Introduction

Seumas Miller, Mitt Regan and Patrick F. Walsh

The national security intelligence environment is undergoing profound changes. Powerful new technologies enable the collection, communication and analysis of national security data on an unprecedented scale and now have a central role in intelligence practice. The Snowden leaks and other events have prompted considerable debate over how best to reconcile privacy with effective security intelligence collection in the face of such technologies, as well as how to ensure effective accountability of intelligence agencies. In addition, the threat of transnational terrorism has challenged traditional institutional arrangements based on the distinction between domestic and foreign intelligence. The increasing use of algorithms in intelligence operations also raises a wide range of issues regarding the human-machine relationship in these operations, the ability to exploit such technology to disrupt elections and other political processes, and the stability of traditional analyst culture in the intelligence community. Furthermore, that community itself is under increasing scrutiny with respect to its independence vis-à-vis political decision makers. These are but a few of the urgent challenges facing intelligence operations by liberal democracies that call for rigorous and innovative analysis rooted in appreciation of the core values of the liberal democratic tradition. That analysis, however, must also be rooted in an understanding of the dynamics of intelligence operations.

Historically, the intelligence studies literature has been slow to identify the ethical dimensions of intelligence practice for organizations and its practitioners and to date there have been no works that provide a relatively comprehensive set of analyses of the ethical issues in national security intelligence collection, analysis and dissemination. Moreover, the growing complexity of the security environment (e.g. CBRN – chemical, biological, radiological and nuclear – threats posed by non-state actors, use of intelligence and surveillance tools to combat pandemics such as COVID-19, the blurring of domestic and international security, globalization and rapid growth of cyber technology) make especially urgent the need for ethical analyses to be informed by relevant empirical work. Scholars from intelligence studies background, or knowledgeable practitioners with a depth of understanding of the actual practices and problems confronted by the intelligence community are the best source of such work. In this edited collection, we have sought to provide a relatively comprehensive set of analyses of the ethical issues

in national security intelligence collection, analysis and dissemination, and in doing so we have brought together both scholars and practitioners.

Most of the chapters originated as contributions to two research workshops held at the University of Oxford and Georgetown University, respectively, in 2019 under the auspices of a European Research Council Advanced grant on counter-terrorism ethics and an Australian Research Council Discovery Grant on national security intelligence ethics.

The collection is divided into six parts. The first part, “The just intelligence model”, is theoretical in character and comprises three chapters. Ross Bellaby argues that the currently most influential normative theory of intelligence activities, the so-called Just Intelligence Model derived from Just War Theory, offers a number of underlying ethical contributions that can help us better understand when intelligence should be licensed and when it should be limited. In Chapter 2, Seumas Miller offers analyses of the key principles of discrimination, necessity and proportionality – each of which is a constitutive principle of the Just Intelligence Model. He shows in general terms how they apply, or ought to apply, to national security intelligence activity. He also argues that there is an additional normative principle governing espionage, in particular, that is not constitutive of the Just Intelligence Model, namely, a principle of reciprocity. In the final chapter in this part, David Omand and Mark Phythian shift the focus onto new technology and consider ethical issues such as intelligence agency and law enforcement access to bulk data sets, and the use of AI and algorithms to search and mine them. They argue that these issues in “techno-ethics” can be informed by principles derived from Just War Theory and seek to address the question as to how far these principles can be used as the basis of a model that can guide thinking about the technoeithics of contemporary intelligence practice.

The second part, “Espionage”, comprises four chapters. In Chapter 4, David Perry examines a broad range of ethical issues, challenges and dilemmas in human intelligence (HUMINT), and assesses how best to interpret them in connection with several important *prima facie* ethical principles. Recognizing that the motivations of espionage agents can be complex and varied, Perry frames his analysis in terms of agents’ freedom of action, distinguishing between those who act voluntarily, those who are deceived by false-flag tactics and those who are compelled by threats of blackmail and the like. In the following chapter, Michael Skerker focuses on the rights of foreign intelligence targets. He articulates a conservative cosmopolitan model for just intelligence collection directing all states with a certain character to adhere to the same norms when and if they engage in intelligence collection on foreign targets.

Students of the history of espionage and readers of spy novels alike will be well aware of the phenomenon of so-called sleeper-cells. In Chapter 6 in this part Kevin Macnish introduces and discusses what he refers to as digital sleeper cells. These consist in code which can be placed on an adversary’s network and left dormant for a period of time, before being activated if, and when, needed. Such new opportunities bring with them new risks, including ethical risks. In the final chapter in this part, David Letts reviews a number of scenarios where

coalition states provide intelligence to other coalition partners while knowing that there is some possibility that an operational partner state may use that intelligence to undertake an activity that does not correspond with the legal obligations that apply to the “providing” state. Reviewing some of the challenges involved in sharing intelligence among coalition partners can help to identify where the legal and ethical risk lies for coalition states so that conscious decisions regarding intelligence sharing can be included in the planning of such operations.

The third part, “Bulk data collection and analysis”, comprises two chapters. In Chapter 8, Tom Sorell addresses the question as to whether or not bulk data collection is morally legitimate *on balance* because of its operational utility for the security services, and the overriding importance of the purposes that these services pursue, notwithstanding the violations of privacy involved. In Chapter 9, Jessica Davis focuses on the ethical implications of current data collection and analysis practices being used to combat COVID-19, such as collecting data on citizens from cell phones, financial transactions, and social media intelligence, and combining it with health data. She argues that parallels can be drawn between the global pandemic and the post-9/11 era, which saw significant broadening of state surveillance and intelligence powers around the world – powers that were never rolled back, and have instead become part of the fabric of the state intelligence and security apparatus.

The fourth part, “Covert operations”, comprises two chapters. In Chapter 10, Loch Johnson explores the legal foundations of covert action, along with the degree to which these methods are subjected to accountability; its successes and failures around the world; and, central throughout the analysis, the ethical issues posed by its use. He suggests that there have been positives, for example its use in its paramilitary forms as a supplement to overt US warfare, and negatives, for example the excessive use of drone assassinations by the United States. In Chapter 11, Nicholas Melgaard and David Whetham focus on information warfare. They explore the ethical landscape of information warfare in the twenty-first century and examine the principles that should govern the way liberal democracies understand both the behaviour of other actors and also their own activities in this area.

The fifth part, “Accountability”, comprises three chapters. As past and recent history demonstrates, it is of great importance that national security intelligence agencies are subjected to accountability by way of robust institutional mechanisms. This is especially crucial in light of the fact that, in contrast with many other political activities, there can be significant limits to public transparency about operations of the intelligence community. Chapter 12 by Genevieve Lester and Frank Leith Jones describes the historical dynamics that led to the adoption of the US system of accountability in relation to intelligence activities. They argue that the development of intelligence oversight in the United States has been driven by the executive-legislative relationship. Chapter 13 by Mary B. DeRosa focuses on the effectiveness of congressional oversight of US intelligence activities. The United States has adopted the most detailed system of external oversight of the intelligence community, which has served as an impetus for increasing demands for greater oversight in other countries. Finally, the chapter by Mitt

Regan and Michele Poole examines oversight of covert action, an area in which it is especially challenging to ensure accountability. It provides a useful comparative perspective by analysing the strengths and weaknesses of the US and the UK approaches to oversight of this activity.

The sixth part, “Future directions”, comprises three chapters. In Chapter 15, Robert Cardillo focuses on the new and emerging GEOINT technologies and suggests that its holistic collection practices will facilitate a detailed model of the planet and much that is happening on it. He suggests that there are many benefits of such a model, including natural disaster preparedness and response, enhanced measurements of the environment and real-time detection of nefarious actors. However, Cardillo also argues that such a world will demand a radical rethinking of privacy, requiring us to find the optimum balance between the benefits of this technology, their implications for our privacy and the potential for misuse. Exploring that balance is the overriding purpose of his chapter. Chapter 16, Patrick F. Walsh assesses CBRN threats posed by non-state actors. It explores how these threats have diverged from classical WMD scenarios (that shaped the Cold War) to ones where threat trajectories are less certain due to an increasing number of complex political, social and technological factors. The focus is on how non-state actor CBRN threats may evolve in the future rather than state-based ones. In the final chapter, Gregory F. Treverton assesses challenges for the future of intelligence, many of which have long been with us but are newly reconfigured: balancing tactical and strategic intelligence; building and adjusting stories in a shapeless world; dealing with transparency and big data; finding new ways to add value; intelligence as an argument for policy; breaking the tired intelligence cycle and dealing with new competitors who are also potential colleagues. Treverton says that would have been his list of challenges had Donald Trump not been elected president. However, Treverton suggests that the Trump administration scrambled the deck, injecting enormous uncertainty. It raised the last and most worrisome challenge: how to deal with a world in which truth is personal or subjective, and, indeed, the very idea of truth is under attack.