS) abruptly changed the process used by hospitals to submit daily COVID-19 reports about testing, hospitalizations, and hospital capacity in July 2020. Hospitals were instructed to submit data through a system developed by a commercial contractor – TeleTracking Technologies Inc. Data would then be aggregated and analyzed using a new platform, called HHS Protect, built by another commercial entity – Palantir Technologies Inc., effectively bypassing the CDC.
>
> (Subbian et al. 2021, 185)

Palantir was largely developed from investment by the CIA, and surveillance technologies used during COVID-19 come from their deployment in national security contexts, particularly counterterrorism. In addition to already starting partnerships with CDC in the US and NHS in the UK, according to Bloomberg (Fouquet and Torsoli 2020), Palantir also sought to use its existing information technologies and intelligence tools for new customers, pitched its analytics software (e.g. Foundry) and tools (e.g. Gotham) to government officials in France, Germany, Switzerland, and Austria. Gotham is best-known for helping intelligence and law enforcement agencies globally track terrorists and criminals (Hatmaker 2019; Ongweso Jr. 2020). Hickok suggested that the Palantir suite of tools being proposed to European health agencies were "a blended solution that could help countries get a bird's-eye view of the pandemic" (Hickok 2020, 3). Palantir analytical software was also used briefly to help some Australian state health agencies speed up their contact tracing and other public health management in collaborations between them and the Australian Criminal Intelligence Commission (ACIC) (Walsh 2020).

Finally, throughout the COVID-19 pandemic, we saw incidents where institutional actors sought access to personal data originally gathered for public health purposes for other ends. For instance, police in the Australian state of Western Australia accessed contact tracing data required for attendance at a public event to identify individuals suspected of involvement in organised crime (McGuirk 2022). In Israel, Shin Bet was accused of using COVID-19 surveillance technologies "to send threatening messages to Israel's Arab citizens and residents whom the agency suspected of participating in violent clashes with police. Some of the recipients, however, simply lived or worked in the area, or were mere passers-by" (Pathi and Wu 2022). This mission creep was found to be relatively widespread.

> For more than a year, [Associated Press] journalists interviewed sources and pored over thousands of documents to trace how technologies marketed to "flatten the curve" were put to other uses. Just as the balance between privacy and national security shifted after the Sept. 11 terrorist attacks, COVID-19 has given officials justification to embed tracking tools in society that have lasted long after lockdowns… from Beijing to Jerusalem to Hyderabad, India, and Perth, Australia, The Associated Press has found that authorities used these technologies and data to halt travel for activists and ordinary people, harass marginalized communities and link people's health information to other surveillance and law enforcement tools. In some cases, data was shared with spy agencies.
>
> (Pathi and Wu 2022)

This suggests that the COVID-19 intelligence was regularly used in ways beyond its public health justifications.

To be clear, this is not to say that such intelligence is unjustified – states have a responsibility to protect their citizens against risks and threats, and they require intelligence to understand and respond to those risks and threats. Our point is that the use of public health surveillance information does not directly justify its use in pursuit of other national security ends. In order to protect the trust in our intelligence practices and institutions, any such uses must be constrained and require new justifications that go through a proper justificatory process.

Second to this, this highlights the importance of the fit for purpose criterion. In a number of the cases where public health surveillance information has been used for other ends, the ultimate justification is still national security. And, if we were to simply assess those uses by reference to the just cause for intelligence criterion, then it would seem that they are both justified. However, the particular mechanics of those two justifications differ in their detail. This, we suggest, is captured by the fit for purpose criterion, in a way that is not captured by the just cause for intelligence criterion.

Towards the Future: Post-Acute COVID-19 Surveillance Technologies and Applications

Beyond the acute phase of the COVID-19 pandemic (2022 and onwards), it is clear that the mobile phone-facilitated and other broader disease surveillance systems will continue to proliferate, but also be a part of a larger range of surveillance technologies and tools used globally to better manage this and future pandemics. This not a new trend; AI/machine learning and big data systems have been deployed, with varying degrees of success, over the last three decades in a range of public health settings, including to forecast disease spread (Barbosa et al. 2014; Brownstein, Freifeld, and Madoff 2009; Walsh 2020; Wark 2021). The new development will be the speed with which new innovations in AI/machine learning will be applied to the surveillance of future pandemics. Bragazzi et al. (2020) and Nguyen et al. (2020) provide comprehensive overviews on the big data and AI innovations currently underway that may improve the accuracy, estimation, treatment, and management of infectious diseases beyond what has been achieved so far with the development of many mobile phone-facilitated surveillance systems. AI/machine learning innovations, particularly those focused on deep learning, could improve understanding disease dynamics (e.g. estimating R0, transmission rate, spatio-temporal disease dynamics), health response (ICU beds, staffing), non-pharmaceutical interventions (social distancing, quarantine, contact tracing and border closure, public health communication and misinformation), and pharmaceutical measures (vaccination and antiviral strategies) (Syrowatka et al. 2021, 96; Nguyen et al. 2020, 3). Bragazzi et al. classify these big data and AI innovations based on their likely sources and including the following:

1 Molecular big data (obtained by means of wet-lab techniques and OMICS-based approaches, such as genomics, and post-genomics specialties, including proteomics and interactomics).
2 Imaging-based big data (like radiomics or the massive data-mining approach to extract clinically meaningful, high-dimensional information from images).
3 Sensor-based big data (wearable sensors).
4 Digital and computational big data (with an incredible wealth of data produced by the internet, smart phones, and other mobile devices) (2020, 2).

Although various studies have been published demonstrating the significant potential of AI/machine learning and Internet of Things (IoT) technologies for future health surveillance, studies detailing the actual application of them against COVID-19 beyond medical imagery and biological sequencing seem limited (ibid.). It is clear that further research is needed on how to validate various potential AI/machine learning applications such that they may be utilised for the preparedness and response activities.

As discussed in Chapter 10, new technologies and behaviours are blurring the distinction between "traditional intelligence" and the future of intelligence. We see this blur occurring between health security and intelligence as the same computing AI can be utilised for the preparedness and response activities, as well as against the unprecedented national and global crisis.

> For example, AI using natural language processing can be used to create systems that help understand the public responses to intervention strategies, e.g. lockdown and physical distancing, to detect issues by measuring mental health and social anxiety, and to aid governments in making better public policy. [Natural Language Processing] technologies can also be employed to develop chatbot systems able to remotely communicate and provide consultations to people and patients about the coronavirus. AI can be used to eradicate fake news on social media platforms to ensure clear, responsible and reliable information about the pandemic, such as scientific evidence relevant to the virus, governmental social distancing policies or other pandemic prevention and control measures.
>
> (Nguyen et al. 2020, 9)

Additionally, a range of new technologies in the form of the IoT is showing some potential surveillance applications for predicting, preventing, and monitoring emerging infectious diseases. The IoT is an "interconnected web of smart devices, sensors, and individuals through which data can be collected in its raw form and transmitted through the internet to be analyzed for patterns or trends" (Rahman et al. 2020, 137). For example, IoT-enabled health-monitoring systems can provide real-time surveillance through the use of wearable health-monitoring devices, cloud-based remote health testing, and AI. These monitoring systems can use a range of data sources in real time and allow remote monitoring systems between patient and doctor (ibid.).

It is likely that future applications will also be confronted with the usual technical, legal, and policy difficulties, described earlier, in the acute phase of COVID-19. These include algorithmic bias and error, which will need peer reviewing for their technical robustness, but also sense checked from a policy and legal perspective to ensure algorithmic classifications support public health outcomes and not result in the unnecessary stringent restrictions of individual freedoms (ibid.).

For example, equity issues and under-representation of some populations from data from healthcare providers or laboratories will likely persist with those who have restricted access to the internet or mobile phones (Mello and Wang 2020, 952). Similarly poor data integrity, insufficient, or historical data may limit AI applications' ability to validate health-related data in ways that allow reliable contact tracing, social distancing, and quarantine measures. Poor data or faulty algorithmic development can also create errors, which can create unnecessary financial, social, and psychological burdens on individuals, who are subjected to stay at home, or business closures on individuals. Recourse to unfair and incorrect public health orders may be difficult in many cases given, because the use of algorithmic logic will often not be transparent to citizens (ibid., 952; Zhao et al. 2021, 1).

The COVID-19 pandemic also drew attention to the importance of the deployment of digital detection surveillance systems to support early warning and monitoring of infectious diseases. So far some intelligence studies scholars have come out and suggested that COVID-19 represents both a public health and intelligence failure (Wark 2021; Gradon and Moy 2021). Others, however, have argued that warning systems used by some intelligence agencies and public health agencies were able to provide diffuse warning of an impending pandemic, if not specific warning of the kind of virus (Gressang and Wirtz 2022). It is clear that a number of data-driven early warning systems have already demonstrated shortcomings (Bloodworth, Breton, and Gully 2021). Web-based tools for surveillance of the flu virus (influenza) have been utilised for several years with varying degrees of success. For example, Google Flu Trends (GFT) was tracking health-related search engine queries in order to monitor, in real-time, influenza activity. However, GFT was discontinued due to concerns regarding data inaccuracy. The flaw in GFT highlights a commonplace issue in big data analysis (and any data analysis), overfitting of data to a small number of cases. The failure of GFT emphasises the utilisation of other real-time health data for predicting trends in infectious diseases (Rahman et al. 2020, 137). Smart disease surveillance systems based on IoT would provide simultaneous reporting and monitoring, end-to-end connectivity and affordability, data assortment and analysis, tracking and alerts, as well as options for remote medical assistance to be adopted, to detect and control zoonotic infectious disease outbreaks in China and other affected countries. More research must be carried out for the development of automated and effective alert systems to provide early and timely detection of outbreaks of such diseases in order to reduce morbidity, mortality, and prevent global spread. These prompt and effective public health measures need to be taken to avoid the risk of continuing outbreaks and the possibility of a local outbreak turning into a global pandemic, such as this one (Rahman et al. 2020, 137). Further research is needed on the technical, policy, and governance principles on what will improve early warning systems in the future.

The Future and Ethics of Intelligence

What does this mean for the ethics of intelligence? Two immediate lessons must be learned from the increased interactions between intelligence and public health. First, the practice and institutions of intelligence are significantly different from the practice and institutions of the military, *and* from public health/healthcare. Second, that a value like trust must be included in any ethical assessment of modern intelligence practice – to be discussed in the next section.

On the issue of practices and institutions, we want to be explicit that there are a range of ethical issues related to public health surveillance.[6] In line with our notion of intelligence as a joint epistemic activity, public health surveillance is also an intelligence activity.[7] At the same time, the sort of information, and the way that it can be used, means that public health surveillance also fits in the realms of bioethics and public health ethics. As such, there are three approaches to the ethics of intelligence and public health surveillance. First is to apply the just war model to public health surveillance. This approach would see if the intelligence operation has just cause, legitimate authority, and so on. Moreover, the particular surveillance operation would need to be discriminate, necessary, and proportionate. However, as we have argued throughout this book, this approach is too coarse – while the just cause criterion is a necessary element in justifying intelligence actions, it has to be contextualised to the specific intelligence action for it to make sense. Likewise, questions about who is a legitimate authority need to be reframed to the context of intelligence, and in this case, to the context of public health situations. Such conceptual adjustments need to be made for the other *jus ad intelligentiam* criteria. Finally, the discrimination, necessity, and proportionality calculations need to be adapted such that they actually make sense for epistemic actions in a context of public health rather than acts of physical violence, or indeed traditional national security threats. Who is a legitimate target for public health intelligence and what features need to be counted for a proportionality calculation differ significantly in a situation like a global pandemic than in a situation of national threats, such as posed by a terror group. We do not offer suggestions here as to just how to engage in discrimination, necessity, or proportionality considerations; these points are worthy of full-book treatments themselves and we do not have the space to go into them here. The collection on *Surveillance in Times of Emergency* (Macnish and Henschke 2023) covers a number of these discussions in detail; Nick Evans engages in an extended discussion of health security and related principles (Evans 2023). Our point is more general – the use of intelligence actors and institutions for public health surveillance reinforces our argument that simply applying the just war model to intelligence is not going to be sufficient moving forward. As intelligence practices and institutions evolve, a just intelligence model needs to evolve as well. Our formulation for the JIT principles is the beginning of this evolution, and we would hope that they can be, and are, updated and evolve as intelligence practices and institutions evolve.

A second approach is to look to bioethics and public health, how they consider surveillance, and use those discussions to ground the ethics of public health surveillance. Again, however, this approach is complicated and falls short when considering *intelligence* and public health surveillance. First, there are significant differences between clinical bioethics and public health ethics (Latheef 2023). What we mean here is that bioethics, at least narrowly construed, is focused on the individual and their relationships with primary care providers. In short, this model draws from clinical bioethics to explore surveillance by reference to principles such as patient autonomy, non-maleficence, beneficence, and justice. However, public health ethics takes a less individualistic approach and sees things more at a population level. As such, considerations of pandemic surveillance must take into account the risk that infectious diseases pose to populations. As Sahar Latheef argues:

> While medicine focuses on providing treatment and care for individuals as patients, public health focuses on preventing disease and disability for the greater population. Medicine involves a relationship between a physician and an individual as a patient. Public health involves relationships between members in the community, various professionals and the government.
>
> (Latheef 2023)

Given this focus on communities of people, and the role of government in needing to consider population-level health, not simply individual health,

> Discussions in public health ethics that argue in favour of public health as a public good, are frequently founded on Mill's Harm Principle. Public health or preventing harm to others, takes precedence over individual liberty and in extension, informed consent and individual's right to autonomy.
>
> (Latheef 2023)

What we suggest here is that the ethical considerations typical to clinical bioethics roughly parallel the approach taken in *jus in bello*.[8] In order to determine what is the morally correct thing for a medical professional to do in a clinical setting, one must look to the specific conditions facing the patient, the particular skills and responsibilities of the medical professionals caring for the patient, and the relationships between patient and professionals. In this way, clinical bioethics is somewhat similar to *jus ad intelligentia*, where the focus is on what a particular intelligence officer ought to do in a particular intelligence context. Instead of discrimination, necessity, and proportionality, however, the ethical analysis is likely going to involve principles of autonomy, non-maleficence, beneficence, and justice (Beauchamp and Childress 2001). In contrast, public health ethics is typically concerned with a higher layer of analysis, looking at the decisions and ethical principles that arise at the population level (Latheef 2023). In this way, public health ethics has more in common with the *jus ad bellum*/*jus ad intelligentium* considerations, where the considerations concern the aggregation of individual concerns, and the decision-makers may need to take a path that results in rights restrictions or harms to individuals if it will benefit the population as a whole. While contestable, on a public health ethics approach, such population-level surveillance is justifiable (Latheef 2023). Again, our point is not to settle this bioethics/public health ethics issue, but to show that there are different approaches to dealing with pandemic surveillance.

The third approach to intelligence and health surveillance is to, instead, draw from the JIT principles, which have a different telos to clinical and public health, so operate differently. The reason for this comes from the institutional setting of such surveillance – intelligence actors and institutions have different methods and different purposes to those actors and institutions engaged in clinical care and public health. In clinical care, the primary ethical justification for patient surveillance would be the health of that patient. For public health, the primary ethical justification for population-level surveillance would be the need to provide and protect public health. In contrast, when using national security intelligence actors and institutions, the primary justification is the servicing of national security. As we discussed earlier in this chapter, while clinical care, public health, and national security converge and overlap in a pandemic situation, they each have different ends, and so the actions are justified differently.

To demonstrate this difference, consider the ways that the different institutional tele understand and may justify different responses to COVID-19 lockdown protests. All around the world, as governments enacted large-scale lockdowns, and then vaccine mandates, large numbers of people organised and participated in protests, with a number of protests becoming violent. These protests posed two significant surveillance challenges – first is the health surveillance issue, as these public gatherings not only contravened lockdown policies, but actually raised concerns about them being super-spreader events. So, here we see an overlap between national security concerns, where the agents and the institutions of national security needed to cooperate with public health officials to monitor and assess whether these protests posed not just a security threat but increased the spread of the pandemic.

The second surveillance issue is whether national security intelligence actors should have access to health surveillance data. These protests posed risks to public health, as well as potential national security risks. As we argued earlier in this chapter, information collected for public health reasons cannot simply be accessed and used for national security reasons, even if intelligence agencies are involved in both aspects of surveillance. In the case of the national security risks posed by COVID-19 protests, given free speech, free assembly, and free movement are fundamental and defining features of liberal democracies, it is not enough to say that simply because there is a protest going on that public health surveillance can be used for national security concerns. There has to be a significant and real risk to national security; the gatherings and protests must either turn violent, or there must be significant intelligence gathered through other means to give credibility to concerns that the protests will turn violent. We want to point out here that there are typically significant constraints on what sorts of surveillance can be conducted on such gatherings and protests, and these constraints need to be maintained. Moreover, there must be clearly defined and well-communicated legal separations between data collected for health surveillance and national security surveillance. That is, there must be practices, oversight, and accountability measures in place to *ensure* that informational injustices do not occur, and to *assure* the public that informational injustices have not and will not occur (Robbins and Henschke 2017). The overall point is that there needs to be a justifying cause for national security intelligence access to, and use of, data gathered in service of health security.

A further issue that demonstrates the overlap and blur between health security surveillance and national security intelligence is the rise of active disinformation campaigns and related conspiracy theories during the pandemic. This draws in the discussion from Chapter 7 about the ethics of PSYOP and propaganda. In mid-2021, it was publicly reported that foreign powers were actively seeking to spread disinformation about US, UK, and European vaccines. "The Russian and Chinese disinformation has tried to magnify the potential side effects of the Pfizer and Moderna vaccines, suggesting that the mRNA technology they are based on is untested or risky, [US] State Department officials said this week" (Barnes 2021). Parallel with these active disinformation campaigns, the COVID-19 pandemic saw an explosion in conspiracy theories, relating to the pandemic itself, to treatments and vaccination programmes, and to the malevolent motivations of political and public health actors. These conspiracies were driven in a major way by what the World Health Organization dubbed an "infodemic":

> An infodemic is too much information including false or misleading information in digital and physical environments during a disease outbreak. It causes confusion and risk-taking behaviours that can harm health. It also leads to mistrust in health authorities and undermines the public health response. An infodemic can intensify or lengthen outbreaks when people are unsure about what they need to do to protect their health and the health of people around them. With growing digitization – an expansion of social media and internet use – information can spread more rapidly. This can help to more quickly fill information voids but can also amplify harmful messages.
>
> ("Infodemic" n.d.)

This becomes an issue for intelligence actors and institutions in two overlapping ways. First, if a foreign power is actively engaging in information operations, then it is the state's intelligence agencies who have a responsibility to understand these disinformation campaigns and to respond in ways that – as per the discussion of PSYOP in Chapter 7 – blunt the force of such attacks.

Complicating the need for good trustworthy intelligence, and the rise of active disinformation campaigns and general social unrest, is the need for critical reflection on how states and intelligence institutions respond to emergencies. First, it is undeniable that lockdowns and other COVID-19 control measures have had an adverse impact on people. Second, in hindsight, it is contested whether harsh lockdown measures and social distancing practices were the best way of responding to such a pandemic. Sweden, for instance, followed its pandemic plans by having only limited lockdowns. "In later stages of the pandemic, their excess mortality was worse than those of their Scandinavian neighbors but still significantly lower than the rest of Europe's" (Kluth 2023). At the same time, by one assessment at least, New Zealand fared the best overall in its responses (Fickling 2023). Recognising the complexity here, the third point is the need to recognise that such public emergencies rely heavily on information being communicated between health, security, or other relevant experts, and the public in ways that rely on mutual trust. Given that intelligence as defined throughout this book is concerned with epistemic competition, critical reflections on, responses to, and criticisms of extreme public health measures are potential tools for malicious actors. This is not to say that people should not critically reflect on and assess such policies. Rather, we need to recognise that such criticisms must be seen as offering potential vulnerabilities and targets for malicious actors.

There are two lessons here for the future of intelligence. First is that any use and application of intelligence practices and institutions must take significant care to recognise what the justifying cause for intelligence, the JCI. From the JCI, we derive a recognition of who the legitimate authority for intelligence (LAI) is. This is tied squarely to the institutions engaged in the particular intelligence operation. The COVID-19 discussion draws out the recognition that intelligence institutions and other social institutions are likely to be cooperating more and more into the future. Moreover, given the sensitivity and power of information in the modern world, as discussed in Chapter 8, any intelligence gathered and produced must have the right intention for intelligence (RII). If the ends are national security, then the RII, discussed in Chapter 3, would hold that the intelligence institution undertakes these intelligence activities only for the ultimate purpose of enabling the protection against or the competitive advantage over the threat to its national security posed by an adversarial country. Emergencies, such as public health crises, natural disasters, and so on, would have a different motivation, and so the RII would need to be adapted also. The relevant intelligence institution undertakes these intelligence activities only for the ultimate purpose of enabling the protection against or the competitive advantage over the threat to its national security posed by the public health emergency, natural disaster, and so on. The JCI, LAI, and RII are essential to ethically legitimate intelligence actions, and in particular circumstances like a global pandemic, these terms may, in fact, be different from national security intelligence.

Likewise, intelligence needs to be constrained by logical resort (LRI). The sort of intelligence gathered for a public health emergency, and the means used to gather that intelligence, will need to be responsive to the knowledge and risk of the given public health emergency. The same would hold if/when intelligence is needed for other emergencies that are not directly national security in nature. As we have discussed already, the intelligence practices and institutions need to be fit for purpose. As before, if the purpose of this intelligence changes, then the questions about whether it is fit for purpose also need to change. We ask here, “does the intelligence operation and/or institution reliably assist in public health decision making?”. Finally, the proportionality principle for intelligence is going to be understood against the particular risks being faced, the options of doing nothing, and the risks to privacy, etc.

The second lesson is that the JIT principles, we have introduced and discussed throughout, are necessary principles to *ensure that intelligence practices and institutions are ethically justified*. As we have discussed and demonstrated, the JIT principles, introduced in Chapter 3, must be adapted further to meet non-national security contexts and applications. As the need for intelligence to inform and support decision-making increases in our modern world, there will be increasing demands and expectations for intelligence institutions to be supplement non-national security decision-making. What we suggest here is that the JIT principles can and should be used, and adapted where needed, to ensure that such practices and the larger institutions conducting the practices are acting ethically.

Trust and the Risk of Transparency

The COVID-19 pandemic also drew attention to the risks posed by misinformation and disinformation. In addition to considering if and when national security intelligence should support something like a public health emergency, we must confront the ethically complicated terrain of how a state's intelligence agencies ought to engage in counter-intelligence operations on their own citizens. On the one hand, one of the most effective ways of countering active disinformation campaigns, and reducing the rise and spread of conspiracy theories, is to make citizens resilient to such attacks. On the other hand, such resilience programmes are ethically fraught. This is for a range of reasons. First, liberal democracies pride themselves not just on freedoms around speech, assembly, and so on, but the freedom of belief and conscience. Citizens can believe whatever it is that they want, no matter how well informed, stupid, or irrational. Second, the use of intelligence agencies to investigate, and not just protect but guide the beliefs of citizens, is essentially a feature of an authoritarian state whose commitment to ideology supersedes their citizen's right to free belief. Our solution is to look to and expand the discussion from Chapter 9 on trust, and to introduce a final JIT principle, the risk of transparency (ROT), where any intelligence institution, or institutional actor using intelligence, should act in such a way that should those actions be made public, they will not undermine the justificatory purpose of the action.

The basic argument here is that intelligence actors and agencies need to be trusted by the citizens, and indeed political actors, that they are working for, and in whose name they derive their moral legitimacy. As we have argued throughout this book, intelligence practices and institutions pose special moral challenges due to the fact that they are not only permitted but at times required to engage in behaviours and to make decisions that would normally be morally impermissible. Yet, given the importance of their role in protecting the rights of people, and aiding the security of their nations, intelligence actors and agencies are granted exceptional privileges, not normally granted to other actors or agencies. This moral exceptionalism parallels that of military practices and institutions, but given that intelligence is an epistemic action, the just intelligence model differs significantly from the just war model. A further key distinguishing feature of intelligence actors and agencies is their relationship to the people that they are charged to protect, and in whose name they gain moral legitimacy.

This brings us to back trust – those people must be able to trust their intelligence actors and agencies. As was covered in Chapter 9, trust is an essential feature of intelligence institutions. Given the special nature of intelligence activities, in particular the fact that intelligence is an ongoing set of epistemic joint actions conducted in a context of competition, many aspects of intelligence need to be kept secret. As discussed in Chapters 1 and 2, in many accounts of intelligence, secrecy is considered to be a necessary and defining feature of intelligence.

However, intelligence, even national security intelligence, does not necessarily involve secrecy. There are many national security activities that are not secret. Even when considering those intelligence activities that do rely on secrecy, as we saw in Chapter 10, new information and communication technologies not only increase the capacity for intelligence actors to gather and analyse information on targets, but they also increase the risk that intelligence activities, means, methods, and decisions will be made public. What we suggest is that intelligence actors in liberal democracies need to consider what would happen if their activities were made public. The basic value that intelligence actors need to consider here is trust – will their publics trust in the intelligence institutions if those publics know what the intelligence actors and agencies are doing?

Bringing this back to pandemic security, and the collaborations between public health actors and intelligence actors, we can compare two different uses of health surveillance data and public health practice to show how trust and the risk of transparency are related to ethical intelligence practice. The first example is concerned with how US intelligence actors sought to use a polio vaccination programme in Pakistan to gather information that might help identify Bin Laden. The basic story is this: A medical doctor, Shakil Afridi, became involved with the CIA, due to his activity with vaccination programmes in Pakistan. "Vaccination campaigns were considered a good front for spying: DNA information could be collected from the needles used on children and analyzed for leads on the whereabouts of al Qaeda operative for whom the CIA already had information" (Mazzetti 2014, 282). The CIA instructed Afridi to focus his efforts in Bilal Town, a suburb of Abbottabad, which he subsequently realised was part of an effort to identify if Osama Bin Laden and some family members were hiding in a compound in Bilal Town. The CIA hoped that Afridi would be able to gather some DNA samples to help identify if Bin Laden was actually in the compound or not. Though it is unclear if Afridi's efforts actually did obtain any Bin Laden DNA (BBC 2011), the US determined that Bin Laden was in the compound, and on 11 May 2011, the US successfully gained access to the compound and killed Bin Laden. Afridi was eventually jailed by Pakistan under suspicion of his involvement with the CIA (Mazzetti 2014, 296).

The problem with this is twofold. First, that people in Pakistan and around world became aware of the fact that US intelligence agencies had sought to use a vaccination programme to gather national security intelligence. As a secret intelligence operation, it failed. Second, and flowing directly from this intelligence failure, it has led to a decline in people in particular regions taking up vaccines. As one criticism in 2014 stated

> The harms already produced are palpable. Of the 115 polio cases reported this year (as of July 9 [2014]), 90 were in Pakistan… In addition, cases in Afghanistan, Iraq, and war-torn Syria are genetically linked to Waziristan, demonstrating the deep connections among terrorism, political instability, and public health. Nigeria, as well, is a polio-endemic area of global concern; in

> February 2014, the Islamist militant group Boko Haram shot dead at least 9 women administering polio vaccinations in northern Nigeria.
>
> (Gostin 2014)

Ultimately, because people became aware of the fact that health security actors and operations were being used by or in collaboration with national security intelligence, people were then less inclined to trust public health actors.

> The CIA's ploy created political cover for militants seeking to exploit preexisting fears. Disinformation campaigns, for example, have linked polio vaccination campaigns to Western plots to sterilize Muslims. Rumors also have circulated asserting that the vaccines contained porcine contaminants, which violate the Muslim faith. Indeed, the interconnection of immunization, ideology, and religion has created a toxic mix, for which poor children are most likely to suffer.
>
> (Gostin 2014)

Insofar as we need public health actors to be worthy of trust, one response to this problem is that public health actors should not work with intelligence actors. Moreover, this would apply more generally – wherever there are political or social institutions that rely on public trust, then there should be normative structures to prevent these political and social institutions from working with intelligence actors. Much like the independence myth discussed in Chapter 9, the institutions of intelligence should be effectively sealed off from most, if not all, other political and social institutions.

However, as was discussed, this sort of independence is neither feasible nor desirable. Further to this, as we have noted in this chapter, intelligence actors and institutions have significant skills and expertise which are vital in situations like public health emergencies, national disasters, and so on. So, it would actually be foolish to suggest that intelligence actors and agencies do not interact with public health actors, much less with other social or political institutions. That said, the polio vaccine example does highlight a very significant concern with intelligence, and as we have argued throughout this chapter, the COVID-19 pandemic has shown that the future of intelligence will be a need for greater cooperation between intelligence institutions and other political and social institutions. So, what ought we do? How ought intelligence institutions operate in this new informational environment?

The solution to this is trust. Much like the chapter on independence and trust, what we need are intelligence institutions that are trustworthy. When considering the future of intelligence, we can look to lessons learned from the COVID-19 pandemic. We have already shown that the need for health surveillance during the COVID-19 pandemic meant that intelligence actors and institutions became important aspects of health security.

While there were many people who suspected malign intentions of government actors generally, in most countries, the majority of people trusted the capacities and motivations of a range of government actors and agencies to engage in pandemic, vaccine, and general health surveillance (Organisation for Economic Co-operation and Development 2022). Even when national security actors like the military, national guard, and police were involved in epistemic and enforcement actions, many people had trust in these actors and institutions. We suggest here that part of the reason for this trust is that such activities were conducted openly, it was not a secret that these national security actors and agencies were involved. In fact, in a number of countries, there was frustration that groups like the military were not involved sooner and more comprehensively.

That said, there were and still are significant portions of communities around the world who not only did not trust the public health measures but also explicitly saw these actions as efforts by malign political and/or national security actors to seize control of the government (McCarthy et al. 2022). Fear about malign intent regarding COVID-19 responses was driven, in no small part, by fears that public health actors were in fact intelligence actors operating in secret.

Much can be said about the conspiracism here, but we want to point out two sets of features that were necessary for intelligence actors to collaborate with public health actors: institutional mechanisms that *ensure* constraints on intelligence actors, and *assure* the public that such constraints are in place and being followed. Because of the particular power that intelligence institutions wield, there need to be significant and well-crafted laws and policies that ensure that any intelligence gathered in pursuit of public health ends is effectively restricted to public health purposes. While there may be particular cases where such public health intelligence might potentially be justifiably used by intelligence actors, this new use needs explicit and particular justification. There is a risk that too much overlap between public health and intelligence actors can blur the different institutional ends; particular institutional mechanisms are required to ensure that the gathering and use of intelligence for national security ends are justified by those ends.

A second set of features is *assurance* mechanisms, those mechanisms that let the public know that information is being used by whom, when, and why. While these mechanisms are complicated when considering standard national security intelligence areas, we suggest here that the assurance mechanisms in the area of public health security are a little simpler. One of the reasons for widespread public support for public health surveillance, and so on, was that many political and public health actors took considerable pains to engage with the public in what was happening and why. The Australian state of Victoria, for instance, had the some of the world's longest and toughest pandemic lockdowns – with the state capital Melbourne receiving a stringency rating of around 95 out of 100, with the most extreme ranking being 100 (Hope 2021). Despite this, the political and public health leaders of Victoria received widespread and sustained public support throughout a series of lockdowns and ongoing surveillance practices, with the state Premier being returned with a significant majority. This public support was maintained and developed in no small part due to daily press conferences involving the state leader, the public health advisors, and relevant national security actors. Importantly for our point here, these press conferences were very open and explicit about what public health measures were being enacted, when, and why. Moreover, as the risks of the pandemic receded, first through successful eradication in late 2020, and then due to widespread vaccination uptake through 2021–2022, the state scaled back and withdrew many of the public health measures. The overall point here is that trust was maintained through openness and effective public engagement by political, public health, and national security leaders. The public were assured by effective engagement. Compare this to the Pakistan/polio example, where trust in the public health actors was degraded and suffered long-term consequences due to the secrecy of the actions.

This all leads us to trust and the ROT principle –

> Risk of Transparency (ROT): Act in such a way that, should those actions be made public, they will not undermine the justificatory purpose of the action.

We wish to close with as a final principle to add to our JIT principles. The ROT should be considered as a guide for all intelligence practices and be considered by all intelligence institutions. The connection between the ROT and the other JIT principles of *jus ad intelligentium* and *jus in intelligentia* is that these principles need to act as justifications in consideration of a given intelligence action, operation, or institutional practice being made public. That is, first, with any decision to use intelligence, that decision has to meet the *jus ad intelligentium* criteria. Much like the way that the six *jus ad bellum* criteria determine if a military is permitted to go to war, our six *in intelligentium* criteria need to be met in order for an intelligence operation at the macro level to go ahead. Then, looking at specific intelligence practices and actions, they must be discriminatory, necessary, proportionate, and may need to consider reciprocity. In this way, the JIT criteria are prospective, they are future orientated.

However, as per the ROT, they are also retrospective – when a given intelligence action has occurred, and/or there is incoming intelligence that guides the next step in a set of decisions – in liberal democracies, those decisions are ultimately accountable to the citizens of those countries in some way. As effective accountability mechanisms go, they would need to have access to the justifications used for the given intelligence practices. That is, accountability would require that the intelligence institutions can show that the JIT criteria were considered, how they were considered, and if the particular practices actually met, what was required by the criteria. The key question for the ROT is whether a particular intelligence decision would be justified if it was made public.

Note here that we are not saying that any and all intelligence, and the decisions around intelligence should be completely open and publicly accessible. Rather, our first point is that there needs to be policies and practices that ensure adherence to particular principles and laws. Second, that there needs to be some way in which the oversight mechanisms can communicate to the public that these decisions do adhere to the particular principles and laws, that is, there must be assurance mechanisms.

Finally, we note that there is a temporal blur here – as noted in Chapters 1 and 2, unlike warfare, intelligence is an ongoing and dynamic set of practices, with no clear beginning or end. Thus, in order for intelligence institutions to meet their ethical obligations, accountability must be ongoing and responsive to the ongoing national security risks and threats as they arise and evolve. The dynamic nature of intelligence is already recognised by the somewhat circular nature of the intelligence cycle (Burke 2022). What we are saying is that intelligence accountability, particularly as it relates to the JIT principles that we have outlined in this book, is an ongoing process.

Conclusions

To sum up, throughout this chapter, we have shown that intelligence needs to be considered as an evolving set of practices increasingly adopted by institutions whose ends are not necessarily going to be national security. Taking into account the ways that intelligence practices and institutions were used and, at times, abused during the COVID-19 pandemic, we can discuss the strengths of the JIT approach developed throughout the book. In particular, we have demonstrated the practical value of framing the JIT by reference to institutions.

As the world changes, and the demands on political leaders change, the role of intelligence in aiding decision-making is also changing. COVID-19 presented the world's decision-makers with a set of challenges requiring more information, relying on the methods of intelligence practitioners, and drawing from intelligence institution's deep expertise. However, the COVID-19 example, in which intelligence was used for public health decision-making, rather than national security decision-making, shows the dangers of blurring these different institutional identities and purposes. Intelligence gathered in problematic ways, and used for ends not tied to the justifying cause, may either fail to be fit for purpose and can significantly undermine trust in public health institutions.

What we have showed in this chapter is how the JIT model, the *jus ad intelligentia* principles in particular, can be used to ensure that intelligence is conducted ethically. Moreover, we have argued that use of intelligence practices and institutions for non-national security ends also requires assurance mechanisms. Evidence that the JIT principles are guiding and constraining intelligence practices is central to effective assurance.

We also suggest here that one of the significant strengths of our JIT principles is that they can be updated and adapted to new intelligence challenges and problems. The just war criteria have developed, evolved, and changed through history. They are the subject of ongoing debate, and are continually the focus of critical attention. We would hope that our principles are well formed and robust enough to undergo similar critical attention and revision. We consider our principles and the book's wider discussions on the ethics of intelligence institutions to be part of an ongoing discussion about the ethics of intelligence. Ideally, the principles suggested here would be foundation for ongoing evolution in intelligence. By putting the institutions of intelligence as central to ethics of intelligence, we consider that this fills an important gap in those discussions.

The future intelligence is as uncertain and unpredictable as the future itself. However, one thing is certain: as the world changes, intelligence will need to change with it. Decision-makers will need good intelligence, and intelligence must be both practically and ethically good. While we cannot predict the future, by setting out concepts and ethical principles of intelligence, we hope to provide a set of tools that can guide good intelligence practice into the future.

Notes

[1] For more on health security, see Rushton and Youde (2014).

[2] For more on ethical issues with the securitisation of health, see Selgelid and Enemark (2012).

[3] For more on surveillance, particularly as it relates to joint epistemic activity, see Henschke (2017, 56–86).

[4] Space limitations do not allow either a comprehensive categorisation of all surveillance applications or an analysis of their effectiveness here. For more on these, see Macnish and Henschke (2023).

[5] Throughout this chapter, we use the term "mobile phone" to refer to the cluster of technologies, sometimes called smart phones, cell phones, or similar.

[6] See also *Ethics and Surveillance in Times of Emergency* (Macnish and Henschke 2023).

[7] This also draws from the argument that surveillance is a form of epistemic labour. See Chapter 3 of *Ethics in an Age of Surveillance* for a detailed argument on this (Henschke 2017).

[8] We note here recent efforts like that of Nick Evans which seek to adapt principles from the JWT to health, in the theory of just health security (Evans 2023).

References

Albert, Craig, Amado Baez, and Joshua Rutland. 2021. "Human security as biosecurity: Reconceptualizing national security threats in the time of COVID-19". *Politics and the Life Sciences* 40(1): 83–105.

Barboza, P., Vaillant, L., Le Strat, Y., Hartley, D.M., Nelson, N.P., Mawudeku, A., Madoff, L.C., Linge, J.P., Collier, N., Brownstein, J.S. and Astagneau, P. 2014. Factors influencing performance of internet-based biosurveillance systems used in epidemic intelligence for early detection of infectious diseases outbreaks. *PloS one*, 9(3), p.e90536.

Barnes, Julian E. 2021. "Russian Disinformation Targets Vaccines and the Biden Administration". *The New York Times*, 5 August. www.nytimes.com/2021/08/05/us/politics/covid-vaccines-russian-disinformation.html

Battin, Margaret P., Leslie P. Francis, Jay A. Jacobson, and Charles B. Smith. 2008. *The Patient as Victim and Vector: Ethics and Infectious Disease*. Oxford: Oxford University Press.

BBC. 2011. "Bin Laden Death: 'CIA Doctor' Accused of Treason". *BBC News*, 6 October. www.bbc.com/news/world-south-asia-15206639

Beauchamp, Tom L. and James F. Childress. 2001. *Principles of Biomedical Ethics*. Oxford: Oxford University Press.

Bloodworth, Margaret, Mylaine Breton and Paul Gully. 2021. The Global Public Health Intelligence Network (GPHIN) Independent Review Panel: Final Report. July 12. Ottawa, ON: PHAC. www.canada.ca/content/dam/phac-aspc/ documents/corporate/mandate/about-agency/external advisory-bodies/list/independent-review-global-publichealth-intelligence-network/final-report/final-report-en.pdf

Bragazzi, Nicola Luigi, Haijiang Dai, Giovanni Damiani, Masoud Behzadifar, Mariano Martini, and Jianhong Wu. 2020. "How big data and artificial intelligence can help better manage the COVID-19 pandemic". *International Journal of Environmental Research and Public Health* 17(9): 3176.

Brownstein, John S., Clark C. Freifeld, and Lawrence C. Madoff. 2009. "Digital disease detection – harnessing the Web for public health surveillance". *New England Journal of Medicine* 360(21): 2153.

Burke, Paul. 2022. "Intelligence and National Security: The National Security Problematique". In *The Palgrave Handbook of National Security*, edited by Michael Clarke, Adam Henschke, Matthew Sussex, and Tim Legrand, 351–70. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-53494-3_15

Davis, Jessica. 2021. "Surveillance, intelligence and ethics in a COVID-19 world". In *National Security Intelligence and Ethics*, 156–166. Routledge.

Evans, Nicholas G. 2023. *War on All Fronts: A Theory of Health Security Justice*. Massachusetts: MIT Press.

Fickling, David. 2023. "New Zealand: Decisiveness Saved the Most Lives". *Bloomberg*, 15 March. www.bloomberg.com/graphics/2023-opinion-lessons-learned-from-covid-pandemic-global-comparison/

Fouquet, H., and A. Torsoli. 2020. "Palantir in Talks with Germany, France for Virus-Fighting Tool". *Bloomberg*.

Gerke, Sara, Carmel Shachar, Peter R. Chai, and I. Glenn Cohen. 2020. "Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19". *Nature Medicine* 26(8): 1176–1182.

Gostin, Lawrence O. 2014. "Global Polio Eradication: Espionage, Disinformation, and the Politics of Vaccination". *The Milbank Quarterly* 92(3): 413–17. https://doi.org/10.1111/1468-0009.12065

Gradon, Kacper and Wesley R. Moy. 2021. "COVID-19 Response – Lessons from Secret Intelligence Failures". *The International Journal of Intelligence, Security, and Public Affairs* 23(3): 161–79. https://doi.org/10.1080/23800992.2021.1956776

Gressang, Daniel S., and James J. Wirtz. 2022. "Rethinking Warning: Intelligence, Novel Events, and the COVID-19 Pandemic". *International Journal of Intelligence and Counter Intelligence* 35(1): 131–146.

Hatmaker, T. 2019, August. Secretive Tech Company Palantir Doubles Down on Its ICE Contracts. www.thedailybeast.com/palantir-secretive-tech-company-doubles-downon-its-ice-contract

Henschke, Adam. 2017. *Ethics in an Age of Surveillance: Virtual Identities and Personal Information*. New York: Cambridge University Press.

Hickok, Merve. 2020. "Ethical Al and Big Data in Times of Pandemic". *Journal of Leadership, Accountability and Ethics* 17(4): 104–113.

Hope, Zach. 2021. "Toughest Lockdown? Melbourne's Dark 2020 in Global Context". *The Age*, 8 May. www.theage.com.au/national/victoria/toughest-lockdown-melbourne-s-dark-2020-in-global-context-20210508-p57q3j.html

Hoven, Jeroen van den. 2007. "Privacy and the Varieties of Informational Wrongdoing". In *Computer Ethics*, edited by John Weckert, 317–30. Aldershot: Ashgate Publishing.

'Infodemic'. n.d. Accessed 16 March 2022. www.who.int/westernpacific/health-topics/infodemic

Kluth, Andreas. 2023. "The Worst Covid Strategy Was Not Picking One". *Bloomberg*, 15 March. www.bloomberg.com/graphics/2023-opinion-lessons-learned-from-covid-pandemic-global-comparison/

Latheef, Sahar. 2023. “Digital Contact Tracing Applications (DCTAs); Is It the End of Informed Consent and Autonomy?’ In *Ethics of Surveillance in Times of Emergency*, edited by Kevin Macnish and Adam Henschke. Oxford: Oxford University Press.

Lodders, Adam, and Jeannie Marie Paterson. 2020. “Scrutinising COVIDSafe: Frameworks for evaluating digital contact tracing technologies”. *Alternative Law Journal* 45(3): 153–161.

Lyon, David. 2009. “Surveillance, Power, and Everyday Life’. In *The Oxford Handbook of Information and Communication Technologies*, edited by Chrisanthi Avgerou, Robin Mansell, Danny Quah, and Roger Silverstone. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199548798.003.0019

Macnish, Kevin and Adam Henschke. 2023. *Ethics of Surveillance in Times of Emergency*. Oxford: Oxford University Press.

Mazzetti, Mark. 2014. *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth*. Penguin Group USA.

McCarthy, Molly, Kristina Murphy, Elise Sargeant, and Harley Williamson. 2022. “Examining the Relationship between Conspiracy Theories and COVID-19 Vaccine Hesitancy: A Mediating Role for Perceived Health Threats, Trust, and Anomie?” *Analyses of Social Issues and Public Policy* 22(1): 106–29. https://doi.org/10.1111/asap.12291

McGuirk, Rod. 2022. “Police in Australia Co-Opted COVID-19 Apps to Fight Crime”. *The Independent*, 20 December. www.independent.co.uk/news/police-ap-western-australia-canberra-mark-mcgowan-b2248401.html

Mello, Michelle M., and C. Jason Wang. 2020 “Ethics and governance for digital disease surveillance”. *Science* 368(6494): 951–954.

Miller, Seumas, and Marcus Smith. 2021. “Ethics, public health and technology responses to COVID-19”. *Bioethics* 35(4): 366–371.

Nguyen, Thanh Thi, Quoc Viet Hung Nguyen, Dung Tien Nguyen, Samuel Yang, Peter W. Eklund, Thien Huynh-The, Thanh Tam Nguyen, Quoc-Viet Pham, Imran Razzak, and Edbert B. Hsu. 2020. “Artificial intelligence in the battle against coronavirus (COVID-19): a survey and future research directions”. arXiv preprint arXiv:2008.07343.

Ongweso Jr., Edward. 2020. “Palantir’s CEO Finally Admits to Helping ICE Deport Undocumented Immigrants”. *Vice*, January 24.

Organisation for Economic Co-operation and Development. 2022. “Governments Seen as Reliable Post-Pandemic but Giving Citizens Greater Voice Is Critical to Strengthening Trust, Says OECD–OECD”. 13 July. www.oecd.org/newsroom/governments-seen-as-reliable-post-pandemic-but-giving-citizens-greater-voice-is-critical-to-strengthening-trust.htm

Pathi, Krutika and Huizhong Wu. 2022. “Police Seize on COVID-19 Tech to Expand Global Surveillance”. *AP News*, 20 December. https://apnews.com/article/technology-police-government-surveillance-covid-19-3f3f348d176bc7152a8cb2dbab2e4cc4

Rahman, Md Siddikur, Noah C. Peeri, Nistha Shrestha, Rafdzah Zaki, Ubydul Haque, and Siti Hafizah Ab Hamid. 2020. “Defending against the Novel Coronavirus (COVID-19) outbreak: How can the Internet of Things (IoT) help to save the world?” *Health Policy and Technology* 9(2): 136.

Robbins, Scott and Adam Henschke. 2017. “Designing for Democracy: Bulk Data and Authoritarianism”. *Surveillance and Society* 15(3): 582–89.

Rushton, Simon and Jeremy Youde. 2014. *Routledge Handbook of Global Health Security*. Routledge.

Selgelid, Michael J and Christian Enemark, eds. 2012. *Ethics and Security Aspects of Infectious Disease Control: Interdisciplinary Perspectives*. Abingdon: Routledge.

Selgelid, Michael J and Christian Enemark. 2008. "Infectious Diseases, Security and Ethics: The Case of HIV/AIDS". *Bioethics* 22(9): 457–65.

Selgelid, Michael J. 2006. "Commentary: Physicians and the Risk of Malevolent Use of Research". *Cambridge Quarterly of Healthcare Ethics* 15(4): 441–47. https://doi.org/10.1017/S0963180106230561

Selgelid, Michael J. 2013. "Biodefense and Dual-Use Research: The Optimisation Problem and the Value of Security". *Journal of Medical Ethics* 39(4): 205–6.

Subbian, Vignesh, Anthony Solomonides, Melissa Clarkson, Vasiliki Nataly Rahimzadeh, Carolyn Petersen, Richard Schreiber, Paul R DeMuro, et al. 2021. "Ethics and Informatics in the Age of COVID-19: Challenges and Recommendations for Public Health Organization and Public Policy". *Journal of the American Medical Informatics Association* 28(1): 184–89. https://doi.org/10.1093/jamia/ocaa188

Sweeney, Yann. 2020. "Tracking the debate on COVID-19 surveillance tools". *Nature Machine Intelligence* 2(6): 301–304.

Syrowatka, Ania, Masha Kuznetsova, Ava Alsubai, Adam L. Beckman, Paul A. Bain, Kelly Jean Thomas Craig, Jianying Hu, Gretchen Purcell Jackson, Kyu Rhee, and David W. Bates. 2021. "Leveraging artificial intelligence for pandemic preparedness and response: a scoping review to identify key use cases". *NPJ Digital Medicine* 4(1): 96.

Walsh, Patrick F. 2018. *Intelligence, biosecurity and bioterrorism*. Springer.

Walsh, Patrick F. 2020. "Improving 'Five Eyes' health security intelligence capabilities: leadership and governance challenges". *Intelligence and National Security* 35(4): 586–602.

Wark, Wesley. 2021. "Building a better global health security early-warning system post-COVID: The view from Canada". *International Journal* 76(1): 55–67.

World Health Organization. n.d. "WHO Coronavirus (COVID-19) Dashboard". Accessed 1 May 2023. https://covid19.who.int

Zhao, Ivy Y., Ye Xuan Ma, Man Wai Cecilia Yu, Jia Liu, Wei Nan Dong, Qin Pang, Xiao Qin Lu, Alex Molassiotis, Eleanor Holroyd, and Chi Wai William Wong. 2021. "Ethics, integrity, and retributions of digital detection surveillance systems for infectious diseases: systematic literature review". *Journal of Medical Internet Research* 23(10): e32328.

Index

Note: Endnotes are indicated by the page number followed by "n" and the note number e.g., 140n20 refers to note 20 on page 140.