

National Security Intelligence and Ethics

Miller, S.R.M.; Regan, Mitt; Walsh, Patrick F.

DOI

[10.4324/9781003164197](https://doi.org/10.4324/9781003164197)

Publication date

2021

Document Version

Final published version

Citation (APA)

Miller, S. R. M., Regan, M., & Walsh, P. F. (Eds.) (2021). *National Security Intelligence and Ethics*. Routledge - Taylor & Francis Group. <https://doi.org/10.4324/9781003164197>

Important note

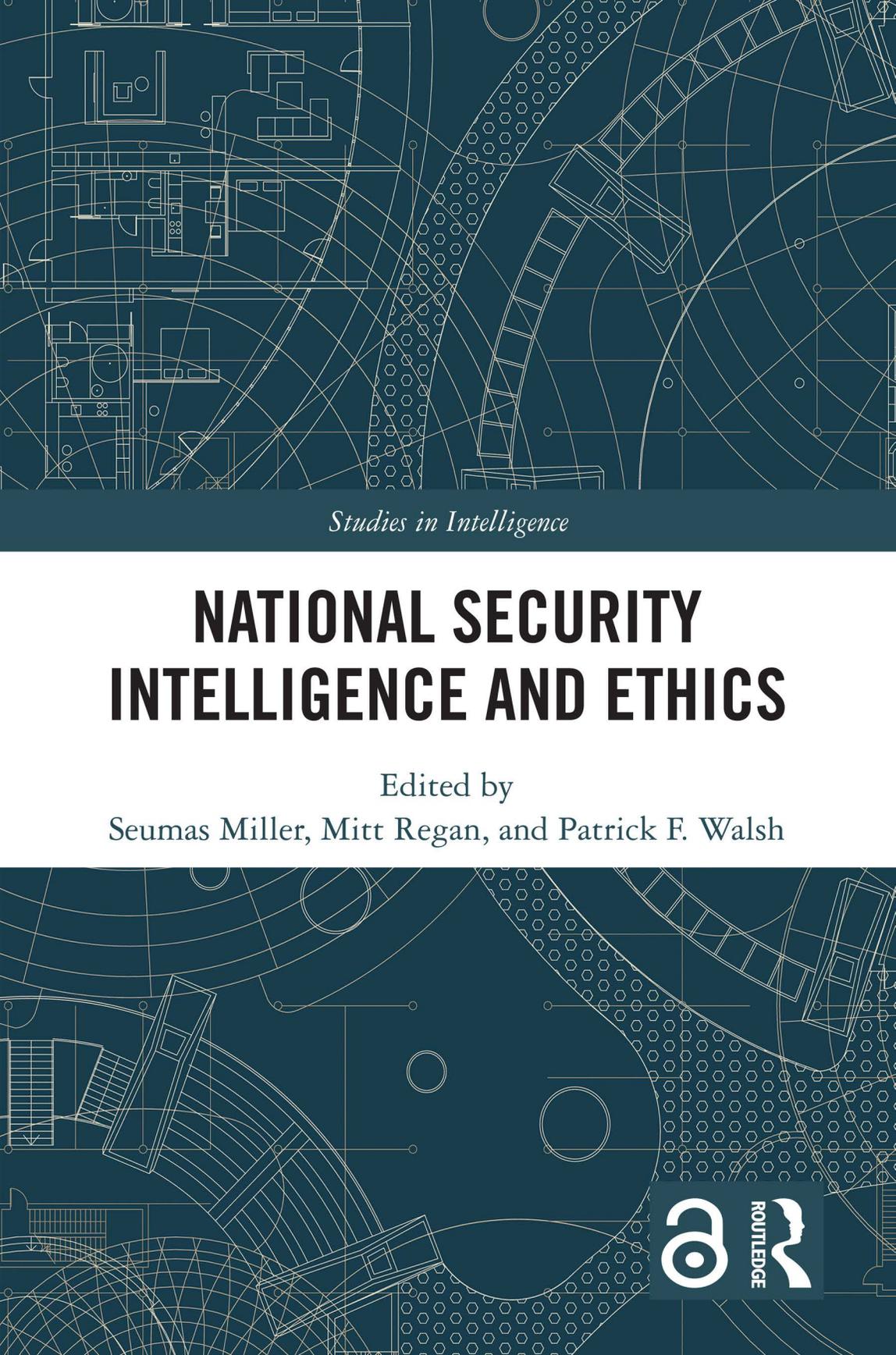
To cite this publication, please use the final published version (if applicable). Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.

The background of the cover is a complex architectural line drawing in white on a dark blue background. It features various geometric shapes, including circles, rectangles, and lines, suggesting a floor plan or a technical drawing of a building. The drawing is dense and intricate, with many overlapping lines and shapes.

Studies in Intelligence

NATIONAL SECURITY INTELLIGENCE AND ETHICS

Edited by
Seumas Miller, Mitt Regan, and Patrick F. Walsh



National Security Intelligence and Ethics

This volume examines the ethical issues that arise as a result of national security intelligence collection and analysis.

Powerful new technologies enable the collection, communication and analysis of national security data on an unprecedented scale. Data collection now plays a central role in intelligence practice, yet this development raises a host of ethical and national security problems, such as privacy; autonomy; threats to national security and democracy by foreign states; and accountability for liberal democracies. This volume provides a comprehensive set of in-depth ethical analyses of these problems by combining contributions from both ethics scholars and intelligence practitioners. It provides the reader with a practical understanding of relevant operations, the issues that they raise and analysis of how responses to these issues can be informed by a commitment to liberal democratic values. This combination of perspectives is crucial in providing an informed appreciation of ethical challenges that is also grounded in the realities of the practice of intelligence.

This book will be of great interest to all students of intelligence studies, ethics, security studies, foreign policy and international relations.

Seumas Miller holds research positions at Charles Sturt University, Australia, TU Delft, the Netherlands and the University of Oxford, United Kingdom.

Mitt Regan is McDevitt Professor of Jurisprudence and Co-Director of the Center on National Security and the Law at Georgetown University Law Center, USA. He also serves as a senior fellow at the Stockdale Center for Ethical Leadership at the U.S. Naval Academy.

Patrick F. Walsh is a former intelligence analyst and Associate Professor of intelligence and security studies at Charles Sturt University, Australia.

Studies in Intelligence

General Editors: Richard J. Aldrich and Christopher Andrew

The CIA and the Congress for Cultural Freedom in the Early Cold War

The limits of making common cause

Sarah Miller Harris

Understanding Intelligence Failure

Warning, response and deterrence

James J. Wirtz

Intelligence Elites and Public Accountability

Relationships of Influence with Civil Society

Vian Bakir

Intelligence Oversight in the Twenty-First Century

Accountability in a changing world

Edited by Ian Leigh and Njord Wegge

Intelligence Leadership and Governance

Building Effective Intelligence Communities in the 21st Century

Patrick F. Walsh

Intelligence Analysis in the Digital Age

Edited by Stig Stenslie, Lars Haugom, and Brigit 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

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

National Security Intelligence and Ethics

**Edited by Seumas Miller, Mitt Regan,
and Patrick F. Walsh**

First published 2022
by Routledge
2 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

© 2022 selection and editorial matter, Seumas Miller, Mitt Regan, and Patrick F. Walsh; individual chapters, the contributors

The right of Seumas Miller, Mitt Regan, and Patrick F. Walsh to be identified as the authors of the editorial material, and of the authors for their individual chapters, has been asserted in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

The Open Access version of this book, available at www.taylorfrancis.com, has been made available under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 license

Trademark notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data

Names: Miller, Seumas, editor. | Regan, Milton C., Jr., 1952– editor. | Walsh, Patrick F., 1964– editor.

Title: National security intelligence and ethics / edited by Seumas Miller, Mitt Regan, and Patrick F. Walsh.

Description: Abingdon, Oxon ; New York, NY : Routledge, [2022] | Series: Studies in intelligence | Includes bibliographical references and index.

Identifiers: LCCN 2021030190 (print) | LCCN 2021030191 (ebook) | ISBN 9780367758318 (hardback) | ISBN 9780367758325 (paperback) | ISBN 9781003164197 (ebook)

Subjects: LCSH: Intelligence service—Moral and ethical aspects. | National security—Moral and ethical aspects.

Classification: LCC JK468.I6 N374 2022 (print) | LCC JK468.I6 (ebook) | DDC 172/.4—dc23

LC record available at <https://lcn.loc.gov/2021030190>

LC ebook record available at <https://lcn.loc.gov/2021030191>

ISBN: 978-0-367-75831-8 (hbk)

ISBN: 978-0-367-75832-5 (pbk)

ISBN: 978-1-003-16419-7 (ebk)

DOI: 10.4324/9781003164197

Typeset in Times New Roman
by Apex CoVantage, LLC

Contents

<i>Acknowledgements</i>	viii
<i>List of contributors</i>	ix
Introduction	1
SEUMAS MILLER, MITT REGAN AND PATRICK F. WALSH	
PART I	
The just intelligence model	5
1 Intelligence and the just war tradition: the need for a flexible ethical framework	7
ROSS BELLABY	
2 Truth-seeking and the principles of discrimination, necessity, proportionality and reciprocity in national security intelligence activity	21
SEUMAS MILLER	
3 The technoethics of contemporary intelligence practice: a framework for analysis	39
DAVID OMAND AND MARK PHYTHIAN	
PART II	
Espionage	61
4 Ethics in the recruiting and handling of espionage agents	63
DAVID PERRY	
5 The rights of foreign intelligence targets	89
MICHAEL SKERKER	

6 Digital sleeper cells and the ethics of risk management	107
KEVIN MACNISH	
7 Intelligence sharing among coalition forces: some legal and ethical challenges and potential solutions	123
DAVID LETTS	
PART III	
Bulk data collection and analysis	139
8 Privacy, bulk collection and “operational utility”	141
TOM SORELL	
9 Surveillance, intelligence and ethics in a COVID-19 world	156
JESSICA DAVIS	
PART IV	
Covert operations	167
10 Ethics and covert action: the “Third Option” in American foreign policy	169
LOCH JOHNSON	
11 Jus ad vim: war, peace and the ethical status of the in-between	186
NICHOLAS MELGAARD AND DAVID WHETHAM	
PART V	
Accountability	199
12 Reaching the inflection point: the Hughes-Ryan Amendment and intelligence oversight	201
GENEVIEVE LESTER AND FRANK LEITH JONES	
13 Congressional oversight of US intelligence activities	216
MARY B. DeROSA	
14 Accountability for covert action in the United States and the United Kingdom	232
MITT REGAN AND MICHELE POOLE	

PART VI

Future directions 249

15 GEOINT and the post-secret world: who guards the guards? 251

ROBERT CARDILLO

**16 Evolving chemical, biological, radiological and nuclear
(CBRN) terrorism: intelligence community response
and ethical challenges** 261

PATRICK F. WALSH

17 Reflections on the future of intelligence 280

GREGORY F. TREVERTON

Index 291

Acknowledgements

The research was conducted under the auspices of: (i) the European Research Council's Advanced Grant programme as part of the grant entitled, "Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies" (GTCMR. No. 670172) (Principal Investigator: Professor Seumas Miller) and (ii) the Australian Research Council's Discovery Grant programme as part of the grant entitled, "Intelligence and National Security: Ethics, Efficacy and Accountability" (DP180103439) (Chief Investigators: Professor Seumas Miller, Associate Professor Patrick F. Walsh, Professor Roger Bradbury and Dr Adam Henschke).

We wish to thank the editor of the following academic publication of Seumas Miller for use of some of the material contained therein: "Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: Principles of Discrimination, Necessity, Proportionality and Reciprocity", *Social Epistemology*, vol. 35, 2021.

Contributors

Ross Bellaby, Ph.D., is a senior lecturer at the University of Sheffield's Politics Department. His main research examines the application of ethics to violence and war, with specific attention to developing an ethical framework for intelligence activity. This involves developing ethical frameworks for intelligence, terrorism, counterterrorism and cybersecurity. His ethical framework is set out in his book, *The Ethics of Intelligence: A New Framework*. Recent works also examine the dark-web and hacker groups as ethical vigilantes and the moral obligation that intelligence professionals have to blow the whistle when they witness wrongdoing.

Robert Cardillo is the president of The Cardillo Group (TCG). TCG delivers strategic and operational expertise to create an enhanced awareness of our planet to enable improved decision-making. TCG's portfolio includes academic, non-profit and national security-related clients. Before TCG, Robert held leadership positions with the Chairman of the Joint Chiefs of Staff, Defense Intelligence Agency and Office of the Director of National Intelligence. Until 2019, Robert was the sixth director of the National Geospatial-Intelligence Agency. He transformed the agency's future value proposition through innovative partnerships with the growing commercial geospatial marketplace.

Jessica Davis is the President of Insight Threat Intelligence, and is President of the Canadian Association for Security and Intelligence Studies. Jessica had an 18-year career in the Canadian government, with senior analytic roles at Canada's financial intelligence unit, FINTRAC and the Canadian Security Intelligence Service. Jessica is the author of *Women in Modern Terrorism: From Liberations Wars to Global Terrorism and the Islamic State* (2017) and *Illicit Money: Terrorist Financing in the 21st Century* (forthcoming with Lynne Rienner in 2021).

Mary B. DeRosa is a professor from Practice at Georgetown Law, where she focuses on national security law and practice. Previously, she served as Deputy Counsel to the President and NSC Legal Adviser in the Obama Administration and as NSC Legal Adviser in the Clinton Administration. She also served as Chief Counsel for National Security on the Senate Judiciary Committee, Special Counsel at the Department of Defense and was a member of the President's Intelligence Advisory Board.

Loch Johnson is Regents Professor of International Affairs Emeritus, University of Georgia, and author of *Spy Watching* (Oxford, 2018). He served as assistant to the chairman, Senate Intelligence Committee Intelligence; staff director of the Oversight Subcommittee on Oversight, House Intelligence Committee and assistant to the chairman, Presidential Commission on Intelligence.

Frank Leith Jones is Professor of security studies at the U.S. Army War College, Carlisle, Pennsylvania, USA. He is the author of *Sam Nunn: Statesman of the Nuclear Age*; *Blowtorch: Robert Komer, Vietnam and American Cold War Strategy and Buying Time, 1965–1966*, U.S. Army Campaigns of the Vietnam War, published by the U.S. Army Center of Military History. He received his Ph.D. from the School of Government and International Relations, Griffith University, Queensland, Australia.

Genevieve Lester is the DeSerio Chair of Strategic and Theater Intelligence at the US Army War College. Prior to her position at the US Army War College, Dr Lester was faculty at the National Defense University and Georgetown University, a fellow at IISS and a Fulbright Scholar. She holds a Ph.D. and M.A. from the University of California, Berkeley, an M.A. from the Johns Hopkins University, School of Advanced International Studies, and a B.A. in history from Carleton College.

David Letts is the Director of the Centre for Military and Security Law at the Australian National University College of Law. Prior to embarking on an academic career, David served in the Royal Australian Navy for more than 30 years. He has served in coalition forces in East Timor (2002) and Iraq (2004), has been a visiting fellow at the Lauterpacht Centre for International Law at Cambridge University and is a member of the teaching faculty at the International Institute of Humanitarian Law (IIHL), San Remo, Italy.

Kevin Macnish is Consulting Manager in Digital Ethics at Sopra Steria. A former assistant professor in Philosophy at the University of Twente and visiting research fellow at the University of Leeds, he has published widely on the ethics of privacy, surveillance and cybersecurity. Kevin has been interviewed by BBC national television and radio and has spoken at both the House of Commons and the House of Lords in relation to his research.

Nicholas Melgaard is currently preparing to submit his PhD doctoral thesis on Immanuel Kant's moral philosophy and the use of technology in modern armed conflict. In particular, this includes issues around 'victory', jus post bellum, artificial intelligence, and teleology in political competition. His position will draw on Kant's practical philosophy to establish a new revisionist, deontological just war theory, grounded in a long-term teleological reading of jus post bellum. A part-time doctoral candidate through the King's College London Defence Studies programme, Nick works full time for a language technology company, supporting private sector and government clients in the implementation of AI. Prior to this, Nick served for seven years as an infantry officer in the British Army, deploying on a range of operations and specialising

later in information operations and intelligence. He holds undergraduate and masters degrees in Philosophy and the History of Philosophy respectively from the University of Cambridge, and a masters in international relations and Middle Eastern studies from the School of Oriental and African Studies (SOAS).

Seumas Miller holds research appointments at the Australian Graduate School of Policing and Security & Cooperative Research Centre in Cybersecurity at Charles Sturt University (Canberra), 4TU Centre for Ethics and Technology at Delft University of Technology (The Hague) and the Uehiro Centre for Practical Ethics at the University of Oxford. He is the author or coauthor of 20 books including *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force* (Oxford University Press, 2016) and *Institutional Corruption: A Study in Applied Philosophy* (Cambridge University Press, 2017). He is the principal investigator on a European Research Council Advanced Grant on the ethics of counter-terrorism.

Sir David Omand GCB is a visiting professor in the War Studies Department, King's College London and at PSIA, Sciences Po, Paris. He was previously UK Security and Intelligence Coordinator, Permanent Secretary of the Home Office and Director, GCHQ. He is the author of *Securing the State* (Hurst, 2020) and, with Professor Mark Phythian, *Principled Spying: The Ethics of Secret Intelligence* (Oxford University Press, 2018).

David Perry is Director of the Practical Ethics Institute on Bainbridge Island, Washington. He is the author of *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation*, and several related articles. He earned a Ph.D. in Ethics and Society at the University of Chicago Divinity School, and taught for 24 years at the U.S. Army War College and four undergraduate schools.

Mark Phythian is Professor of Politics in the School of History, Politics and International Relations at the University of Leicester. He has published widely on intelligence and security issues. Recent books include *Principled Spying: The Ethics of Secret Intelligence*, with David Omand (Oxford University Press/Georgetown University Press, 2018), and *Intelligence in an Insecure World*, with Peter Gill (3rd ed. Polity Press, 2018). He is the co-editor of the journal *Intelligence and National Security* and a Fellow of the Academy of Social Sciences.

Michele Poole served in the U.S. Navy as a surface warfare officer, strategist, and Afghanistan hand. She is a graduate of the U.S. Naval Academy, Naval Postgraduate School, Naval War College, and Georgetown University Law Center, and most recently completed an LL.M. in National Security Law at Georgetown. She is the co-author of the RAND Monographs *After the War: Nation-Building from FDR to George W. Bush* and *Small Ships in Theater Security Cooperation*.

Mitt Regan is McDevitt Professor of Jurisprudence, Director of the Center on Ethics and the Legal Profession, and Co-Director of the Center on National Security and the Law at Georgetown University Law Center. He is also a Senior Fellow at the Stockdale Center for Ethical Leadership at the U.S. Naval Academy.

Michael Skerker is an associate professor in the Leadership, Ethics, and Law department at the U.S. Naval Academy. His academic interests include professional ethics, just war theory, moral pluralism, theological ethics and militant jihadism. Publications include articles and chapters on ethics and asymmetrical war, collective responsibility, police ethics, intelligence ethics and the book *An Ethics of Interrogation* (University of Chicago Press, 2010). His most recent book *The Moral Status of Combatants: A New Theory* (under contract with Routledge) defends the post-Westphalian idea of the moral equality of combatants.

Tom Sorell is Professor of Politics and Philosophy at Warwick University. He works on, among other topics, ethics and security technology, permissible state action in emergencies, counter-terrorism and cybersecurity. He directs Warwick's Interdisciplinary Ethics Research Group, which undertakes a wide range of funded projects and ethics advisory work. He is the author of eight monographs and editor or co-editor of a dozen collections of articles.

Gregory F. Treverton stepped down as Chair of the National Intelligence Council in January 2017. He is Chair, Global TechnoPolitics Forum and senior adviser to the Transnational Threats Project at the Center for Strategic and International Studies (CSIS) and a professor of the practice of International Relations and Spatial Sciences at the University of Southern California. Earlier, he directed the RAND Corporation's Center for Global Risk and Security and before that its Intelligence Policy Center and its International Security and Defense Policy Center. He has served in government for the first Senate Select Committee on Intelligence, the National Security Council and Vice Chair of the National Intelligence Council.

Patrick F. Walsh, Ph.D., is a former intelligence analyst who has worked in Australian national security and law enforcement agencies. He is an associate professor, intelligence and security studies at the Australian Graduate School of Policing and Security, Charles Sturt University, Australia. He consults to the government and his research focuses on a range of intelligence capability issues including governance, leadership, intelligence and ethics, biosecurity, health security and cyber. He is the author of *Intelligence and Intelligence Analysis*, Routledge, UK 2011; *Intelligence, Biosecurity and Bioterrorism*, Palgrave Macmillan, UK, 2018; and *Intelligence Leadership and Governance, Building Effective Intelligence Communities in the 21st Century*, Routledge, 2020.

David Whetham is Professor of Ethics and the Military Profession in the Defence Studies Department of King's College London. He is the Director of the King's Centre for Military Ethics and delivers or coordinates the military ethics component of courses for around two thousand British and international officers a year at the UK's Joint Services Command and Staff College. Publications include *Ethics, Law and Military Operations* (Palgrave, 2010), *Just Wars and Moral Victories* (Brill, 2009) and with Andrea Ellner & Paul Robinson (Eds), *When Soldiers Say No: Selective Conscientious Objection in the Modern Military* (Ashgate: 2014).

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 technoethics 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.

Part I

The just intelligence model



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

1 Intelligence and the just war tradition

The need for a flexible ethical framework

Ross Bellaby

Introduction

It is impossible to think of one “just war doctrine”, with a single point of lineal development from a single idea. Rather, “just war” is better thought of as a set of “recurrent issues and themes in the discussion of warfare . . . reflecting a general philosophical orientation towards the subject” (Clark 1988, 31) – a collection of underlying ethical arguments that have evolved over time in response to security challenges. As a broad body of thought the just war tradition “remains one of the most popular frameworks for evaluating the morality of war and warfare” (Fitzsimmons 2015, 1069);¹ influencing and becoming reflected in political rhetoric and legal cannon.² Indeed, many theorists have adapted the just war tradition to tackle emerging ethical-security problems of the day, from acts of terrorism and counter-terrorism policy,³ drone warfare,⁴ biosecurity,⁵ private military companies⁶ and civil wars.⁷

For intelligence the ethical dilemma faced includes recognizing and reconciling that it necessarily includes practices that “unavoidably entail doing something that is seriously contrary to the moral rules accepted as governing most human activity” (Quinlan 2007, 2) with the argument that without secret intelligence states cannot “understand sufficiently the nature of some important threats” (Omand 2007, 116). That on the one hand it can be argued that over the last century intelligence has become one of the most vital tools a political community has in providing timely information designed to serve and protect its members and, as such, represents an ethical good. While on the other hand, it can also be argued that secret intelligence often necessarily involves violating people’s vital interest in privacy and autonomy and so there should be limits on its use. There is a need, therefore, for an ethical framework that can evaluate and reconcile these two tensions, offering both a limitation on the harm that is caused by intelligence collection, while also outlining exactly when this harm is justified. By establishing the criteria of just cause, legitimate authority, right intention, last resort, proportionality and discrimination, it can be argued that the harm intelligence can cause is limited while also outlining if and when its use is justified.

There are, however, some key concerns levied at using the just war tradition as a basis for developing an ethical framework for intelligence. Key amongst

them is that intelligence is not a war. That is, a lot of what intelligence does focuses on domestic surveillance with activities closer to police work; it is not on a battlefield, weighing up the costs of killing the soldier in front of you, but rather involves extensive and systematic collection of data. Intelligence is not necessarily about examining the ethical cost of killing an individual in order to protect one's own or another's life. It is about data collection and analysis in order to prevent threats from actually causing significant harm to another. For some, therefore, it is better if intelligence was located within the political as compared to the security sphere, where questions on its activity should reflect existing domestic oversight structures. There are concerns that equating intelligence with war makes its activities too permissive; the supreme emergency often associated with war heightens the pressure to act and lowers the ethical threshold, making it an ill fit for a broad set of activities which are often carried out in times of peace and against one's own population.

However, while intelligence is not war, it is also not police work. Indeed, although it is actually difficult to place a clear set of boundaries around what intelligence is – as it ranges from data collection and analysis to more active forms of paramilitary operations – intelligence is quintessentially an activity that concerns itself with “national security”, dealing with threats greater in their impact both in terms of areas of national importance and number of people affected. It is tasked with detecting threats that can represent a significant harm to a large number of individuals and works within the national security infrastructure to provide security to the community as a whole. The argument put forward here, therefore, is that by looking at the underlying tensions presented by intelligence activity and the justifications found within the just war tradition a set of specialized just intelligence principles can be established.

Indeed, on a theoretical level the just war tradition gives an important starting point in the need to understand the fundamental harm caused to the individual – that is, the impact it has on our most fundamental vital interests – and how this relates to the harm that the national security agenda is seeking to prevent. Just as the just war tradition recognizes a general presumption against killing to be justified within a set of given limits, the impacts of secret keeping on people's autonomy and other vital interests means there is also a general presumption against secrecy unless a direct justification is given (Calhoun 2001). The tradition then invites us to break down the justification into a set of ethical sub-questions and debates to be had that, in combination, provide an extensive understanding as to whether the act is just or not. These criteria are well versed in dealing with the types of ethical debates that are raised in the security sphere, drawing on both absolutist and utilitarian questions and concerns. For example, the principle of just cause asks us to consider the underlying reason given for why the harm is justified, drawing on wider ethical arguments on self-defence and the duty of the state to protect the political community, explored through hypotheticals and real-life or historical cases to understand what reasons are justifiable for different acts. The principle of legitimate authority places the political community at the centre, challenging both oversight internal to the intelligence community and

those external structures that are pulled into the protective shield of secrecy to lose much of their potency. While the principle of proportionality delineates what costs and benefits should be included in the calculation and ensures that the overall benefit is in the positive, the principle of discrimination seeks to distinguish the rights and obligations the state has to different groups of people, outlining who is a legitimate target and who is protected. Not only does the just war tradition direct us to ask certain ethical questions that are relevant in the security world but it also establishes a body of thought to guide the types of debates we should be having, and the variety of answers available to us.

One important difference, however, between war and intelligence is that in the former there is a sharp distinction between the justice of going to war, *jus ad bellum*, and the justice of actions within war, *jus in bello*. This distinction does not work when we consider cyber-intelligence collection. There is not the same division between evaluating and sanctioning the general act of intelligence collection and the carrying out of the variety of acts under this authorization that is seen with war. There is no “time of war/time of peace” distinction for intelligence, but rather operations are running continuously. So, with intelligence, the evaluation must be done continuously, whereby each operation must fulfil all the just cyber-intelligence principles described later, with an operation being sanctioned according to who is being targeted, taking into account whether there is a specific just cause for the operation, ensuring that there is a right intention, and that the method chosen is proportionate the proposed gains.

Adapting just war for just intelligence

Reconceptualizing the idea of security

In order to create this new ethical framework how we conceive of “security” needs reconceptualizing. While Zedner is correct in that security is another “promiscuous concept” (Zedner 2009, 9) – ranging in content, referent object and means of provision⁸ – the value of security, and from there the right or expectation to have security, for this chapter is directly linked to the value that an individual has in maintaining their vital interests.⁹ That is, security is the condition by which one’s vital interests are maintained and protected. This means contemplating security as the processes and protections designed to maintain people’s vital interests. For example, at its core the vital interest in maintaining one’s physical integrity gives rise to the understanding of security as personal safety, thus “usually understood to refer to the protection against physical or other harm” and to provide security therefore includes “the prevention of or resilience against deliberate attack” (Schneier 2006, 12).¹⁰ Or, in terms of privacy, security refers to the protections one has, both physically and symbolically, that prevent outsiders from intruding on private spaces or accessing personal information without authorization.

Security is therefore not separate from people’s interests, but an overarching formula by which they are ensured, and the role of the state is to negotiate the tensions between the various vital interests and seek to provide the necessary

protections so that individuals can fulfil their own version of the good life. The provision of security means understanding the complex interrelation between an individual's vital interests and offering them the necessary protections, and that harming someone is the way and degree to which these vital interests are violated. What this understanding provides is a way of detailing the impact, or harm, that intelligence can have on individuals, which can then be reconciled with the threat the intelligence community is seeking to prevent. Importantly, this means that security and human rights are not opposing attributes to be "balanced" against each other but are different aspects of the same phenomenon. Indeed, narratives that portray security and liberties as opposing qualities that must be traded or balanced, while pervasive, are dangerous (Waldron 2003; Pozen 2015; McArthur 2001). By framing it as a trade-off between privacy and security, where you can have either security or privacy but not both and, importantly, where security is seen as a trump card (Thompson 2001; Dragu 2011; Bambauer 2013),¹¹ it is not surprising that "After 9/11 countries around the globe unhesitatingly adopted policies to enhance their government's capacity to prevent terrorism . . . at the expense of individual civil liberties" (Dragu 2011).¹² While Jeremy Waldron warns that even these framings are problematic in terms of unequal distribution of the trade-off, unclear returns for any given exchange and the problem of trading liberties at will (Waldron 2003), it is argued here that these framings fail to see how the matrix of vital interests should be taken as a whole, viewed holistically in order to provide an individual with enough of his vital interests that he can carry out his goals, and therefore be deemed secure. This means that "the overlapping or even isomorphic relationship between privacy and security is far more subtle than it might be imagined and cannot be glossed over by a rhetoric of 'opposed' rights or values of security and privacy" (Raab 2017).

Therefore, it is important to understand the harm that an intelligence activity represents through its aim of providing security to people so that this can be reconciled with the harm that it seeks to prevent by forestalling a threat from being realized. As a process this means, first, recognizing that while some vital interests such as physical and mental integrity might appear to take precedence over the other interests such as autonomy, liberty, self-worth or privacy, they should be taken together as a complex matrix that all need to be maintained.¹³ That in maintaining the security of the individual an excess of one vital interest will not necessarily make up for the lacking of another interest: an excess of physical security cannot be used as a justification for undermining people's privacy; it cannot be argued that people are physically very safe in exchange for having no privacy (Feinberg 1984, 37; Rescher 1972, 5).

Secondly, in making this calculation, it is important to understand that these vital interests are not binary, whole one minute and utterly destroyed the next, but exist to varying degrees given the context. The negotiation therefore involves understanding which and to what extent both the state and a perpetrator are threatening vital interest(s). For example, privacy can be perceived as consisting of different levels where the more personal or intimate the information, the greater the expectation of privacy (Marx 2004, 234; Von Hirsch 2000). Therefore, there

must be a greater threat to someone's other vital interests to justify the privacy intervention. Part of this negotiation is understanding whether the target has acted in some way so as to waive or forfeit their immediate vital interests, the potential threat to other people's vital interests represented by the aggressing actor and that the state is itself not representing the greater threat to our vital interests.

Proportional problems and proportional responses

I have spoken elsewhere about a metaphorical "ladder of escalation" which can be used to separate out different intelligence collection activities according to the harm they cause, which can be set against the level of threat they seek to prevent. This flexibility allows for a differentiation across the large range of intelligence activities and situations with a flexible set of just intelligence principles, each with their own series of internal spectrums or proportional calculations. For example, in terms of just cause and self-defence the type of defence one should muster should be proportional to the type of threat. That is, if the threat is of lesser magnitude than killing or severe suffering, while there might not be a justification to kill in self-defence there could be justification for a low-level physical response, loss of property and resources, or sanctions (Pattison 2018). For intelligence, this means the justified intelligence activity should reflect the potential threat represented. Equally, for authority then different measures need to be in place to offer flexible but increasing oversight as the harm caused goes up, whereby the level of blame is not diminished but more securely located with those in charge. While for discrimination this allows those tangentially involved with a threat to be included for low-level intelligence activities, while being protected from more intrusive forms lest evidence shows they have a greater involvement.

Temporal quality

One of the key differences between war and intelligence is that in the former the threat is relatively known, whereas intelligence activity can, and should, come long before the threat is known for it is the purpose of the intelligence operative to locate the threat in the first instance. Therefore, intelligence can involve targeting individuals before their threat status is known, which means decisions are being made on whether or not to use an intelligence activity before one is able to make an ethical calculation as to whether it is justified or not. In order to reconcile this it is necessary to think of intelligence as a form of pre-emptive or preventive self-defence. This is based on the argument that there is a distinction between "self-defence against present definite threats . . . definite future threats . . . as well as indefinite potential threats" (Lee 2018, 346; Walzer 2015). For example, pre-emptive self-defence counters threats that, while not realized, have a clear likelihood and close temporal quality, while preventive self-defence has a much broader temporal range, being years down the line or where it is unclear if the threat will materialize. By understanding intelligence as a flexible, proportional activity it is possible to use those activities which cause a lower level of harm to

gather initial information on a situation and target, and then use this information to either escalate up through more harmful intelligence activities or by abandoning the target.

Developing and applying just intelligence principles

Following from these initial principles a set of “just intelligence principles” can be created. These principles reflect the underlying ethical arguments found within the just war tradition but are appropriately adapted for intelligence activity. These just intelligence principles are as follows (Bellaby 2014, 109):

- **Just cause:** there must be a sufficient threat to justify the harm that might be caused by the intelligence collection activity.
- **Authority:** there must be legitimate authority, representing the political community’s interests, sanctioning the activity.
- **Intention:** the means should be used for the intended purpose and not for other (political, economic, social) objectives.
- **Proportionality:** the harm that is perceived to be caused should be outweighed by the perceived gains.
- **Last resort:** less harmful acts should be attempted before more harmful ones are chosen.
- **Discrimination:** there should be discrimination between legitimate and illegitimate targets.

While a direct transfer of the just war tradition’s principles to just intelligence is both inaccurate and unhelpful, by following the underlying ethical arguments made they can be applied to different areas of intelligence activity.

Just cause

The criteria of “just cause” is often considered to be one of the most important of the just war principles as it outlines the main reason for going to war and the main argument for its ethical justification. Over the years, acting in self-defence has been defined as the main, acceptable just cause for going to war. In comparison, the just cause equivalent for intelligence collection could be interpreted as preventing the realization of a threat against the political community. This is because it is the role of the intelligence to firstly detect, provide information on and initiate some prevention of any and all threats that face the political community. In this way, depending on the nature of the threat, it can act as a just cause to justify the use of the intelligence activity and the harm it can cause. Therefore, by acting to detect and prevent these threats intelligence activity works as an act of a preventive self-defence, averting the actualization of threats against the political community (Bellaby 2014, 26).

However, protecting the political community is more than just protecting the state, and includes its ethical, moral, social and legal norms. The purpose of the

just cause is not necessarily to balance these, but to highlight what they are and interrogate them.¹⁴ Reconciling these different conceptions of security and determining if there is a suitable threat to the political community means understanding the threat from both other actors' and the state's own national security efforts if they excessively or unnecessarily violate people's vital interests. For example, when the National Security Agency (NSA) programmes to collect as much information as possible (through surveillance programs referred to as Upstream, Quantuminsert, Tempora) were revealed, by doing this the intelligence services were seen to be significantly violating the privacy of people *en masse* (Feinberg 1984, 35; Bellaby 2016). Therefore while there was not a just cause for such intelligence activity because there was no clear, direct threat to act as a justification, there is in fact a just cause for someone to reveal the information and blow the whistle given the harm being caused. What this means for intelligence is that there is actually a just cause for revealing the secret activity of the intelligence community when their activity itself represents a threat to the political community. When the state, or its representatives, is the source of an unjustified threat to the individual's and society's vital interests then there is a just cause to act.

Just authority

In the just war tradition the principle of legitimate authority determines that in order for a war to be considered morally permissible it must be authorized by the right (or legitimate) authority. That is, those who have the right to command by virtue of their position: "since the care of the common weal is committed to those who are in the right authority, it is their business to watch over the common weal" (Aquinas 2002, 214). This authorizing actor must have both the moral weight of representing and protecting the needs of the political community and ensuring practical considerations such as having the physical, intellectual and emotional ability to take into account the different factors involved while limiting personal costs or bias. While traditionally the legitimate authority rested with the state and its representatives as the most appropriate actor to fulfil these needs, this does not necessarily have to be the case. The state will often represent a good choice as it has extensive experience and a wide breadth of knowledge and in many instances is a manifestation of the political community's best form of protection and ability to represent the wishes of the people. However, at its core the just war tradition seeks to place authority within those who best represent and will act in the interests of the political community and its people. What this means is that when the state fails in this task or begins to represent the source of the problem then there is a need to rest the legitimate authority elsewhere.

Initially, therefore, this should (uncontentiously) mean bringing oversight out of the intelligence community's purview as those planning, performing or managing operations have heavily invested interests. However, while this oversight has traditionally been placed predominantly in the hands of the executive, with additional oversight through the legislature and judiciary, historically many administrations have covered up wrongdoing that would have resulted in individual

repercussions for members of government and embarrassment for the administration as a whole (Wells 2004, 1203; Ambinder 2013, 6). Existing institutions have proven unable to act without bias and act outside their political objectives, and are therefore ill-suited for balancing the ethical and security concerns. Indeed, Rahul Sagar has shown that in the United States “Given the President’s stronghold over the flow of national security information, there is little reason to believe that lawmakers will be able to *take the lead* in uncovering policies and actions” (Sagar 2016, 128).¹⁵ Whereas in terms of the judiciary he argues that “judges are not trained, and the courts not equipped, to make politically charged decisions about what state secrets are appropriate” coupled with a “judicial deference towards the executive’s claims about the harm likely to be caused by the disclosures” (Sagar 2016, 74). Moreover, in those courts where the whole proceedings are kept secret – the Foreign Intelligence Surveillance Court being a notable case – the secrecy limits opportunity for engaged reflection and debate on the legal interpretation as judicial peer review and the right to appeal is prevented.¹⁶ What this highlights is that these existing political structures lack the physical power to keep the intelligence community in check, and are insufficient in manpower, intellectual mandate or drive to do so or cannot separate their own political interests from their role as overseer. The problem seen is that the secrecy necessarily attached to intelligence is extended over the political oversight mechanisms, which in turn insulates them from the piercing power of democratic observation and rather than these actors interrogating intelligence they become habitualized by a national security elitism that distorts their oversight role.

Rather, there needs to be a new, proactive and imbedded set of oversight mechanisms to systematically examine conduct and information collected to determine if it should be released or not.¹⁷ In designing this new oversight actor several principles can be highlighted. First, at its core the principle of legitimate authority distills the idea that the review should be examined before rather than after the event. The wars must pass the initial criteria before any attack is deemed legitimate. This means that the review should be penetrative. The oversight actor should have the power and expectation to review operations, policies, practices and trends within the intelligence community in real time, including whether there are tendencies towards too much secret keeping as well as acting to review individual cases to determine if they should keep the information or not.

Secondly, since the authority should represent the political community, it does not have to be limited to state representatives nor do they necessarily have to be elected or subject to populous demands – as restricting it in this way can be more detrimental to the actual review. Therefore, alternative representative mechanisms can be utilized such as using legal, moral and societal experts or representatives, chosen because of their expertise rather than because of their elected status. In order to avoid the same popular pressures faced by elected officials they should not be subjected to direct democratic elections, but rather represent experts in the relevant fields of intelligence oversight, preferably legally trained, nominated and confirmed by the legislative in a public debate where their suitability is tested.

Thirdly, to limit the distortive effect of political interference the body should be able to determine for itself what information should be released free from political censure. If it detects intelligence activity that contravenes the principles outlined in the other criteria it should be free to determine for itself what to reveal according to the interests of the community and free from worries of political scandal.

Last resort

In the just war tradition the need that war only be undertaken as a last resort is an attempt to allow those means that can cause a lower level of harm, like diplomacy or economic pressure, to be given a chance to resolve the issue before the higher harms seen in war are permitted. This way the more harmful acts are avoided if possible. Based on this conception of last resort, one can argue for a similar rationale for the just intelligence principles. In order for an intelligence collection means to be just it must only be used once other less harmful means have been exhausted or are redundant. In this way, the principle of last resort ensures that the intelligence collection means with the lowest level harm is used first in an attempt to deal with the threat, and thus give the opportunity for more harmful activities to be avoided. While there is no rigid methodology or steps that must be worked through, it does require that some of the more harmful actions are not resorted to out of ease or expediency.

Proportionality

The idea of proportionality is one of the oldest principles not only of the just war tradition but also of moral theory and armed strategy in general. Leaders and individuals alike often weigh up the costs of an action against what can be gained from it. The notion of proportionality seeks to ensure that the harm caused in war is proportionate to the threat that it is meant to overcome, placing a limit on the amount of harm allowed for a given action. What is important is that all the harms are included in the calculation and only those benefits that are directly linked to the just cause should count (Hurka 2005; McKenna 1960; Regan 1996). For example, in terms of war while we would not consider the boost to the economy as a relevant good, the fact that it might hurt the economy would be counted as a negative. Therefore, while wider damages can be included when assessing the need to release the information only specific goods directly relating to the just cause can be included when arguing for information retention.

Similar to the consequentialist calculation one can argue that in order for the intelligence collection to be just the level of harm that one perceives to be caused by the collection should be outweighed by the perceived gains. As David Omand asks, “is the likely impact of the proposed intelligence gathering operation, taking account of the methods to be used, in proportion to the seriousness of the business at hand in terms of the harm it seeks to prevent?” (Omand 2007, 162). On the one hand the costs and gains can be examined in terms of Herman’s “balance sheet” approach, where “knowledge and activities can be examined separately, and then

can be integrated into an ethical balance sheet” (Herman 2002, 290). This moral accounting allows us to balance the overall good effect of intelligence knowledge against some of the less desirable methods. If it is discovered “at the bottom of the ledger that the benefits of intelligence knowledge is found to be in credit, then the means employed to gather intelligence can be morally justified by the positive impact of knowledge acquired” (Erskine 2004, 366).

In addition to these direct costs, however, we need to include wider costs such as the impact on individuals’ autonomy, society, degradation to important social norms and practices and the cohesion of the political community. Richard Matthews argues that no individual is an island, but is a part of a complex set of social networks that are also damaged when someone is affected by intelligence practice: “its run-on effect is well documented and involves wide-ranging pain and suffering across the communities and contexts” (Matthews 2012, 466). For example, additional costs associated with intelligence collection activities can include degradation to social cohesion as minorities are over-represented and excessively targeted, marginalizing them from the greater social whole and reinforcing distorted criminal statistics, often with individuals unaware that their information is being used (Benetto 2005, 5).

Discrimination

The requirement that an attack must discriminate between combatants and non-combatants is one of the most stridently codified just war rules and is reflected in the international law of war as such. Soldiers charged with the deployment of force and violence cannot do so indiscriminately. They have an obligation to exert a particular effort to discriminate between legitimate and illegitimate targets. The target has to have “something about them” to justify being a legitimate target (Nagel 1979, 124). That is, either the target represented a threat of some form and attacking him is justified as an act of self-defence, or that when the individual became a soldier he waived his normal protective rights in some way.

For intelligence one can argue that, just as soldiers are legitimate targets because they are a threat and they give up certain protective rights, arguably any individual can act in a way as to make themselves a threat or to forfeit certain protective rights. Holding a particular job; being in possession of important information and being a member of a state’s infrastructure are all examples of how an individual can make himself liable for the threat or consent to the waiving or forfeiting of certain rights. For example, “consent to participate in the world of national security on all levels of a country’s self-defence structure together with the quality of the information possessed” puts the individual liable to the threat and as such justifies them as targets (Pfaff and Tiel 2004, 6).

Notes

- 1 For a summary of the various different historical thematic and contemporary intellectual developments see Johnson (2006).

- 2 For political use, see Kelsay (2013). For the principle of discrimination, see Article 48, first additional protocol to the Geneva Conventions; for the principle of proportionality, see Article 51(4b), first additional protocol to the Geneva Conventions; for the principle of just cause, see Article 51 UN Charter.
- 3 For example, see Lowe (2003), Walzer (2006), Crawford (2003), Sussmann (2013), Valls (2000) and Steinhoff (2004).
- 4 For example, see Williams (2015).
- 5 For example, see van der Bruggen (2013).
- 6 For example, see Fitzsimmons (2015) and Pattison (2008).
- 7 For example, see Meisels (2014) and Scheid (2012).
- 8 For work on “security studies” and the changes in referent object, the construction of security threats and security actors, see Buzan, Wæver, and de Wilde (1997), Browning and McDonald (2011) and Katzenstein (1996).
- 9 For more on there being a “right” to security, see Lazarus (2007), (2012).
- 10 This is different from the instrumentalist arguments made by people such as Henry Shue whereby security is necessary for the enjoyment of other rights. See Lazarus (2012).
- 11 For arguments against security necessarily trumping privacy, see Moore (2011). For arguments for security trumping privacy, see Himma (2007).
- 12 Also see Ackerman (2006) and Hardin (2004).
- 13 Isaiah Berlin declared that in much the same way that boots were more important than the words of Shakespeare, liberty and autonomy are not necessarily the total first needs of an individual (Berlin 1969, 124).
- 14 For McMahan the principle of proportionality is therefore directly connected to the principle of just cause as it enables the balancing of the just cause against the various potential harm to be caused by the act of war (McMahan 2005).
- 15 Also see Born (2003, 22).
- 16 For the role of the right to appeal and the importance of multi-layered court systems, see Dalton (1985), Lennerfors (2007) and Nobles and Schiff (2002).
- 17 This builds on Rahul Sagar’s discussion on the limits of retrospection as a form of oversight (Sagar 2007, 414–17).

References

- Ackerman, Bruce. 2006. *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism: Emergency Powers in an Age of Terrorism*. New Haven: Yale University Press.
- Ambinder, Marc. 2013. *Deep State: Inside the Government Secrecy Industry*. Hoboken, New Jersey: Wiley.
- Aquinas, Thomas. 2002. “From Summa Theologiae”. In *International Relations in Political Thought: Texts from the Ancient Greeks to the First World War*, edited by Chris Brown, Terry Nardin, and Nicholas Rengger. Cambridge; New York: Cambridge University Press.
- Bambauer, Derek E. 2013. “Privacy versus Security”. *Journal of Criminal Law and Criminology* 103 (3): 667–83.
- Bellaby, Ross W. 2014. *The Ethics of Intelligence: A New Framework*. London; New York: Routledge.
- . 2016. “Justifying Cyber-Intelligence?” *Journal of Military Ethics* 15 (4): 299–319. <https://doi.org/10.1080/15027570.2017.1284463>.
- Bennetto, Jason. 2005. *Police and Racism: What Has Been Achieved 10 Years after the Stephen Lawrence Inquiry Report?* London: Equality and Human Rights Commission. www.equalityhumanrights.com/en/file/6316/download?token=4QCFPaJj.

- Berlin, Isaiah. 1969. *Four Essays on Liberty*. London; New York etc.: Oxford Paperbacks.
- Born, Hans. 2003. *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices*. Edited by Philipp Fluri, Anders B. Johnsson, and Born Hans. Geneva: IPU-DCAF.
- Browning, Christopher S., and Matt McDonald. 2011. "The Future of Critical Security Studies: Ethics and the Politics of Security". *European Journal of International Relations*, October. <https://doi.org/10.1177/1354066111419538>.
- Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1997. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.
- Calhoun, Laurie. 2001. "The Metaethical Paradox of Just War Theory". *Ethical Theory and Moral Practice* 4 (1): 41–58. <https://doi.org/10.1023/A:1011440213213>.
- Clark, Ian. 1988. *Waging War: A Philosophical Introduction*. Oxford; New York: Clarendon Press.
- Crawford, Neta C. 2003. "Just War Theory and the U.S. Counterterror War". *Perspectives on Politics* 1 (1): 5–25. <https://doi.org/10.1017/S1537592703000021>.
- Dalton, Harlon. 1985. "Taking the Right to Appeal (More or Less) Seriously". *Yale Law Journal* 95 (1): 62–107.
- Dragu, Tiberiu. 2011. "Is There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention". *American Political Science Review* 105 (1): 64–78. <https://doi.org/10.1017/S0003055410000614>.
- Erskine, Toni. 2004. "'As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering". *Intelligence and National Security* 19 (2): 359–81. <https://doi.org/10.1080/0268452042000302047>.
- Feinberg, Joel. 1984. *The Moral Limits of the Criminal Law: Harm to Others v. 1*. New York: Oxford University Press Inc.
- Fitzsimmons, Scott. 2015. "Just War Theory and Private Security Companies". *International Affairs* 91 (5): 1069–84. <https://doi.org/10.1111/1468-2346.12398>.
- Hardin, Russell. 2004. "Civil Liberties in the Era of Mass Terrorism". *The Journal of Ethics* 8 (1): 77–95. <https://doi.org/10.1023/B:JOET.0000012253.54321.05>.
- Herman, Michael. 2002. *Intelligence Services in the Information Age: Theory and Practice*. London: Frank Cass Publications.
- Himma, Kenneth E. 2007. "Privacy versus Security: Why Privacy Is Not an Absolute Value or Right". *San Diego Law Review* 44: 857–920.
- Hurka, Thomas. 2005. "Proportionality in the Morality of War". *Philosophy & Public Affairs* 33 (1): 34–66. <https://doi.org/10.1111/j.1088-4963.2005.00024.x>.
- Johnson, James T. 2006. "The Just War Idea: The State of the Question". *Social Philosophy and Policy* 23 (1): 167–95. <https://doi.org/10.1017/S0265052506060079>.
- Katzenstein, Peter. 1996. *The Culture of National Security: Norms and Identity in World Politics*. New York, NY: Columbia University Press.
- Kelsay, John. 2013. "Just War Thinking as a Social Practice". *Ethics & International Affairs* 27 (1): 67–86. <https://doi.org/10.1017/S0892679412000780>.
- Lazarus, Liora. 2007. "Mapping the Right to Security". In *Security and Human Rights*, edited by Benjamin Goold and Liora Lazarus, 1st edition. Oxford; Portland, OR: Hart Publishing.
- . 2012. "The Right to Security: Securing Rights or Securitising Rights". In *Examining Critical Perspectives on Human Rights*, edited by Rob Dickinson, Elena Katselli, Colin Murray, and Ole W. Pedersen. Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9781139026291>.

- Lee, Hsin-Wen. 2018. "A New Societal Self-Defense Theory of Punishment: The Rights-Protection Theory". *Philosophia* 46 (2): 337–53. <https://doi.org/10.1007/s11406-017-9931-z>.
- Lennerfors, Thomas Taro. 2007. "The Transformation of Transparency: On the Act on Public Procurement and the Right to Appeal in the Context of the War on Corruption". *Journal of Business Ethics* 73 (4): 381–90. <https://doi.org/10.1007/s10551-006-9213-3>.
- Lowe, Scott. 2003. "Terrorism and Just War Theory". *Perspectives on Evil and Human Wickedness* 1 (2): 46–52.
- Marx, Gary. 2004. "Some Concepts That May Be Useful in Understanding the Myriad Forms and Contexts of Surveillance". *Intelligence and National Security* 19 (2): 226–48. <https://doi.org/10.1080/0268452042000302976>.
- Matthews, Richard. 2012. "An Empirical Critique of 'Interrogational' Torture". *Journal of Social Philosophy* 43 (4): 457–70. <https://doi.org/10.1111/josp.12004>.
- McArthur, Robert L. 2001. "Reasonable Expectations of Privacy". *Ethics and Information Technology* 3 (2): 123–8. <https://doi.org/10.1023/A:1011898010298>.
- McKenna, Joseph C. 1960. "Ethics and War: A Catholic View". *American Political Science Review* 54 (3): 647–58. <https://doi.org/10.1017/S0003055400122609>.
- McMahan, Jeff. 2005. "Just Cause for War". *Ethics & International Affairs* 19 (3): 1–21. <https://doi.org/10.1111/j.1747-7093.2005.tb00551.x>.
- Meisels, Tamar. 2014. "Fighting for Independence: What Can Just War Theory Learn from Civil Conflict?" *Social Theory and Practice* 40 (2): 304–26. <https://doi.org/10.5840/soctheopract201440218>.
- Moore, Adam D. 2011. "Privacy, Security, and Government Surveillance: WikiLeaks and the New Accountability". *Public Affairs Quarterly* 25 (2): 141–56.
- Nagel, Thomas. 1979. *Mortal Questions*. Cambridge: Cambridge University Press.
- Nobles, Richard, and David Schiff. 2002. "The Right to Appeal and Workable Systems of Justice". *The Modern Law Review* 65 (5): 676–701. <https://doi.org/10.1111/1468-2230.00403>.
- Omand, David. 2007. "Reflections on Secret Intelligence". In *The New Protective State: Government, Intelligence and Terrorism*, edited by Peter Hennessy, 1st edition. London; New York: Continuum.
- Pattison, James. 2008. "Just War Theory and the Privatization of Military Force". *Ethics & International Affairs* 22 (2): 143–62. <https://doi.org/10.1111/j.1747-7093.2008.00140.x>.
- . 2018. *The Alternatives to War: From Sanctions to Nonviolence*. Oxford, UK; New York: OUP Oxford.
- Pfaff, Tony, and Jeffrey R. Tiel. 2004. "The Ethics of Espionage". *Journal of Military Ethics* 3 (1): 1–15. <https://doi.org/10.1080/15027570310004447>.
- Pozen, David. 2015. "Privacy-Privacy Tradeoffs". *University of Chicago Law Review* 83 (1): 221–47.
- Quinlan, Michael. 2007. "Just Intelligence: Prolegomena to an Ethical Theory". *Intelligence and National Security* 22 (1): 1–13. <https://doi.org/10.1080/02684520701200715>.
- Raab, Charles D. 2017. "Security, Privacy and Oversight". In *Security in a Small Nation: Scotland, Democracy, Politics*, edited by Andrew W. Neal. Open Book Publishers. <https://doi.org/10.11647/OBP.0078>.
- Regan, Richard J. 1996. *Just War: Principles and Cases*. Washington, DC: The Catholic University of America Press.
- Rescher, Nicholas. 1972. *Welfare: The Social Issues in Philosophical Perspective*. 1st edition. Pittsburgh: University of Pittsburgh Press.

- Sagar, Rahul. 2007. "On Combating the Abuse of State Secrecy". *Journal of Political Philosophy* 15 (4): 404–27. <https://doi.org/10.1111/j.1467-9760.2007.00283.x>.
- . 2016. *Secrets and Leaks: The Dilemma of State Secrecy*. Revised edition. Princeton, NJ: Princeton University Press.
- Scheid, Anna F. 2012. "Waging a Just Revolution: Just War Criteria in the Context of Oppression". *Journal of the Society of Christian Ethics* 32 (2): 153–72. <https://doi.org/10.1353/sce.2012.0035>.
- Schneier, Bruce. 2006. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. 2003. Corr. 2nd edition. New York: Springer-Verlag New York Inc.
- Steinhoff, Uwe. 2004. "How Can Terrorism Be Justified?" In *Terrorism: The Philosophical Issues*, edited by Igor Primoratz, 97–109. UK: Palgrave Macmillan. <https://doi.org/10.1057/9780230204546>.
- Sussmann, Naomi. 2013. "Can Just War Theory Delegitimize Terrorism?" *European Journal of Political Theory* 12 (4): 425–46. <https://doi.org/10.1177/1474885112464478>.
- Thompson, Paul B. 2001. "Privacy, Secrecy and Security". *Ethics and Information Technology* 3 (1): 13–9. <https://doi.org/10.1023/A:1011423705643>.
- Valls, Andrew. 2000. "Can Terrorism Be Justified?" In *Ethics in International Affairs*, edited by Andrew Valls, 65–79. Lanham, Maryland: Rowman & Littlefield Publishers.
- van der Bruggen, Koos. 2013. "Biosecurity and the Just-War Tradition". In *On the Dual Uses of Science and Ethics: Principles, Practices, and Prospects*, edited by Michael J. Selgelid and Brian Rappert. ANU E Press. <https://research.monash.edu/en/publications/on-the-dual-uses-of-science-and-ethics-principles-practices-and-p>.
- Von Hirsch, Andrew. 2000. "The Ethics of Public Television Surveillance". In *Ethical and Social Perspectives on Situational Crime Prevention*, edited by Andrew Von Hirsch, David Garland, and Alison Wakefield, 59–76. Studies in Penal Theory and Penal Ethics. Oxford: Hart.
- Waldron, Jeremy. 2003. "Security and Liberty: The Image of Balance". *Journal of Political Philosophy* 11 (2): 191–210. <https://doi.org/10.1111/1467-9760.00174>.
- Walzer, Michael. 2006. "Terrorism and Just War". *Philosophia* 34 (1): 3–12. <https://doi.org/10.1007/s11406-006-9004-1>.
- . 2015. *Just and Unjust Wars*. 5th edition. New York: Basic Books.
- Wells, Christina E. 2004. "'National Security' Information and the Freedom of Information Act". *Administrative Law Review* 56 (4): 1195–1221.
- Williams, John. 2015. "Distant Intimacy: Space, Drones, and Just War". *Ethics & International Affairs* 29 (1): 93–110. <https://doi.org/10.1017/S0892679414000793>.
- Zedner, Lucia. 2009. *Security*. 1st edition. London; New York: Routledge.

2 Truth-seeking and the principles of discrimination, necessity, proportionality and reciprocity in national security intelligence activity

Seumas Miller

Introduction

National security intelligence is information or other data collected, analyzed and disseminated by intelligence agencies (in particular) and done so in the service of these agencies' primary institutional purpose (Miller 2010), at least in liberal democracies. Here it is understood that this institutional purpose and these actions are to be understood normatively, that is in terms of what *ought to be* done, as opposed to *what is* in fact being done. Here, the term "normative" has a moral or ethical loading, for example what ought to be done is typically what morally ought to be done all things considered (including consideration of the empirical facts).¹ Moreover, these essentially *epistemic* (from the Greek word, "episteme", meaning knowledge) or evidence-based truth-seeking activities of collection, analysis and dissemination are the main ones performed by national security agencies. That said, many of these agencies also perform *kinetic* tasks, for example the covert operations conducted by the United States CIA (Central Intelligence Agency), and on occasion tasks that might be referred to as *quasi-epistemic*, for example psychological "warfare".

Further, the definition of national security is highly problematic; the concept of national security is ill-defined, indeterminate, shifting, open-ended and contestable (Williams 2003, 511–31, 514; McDonald 2008, 563–87, 567; Buzan, Wæver, and de Wilde 1997, 24). For instance, the US National Intelligence Strategy has as one of its purposes to promote American prosperity.² However, let us assume that national security intelligence is, at the very least, intelligence pertaining to serious internal or external threats to the nation-state itself, or to one of its fundamental political, military or criminal justice institutions, and that these threats might emanate from state or non-state actors, for example terrorist groups. So national security intelligence includes not only military intelligence but also some criminal intelligence and economic intelligence, since the latter may have national security implications, for example intelligence on drug cartels destabilizing governments or on fighter aircraft being built by private companies.

It might be claimed that unlike, for instance, much of the intellectual work conducted in universities,³ intelligence collection, analysis and dissemination is

not an end in itself but rather the means to some further end; that is, the end point of the intelligence process is actionable intelligence, that is intelligence provided to relevant decision makers that is a means to kinetic action. In one sense this claim is true. Intelligence does need to be actionable; intelligence collection and analysis has a purpose beyond acquisition of the truth (so to speak). However, in another sense it is false. For the acquisition of the truth (or, at least, of probable truth) is (or ought to be) an end in itself for intelligence officers, notwithstanding the further requirement that the truths acquired be actionable. Let me explain.

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 or an interest in neither but rather only in “playfulness” (a la postmodernists) or self-interest (a la demagogues, such as former US President, Donald Trump, who have a tendency to say whatever they believe might be useful to them and do so without regard for the truth). Rather truth is internally connected to intelligence activity. Thus aiming at truth is aiming at truth as an end in itself. (This is, of course, consistent with also aiming at truth as a means to some other further end, such as apprehending an offender or 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 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 in independence and in which intelligence officers’ desire to please or, more likely, desire not to antagonize their political masters (e.g. some 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, 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, but end up over time 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, end up becoming something akin to pseudo-intelligence officers.

There is an important institutional implication of the earlier discussion. As we have just seen, whereas the primary institutional purpose of national security intelligence agencies is essentially epistemic, the realization of this epistemic purpose serves a larger national security purpose only realizable by the kinetic activity of other institutions, for example the military. Accordingly, there is an institutional division of labour; the intelligence agency provides knowledge (or weaker epistemic goods) to the decision makers, for example politicians and military 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 and, therefore, that the epistemic activity of the intelligence agencies is not unduly influenced or otherwise undermined by the institutions which they serve, for example 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 overrides 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 realize 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.

In relation to national security intelligence and the normative theory thereof, a threefold distinction needs to be kept in mind, namely:

1. **Institutional level** – the core activities, structures, resources and institutional purposes of national security intelligence agencies, for example the *raison d'être* for the establishment and continued existence of MI5 in the United Kingdom
2. **Macro-activity level** – the mid- to long-term goals, strategies and campaigns of national security intelligence agencies, for example to win the Cold War, increased reliance on electronic rather than human intelligence
3. **Micro-activity level** – immediate, specific, operations of national security intelligence agencies, for example surveillance of a given terrorist suspect

Note that these three levels interact, for example level 1 drives level 2 which in turn drives level 3 (and the reverse interactive process from level 3 to level 2 to level 1 is also the case).⁴ Moreover, the distinction between the three levels is not necessarily clear-cut, for example when does a short-term goal, such as collecting intelligence on the perpetrators of 9/11, become a mid- or even long-term goal, such as collecting intelligence on Al-Qaeda? For our purposes in this chapter, it is important to note the difference between a normative theory of an institution in

an avowed liberal democracy [e.g. of Israel's Mossad or of the United States NSA (National Security Agency)], a normative framework for the conduct of macro-level activity (e.g. of UK secret intelligence activity in the Cold War or of bulk data collection and analysis by the NSA) and a set of ethical guidelines for the conduct of micro-level activity (e.g. ethical guidelines in relation to intelligence collection on a member of a home-grown extremist right-wing subversive group or on "turning" a member of a foreign intelligence agency).

Regarding the normative theory of institutions, we have serviceable normative theories of police organizations [e.g. as the protection by means of police use of coercive force – or the threat thereof – of the legally enshrined, justifiably enforceable, moral rights of citizens from violation by fellow citizens (Miller and Blackler 2016, chap. 1)] and of military organizations [e.g. as the protection by means of military use of lethal force – or the threat thereof – of the legally enshrined, justifiably enforceable, joint moral rights of citizens – e.g. territorial rights – from violation by members of the armed forces of foreign nations or of other political entities (Miller 2016b, chap. 3)]. Accordingly, we can derive serviceable normative theories of intelligence agencies engaged in (respectively) criminal intelligence and military intelligence; the realization of the epistemic purposes definitive of these intelligence agencies ultimately serves in turn the institutional purposes of police and military organizations (respectively). But what of national security intelligence agencies? Their remit is wider in some respects than that of criminal intelligence agencies and that of military intelligence agencies (and also narrower in some respect than each of these types of intelligence agencies, i.e. a great deal of criminal intelligence is not national security intelligence and – arguably – not all military intelligence is of interest to national security agencies, e.g. intelligence at the micro level concerning a small-scale enemy troop movement that is without much strategic significance). Evidently, we do not yet have a serviceable normative theory of national security intelligence agencies (or even an acknowledgement that one is needed). This is a significant gap in normative theory and, given the expanding role of national security intelligence agencies, for example in relation to pandemics and the impact of climate change or as a result of technological developments such as in respect of GEOINT, one with potentially important practical implications. On the other hand, it might be argued that in place of a normative theory, a set of relatively concrete, historically relative, national security purposes could be specified, such as collecting and analyzing intelligence required for counter-terrorism purposes or that will assist the armed forces engaged in combat, and ascertaining the intentions and capabilities of hostile, dangerous, authoritarian states, such as Russia, China, Iran and North Korea. However, ultimately, the selection of these national security purposes would need to be justified, at least in part, by recourse to a normative theory of national security, for example self-defence (an unduly narrow account) or national interest (an unduly wide account).

Importantly, this aforementioned threefold distinction does not parallel the twofold distinction in traditional Just War Theory between the *jus ad bellum* (the principles justifying waging war) and the *jus in bello* (the principles under which

the war once embarked upon should be conducted), and even less so the contemporary fivefold distinction between *jus ad bellum*, *jus in bello*, *jus post bellum* (the principles applicable once hostilities have ceased) and *jus ad vim* (the principles governing the use of force short of war).⁵ This so notwithstanding recent attempts to apply Just War Theory to national security intelligence activities via the so-called Just Intelligence theory (Bellaby 2014; Quinlan 2007); evidently the morality of national security intelligence activities does not parallel the morality of kinetic military activities (Miller 2021).

There are a number of reasons for this. Firstly, as mentioned the constitutive (proximate) end of intelligence activity is knowledge, that is it is a form of truth-seeking. By contrast, the constitutive end of military activity is non-epistemic, that is it is a form of kinetic activity. Secondly, as a result of intelligence activity being epistemic activity (“knowing things”), it is inherently less harmful than kinetic military action (“killing people and breaking things”). Thirdly, intelligence and military activities 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); hence intelligence collection is the first resort and the use of military force the last resort (and, indeed, the principle of last resort is constitutive of Just War Theory but not of intelligence activity). Fourthly, national security intelligence activity is a continuous, ongoing (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).⁶

Notwithstanding that intelligence activity has knowledge as its constitutive end and military activity does not, there do seem to be a number of moral principles that govern both sets of activities, for example the principles of necessity and proportionality. These principles, at least, are in part constitutive of normative theories of intelligence agencies, normative frameworks for ongoing intelligence campaigns and sets of moral guidelines for intelligence operations, and they apply at each of the three levels mentioned earlier. Indeed, *some* of these principles, or analogues of them, are constitutive of quite different types of security agency and their activities, for example military organizations versus police organizations. Consider, for example, Just War Theory⁷ and its supposed analogue in intelligence work, Just Intelligence Theory.⁸ However, appearances notwithstanding, these principles apply differently in these different institutional settings and within a given institutional setting (e.g. of national security intelligence settings) at each of these three levels. Indeed, each of these principles might actually consist of a set of somewhat diverse principles. For instance, the so-called principle of necessity might in fact denote more than one principle, for example the principle of military necessity typically concerned with avoiding civilian casualties *and* the principle of necessity in policing typically concerned with avoiding death or injury to offenders (Miller and Blackler 2016). Moreover, the principle of necessity might apply at the institutional level (e.g. is it necessary to have a national security

intelligence agency?), at the macro level (e.g. is it necessary to collect secret intelligence on one's allies?) and at the micro level (e.g. is it necessary to intercept the communications of a suspected terrorist with his children?).

The focus of this chapter is with the analysis and application of four moral principles, namely discrimination, necessity, proportionality and reciprocity in national security intelligence activity. However, in doing so we need to keep in mind, firstly, the twofold distinction between these moral principles and the closely associated legal principles; secondly, the twofold distinction between the essentially evidence-based truth seeking *epistemic* activity of national security intelligence agencies and the *kinetic* activities of military and police organizations (and some national security intelligence agencies at times, notably covert action) and thirdly, the threefold distinction between the institutional, and the macro and the micro levels. We begin with the moral principle of discrimination (Green 1993).

Principle of discrimination

The context for the application of the principle of discrimination is typically taken to be a theatre of war in which (especially) the lives of non-combatants are at risk from the combatants waging the war in question. According to this principle it is prohibited for combatants to deliberately target non-combatants. This is consistent with the deaths of non-combatants being an unintended consequence, even a foreseen unintended consequence, of the actions of combatants (although, under an associated precautionary principle combatants are required to take steps to minimize the risks to non-combatants).⁹ The principle of discrimination is potentially implicated in national security intelligence activity in so far as it is an expression of a more general moral principle according to which innocent persons ought not to be deliberately harmed or otherwise have their rights deliberately 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 on an ongoing basis for intelligence purposes and quite another for this to be done on an ongoing basis for intelligence purposes to a citizen known to be innocent of any crime, e.g. on the off-chance that some useful intelligence might be picked up. Surveillance of the terrorist would in this instance be *morally justified infringement* of the right to privacy, whereas surveillance of the innocent citizen would evidently be a *violation* of the right to privacy.

However, as just mentioned, the principle of discrimination as it applies in armed conflict assumes a distinction between combatants and non-combatants and prohibits combatants from deliberately targeting non-combatants. By contrast, the analogous (let us assume) principle of discrimination in national security intelligence activities (referred to as the principle of discrimination*) does not consist of a general prohibition on targeting innocent persons and with good reason; innocent persons may be a useful source of national security intelligence. Of course, innocent persons will often willingly provide intelligence if asked (whereas non-combatants are unlikely to consent to being deliberately killed).

Indeed, it is permissible for intelligence officials to collect intelligence from innocent persons even without their consent. For instance, it is permissible for an intelligence official to deliberately obtain information about a terrorist from the terrorist's innocent relative without the latter's consent, for example by accessing their private communication without their permission, or by deception, for example by telling a lie. By contrast, deliberately killing the terrorist's innocent relative is obviously prohibited (with or without their consent).

Intelligence activities ultimately aimed at identifying terrorists and thwarting acts of terrorism now involve the application of machine learning techniques to bulk databases that consist in the main of the communication and other data of innocent civilians – indeed, frequently innocent fellow citizens, that is the data of innocent civilians is deliberately collected and accessed (or, at least, filtered and accessed). It can be argued that while the data of these innocent persons is “read” by a machine it is not seen by human eyes or, at least, it is only the data that results from the application of the machine learning process that is seen by human eyes; however, the argument might continue, such data meets 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,¹⁰ 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, even as a means to some further legitimate end. The reason for this difference between the principle of discrimination* applicable in intelligence activities and the principle of discrimination applicable to the use of lethal force by combatants reflects the much greater moral significance that attaches to deliberately taking an innocent person's life than attaches to deliberately invading an innocent person's privacy or deliberately deceiving them. This difference in moral significance in turn reflects, indeed in large part is derived from, the greater moral weight that attaches to life than to privacy or truth-telling. Hence there is an (more or less) absolute legal prohibition on deliberately killing the innocent (even in wartime), but not on deliberately invading their privacy or on telling lies to them (even in peacetime).

We have seen that the principle of discrimination assumes a twofold distinction between combatants and non-combatants (even if, at times, there are problems determining whether a person is a combatant or a non-combatant and even if there is a third category of civilians who are engaged in hostilities at particular times but who are not combatants *per se*). By contrast, police operate with a threefold distinction between innocent persons, suspects and known offenders. Innocent persons ought not to be deliberately harmed whereas known offenders may be, for example police may target known offenders using coercive, incapacitating or even lethal force. But what of suspects? Suspects are the targets of police investigation; that, is an essentially epistemic activity in part constitutive of policing. By

contrast, combatants are not investigators, even if at times they need to determine whether or not a person presenting as an innocent civilian is in fact a combatant. This threefold distinction in policing cuts across the combatant/non-combatant distinction. For instance, combatants are not necessarily suspected of crimes or offenders and neither suspects nor offenders are necessarily combatants. What of national security intelligence officers?

As we have seen, the targets of intelligence officers can be willing or unwilling providers of intelligence (let us take a willing provider to be someone who has consented to provide information). Moreover, those who are willing might be individually contacted or the information they willingly provide (in effect) might already be publicly available. Those who unwillingly provide intelligence might do so without knowing they have done so, for example as a result of a surveillance operation or an undercover operative who deceives them, or they might do so knowingly, for example as a result of a coercive interrogation. Moreover, the “providers” of intelligence might have had the intelligence stolen from them by a field officer, for example a spy. Note that some publicly available information might, nevertheless, not have been willingly provided to intelligence officers, for example some information regarding an adult might be posted on social media by his naïve adolescent daughter who is unaware that it might be accessed by and of interest to intelligence officers.

An additional important point to be made here is that whereas each single item of an integrated body of information might have been willingly provided the aggregate of that information, once analyzed to create the integrated body of information, might not have been willingly or even knowingly provided. For instance, intelligence officers might construct a fairly detailed picture of the characteristics, behaviour and movements of an individual on the basis of multiple, single, incremental items of publicly available information, including information extracted from social media. An analogous, but more alarming, point can be made in relation to intelligence activity at the macro level and, indeed, at the institutional level. What if such detailed pictures can be constructed of most of the members of an entire population? Evidently, the Chinese state is aiming to do just this, notably in Xinjiang, and, thereby, displaying a *de facto* institutional purpose of its intelligence agencies: social control in the name of national security. It should be noted that this projected surveillance society (Chinese style) is to make use of a wide range of integrated databases of personal and public information much of which is not readily available to intelligence officers (or members of other security agencies) in liberal democracies.

The fundamental point to be made in the light of the earlier discussion is that the principle of discrimination* applicable to intelligence officers is only very loosely analogous to the principle of discrimination applicable to combatants and non-combatants, since the targets of intelligence officers could be virtually anyone (even if not everyone) and the moral constraints on their intelligence activity pertain more to the nature and extent of the intelligence being sought (e.g. is it the confidential or private information of large cohorts of people?) and the particular methods used to collect it, for example coercive interrogation, deception, intrusive surveillance or theft.

A final point regarding the principle of discrimination* (i.e. discrimination as it applies to intelligence activities) does pertain to the targets of intelligence officers. This point arises from differences between internal and external national security threats and it is, therefore, relevant not only to the micro level but also to the macro level. In liberal democracies at least, foreigners who are the targets of national security intelligence activities enjoy few – if any – protections and in this respect they are unlike fellow citizens who are the targets of national security intelligence activities. Yet, the innocent citizens of enemy authoritarian states have moral rights, including privacy rights (whatever their legal rights may be or, more likely, not be). On the other hand, it does seem that given the purpose of the intelligence activities in question is national security, it is perhaps 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 to foreigners than to fellow citizens.¹¹ We return to this issue in the final section.

Principle of necessity

As we saw in the introduction, the principle of necessity applies to both kinetic military and kinetic law enforcement activity and to epistemic intelligence activity, and does so at all three levels, that is the institutional, macro and micro levels. Thus, in respect of epistemic national security intelligence activity, it is necessary to, firstly, have a national security intelligence agency (institutional level), secondly, to spy on hostile enemy powers (macro level) and, thirdly, to intercept the communications of, for instance, Osama bin Laden's trusted courier in order to locate his leader (micro level).

Elsewhere I have provided an analysis of the principle of necessity (or, perhaps, principles of necessity) (Miller 2021) and one that differs from the standard account (Lazar 2012). According to my own analysis, the principle of necessity has at its core a means/end principle and the necessity in question refers to the necessary means to an end (whether it be the end of personal self-defence, or a military, law enforcement or national security intelligence end). Thus if the only available means to achieve an intelligence end is intrusive surveillance of a target then the necessity principle might require that this means be used, notwithstanding that it infringes the target's privacy. If, on the other hand, there was an alternative means, say, collecting the metadata from the target's phone then neither of these two methods would be a necessary means (although it would be necessary to choose one or other of these two methods if the end was to be realized).

However, there is a further factor in play. For it will be claimed that the means that ought to be relied on is metadata collection 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 realize some end it does not follow that it ought not to be chosen. After all, *ex hypothesi* neither of the two available means is a necessary means to achieve the end in question and it would be irrational not to choose any of the available means to one's ends. Clearly, the idea is that the less harmful means morally ought to be chosen. Metadata collection ought to be preferred to

intrusive surveillance since it is the less harmful means. Evidently, there is another end in play here; an end in addition to the end of acquiring intelligence. The end in question is the moral end to minimize harm, from which can be derived the moral principle to minimize harm to others. So the necessity principle is to be analyzed in terms of a core means/end principle and an implied harm minimization principle. Notice that the necessity principle in play in intelligence activity (the principle of necessity*) is different from the principle of military necessity (and from the principle of necessity applicable in law enforcement) by virtue of the different constitutive ends of the two principles: an epistemic end and a kinetic end (respectively). Since both of these constitutive ends are morally significant the principle of necessity and the principle of necessity* are moral principles twice over (given they are also moral principles by virtue of their implied harm minimization principle).

While epistemic actions, including intelligence activity, have knowledge as their constitutive end, kinetic actions, including military activity, do not; rather military activity has the end of winning battles (and, ultimately, wars). However, as we also saw, intelligence activities and kinetic military activities (and, also intelligence activities and kinetic law enforcement activities, respectively) stand in the relationship of knowledge to action; the decision to perform a kinetic action presupposes knowledge with respect to the why, how, what, when, where, who etc. of the kinetic action in question. Hence, intelligence collection is temporally and logically prior to the use of military force; intelligence collection is, for these reasons, the first resort. Moreover, the use of military force, unlike intelligence collection and analysis, is inherently extremely harmful; it involves killing people rather than merely coming to know things. Hence, the use of military force is a last resort – this time for moral reasons.

While obviously the principle of necessity* thus analyzed (as an amalgam of a core means/epistemic end principle and an implied harm minimization principle) is applicable to national security intelligence activities in some circumstances, a question arises as to the extent of this applicability; perhaps its applicability is actually quite limited, unlike the analogous principle of military necessity, for instance. Thus intelligence activities, including collection, might not be necessary to a strategic or operational end but might, nevertheless, be justified on some weaker basis, such as being potentially useful. A related point is that the intelligence value of some collected intelligence is not known prior to analysis of it; that is, at the point of collection the intelligence might only be believed to be potentially useful (and possibly true), but certainly not believed to be necessary. Again, under a policy of redundancy a number of informers might be deliberately cultivated in relation to some national security task only one, or at most two, of whom might be necessary, that is any one (or at most two) of the informers would be sufficient for the task. However, multiple informers might increase the likelihood that the intelligence collected was reliable. By contrast, it would be hard to justify shooting dead all the members of a large cohort of enemy combatants (let alone embarking on a war against another nation-state), on the grounds that while unnecessary it was potentially useful. So the applicability of the principle of

military necessity to military action is wide and strict whereas the applicability of the corresponding principle of necessity* to national security intelligence activities is much more limited and much less strict.

The width and strictness of the applicability of the principle of necessity to military action reflect the obvious fact, as mentioned earlier, that the means to achieve military ends, that is use of lethal force, are inherently extremely harmful, whereas the means to achieve epistemic ends, including epistemic national security intelligence ends, typically are not, or need not be. Of course, the realization of epistemic national security intelligence ends is the means to kinetic ends that can be inherently extremely harmful, for example war. However, in and of itself the proximate end state of successful epistemic national security intelligence activity is not harmful, even if the means to that end state are, for instance, violations of privacy, since this end state simply consists in intelligence officers (and those who receive their intelligence) being in a state of knowledge. Whether harm results from this knowledge depends on the decision makers who receive this knowledge from the intelligence officers, for example if these decision makers decide to go to war on the basis of the intelligence they have received. Accordingly, it is the decision makers, such as military leaders and politicians, who are directly morally responsible for the harm resulting from their decisions. On the other hand, the intelligence officers who provide them with the intelligence which informs their decisions bear a degree of indirect moral responsibility for the harms (as well as benefits) that result from these decisions. Indeed, in the case of avoidable great harm resulting from bad intelligence the relevant intelligence officers may well have a high degree of moral culpability [albeit in the context of being morally responsible jointly with the decision makers, i.e. there is collective responsibility (Miller 2016b)].

Notwithstanding the contrast with lethal force in theatres of war, the means used to achieve epistemic national security intelligence ends may well be somewhat, even very, harmful, for example coercive interrogation, and frequently involve infringement of privacy, confidentiality or informational property rights. Accordingly, it is important to consider the threshold at which the use of harmful methods and, in particular, methods involving privacy/confidentiality infringements/violations or information theft might justifiably be used to collect national security intelligence. The threshold at which discrete national security intelligence operations *at the micro level* can justifiably be conducted if, for example, they infringe some individual's privacy, confidentiality or property rights is somewhat unclear. It might be thought that the notion of reasonable suspicion could be invoked in relation to domestically focused national security intelligence operations, as it is invoked in relation to criminal investigations (a related essentially epistemic activity). However, intelligence collection cannot be expected to wait for reasonable suspicion; after all, it is often intelligence collection that generates reasonable suspicion. Accordingly, reasonable suspicion seems too high a threshold standard for intelligence collection to have to meet. Of course, intelligence collection which is restricted to information already in the public domain (or otherwise uncontroversially, justifiably accessible to security agencies, e.g. in the case files

of past investigations) can generate reasonable suspicion. However, this suggestion runs into the problem mentioned earlier of privacy/autonomy violations arising from the creation of detailed profiles of individuals based solely on publicly available information (in conjunction with other information uncontroversially, justifiably available to security agencies).

In the absence of a principle-based solution to this first threshold problem it is unclear where the line is to be drawn in relation to (at least) domestically focused national security intelligence collection. Moreover, it has implications for our question concerning the extent of the applicability of the principle of necessity* to national security intelligence activities. For a solution to the threshold problem would, in effect, place a prior constraint on national security intelligence collection such that even if the collection in question was reasonably judged to be necessary it might, nevertheless, not be morally (or legally, if the relevant law tracked morality) permissible. In this respect, the prior constraint would interact with the principle of necessity* in a way analogous to the way the principle of discrimination interacts with the principle of military necessity, that is combatants cannot deliberately kill innocent civilians, even if it is reasonably judged to be militarily necessary to do so.

There is a second related threshold problem, namely one with respect to the threshold at which national security-based bulk data collection and/or use *at the macro level* can justifiably be undertaken, given the potential for such collection/use to increase to the point where it compromises liberal democracy.¹² Consider in this connection the establishment of biometric databases and their integration with existing criminal justice, financial, health and so on databases (Miller and Smith 2021). Perhaps it can be justified in relation to bulk data pertaining to specific foreign powers who have by their hostile and other actions already met the threshold standard of reasonable suspicion. However, the creation of, or access to, such bulk data collections might be made difficult, if not impossible, by the foreign power in question. It is, presumably, far easier to create bulk data collections pertaining to one's own citizenry. However, doing so may lead to a power imbalance between the state and the citizenry that compromises liberal democracy. Accordingly, in the absence of a solution to this second threshold problem it is unclear where the line is to be drawn in relation to national security intelligence collection. On the other hand, a solution to this second threshold problem would, in effect, place a prior constraint on national security intelligence collection such that even if the collection in question was reasonably judged to be necessary (and not merely potentially useful) for national security ends, it might, nevertheless, not be morally (or legally, if the relevant law tracked morality) permissible.

Principle of proportionality

In national security intelligence activities, as in personal self-defence, law enforcement and waging war, the application of the principle of necessity* implies the application of the principle of proportionality (in the weighing of means against ends) or, at least, a principle of proportionality (principle of proportionality*);

and the application of the principle of proportionality* presupposes the application of the principle of discrimination*. Moreover, the implied principle of harm minimization is also in play.

On the one hand, harm in terms of privacy infringements, deception and theft of information (as opposed to, say, coercive interrogation) 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. On the other hand, the principle of proportionality* presupposes the provision of some moral weight to be accorded to national security (the ultimate end, we are assuming, of the activity) or, at least, to be accorded to the likely national security outcome that might result from the use of the intelligence to be collected, analyzed and disseminated. Hence the application of the principle of proportionality* presupposes the principle of necessity*. Here we should also note that inherent differences between epistemic action and kinetic action mentioned earlier infect the application of the principle of proportionality* as they did the application of the principle of necessity*. We saw earlier that the intelligence value of some collected intelligence is not known prior to analysis of it; that is, at the point of collection the intelligence might only be believed to be potentially useful (and possibly true), but certainly not believed to be necessary. Accordingly, it will be difficult at the point of collection to determine whether or not a harmful method, for example deception of an innocent person, necessary to collect the intelligence is disproportionately harmful.

As argued before, national security intelligence activity exists at both micro and macro levels. This has implications for the application of the principle of proportionality* (as we saw it had for the application of the principle of necessity*). Consider in this connection national security intelligence bulk data collection. At the micro level, the application of the principle of proportionality* (and of the principle of necessity* and of discrimination*) is on specific intelligence operations directed at particular targets, for example collecting information concerning the associates of a suspected terrorist. Thus, a question to be addressed might be: is intrusive surveillance proportionate? What of the macro level? Key ethical issues at the macro level pertain to proportionality of the establishment and general uses of the bulk databases themselves (Anderson 2016).

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 utilization of bulk data. Concerns in this area are somewhat allayed by the fact that the bulk data collected and analyzed is typically in an anonymized form (e.g. by means of machine learning techniques), and, therefore, only the privacy rights of genuine suspects are infringed (i.e. the individuals identified upon completion of the

analysis). However, these harms, such as the aforementioned power imbalance between citizens and the state arising from extensive privacy infringements by intelligence agencies, and a diminution in public trust as a consequence of the secret nature of national security intelligence activities, may be incremental in character and difficult to quantify.

Accordingly, an aspect of the aforementioned threshold problem comes into view. For it can be difficult to know exactly where to draw the line between proportionate and disproportionate intelligence activities when it comes to the utilization of bulk data for national security purposes. Consider in this connection the aforementioned potential utilization 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, in effect, the power imbalance already mentioned. More specifically, there is a threat to individual autonomy posed by comprehensive, integrated biometric and non-biometric databases utilized 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.

Espionage and the principle of reciprocity

Thus far I have provided an analysis 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. I have done so in the context of knowledge derived from evidence-based truth-seeking being the constitutive (proximate) normative end of national security intelligence activity and the fundamental normative institutional purpose of national security intelligence agencies. I now want to argue that there is an additional normative principle governing external national security intelligence activities (call it espionage), in particular; this is a principle of reciprocity. Since I have discussed this in detail elsewhere I will be brief.¹³

Intelligence gathering, surveillance and so on of citizens by domestic law enforcement agencies might be thought to be reasonably well defined and regulated; hence the *apparent* feasibility of simply extending the law enforcement model to national security intelligence collection within domestic jurisdictions. However, this domestic law enforcement model is clearly too restrictive, and not practicable, in relation to external national security intelligence gathering from, for example, hostile foreign states during peacetime, let alone wartime. So the question arises as to whether some different moral principle(s) needs to be invoked in relation to espionage, in particular. I argue that two principles of reciprocity need to be invoked: a retrospective and a prospective principle.¹⁴

The retrospective principle of reciprocity would justify nation-state, A, engaging in espionage against nation-state (or non-state actor), B, in circumstances in which B had engaged, or was engaging, in unjustifiable espionage on A, but only

if A's espionage was in the service of A's morally justifiable political purposes, namely, national security.

The prospective principle of reciprocity is a tit-for-tat principle in the service of bringing about a morally desirable future state of affairs. 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. 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, in this case, espionage and, thereby, move relevant nation-states into some form of a social contract.

On the one hand, the United States and its allies cannot be expected to defend their legitimate national interests with their hands tied behind their backs. So their recourse to espionage seems justified and the retrospective principle of reciprocity 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, I make 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.

Under existing arrangements the United States, the United Kingdom, 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 ought to make good on their claims to respect privacy 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, for example, 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, in so far as it is practicable, in ensuring compliance with some of the standard moral principles protecting privacy and confidentiality rights, such as probable cause/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.

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.

What of authoritarian states known to be supporting international terrorism and/or engaging in hostile covert political operations, including espionage and cyber-espionage, for example 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.¹⁵ 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

In this chapter I have framed intelligence activity as evidence-based truth-seeking epistemic activity (by contrast with, for instance, military activity or covert action), offered analyses of the key principles of discrimination, necessity and proportionality, and shown in general terms how they apply, or ought to apply, to national security intelligence activity. I have also introduced and analyzed a principle of reciprocity and argued that it needs to be introduced to govern espionage, in particular.

Notes

- 1 I use these terms more or less interchangeably in this chapter, although distinctions are sometimes made (Alexandra and Miller 2009).
- 2 See *National Security Strategy of the United States of America*, 2017, p. 4 “Second, we will *promote American prosperity*. We will rejuvenate the American economy for the benefit of American workers and companies”, available at www.hsdl.org/?view&did=806478.
- 3 Or at least I assume that many, if not most, academics believe this. More specifically, I assume that most academics believe that intellectual work in universities is an end-in-itself *and* that it is in the service of further ends, for example. community well-being.
- 4 This point relates to the so-called intelligence cycle. See, for instance, Hulnick (2006).
- 5 See, for instance Walzer (2015).

- 6 See Mark Phythian in Omand and Phythian (2018, 85) for this kind of point and David Omand in same (91–2) for a response to it.
- 7 See, for instance, Walzer (2015).
- 8 See, for instance, Bellaby (2014), Quinlan (2007) and Omand and Phythian (2018, chap. 3).
- 9 There are various different versions and interpretations of the legal and moral principle of discrimination and, for that matter, of the legal and moral principles of precaution, necessity and proportionality. My concern is with these principles understood as *contested* moral principles. Accordingly, I take myself to have a significant degree of licence in formulating these principles.
- 10 See, for instance, Sorell (2018).
- 11 See, for instance, Miller (2009).
- 12 See Macnish (2017, Chap. 5) for an account of the ethical issues in this area.
- 13 An earlier version of this section appeared in Miller (2016a).
- 14 Reciprocity-based principles are related to, but distinct from, consent-based principles. In relation to the latter applied to espionage, see Pfaff and Tiel (2004).
- 15 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, for example China's cyber-theft operations. For reasons of space I cannot pursue these here.

References

- Alexandra, Andrew, and Seumus Miller. 2009. *Ethics in Practice: Moral Theory and the Profession*. 1st edition. Sydney: University of New South Wales Press.
- Anderson, David. 2016. *Report of the Bulk Powers Review*. London: HMSO. <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>.
- Bellaby, Ross W. 2014. *The Ethics of Intelligence: A New Framework*. 1st edition. London; New York: Routledge.
- Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1997. *Security: A New Framework for Analysis*. 1st edition. Boulder, CO: Lynne Rienner Publishers.
- Green, Leslie C. 1993. *The Contemporary Law of Armed Conflict*. Manchester; Canada: Manchester University Press.
- Hulnick, Arthur S. 2006. "What's Wrong with the Intelligence Cycle". *Intelligence and National Security* 21 (6): 959–79. <https://doi.org/10.1080/02684520601046291>.
- Lazar, Seth. 2012. "Necessity in Self-Defense and War". *Philosophy & Public Affairs* 40 (1): 3–44. <https://doi.org/10.1111/j.1088-4963.2012.01214.x>.
- Macnish, Kevin. 2017. *The Ethics of Surveillance: An Introduction*. 1st edition. London; New York: Routledge.
- McDonald, Matt. 2008. "Securitization and the Construction of Security". *European Journal of International Relations* 14 (4): 563–87. <https://doi.org/10.1177/1354066108097553>.
- Miller, Seumas. 2009. *Terrorism and Counter-Terrorism: Ethics and Liberal Democracy*. Blackwell. <https://doi.org/10.1002/9781444302837.ch4>.
- . 2010. *The Moral Foundations of Social Institutions: A Philosophical Study*. Cambridge; New York: Cambridge University Press.
- . 2016a. "Cyberattacks and 'Dirty Hands': Cyberwar, Cybercrime, or Covert Political Action?" In *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley J. Strawser, 228–50. New York: Oxford University Press.

www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190221072.001.0001/acprof-9780190221072.

- . 2016b. *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*. New York: Oxford University Press.
- . 2021. “Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis”. *Social Epistemology* 35.
- Miller, Seumas, and John Blackler. 2016. *Ethical Issues in Policing*. 1st edition. London: Routledge.
- Miller, Seumas, and Marcus Smith. 2021. *Biometrics, Ethics and Law*. Dordrecht: Springer.
- Omand, David, and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Washington, DC: Georgetown University Press.
- Pfaff, Tony, and Jeffrey R. Tiel. 2004. “The Ethics of Espionage”. *Journal of Military Ethics* 3 (1): 1–15. <https://doi.org/10.1080/15027570310004447>.
- Quinlan, Michael. 2007. “Just Intelligence: Prolegomena to an Ethical Theory”. *Intelligence and National Security* 22 (1): 1–13. <https://doi.org/10.1080/02684520701200715>.
- Sorell, Tom. 2018. “Bulk Collection, Intrusion and Domination”. In *Philosophy and Public Policy*, edited by Andrew I. Cohen, 39–60. London; New York: Rowman & Littlefield Publishers.
- Walzer, Michael. 2015. *Just and Unjust Wars*. 5th edition. New York: Basic Books.
- Williams, Michael C. 2003. “Words, Images, Enemies: Securitization and International Politics”. *International Studies Quarterly* 47 (4): 511–31.

3 The technoethics of contemporary intelligence practice

A framework for analysis

David Omand and Mark Phythian

Introduction

Intelligence agencies have a history of rapid exploitation of the latest scientific and technological advances, from the electric telegraph to radio transmissions and satellite observation. As with warfare, the history of intelligence can be told in terms of the relative advantage bestowed by a series of technological innovations (McNeill 1983; Warner 2014). This historically close relationship between intelligence and technology marks out intelligence as a sphere of activity where issues of “technoethics”¹ – of the way in which technological developments impact on the nature of ethical frameworks and judgements and the inter-relationship between the two – are prevalent. The digitization of information of all kinds is the latest field of technological innovation to generate ethical dilemmas for intelligence practice. Some of the ethical issues raised by intelligence use of digital information are simply modern forms of age-old dilemmas now being shaped by new technologies, such as judging when invasions of privacy are justified. Others arise *because* of the development of digital technology itself, such as the application of Artificial Intelligence (AI) algorithms to enable facial recognition or the placing of malware on a target computer network. Taken together, these questions about the ethics of using digital technology for intelligence purposes call for a specific examination of “technoethics”, drawing where relevant on the ethical guidance available from other disciplines such as for the safe use of advanced medical devices and artificial intelligence algorithms.

In this chapter our focus is on the ethical challenges posed by the still rapidly developing sphere of digital intelligence. Indeed, so pervasive are the challenges it poses that, as we emphasize in this chapter, it is increasingly misleading to approach it as a discrete sphere of activity. It proceeds as follows: we begin by recalling the fundamental origin of the ethical concerns over intelligence activity and set out the ethical principles that we have derived in our previous work from the Just War tradition (Omand and Phythian 2018). We then discuss the contemporary landscape of intelligence technoethics, followed by a proposed framework for thinking about the technoethics of intelligence, using *jus in intelligentia* concepts and focusing on the importance of norm development, and the requirements for effective norm development, in this area.

An ethical framework for secret intelligence

States invest in intelligence and data collection to provide a sound basis for their decisions, especially regarding the security, safety and health of their citizens. Much of the information needed to protect the public can come from open sources. But there are threats emanating from beyond and within national borders from malign actors (hostile states, terrorists, cyber criminals and their ilk) who are determined to conceal their capabilities and intentions and to expose them requires secret intelligence (Omand and Phythian 2018, chap. 1). The means by which states, via investment in intrusive information gathering, seek to protect against such threats and protect their interests more widely, including from natural hazards, can create tensions in relation to liberal principles. Consequently, there is a strong case for accepting that intrusive data gathering and secret intelligence, if judged necessary, requires a code of ethics different from that we would want to regulate everyday conduct in a liberal democracy.

This is because, fundamentally, espionage is about acquiring secrets held by another (“stealing secrets”) in conditions where the person with the secret may go to extreme and often violent means to prevent their secrets being compromised. Having to overcome the determined will of the person with the secret takes us into behaviours that could never satisfy the kind of ethical threshold mandated by Kantian ethics. Using people as means to an end, subverting them from their duty in order that they spy on your behalf, intruding on personal privacy and employing deceptive practices are the essence of intelligence tradecraft. Only preventing serious harm to others can morally justify such methods. However, there are sufficient serious threats facing the democracies to provide the justification.

Yet, the exercise of secret intelligence activity in liberal democracies cannot be without ethical and legal constraints. Rather like the technologist in Mario Bunge’s mid-1970s outline of a “technoethics”, the intelligence professional in the liberal state is caught between conflicting demands that cannot necessarily be pursued independently of each other but need to be balanced (Bunge 1977, 98).² The professional cannot slough off ethical responsibility onto the policy maker just as the technologist cannot simply hide behind the user of the technology. A case can be made for seeing basic science as value-neutral but its technological application is a human-directed activity and the developers of technology need to be aware of how their innovations may be used for ill as well as good. But how should liberal democracies arrive at ethical guidelines that govern intelligence practice? How should they seek to arrive at this balance? One solution to this knotty problem is to look to draw parallels with the development over the centuries, under the Just War tradition, of ways to constrain the conditions under which states may go to war (*jus ad bellum*) and the conduct of their armed forces when so engaged (*jus in bello*). If the application of the extreme violence of armed conflict can be constrained by an ethically based code then on the legal principle of *omne majus continet in se minus* it should be possible to envisage ethical limitations on secret intelligence activity – a *jus ad intelligentiam* informed by thinking in terms of *jus ad bellum* and a *jus in intelligentia* based on thinking around principles of *jus in bello*. This

is not to say that thinking in terms of parallels can offer neat or simple solutions to dilemmas concerning intelligence practice in liberal democracies – any assumption that it could offer anything approaching a tick-box solution would be counter-productive – but it does offer the best available set of concepts for thinking about the ethics of intelligence, one that can be universally applied as states anticipate and address the challenges they will inevitably face. On this basis, in our earlier work we derived such a set of *jus in intelligentia* concepts that we believe can be of use in reaching ethical judgements about the conduct of intelligence activity, including the use of advanced technologies, by the security and intelligence authorities of liberal democratic states (Omand and Phythian 2018, chap. 3):

- **right intention** – acting with integrity and having no ulterior motive or other agenda behind the authorization of intelligence activity or in analysis, assessment and the presentation of intelligence judgements to decision makers
- **proportionality** – ensuring that the ethical risks of operations are in line with the harm that the operations are intended to prevent
- **right authority** – establishing the level appropriate to the ethical risks that may be run and that will then allow for accountability for decisions and oversight of the process
- **reasonable prospect of success** – having adequate justification for the expectation that conducting individual operations will be likely to deliver results of value, given the ethical risks associated with them, including risks to agents and their families
- **discrimination** – having the ability to assess and manage the risk of unintended (collateral) harm, such as privacy intrusion into the lives of those who are not the intended targets of intelligence gathering
- **necessity** – there being no other reasonable way to achieve the authorized mission at lesser ethical risk

Later in this chapter we illustrate the use of these principles as applied to ethical issues arising from the use of digital technology by intelligence agencies.

The technoethics of intelligence: the impact of digitization and the internet

Digitization is the conversion of any form of information into numerical form (usually, but not necessarily, expressed in binary code). Speech and sound, visual images (still and moving), geolocation, text, radar and other electromagnetic radiation, DNA, patterns and logical structures text, and much else by way of information available in analogue form can all be accurately rendered as strings of numbers. Having information held as digital data has great economic and practical advantages:

- Large volumes of numerical data can be moved cheaply in bulk over any distance and terrain (and across oceans), for example by fibre-optic cables, microwave links and satellite links.

- Public key encryption can provide strong end-to-end security for data in motion without effort by the user (thus enabling digital commerce and financial transactions).
- The internet provides a (permissionless) ability to link computer networks together using open protocols, and thus provides global connectivity. The World Wide Web internet carries provide easy access to data in user-friendly formats, one example social media.
- Personal smart mobile devices are now cheap and very powerful, and 5G networks will allow high bandwidth, low latency and connectivity even on the move.
- Digital data can be stored at reasonable cost, with data science developed to provide powerful ways of searching and data mining very large data sets (without needing to structure data with fields defined in advance).
- Machine learning systems and advanced AI algorithms can be used to carry out classification tasks, increasingly more accurately than even trained humans, for example in detecting malign tumours, operating passport facial recognition systems at borders or spotting anomalous behaviour in a computer network.
- The Internet of Things enables everyday household and personal devices (including sports and personal health technology) to be internet connected. Digital cities increasingly have internet-connected infrastructure for congestion charging, traffic light control, water and energy metering and telecoms systems.

These developments have provided exploitable characteristics of interest to national security and intelligence agencies. Given the nature of the international system these exploitable characteristics constitute both opportunities and vulnerabilities. Alex Younger drew attention to these in a rare speech by a serving Chief of the Secret Intelligence Service (SIS, or MI6), delivered at the University of St. Andrews in December 2018, when he set out how we are now, “in the early stages of a fourth industrial revolution that will further blur the lines between the physical, the digital and biological realms” and that he had seen the

damage new technologies can do in the hands of a skilled opponent unrestrained by any notion of law or morality, as well as the potentially existential challenge the data age poses to the traditional operating methods of a secret intelligence agency.

This meant, for Younger, that “We and our allies face a battle to make sure technology works to our advantage, not to that of our opponents” (Younger 2018). We can identify eight core dimensions of the fundamental problem this gives rise to:

- 1 **access to bulk data** – defined as mining a large volume of data containing information almost all of which is known not to be relevant to an intelligence requirement or investigation. Unlike with the rented telephone lines of past

eras the internet works on packet switched networks where the individual packets that make up any form of communication may be directed automatically on different global paths dependent on cost at that instant. Access to bulk traffic nevertheless provides an opportunity to discover who was calling whom, when, where and how (communications data), or to try to gain access to specific communications of interest (communications content).

- 2 **network exploitation** – the lengthy and complex code used in computer operating systems and applications inevitably contains mistakes and weaknesses that can be discovered and exploited to gain access to networks, machines and communications (including so-called zero-day exploits).
- 3 **attribution** – anonymity is hard wired into the internet protocols, making it difficult for security services and law enforcement to definitively attribute harmful material on the internet, including disinformation, racial and personal abuse and criminal attacks, sabotage and foreign subversion via information operations.
- 4 **data sabotage** – the global nature of the internet allows remote attacks for intelligence gathering and for sabotage, including contaminating and denying stored digital data. Software and some hardware components can if accessed be corrupted covertly or denied to users.
- 5 **criminal ransomware** – ransomware malware attacks demand payment to criminals to restore access. Constraints of space and time no longer hinder the scale of such hostile activity – attacks can arrive against multiple targets in many countries at near the speed of light from jurisdictions that will not cooperate with law enforcement investigations.
- 6 **critical infrastructure vulnerability** – the digital control systems and software that operate almost all critical national infrastructure such as power generation, water supply, manufacturing and logistics, as well as finance, are all vulnerable to cyberattack.
- 7 the **business model of the internet** involves capturing the personal data and internet browsing history of individuals and exploiting this data for marketing purposes – so-called surveillance capitalism (Zuboff 2019). Such “ad tech” involves real-time auctions of space for advertising according to the desired characteristics of the intended viewer, including from targeting their personal data and internet browsing history. Ad tech similarly allows the targeting of personalized political marketing as well as of commercial products and services.
- 8 the **spread of social media** and its use as the main source of information for younger generations creates vulnerabilities for democracies in the face of intimidatory posts, fake news, manipulative marketing and weaponized information.

Hence, while digitization brings significant benefits to society it also facilitates threats from hostile intelligence agencies and sub-state criminal entities. This no more than reflects the contemporary reality that the same digital tools are available to all advanced states, and increasingly to non-state groups. These tools also

provide equivalent opportunities for the security and intelligence agencies of liberal democracies to pose the same types of threat as they face and experience from other states in the international system. This is the landscape of the modern digital battlefield where *jus in intelligentia* rules are needed.

One characteristic of this landscape is its complexity which has washed away notions of binary divides that traditionally acted as organizing principles in thinking about security challenges. As Younger explained in December 2018:

This complexity has eroded the boundaries we have traditionally relied upon for our security: the boundaries between virtual and real, the domestic and the international, between states and non-state actors and between war and peace. The result is a world of far greater ambiguity.

(Younger 2018)

Neither are notions of security simply about state behaviour and the actions of non-state actors. Yet even when they are not, this complexity remains a defining characteristic, mandating, potentially, multiple roles for intelligence agencies which serve to emphasize the technoethical dimension of contemporary intelligence work.

The example of the COVID-19 pandemic illustrates this well. Modern digital surveillance, including the use of apps on mobile devices and monitoring of digital personal information, has provided health authorities in nations such as South Korea, Singapore and China the public health benefit of powerful tools for assisting in testing and tracking programmes limiting the spread of the virus. For a virus in a globalized world national borders are no longer significant barriers but the unit of account for political decision-making is still the nation-state.

This takes us to the health-security interface. As a number of observers have noted, there are parallels that can be drawn between intelligence analysis and medical diagnosis, giving rise to a space in which mutual learning can take place.³ As we discuss later, we can usefully extend this thinking to cover parallels in intelligence and medical ethics. However, COVID-19 also illustrates three further things around this interface. First, it illustrates well how notions of national security intelligence are in the process of being adapted and how the shift from the Secret State of the Cold War era to the Protecting State of the twenty-first century continues apace (Omand 2010, chap. 1).⁴ National security is increasingly recognized as having a public safety and health dimension, and the COVID-19 pandemic has acted as a catalyst in advancing this recognition. At the same time, the COVID-19 crisis contains a more traditional challenge for western intelligence agencies – preventing others from stealing COVID-19 vaccine secrets (Philp 2020).

Second, the case of COVID-19 illustrates the nature of a modern “infodemic” with the internet and social media rapidly spreading disinformation about (worthless) treatments for the disease or for preventing infection, including the alleged healing powers of hairdryers and malaria medicines (Jankowicz and Otis 2020). COVID-19 also illustrates the deliberate use of social media by foreign states to

spread conspiracy stories, in this case about the origin of the outbreak with both Russia and China in different ways pushing the story that a US military laboratory was the source. This phenomenon in turn poses questions about how targeted states should respond and what role, if any, intelligence agencies should have in this. As Josep Borrell, the High Commissioner of the European Commission, warned in June 2020:

Disinformation in times of the coronavirus can kill. We have a duty to protect our citizens by making them aware of false information, and expose the actors responsible for engaging in such practices. In today's technology-driven world, where warriors wield keyboards rather than swords and targeted influence operations and disinformation campaigns are a recognised weapon of state and non-state actors, the European Union is increasing its activities and capacities in this fight.

(European Commission 2020)⁵

The ease with which digital disinformation can be deliberately constructed and targeted at specific groups is itself a direct threat to democracy when coupled to the increasing susceptibility of the public to digital manipulation. We have evidence, not least from the 2016 US Presidential election, of a readiness uncritically to recirculate realistic fakes, hoaxes and lurid exaggerations. In future we can expect to see more hyper-partisan populist views and conspiracy laden arguments on social media. Accompanying those trends will be a further decline in the intellectual standards of political argument, a coarsening of debate, a failure to defend scientific reasoning and an unwillingness to apply evidence properly to policymaking. Voter cynicism about the motives of politicians and resulting low election turnout are likely consequences (Omand 2020, chap. 11).

Finally, the COVID-19 pandemic also illustrates well how the technoethics of intelligence can trigger liberal democratic concerns over privacy in a domestic context. The National Cyber Security Centre, a part of the Government Communications Headquarters (GCHQ), was involved in the design of the government's planned contact tracing app, assisting NHSX, the technology and digital branch of the National Health Service. GCHQ has long had the responsibility for being the technical authority for the cryptographic security of sensitive national systems. However, while United Kingdom (UK) citizens were keen to accept governmental intervention in the form of pandemic Keynesianism in the economic sphere, some were less enthusiastic about the prospect of comprehensive government health monitoring in the form of a centralized model track and trace app.⁶ Hence, alongside the more pronounced concerns over the potential for the Chinese state to use the COVID-19 crisis as an opportunity to increase surveillance of its citizens, some privacy and security experts in the UK warned of the risk of hackers accessing personal data and of domestic slippery slopes and "Orwellian overtones" (Naughton 2020a). Concerns about the possible consequences of acquiescing in the creation of the "Coronopticon" co-exist alongside recognition of the obvious health benefits of interventions aimed at tracking (*The Economist* 2020).

Such apps to be effective require use by a significant proportion of the public and that level of uptake depends crucially on trust that the authorities will safeguard personal data from hackers and only use the information to be accessed for the stated purpose (Hart et al. 2020).

Meeting the challenges posed by the contemporary technoethics of intelligence

Hence, the COVID-19 global emergency illustrates well the importance of state agencies operating in the digital sphere in order to protect intellectual property, prevent the unchallenged spread of misinformation and collect data on individual exposure to the virus that can allow for interventions intended to limit the spread of the disease. At the same time, it also illustrates how such interventions can give rise to privacy concerns. In thinking about how to balance these competing demands, principles adopted from Just War thinking can make an important contribution. After all, as Danielle Allen and her colleagues note, there are core parallels in the war and pandemic contexts for liberal democratic states:

In both situations, the goal is to defeat the adversary with minimal loss of life and minimal damage to the material supports of a healthy economy and society, without perpetrating injustice, and while also pursuing defeat of the adversary in a way that both lays a foundation for a transition back to a peace-time setting and preserves the polity's political institutions to a maximal extent throughout the crisis and with a view to perpetual sustainability. That is, the goal is not to defeat the adversary at any cost but to preserve one's society, including preserving it as the kind of society it is.

(Allen et al. 2020)⁷

The Just War-derived ethical concepts listed earlier can be used to help unpack the ethical challenges that arise (Omand and Phythian 2018, 79–83).⁸

Right intention and integrity of motive

Right intention and integrity of motive on the part of those initiating, authorizing and conducting operations. The principle of right intention does not rule out deception in the course of an intelligence operation, such as inserting into the digital code of malware clues that attempt to encourage a false-flag attribution to a third country. But there must be no deception of government or Parliamentary oversight, or hidden domestic political or personal agendas lying behind the authorization or the conduct of digital intelligence activity. In the only recorded UK instance of such conduct, a GCHQ employee who deliberately undertook a number of unauthorized digital searches on an individual was sacked on the spot (Norton-Taylor 2015). In line with this approach, the analysis, assessment and presentation of the case for authorization to the relevant executive and judicial decision makers must be scrupulously honest, for example about estimates

of collateral intrusion or other unintended consequences. Public confidence in government's use of digital intelligence technology depends upon upholding this principle.

We can see in this a key difference between intelligence ethics and medical ethics. A key demand of medical ethics is transparency over the risks of any medical procedure linked to the giving of specific informed consent by the patient. This is not possible in the world of secret intelligence – for example, for the individual citizen whose personal data is to be accessed in the course of intrusive surveillance – without vitiating the intelligence gathering operation. Consent has therefore to be given not individually but collectively through Parliamentary regulation following as transparent a debate as possible given legitimate security concerns and with the added protection of informed scrutiny via external oversight.

Similarly, it is an accepted principle in medical research that drug and treatment trials require independent ethical approval and the informed consent of those taking part, and the same is true for academic research involving individual participants. The intelligence agencies also need to research and trial their innovations and new procedures for accessing and mining data (on which they depend to keep one step ahead of their targets), but they have to conduct this activity in secret. Proposals for major trials should nevertheless be subject to independent scrutiny by the senior judge acting as the Investigatory Powers Commissioner to ensure that the proportionality and necessity tests are satisfied, thus protecting the interests of the individual data owners whose information is to be accessed. The Edward Snowden leaks exposed a 2002 case in which GCHQ conducted a major trial (in the end unsuccessful) of a new system for scraping still images from bulk data (Optic Nerve) (Ackerman and Ball 2014). The subsequent controversy added to the case for updating legislation to take account of digital technology and for strengthening oversight arrangements, now in place via the UK's 2016 Investigatory Powers Act.

Proportionality of means in relation to the ends to be secured

Assessing proportionality has to be done by carrying out a balancing exercise in which the risks of intelligence operations – the potential for unintended harm to others – are set against the anticipated harms to the public that they are designed to avert; for example, the access to bulk data containing the communications of those not the subject of investigation set against the threat to life and property averted by uncovering a terrorist attack plot. Such proportionality judgements involve weighing up many kinds of uncertainty, for which the UK Courts have been willing to allow “a margin of appreciation” for the decisions taken by the security and intelligence agencies (Anderson 2014, 76).

There is also an element of counter-factual thinking involved in such balancing when it comes to authorization of an operation since *not* conducting the operation also involves potential ethical risk. As John Stuart Mill pointed out in the mid-nineteenth century: “A person may cause evil to others not only by his actions but by his inaction, and in either case he is justly accountable to them for the

injury” (Mill 1869, chap. 1). This principle is well established in medical ethics, for example in the balancing act that a clinical team may have to make in intervening in medical emergencies in childbirth or following major accidents. Another example of proportionality judgement is in the licensing of new drugs and therapies where the expected benefits to a large number of sufferers from a disease have to be balanced against the risks of adverse side effects for a small number of patients and how far that can be mitigated by training of clinicians and warning leaflets with prescriptions.

Right authority for intelligence activity

“Right” in the secret intelligence context means both that the go-ahead is given by someone who has the authority to give it under rights-compliant law and that the decision is taken at a senior enough level appropriate to the ethical risks that may be run (an important consideration in ensuring that the activity is not “arbitrary” in the words of the UN Universal Human Rights Declaration). In general, the more sensitive the operation the more senior should be the authorizer. Under the UK Investigatory Powers Act 2016, for example, warrants to allow intelligence access by using digital bulk data must be signed by the Secretary of State and then judicially reviewed and counter-signed by a senior judge acting as a Commissioner under the terms of the Act. Authority to access communications data (considered less inherently sensitive than the content of communications) may under the Act be authorized by a designated independent senior officer working for the judicial Commissioner. In addition, since the 1950s there has been a standing instruction from the Foreign Secretary to the UK agencies that any operation that is contemplated, whether domestic or foreign, that could have an impact on foreign policy must be cleared by the Secretary of State or a senior official in the Foreign Office. Such a system ensures that there is an audit trail of who agreed to what. Public confidence issues quickly arise if that is not the case, as was exposed during inquiries into British Army covert intelligence gathering in the Northern Ireland conflict in the period of the 1970s and 1980s before legislation was introduced.⁹

A different application of this key concept comes in the regulation of the use in intelligence and security activity of AI algorithms to categorize data. If such a machine learning system makes a wrong determination about an individual which results in an injustice, such as placing the innocent person on a no-fly list or providing targeting data for a direct intervention, who is to be held accountable – the coder who wrote the algorithm, the senior responsible owner of the decision system in which it was embedded, the senior line manager or minister who authorized the policy for its use for that purpose? With the most advanced AI algorithms it may be hard to establish an audit trail of how the selection system arrived at its result in any particular case. An evolutionary machine learning process can result in the machine being able to select desired characteristics from bulk data without conscious programming of decision rules. There is a heavy ethical responsibility on the technologists designing machine learning systems to ensure that the users

can fully understand the implications of using such systems. The ethics of managing AI accountability in such circumstances (such as driverless vehicle accidents) is an issue going way beyond the realms of security and intelligence activity. However, at present there is no satisfactory ethical code for AI applications that is internationally accepted.

A reasonable prospect of success in achieving the desired ends from the activity

Originally, as part of the Just War tradition, this was an injunction against operations such as vainglorious cavalry charges that needlessly expose the forces involved to extreme danger. In the intelligence context this principle can be said to rule out activity where there is no justification for taking significant ethical risk, for example in “fishing expeditions” that involve engaging the privacy rights of many innocent people with no clear idea in mind as to what is being sought. When intelligence agencies access data in bulk, by definition the majority of individuals contained within the data set are not, and are unlikely to become, of interest to the Security and Intelligence Agencies in the exercise of their statutory functions (Home Office 2016). It is the problem of the haystack and the needle. There needs therefore to be a reasonable belief, on the basis of past experience or specific research, that there can be an expectation of sufficient effectiveness to justify the level of risk being run by the operation. For example, in the case of bulk access to communications data, the application of some filtering or other targeting or selection mechanism has an acceptable likelihood of pulling out for the analyst material that is relevant to an authorized intelligence requirement. Applying this principle rules out “mass surveillance”, or keeping the communications of a large group of citizens under observation in the blind hope that something may turn up to justify the operation.

The effective application of an AI selector also depends on having the algorithm correctly exposed to data that is representative of the real situation. Ethically unacceptable cultural, racial or gender bias in selection decisions can result if the training data is narrowly compiled and does not reflect what will be found in practice. Such biases can be hard to spot (Ledford 2019).

Discrimination

Discrimination is needed to manage collateral harm, in the basic sense of the ability to see the difference between classes of things or people. In the laws of war that emerged from the Just War tradition the military commander faces, on the one hand, legitimate military targets and on the other hand groups of people that require protection such as innocent civilians not participating on the side of the adversary or surrendering soldiers. Before a new type of weapon is introduced into the battlefield there needs to be a legal assessment that the combination of weapon and operator is capable of discriminating between them. By analogy, when a new digital intelligence gathering method is introduced there needs to be

confidence that there will be the human and technical ability to assess and manage the risk of collateral harm, including the implications of privacy intrusion into the lives of those not intended to be the target of intelligence gathering.

Collateral intrusion has always been an issue with interception of fixed line telephones that capture the communications of all users in a home not just the targeted suspect. Bulk access operations have to be operated under clear ethical constraints to take account of the evident fact that almost all bulk data relates to those who are not and would never be the legitimate target of intelligence activity. Agencies must recognize that their privacy rights are engaged, right from the outset of planning such bulk operations, but with careful design of algorithms and procedures for destroying unexamined material after a set period that ethical risk can be managed down to an acceptable level applying the necessity and proportionality tests.

This principle also provides the basis for ethical oversight of the artificial intelligence algorithms that are increasingly being used to question large data sets. In any practical decision system (whether conducted by humans, by humans assisted by machine intelligence or by AI algorithms themselves) what is a reasonable prospect of success has to be defined, given that the possibility of error cannot be excluded. AI applications that have a low rate of false positives are said to have high specificity. Those with a low rate of false negatives have high sensitivity. Where the cursor is set between these will depend upon the consequences of getting it wrong either way. A no-fly security system can be expected to allow more false positives (preventing an innocent passenger from flying) in return for fewer false negatives (allowing a genuine terrorist suspect to board an aircraft). Key to achieving an acceptable balance of results is understanding what the true level of the decision factor is likely to be. For example, an antibody test for corona virus might have a 95% level of both specificity and sensitivity but despite these high levels, applied to a community of 500 people with a 5% infection rate an individual who tests positive only has a 50% chance of genuinely having the antibodies (Frasier 2020).

Necessity

Necessity is the final Just War-derived concept that can be used to judge the ethical adequacy of an operation. Is it really necessary to do this? Additional Protocol I to the 1949 Geneva Conventions applicable to armed conflict places a requirement on a military commander to be able to justify that an operation is a necessary part of achieving his military aim. There needs to be confidence that there is no reasonable alternative way to achieve the ends of the authorized mission at lesser ethical risk. That applies to intelligence activity, for example establishing that wanted information cannot be obtained more easily from open sources, or indeed already exists somewhere in the intelligence community. There are many databases of personal data relating to individuals that can be accessed with appropriate legal authority. Government examples include criminal records, passports and social security records, driving and vehicle licences, voting and

information gathered at the border. Private sector information includes airline bookings (and advanced passenger information shared between nations), credit card and financial data, on-line purchases and internet connection records and mobile telephone usage data. With the right legal authority under data protection legislation, however, such personal data can be accessed (under the European Convention on Human Rights/Human Rights Act 1999) for the purposes of national security, the detection and prevention of serious crime and for the protection of health.

These ethical concepts, especially necessity and proportionality, form a useful framework for *jus in intelligentia* in today's digital world. On the other hand, the *jus ad intelligentiam* to help judge the acceptability of digital intelligence capability itself is harder to pin down. We have to accept the primacy today of the nation-state in relation to the security of the citizen (e.g. as set out in article 4(2) of the Treaty of European Union) and nation-states will choose to maintain the means to defend themselves against digital threats and to be able to exploit to that end the digitized personal data that unavoidably is part of modern life. To that end intelligence activity is the first not the last resort. But the ethical injunction of necessity remains.

The ethics of being a cyber power: offensive cyber capabilities and deterrence in cyberspace

There is nevertheless considerable interest in international legal and diplomatic circles in the development of norms for responsible conduct in cyberspace that might if followed by the democracies eventually become part of accepted international law. Some norms, for example, might take the Geneva Convention's route and identify classes of potential targets to be protected, such as not targeting the core structures of the internet and not deliberately weakening the encryption on which key applications depend, including for financial systems and key protocols such as Secure Sockets Layer (SSL). International Human Rights Law is already considered by many states to apply in cyberspace (as per the Tallinn Manual drawn up by North Atlantic Treaty Organization experts) (Schmitt 2017). Domestic legal regulation and oversight measures can help the search for norms as examples of confidence building measures both for the domestic population and for international confidence in rules-based international order.

Espionage, including digital espionage, is however not regulated by international law, being regarded as "fair game" between nations, with the onus being on a nation to defend itself. Some espionage techniques could nevertheless open weaknesses in the "commons" of the internet and the difference between a digital espionage operation and a cyberattack could be only a few lines of code. Such considerations, along with the impossibility of adequate verification, seem to rule out an arms control approach to limiting hostile activity in cyberspace or to applying the approach of the Hague conventions on weaponry (such as restrictions on landmines) to prohibiting techniques that carry high risk of wider harm (such as seen in the spread of the Wannacry and NotPetya attacks).

Hence, developing norms for state behaviour in cyberspace is as challenging a prospect as it is an important task. However, there have been important recent interventions that represent significant early steps in what is likely to be a long, non-linear, endeavour.

On the basis of these, we can say that one essential foundation on which international norms must be built is robust and transparent national legislation regulating intrusive intelligence practice in the digital sphere. Another is the open and regular discussion of principles that should govern intelligence and security behaviour. There is clear potential for the second of these to act as a confidence-building measure by building on the foundation provided by the first; intelligence managers in liberal democratic states can act as norm entrepreneurs¹⁰ in this field but in doing so they are not operating in a vacuum but in a context underpinned by openly debated and clearly understood national legal frameworks. These give the interventions by intelligence managers much of their force as confidence-building measures.¹¹

A very good example of this process of norm development can be seen in the Fullerton Lecture given by GCHQ Director Jeremy Fleming in Singapore in February 2019, which was widely reported and made easily accessible in both text and video forms (Fleming 2019).¹² This addressed core issues related to being a Cyber Power: “What does it mean? What does a country need to have at its disposal to be a Cyber Power? How should it exercise that power? What rules, regulations and ethics are needed to exercise power responsibly?” (Fleming 2019). His answer was that a cyber power had the following three characteristics:

One, it has to be world class in safeguarding the cyber health of its citizens, businesses and institutions – it must protect the digital homeland.

Two, it has to have the legal, ethical and regulatory regimes to foster public trust – without which we do not have a licence to operate in cyber space.

And three, when the security of its citizens are threatened it has to have the ability – in extremis and in accordance with international law – to project cyber power to disrupt, deny or degrade.

(Fleming 2019)

Ethics and legality were not treated as synonymous, but as complementary requirements to be met that, together, could give confidence that cyber power was being used responsibly:

I’ve always liked the philosopher and scientist Aldo Leopold’s definition of ethics. He said it was about “doing the right thing even when no one else is watching”. Nowhere does that apply so much than in the world of national security. In spying, intelligence gathering, espionage – whatever term you’d like to use – I believe that there are ethical rules and boundaries, and these should always be followed and upheld.

Of course, the UK is a liberal democracy. There is extensive oversight of the work of the intelligence and security agencies. Someone else, typically a senior judge, is always watching over what we do.

It's perhaps easy to be ethical in such a situation – and in our democracies, sometimes we take that oversight for granted. Nonetheless, our analysts are constantly reminded that it is not enough to be able to do something . . . it is not even enough for it to be legal to do something . . . it must also be right to do something.

(Fleming 2019)

Here, then, the foundation of confidence lies in robust national legislation and oversight mechanisms onto which the emphasis on professional ethics in training and professional development added further assurance. One objection to this line of reasoning could be that these are simply words, that talk is cheap. But the words used are significant. The second characteristic of a cyber power identified by Fleming (earlier) was that the “legal, ethical and regulatory regimes” were in place that could “foster public trust”. Without these, “we do not have a licence to operate in cyber space”. Later in the speech, Fleming returned to this idea of “our licence to operate” which “enables us to retain the trust of the societies we serve”. Both of these terms reflected the titles of reports advocating significant reform of the regulatory regimes governing digital intelligence collection and interference in the wake of legal challenges following the Snowden disclosures and part of an extended period in the UK of public discussion of intelligence collection practices. The idea of a “licence to operate” comes from the title of a report from the Independent Surveillance Review, *A Democratic Licence to Operate*, published in July 2015, on which one of us (David Omand) served as a panel member (Independent Surveillance Review 2015). The reference to the importance of retaining trust recalls the title of the June 2015 report by David Anderson, QC, the Independent Reviewer of Terrorism Legislation, *A Question of Trust* (Anderson 2014). Both of these influenced the nature of the 2016 Investigatory Powers Act, the post-Snowden regulatory framework passed (by a large cross-party majority) for digital intelligence collection and use, one feature of which was enhanced oversight.

This act created a powerful Commissioner (a very senior judge), a new system of warrants for access to bulk data and an independent body to authorize law enforcement access to communications data and internet data connection records (the who called whom, when, where and how). It is this oversight capability that adds to confidence in interventions such as this by Jeremy Fleming. For example, the 2016 Investigatory Powers Act provided for the need for prior approval by Judicial Commissioners of warrants for the use of intrusive powers such as interception, equipment interference and the use of surveillance in sensitive environments. It also created the Investigatory Powers Commissioner's Office (IPCO) to consist of around 70 staff comprising 15 Judicial Commissioners (current and recently retired High Court, Court of Appeal and Supreme Court Judges), a Technical Advisory Panel of scientific experts and around 50 official staff, including lawyers and communications experts.

In its 2017 Annual Report, IPCO set out a particular interest in Section 7 Authorizations – those under Section 7 of the Intelligence Services Act 1994,

referring to activity that SIS and GCHQ carry out outside the British Islands where the authorization removes any liability under UK criminal or civil law for what is done. In the course of overseeing these, Sir John Goldring, the deputy IPC,

“conducted two inspections of GCHQ and SIS, in the spring and autumn of 2017, along with two of SIS’s overseas stations in early 2017 [and] separate inspections of the FCO as regards its work with SIS and GCHQ during the summer of 2017”, focusing on “the authorisation and review processes, and particularly whether the Foreign Secretary was provided with a proper understanding of the activity that would be sanctioned by the authorisation”.

(Investigatory Powers Commission 2019, para. 11.1–11.15)

Both of IPCO’s annual reports to date are detailed (131 and 141 pages-long respectively), publicly available, are clear about inspection methodology and set out errors and breaches in relation to warranting. In short, the oversight mechanism provides a firm basis for intelligence managers to build in discussing ethical approaches to cyber power and act as norm entrepreneurs.

Given all of this, when is it right for a cyber power to deploy its offensive cyber capability, “taking action online that has direct real-world effect” in Jeremy Fleming’s words? Here again we can see the utility of drawing on and adapting Just War precepts to guide our thinking. This is one area where we can clearly see the relevance of thinking in terms of an intelligence equivalent of *jus ad bellum*. Underpinning these considerations is the principle that there are boundaries of acceptable state behaviour in cyberspace (Fleming 2019) and that a core characteristic of the responsible cyber power is the way in which it uses that power in a manner that encourages other states to operate within these boundaries and in support of the rules-based international order. This contributes to the development of norms in this still rapidly developing sphere of activity. Where states seek to act outside these boundaries, the responsible cyber power can act to deter by attaching costs, both reputational and/or physical. In this sense, then, applying the notion of deterrence here means influencing others not to act in ways that harm us. There are a number of forms this approach can take, for example:

- working with other nations to expose adversary actions and intentions to criticism
- influencing via diplomacy and nudging, including with sanctions
- offering inducements, such as of a reset in relations with the option to withhold if unacceptable behaviour continues
- emphasizing mutual economic inter-dependence, *deterrence by entanglement* with the potential adversary, as Joseph Nye has called it (Nye 2017)¹³
- making ourselves a harder target and thus making life as difficult as we can for the attackers, exercising *deterrence by denial* of benefit to the aggressor, or at least affecting the cost-benefit calculations of the aggressor

- threatening consequences, including via the use of armed force or offensive cyber means, which provide the essence of *deterrence by punishment*

We could arrange these as a scale of D: from D minor, detection and exposure to disapproval, to discouragement, to deflection, to dissuasion and finally to D major, the formal structures of defence and deterrence found in NATO strategy. Digital intelligence aimed at understanding the capabilities and intentions of potential adversaries is at the heart of decisions about how best to deter potential threats, including through the development of offensive cyber capabilities, at three levels.

First, for armed forces, ours and those of potential adversaries, the digital is now a domain of warfare. Any future armed conflict is likely to involve the use of cyber weapons, just as in the recent past armed forces used electronic warfare. As noted earlier the use of any weapon system needs to be constrained by *jus in bello* ethical considerations, for example adherence to international humanitarian law and the Geneva Conventions. The development of such weapons inevitably involves significant prior intelligence gathering on the digital networks or capabilities that are the target of the system.

Second, many states are acquiring the capability to inflict highly damaging cyberattacks on national infrastructure, potentially causing death and damage that would be equivalent to a kinetic armed attack. For the UK and NATO allies it is important that potential adversaries understand that such “Article 5 level” attacks would engage the full weight of NATO’s defence and deterrence strategy. The Obama Administration warned in 2011 that it would

respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.

(BBC News 2011)

Aggressors must understand that the response to such attacks need not be confined to cyberspace.

But then we have the third level of everyday cyber threat, well below the threshold of armed attack, ranging from fraud to digital subversion of democracy, as seen during the 2016 US Presidential election campaign and described earlier. The acronym CESSPIT encapsulates this as: Crime, Espionage, Sabotage and Subversion perverting internet technology.

The CESSPIT activities below the threshold of armed attack are best managed as a whole of nation effort to reduce the risk to the citizen, including education of business and citizens to operate safely in the digital world. Active cyber defences can seek out and block malware, bad addresses and dodgy websites. Children can be taught critical thinking so that they are better equipped to detect deception, exaggeration and falsehood on-line.

We need to make life as difficult as possible for the attackers by penetrating and disrupting their networks to create difficulty and make attacks more costly in terms of effort. Such persistent engagement is a contribution to deterrence by denial. It could be described as *forward active dissuasion* (FAD), like having police officers on the streets. That contributes to reducing the risk but, like the threat of arrest for criminals, it will not stop them from trying to commit crime.

Conclusions

Intelligence officers are in ethical terms natural consequentialists, wishing to have the acceptability of their methods judged by their results, for example in terms of terrorist plots uncovered and frustrated. This principle underlies the requirement in the UK's 2016 Investigatory Powers Act for proportionality. There has to be a relationship between the ethical risks being run and the harms it is sought to prevent. The principle of necessity is also incorporated into the 2016 Act, that digital operations that involve an ethical risk (which the Act defines) need adequate justification. There is a moral obligation to consider whether the results might be obtained by a method (such as use of open sources) that carries lower ethical risk.

Some democratic societies, including the UK, have insisted on importing a deontological element into the consequentialist ethical approach of their agencies by constraining them to act in accordance with universal human rights, as laid down in the Council of Europe Convention on Human Rights and translated into UK domestic law by the 1999 Human Rights Act. That includes the absolute prohibition on obtaining information by torture and other unlawful interrogation methods. In relation to digital intelligence operations it also requires that balances be sought within the basket of human rights, especially over respecting privacy rights of citizens as well as their right to life and the enjoyment of property, and the protection of freedom of speech. There is also an aretaic, value ethics, element to the recruitment and training of intelligence officers to help them know the settings of their internal moral compasses. Taken together, drawing on these consequentialist, deontological and aretaic traditions, the UK intelligence and security agencies should be better able to demonstrate that their digital activity conforms to domestic law that itself is based on ethical principles that have commanded a significant cross-party majority in Parliament. As technologies continue to be developed, and exploited for intelligence purpose, that "licence to operate" will need to be revalidated and renewed.

The use of AI algorithms to identify individuals of interest and patterns of covert communication is now becoming commonplace. The ethical principle that must be met is that the computer algorithms being used are sufficiently discriminating so as to give an acceptable likelihood of picking out the sought-for communication and a lower risk of selecting irrelevant material. To achieve that there needs to be careful attention to prevent unconscious biases, for example where the data used to train the algorithms does not reflect the actual population of data to which the algorithms will be applied. The agency must therefore be confident that

filtering and selection processes are sufficiently discriminating so as to minimize the extent of invasion of privacy of the innocent.¹⁴

Being pro-active in defending the digital space brings with it legal and ethical issues. Advanced digital intelligence tools will be needed for defensive purposes. As with conventional weaponry, the same tools will be available to the authorities of the autocracies. What matters therefore is to have a system in the democracies of legal authorization, oversight and ethical regulation of the *purpose* for which the technology is to be applied. It is this sense of moral purpose, underpinned by the principle of restraint, that distinguishes the regulated activity of the intelligence agencies of liberal democracies from those of the autocracies.

Recent UK experience is that with greater transparency over the necessity for secret intelligence to prevent harms to the public and an evidence-based vigorous Parliamentary and public debate it is possible to arrive at a democratic consensus over how intelligence activity should be regulated under the law (Independent Surveillance Review 2015). The debate has enhanced public trust in the security and intelligence authorities, whilst the secret agencies and their law enforcement partners have been able to use these powers effectively. The UK Investigative Powers Act 2016 marked a new deal between the British intelligence communities in which a legal “licence to operate” is given for intrusive intelligence methods in return for enhanced ethical safeguards and oversight. Even since 2016, however, digital technology has continued to develop whilst the public has become much more sensitive to the use (and misuse) of their personal data. The long tradition of Just War thinking has provided a set of concepts such as right authority, proportionality and necessity that can be used to help manage the additional ethical risks that come with the application of digital technology and machine learning to the worlds of national intelligence, security and public safety. Offensive cyber capabilities expand the realm in which ethical guidelines need to be applied.

Here, we see again the “3 Rs” framework that defines liberal intelligence in operation: the rule of law; regulation and restraint (Omand and Phythian 2018, 225–39). The transparent **rule of law** which provides for robust **regulation**, evidence of which is made publicly available, forms the basis on which intelligence managers can act as norm entrepreneurs, shaping developments by emphasizing the expectations that surround the exercise of responsible cyber power and setting out principles around this that will guide their state’s and organization’s behaviour. These interventions also set out the costs that are likely to attach to unacceptable conduct in the digital sphere. Notwithstanding the clear exposition of the offensive potential inherent within the notion of a cyber power, and key to its deployment as a deterrent, this is an approach characterized by **restraint**.

Notes

- 1 This represents a revival of the term coined by the Argentinean philosopher of science Mario Bunge in the 1970s (Bunge 1977).
- 2 Bunge wrote of the Technologist being “Torn Between Conflicting Interests” and set out a scenario where:

- “M: The management expects an efficient and profitable plant.
 W: The workers expect satisfactory working conditions.
 N: The neighbors expect a pollution-free operation.
 T: The professional colleagues expect a technologically advanced design, execution and operation of the project.
 C: The consumers expect useful and reasonably priced goods”.

(Bunge 1977)

The possible parallels with the conflicting expectations that can attach to intelligence are obvious.

- 3 For example Marrin and Clemente (2005) and Marrin and Torres (2017).
- 4 On the health security dimension specifically, see Lentzos, Goodman, and Wilson (2020) and the other articles in that special issue on Health Security Intelligence.
- 5 See also Rankin (2020).
- 6 For example, Naughton (2020b) and Urwin and Wheeler (2020). For another perspective, see Foges (2020).
- 7 See also Allen (2020).
- 8 See also Omand and Phythian (2018, 79–83).
- 9 For example, the inquiries by Chief Constable John Stevens and by the Canadian Judge Peter Cory examined allegations of collusion between the British Army and Loyalist paramilitary groups, subsequently investigated in detail by Sir Desmond de Silva, who concluded in his inquiry published in 2012 that there was an absence of clear structures and guidelines to ensure accountability for the use and dissemination of intelligence and to ensure intelligence is not exploited illegally, had been (de Silva 2012).
- 10 The term comes from Sunstein (1996).
- 11 On norms and confidence-building measures in cyberspace (Broeders, Boeke, and Georgieva 2019).
- 12 A further good example is provided by Alex Younger’s December 2018 speech at St. Andrews University.
- 13 See also Mandel (2017).
- 14 The most detailed description of how this operates can be found in the Academy of Sciences report, *Bulk Collection of Signals Intelligence* (Board, Sciences, and Council 2015).

References

- Ackerman, Spencer, and James Ball. 2014. “Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ”. *The Guardian*, February 28. www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.
- Allen, Danielle. 2020. “America Needs to Be on a War Footing”. *Washington Post*, March 20. www.washingtonpost.com/opinions/2020/03/20/america-needs-be-war-footing/.
- Allen, Danielle, Lucas Stanczyk, I. Glenn Cohen, Carmel Shachar, Rajiv Sethi, Glen Weyl, and Rosa Brooks. 2020. *Securing Justice, Health, and Democracy against the COVID-19 Threat*. Cambridge, MA: Edmond J. Safra Center for Ethics, Harvard University.
- Anderson, David. 2014. *A Question of Trust: Report of the Investigatory Powers Review*. London: HMSO. www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review.
- BBC News. 2011. “US Pentagon to Treat Cyber-Attacks as ‘Acts of War’”. *BBC News*, June 1. www.bbc.com/news/world-us-canada-13614125.
- Board, Computer Science and Telecommunications, Division on Engineering and Physical Sciences, and National Research Council. 2015. *Bulk Collection of Signals Intelligence: Technical Options*. Washington: National Academies Press.

- Broeders, Dennis, Sergei Boeke, and Iliana Georgieva. 2019. *Foreign Intelligence in the Digital Age Navigating a State of 'Unpeace'*. The Hague: The Hague Program for Cyber Norms. www.thehaguecybern norms.nl/news-and-events-posts/policy-brief-foreign-intelligence-in-the-digital-age-navigating-a-state-of-unpeace.
- Bunge, Mario. 1977. "Towards a Technoethics". *The Monist* 60 (1): 96–107.
- European Commission. 2020. "Coronavirus: EU Strengthens Action to Tackle Disinformation". European Commission. June 10. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1006.
- Fleming, Jeremy. 2019. "Director's Speech on Cyber Power: As Delivered". March 29. www.gchq.gov.uk/speech/jeremy-fleming-fullerton-speech-singapore-2019.
- Foges, Clare. 2020. "We Need Big Brother to Beat This Virus". *The Times*, April 20. www.thetimes.co.uk/article/we-need-big-brother-to-beat-this-virus-5b0nj168r.
- Frasier, Sarah Lewin. 2020. "False Positive Alarm". *Scientific American*, 20 July 2020.
- Hart, Vi, Divya Siddarth, Bethan Cantrell, Lila Tretikov, Peter Eckersley, John Langford, Scott Leibrand, et al. 2020. *Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 While Mitigating Privacy Risks: COVID-19 Rapid Response Impact Initiative: White Paper 5*. Cambridge, MA: Edmond J. Safra Center for Ethics, Harvard University. <https://ethics.harvard.edu/outpacing-virus>.
- Home Office. 2018. "Security and Intelligence Agencies Retention and Use of Bulk Personal Databases. Code of Practice". https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.
- Independent Surveillance Review. 2015. *A Democratic Licence to Operate*. London: RUSI. https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf.
- Investigatory Powers Commission. 2019. *Annual Report 2017 HC 1780*. London: HMSO. www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190131.pdf.
- Jankowicz, Nina, and Cindy Otis. 2020. "Facebook Groups Are Destroying America". *Wired*, June 17. www.wired.com/story/facebook-groups-are-destroying-america/.
- Ledford, Heidi. 2019. "Millions of Black People Affected by Racial Bias in Health-Care Algorithms". *Nature* 574 (7780): 608–9. <https://doi.org/10.1038/d41586-019-03228-6>.
- Lentzos, Filippa, Michael S. Goodman, and James M. Wilson. 2020. "Health Security Intelligence: Engaging across Disciplines and Sectors". *Intelligence and National Security* 35 (4): 465–76. <https://doi.org/10.1080/02684527.2020.1750166>.
- Mandel, Robert. 2017. *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*. Illustrated edition. Washington, DC: Georgetown University Press.
- Marrin, Stephen, and Efren Torres. 2017. "Improving How to Think in Intelligence Analysis and Medicine". *Intelligence and National Security* 32 (5): 649–62. <https://doi.org/10.1080/02684527.2017.1311472>.
- Marrin, Stephen, and Jonathan D. Clemente. 2005. "Improving Intelligence Analysis by Looking to the Medical Profession". *International Journal of Intelligence and Counter-Intelligence* 18 (4): 707–29. <https://doi.org/10.1080/08850600590945434>.
- McNeill, William H. 1983. *The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000*. Oxford: Basil Blackwell.
- Mill, John Stuart. 1869. *On Liberty*. London: Longmans, Green, Reader and Dyer.

- Naughton, John. 2020a. "When Covid-19 Has Done with Us, What Will Be the New Normal?" *The Guardian*, April 18. www.theguardian.com/commentisfree/2020/apr/18/when-covid-19-has-done-with-us-what-will-be-the-new-normal.
- . 2020b. "Contact Apps Won't End Lockdown: But They Might Kill off Democracy". *The Guardian*, April 25. www.theguardian.com/commentisfree/2020/apr/25/contact-apps-wont-end-lockdown-but-they-might-kill-off-democracy.
- Norton-Taylor, Richard. 2015. "Britain's Spy Agencies: The Only Watchdog Is the Workforce". *The Guardian*, March 12. www.theguardian.com/news/defence-and-security-blog/2015/mar/12/britains-spy-agencies-the-only-watchdog-is-the-workforce.
- Nye, Joseph. 2017. "Deterrence and Dissuasion in Cyberspace". *International Security* 41 (3): 44–71. https://doi.org/10.1162/ISEC_a_00266.
- Omand, David. 2010. *Securing the State*. London: Hurst.
- Omand, David. 2020. *How Spies Think: Ten Lessons in Intelligence*. New York: Viking.
- Omand, David, and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Washington, DC: Georgetown University Press.
- Philp, Catherine. 2020. "State-Sponsored Hackers 'Trying to Steal Coronavirus Vaccine Secrets'". *The Times*, May 5. www.thetimes.co.uk/article/state-sponsored-hackers-trying-to-steal-coronavirus-vaccine-secrets-mrmlzcs.
- Rankin, Jennifer. 2020. "China Joins Kremlin on EU's List of Active Disinformation Threats". *The Guardian*, June 11.
- Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781316822524>.
- Silva, Desmond de. 2012. *The Report of the Patrick Finucane Review*. London: House of Commons. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246867/0802.pdf.
- Sunstein, Cass R. 1996. "Social Norms and Social Roles". *Columbia Law Review* 96: 903–68.
- The Economist*. 2020. "Creating the Coronopticon". May 28.
- Urwin, Rosamund, and Caroline Wheeler. 2020. "Coronavirus Tracker App Could Put Britons under Permanent Surveillance, Warn Tory Rebels". *The Sunday Times*, May 10. www.thetimes.co.uk/article/coronavirus-tracker-app-could-put-britons-under-permanent-surveillance-warn-tory-rebels-5v0w9p5ns.
- Warner, Michael. 2014. *The Rise and Fall of Intelligence: An International Security History*. Washington, DC: Georgetown University Press.
- Younger, Alex. 2018. "MI6 'C' Speech on Fourth Generation Espionage". Gov.Uk. December 3. www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Part II

Espionage



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

4 Ethics in the recruiting and handling of espionage agents¹

David Perry

Introduction

Before delving into the topic of espionage specifically, I'll first indicate to the reader some of the terms, concepts and assumptions in ethics that will frame my analysis.

Among theories and principles of ethics, there is an important distinction between 1) those which consider only the consequences of alternative actions in determining whether those actions are morally right or wrong (i.e. *consequentialist* or *teleological*), 2) those which give moral weight to aspects of actions other than their consequences or in addition to them (i.e. *nonconsequentialist* or *deontological*) and 3) those which focus on motives and character traits rather than right or wrong actions. William Frankena in his classic book *Ethics* called the latter *aretaic* approaches, drawing on an ancient Greek concept of excellence of character (Frankena 1973).² While classifying an ethical claim one way or the other is never enough to prove or disprove it; grasping this tripartite classification framework can enable us fruitfully to examine all sorts of ethical claims and arguments, as well as avoid getting stuck in one category at the exclusion of the others, which can lead to serious mistakes in ethical judgement and deliberation.

I'm persuaded that there are several ethical principles that apply to all rational beings, whether or not they recognize them as such. These principles are objective in that sense, but *prima facie* rather than absolute, since none of them always overrides the others in cases of conflict.³ They include:

- 1 **Compassion:** concern for the well-being of others; avoiding inflicting suffering; preventing and alleviating others' suffering; meeting the needs of the most vulnerable; promoting others' happiness
- 2 **Fairness:** treating people the way they deserve to be treated, as having equal rights unless merit or need justifies special treatment or if their criminal acts cause them to forfeit such rights
- 3 **Respect** for individual autonomy; not manipulating rational people even for their own good
- 4 **Respect** for laws enacted by legitimate governing bodies
- 5 **Honesty:** not deceiving anyone who deserves to know the truth; not making promises that we don't intend to keep

- 6 **Courage** in opposing injustice, defending the innocent from harm etc.
- 7 **Integrity**: upholding our obligations in spite of personal inconvenience; keeping promises that we have freely made

We also accept particular responsibilities when we take on certain roles, which can qualify our fulfilment of those general ethical principles. If I marry and have kids, I implicitly accept responsibilities towards my family that are stronger than those of the average person towards them. If I am hired by a corporation, I implicitly agree to promote the interests of the company's owners (as well as other key "stakeholders"). If I'm a defence attorney, I incur strong obligations of confidentiality towards any client whom I agree to serve. If I'm a journalist, I have a special responsibility to establish the veracity of a story before reporting it as news. If I'm a soldier or police officer, I'm authorized to kill under certain circumstances, but I'm also expected to risk my life to save defenceless people. And if I'm an intelligence officer, I'm permitted and expected to lie when necessary to protect vital national secrets, including intelligence sources and methods.

Business and professional roles can create opportunities to fulfil a wide range of ethical obligations and ideals. Physicians and nurses can alleviate suffering, promote patients' health and respect their informed consent. Journalists can expose government corruption and improve democratic accountability. Lawyers can defend the poor and the wrongly accused from injustice or prosecute dangerous or callous criminals. Businesspeople can meet all kinds of human needs in efficient and imaginative ways, increasing our quality of life. And military and intelligence professionals can provide crucial elements of security for the lives, rights and well-being of their fellow citizens.

But ethical challenges can also arise in business and professional life, where the ethical choice is clear (or should be clear), but where there are personal incentives or organizational pressures to do otherwise. Corporate purchasing staff might be offered bribes to choose certain suppliers over others, undermining the objective judgement they owe to their companies. Physicians may be tempted to refer patients for unneeded tests or treatments if they have a financial stake in them. News organizations might emphasize celebrity scandals and shallow political controversies to entertain their audiences, instead of investing in careful investigative reporting that might actually serve the public good. And salespeople might feel pressure to mislead customers about their companies' products or services in order to meet sales quotas.

Business and professional life sometimes generates genuine ethical dilemmas as well, where multiple ethical principles conflict with one another. Medical treatments might extend the length or improve the quality of life for a patient with advanced dementia, but might also conflict with their previously stated wishes. Journalists might be subpoenaed to reveal the names of sources to whom they've promised confidentiality, or face imprisonment if they refuse. Defence lawyers might discover that their client is guilty of a horrendous crime but refuses to plead guilty. And corporate executives can face decisions that will harm employees and their families but may be necessary to avoid bankruptcy.

One of the more influential misconceptions to have arisen in Western political philosophy is the idea that ethical principles are not appropriate to apply to “statecraft” or international politics, as if in doing so one makes a kind of “category mistake”. Now, clearly it is important to make conceptual distinctions between transactions involving states and those involving individuals, but those distinctions do not necessarily mean that ethical considerations are irrelevant to international relations. An international treaty, for example, is different in many respects from a promise made between individual persons. A treaty that ceases to be beneficial to a country is not necessarily accorded the same legitimacy as a promise that ceases to be convenient to an individual promisor. Yet a treaty is a kind of promise, in that it demands of those who would annul it that they provide convincing justification for doing so. Even the idea of a state’s “national interest” – which might in fact serve as justification for breaking a treaty – itself bears moral weight, an implicit appeal to the rights and well-being of the state’s domestic citizens, though whether a state’s action is indeed in its national interest and whether that conclusively justifies that action are frequently controversial.⁴

Similarly, although society grants to the state the use of deadly force in its behalf, it does not thereby accede to all possible uses of that force. The proscription of cruelty and excessive violence is as relevant to the relations between states as it is to the interactions between persons.

Moreover, although US government⁵ employees – including intelligence officials – are bound to defend a particular Constitution, that Constitution is based upon certain *universal* principles – including the right of consent of the governed affirmed by the Declaration of Independence – which as such apply not only to US domestic citizens but also to the citizens of foreign countries, especially as the latter are affected by US government actions. Respect for the autonomy and consent of persons, whatever their nationality, implies that they not be coerced or deceived unless even weightier ethical principles are at risk.

Espionage and treason

Espionage conflicts with our normal condemnation of treason, since if treason is immoral then it can hardly be ethical to induce someone to commit treason by spying on their own government. Treason is considered morally suspect for both deontological and teleological reasons: it typically involves a betrayal of public trust and a basic obligation of citizenship; and it can expose the nation to subversion or military defeat by hostile states. In addition, covert action conflicts with our moral sensibility that rational adults and their government representatives ought not to be deceived or manipulated, that people generally deserve to be told the truth and allowed to manage their own affairs without paternalistic or hostile interference.

These normal ethical assumptions are challenged in some respects, however, when we explore the question, are there certain states, regimes or organizations which *do not deserve* the loyalty or honesty of their citizens or members? Consider organized crime, which often requires of its members’ rigid loyalty but

which clearly does not actually deserve such loyalty – hence the justification for the FBI and other law-enforcement agencies to penetrate and subvert them by means of informers and undercover agents.

But if treason and other dishonest acts against certain states can be justified, then we can begin also to see the potential justification of espionage and covert action carried out against those same states by *other* states, assuming that the latter are themselves legitimate and are pursuing just goals.⁶

This is a highly loaded assumption, however, since legitimate intelligence goals cannot justify any and all means. Many espionage and covert action techniques remain morally problematic despite their employment in the service of a worthy cause by a justified profession. It is apparent that to manipulate persons into becoming espionage agents, to employ coercive interrogation techniques, or to deceive foreign citizens via covert action, may infringe rights that cannot legitimately be infringed unless outweighed by more compelling ethical reasons. Although the concept of national interest implies the tacit consent of domestic citizens, it cannot unequivocally warrant coercive intelligence methods, in part because it cannot be assumed to satisfy the tacit or even hypothetical consent of foreign citizens.

This is not to argue that, in a “zero-sum” conflict⁷ between the vital interests of domestic and foreign citizens, one cannot justify pursuing the former at the expense of the latter. On the contrary, duties to defend one’s country – as long as that country can plausibly be described as a constitutional democracy – can be justified on the basis of a theory of universal human rights (Gewirth 1988).

The point, however, is that the moral justification of coercive intelligence methods requires either a true zero-sum conflict – a situation which cannot simply be assumed to exist in every relation between enemies – or a credible appeal to foreign citizens’ *hypothetical consent* (in the absence of their expressed consent), meaning that one has good reason to believe that they would concur if they had relevant knowledge and deliberated in an unbiased fashion.⁸

Agent recruiting and handling

Organizations like the Central Intelligence Agency contribute to the formidable task of ascertaining the capabilities and intentions of foreign regimes and significant sub-state actors like terrorist cells. Much of the work of their analysts involves sifting through and evaluating public sources of information as well as data obtained by satellites and monitors of electronic transmissions. Such sources can by themselves elicit tremendously valuable intelligence, all the more so when disparate bits of information can be cross-referenced and pieced together by means of powerful computer systems and software.

But I think we have good reason to believe that espionage using human agents (HUMINT) remains an important intelligence tool, even now the only way in some cases to gain access to an enemy’s sensitive documents, conversations, intentions and plans.

In the efforts of a state’s intelligence service to recruit agents in foreign countries, it may have very specific offensive or defensive goals, or it may wish simply

to build “assets” – human sources of information and influence – for future use. Richard Bissell, CIA’s Deputy Director for Plans, 1958–62, testified before Congress in 1975:

It was the normal practice in the Agency and an important part of its mission to create various kinds of capability *long before there was any reason to be certain whether those would be used or where or how or for what purpose* [emphasis added]. The whole ongoing job of . . . a secret intelligence service of recruiting agents is of that character.

(Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1975, 186)⁹

The literature indicates that foreign citizens become espionage agents for a wide variety of personal reasons. Former clandestine service officer Joseph Smith indicated in his memoir that his trainers boiled down the categories of agents’ motivations to three: financial considerations, ideological convictions and coercion (Smith 1981, 114). Other writers have suggested a broader range of motives and situations enabling the recruiting and handling of agents: the lure of adventure, excitement and secrecy; ideology or sense of duty; desire for money; sexual and other blackmail; agents’ resentment and frustration regarding their overt careers or some combination of these (Felix [McCargar] 1988; 1963; Grodzins 1956; Blum 1972, chaps. 5–6; Cooper and Redlinger 1986, chap. 2; Pincher 1988; 1987).¹⁰

A more instructive approach for our purposes is to distinguish among techniques of agent recruitment and handling according to various *degrees of freedom of action*, although I will also explore ethical issues common to all uses of human agents.

Voluntary agents

Some agents, first of all, require little or no persuasion on the part of intelligence officers to engage in espionage on behalf of countries like the United States, although in the interest of “compartmentation” (the restriction of information to only those who can justify their “need to know” it) they may never be told how the information they provide is actually used. Some voluntary agents are motivated by the sheer excitement of spying and the promise of steady extra income. But many commit espionage out of a deep-seated antagonism towards their native regimes (Jacobs 1978; Smith 1981, 114–15).¹¹ This was true, for example, of a number of high-ranking Soviet military and KGB officials who either passed sensitive documents to the CIA or who defected when they no longer in good conscience could serve the Soviet regime.

One such agent, Pyotr Popov, a Soviet military intelligence officer, supplied valuable information to CIA during the 1950s largely out of repugnance towards the KGB’s treatment of Russian peasants (Hood 1982; 1983; Rositzke 1988, 67–9). Another Soviet defector-in-place, Oleg Penkovskiy, fearing that Khrushchev intended to launch a pre-emptive nuclear strike, provided US intelligence

with thousands of pages of Soviet military documents, including information on Soviet nuclear weapon capabilities that proved vital to President Kennedy's actions during the 1962 Cuban missile crisis (Penkovsky 1965).¹²

One of the more interesting viewpoints to emerge fairly consistently from the memoirs and other writings of former CIA personnel is that intelligence officers and their intermediaries occasionally develop close emotional ties to the agents they supervise (Felix [McCargar] 1988; Phillips 1982, chap. 4; Smith 1981; Copeland 1978, 129–30; Hood 1982; DeForest and Chanoff 1990) especially those agents who engage in espionage out of a sense of duty. For instance, Frank Wisner, CIA's Deputy Director for Operations 1951–58, reportedly suffered a nervous breakdown chiefly as a result of being ordered *not* to aid rebels resisting the Soviet crackdown in Hungary in 1956 (Powers 1979; Ranelagh 1987, 306–7).

It is not too far-fetched to believe that, in a state characterized by an oppressive political system, espionage intended to undermine that system's power and prestige can actually provide authentic hope to agents and dissident groups, and in this way can be ennobling rather than exploitative. Former CIA officer Harry Rositzke argued that although agents sent on missions against the Soviet Union in the late 1940s and early 1950s “knew from the beginning that the cards were stacked against them”, they were nonetheless “highly motivated”, having witnessed the effects of Soviet power in Eastern Europe, the Ukraine and the Baltic States (Rositzke 1988, 26–8).

However, espionage against one's government is considered treason in every part of the world, and if exposed frequently entails severe punishment for the agent. Both Popov and Penkovskiy, for example, were reportedly executed after their capture and interrogation by the KGB. Thus the fact that an agent is a volunteer does not thereby purge his or her CIA case officer of moral responsibility or liability.¹³

Former CIA officer Glenn Carle touched on several of these themes in his fascinating memoir:

The relationship a case officer . . . has with his “assets” – the men and women we recruited and convinced to commit treason, to provide us with classified information, often at the risk of their lives – is the most intense personal relationship in one's life. . . . Trust is critical, and we convince an asset to trust us with his life. Protecting your asset is a case officer's greatest responsibility. And we take that responsibility very seriously.

(Carle 2011, 76)

Similarly, former CIA officer Thomas Mulligan argued:

Our training, and the culture in the field, was that we had a moral responsibility to look to the welfare and the safety of our agents. And even the lousy agents – the fabricators, say – were scrupulously protected both during and after their relationship with the Agency. It is absolutely essential that any intelligence agency comport itself in this way, because if prospective agents

don't have confidence that they will be protected, they will not engage in espionage on our behalf.

(Thomas Mulligan, email message to the author, October 19, 2015)

Although witting agents usually have no illusions about the consequences of capture, their covert sponsors may ask them to accomplish tasks entailing greater risk than they're aware of or would agree to accept. Rositzke described how a nervous double agent was emboldened to meet with his KGB handler: the CIA polygraphed the agent, but then showed him a different graph than his own to convince him that he could successfully withstand a KGB debriefing (Rositzke 1988, 123–4).¹⁴ Pyotr Popov reportedly refused a request by over-eager US officials to organize “a small, tightly knit resistance group” of his military colleagues out of fear of the KGB's wholesale infiltration of society. In fact, Popov wouldn't even provide CIA with the names of anyone who might be a Soviet dissident, fearing that a failed attempt by CIA to recruit any of them could easily “blow back” on him (Hood 1982, 96–7).

Occasionally the desire to ensure the safety of agents can conflict with wider diplomatic objectives. Witness these excerpts from a *New York Times* article:

Two or three undercover agents believed to be working for Israel in a Syrian-based terrorist group were unmasked and killed . . . not long after the United States gave the Damascus Government information about terrorist activities in the country. . . . Officials said the Administration argued that Mr. Assad should be given an unusually detailed briefing about the actions of Syrian-based terrorists to impress upon him the weight of the evidence against his Government. Intelligence officials are said to have warned that such a briefing would put undercover agents and methods of gathering information at risk. “It was quite an argument”, said one official who has been informed of the debate. “The intelligence guys finally told them, ‘O.K., but the blood will be on your hands if something happens.’” Undercover penetrations of terrorist groups are among the most difficult tasks in all espionage, and so the losses of agents are viewed as especially grave.

(Wines 1991)

Agents working against tyrannical organizations have an especially compelling ethical claim to have their clandestine activities very closely guarded by their CIA handlers.

Some voluntary agents, though, have apparently been regarded as “expendable” in the interest of maintaining plausible deniability and the secrecy of intelligence operations and methods (DeForest and Chanoff 1990; Felix [McCargar] 1988, 107). James McCargar, a former operations officer, asserted that some American agents were gratuitously slandered by CIA upon their termination or “disposal” as agents, presumably to render them less credible should they attempt to publicize their former espionage work (Felix [McCargar] 1988, 62–3).¹⁵

British journalist Tom Mangold learned through extensive research into the long tenure of James Angleton as CIA's head of counterintelligence that a number

of *bona fide* Soviet defectors and other CIA agents were grossly mistreated – some even betrayed to the KGB – due to Angleton’s sloppy homework, paranoia and damaging reliance on the bizarre, self-serving opinions of one particular Soviet defector, Anatoliy Golitsyn. To the agency’s credit, following Angleton’s forced retirement it made efforts to compensate some of the agents (and CIA officers) who had unjustly suffered as a result of Angleton’s and Golitsyn’s suspicions (Mangold 1991).

Other issues attending the use of voluntary agents were illustrated in the statement of a character in John le Carré’s novel, *The Little Drummer Girl*, regarding a request from the character’s supervisor to penetrate a terrorist organization:

I’ll find you an agent. I’ll train him, help him trail his coat, gain attention in the right places, feed him to the opposition. . . . And you know the first thing they’ll do? . . . They’ll invite him to authenticate himself. To go shoot a bank guard or an American soldier. Or bomb a restaurant. . . . Terrorist organizations don’t carry passengers. . . . They don’t have secretaries, typists, coding clerks, or any of the people who would normally make natural agents without being on the front line. They require a special kind of penetration. You want to crack the terror target these days . . . you practically have to build yourself your own terrorist first.

(le Carré [Cornwell] 1984, 242)

Former CIA officer James Olson confirms that le Carré’s fictional scenario reflects real life: “Terrorists test one another by blood. No terrorist is fully trusted by the rest of the group until he or she has been directly involved in the planning or execution of a deadly terrorist attack” (Olson 2006, 108).¹⁶ This illustrates a troubling moral dilemma in demanding or condoning the moral corruption of agents to occur in the interest of exposing the members and sponsors of the target organization, an issue also faced domestically by the FBI in using undercover agents and informers against organized crime. (Later in this chapter I’ll also consider the deadly risks to innocent third parties that are often posed by such relationships.)

The CIA has also been criticized for building up the hopes of agents beyond what the US Government really intended to support. McCargar stated that US intelligence developed a cooperative relationship with an unnamed Eastern European monarchist group (probably Albanian), deceiving them into believing that the restoration of the monarchy was intended by the United States (it was not) in order to benefit from the “considerable intelligence” the group provided (Felix [McCargar] 1988, 112–13). John Ranelagh accused the United States of a “cold ruthlessness” in supporting partisans in postwar Ukraine and elsewhere when it had no intention to commit its military forces to save them from being annihilated (Ranelagh 1987, 137, 226–8, 287, 302–9).¹⁷ And historian John Prados similarly assessed CIA support for Tibetan rebels in the 1950s-1960s:

From the beginning Washington knew that Tibet could never be more than a large-scale harassment of the People’s Republic of China. To achieve this the

CIA promised liberation to the Tibetans, caught up in their hopes and dreams, who suffered prolonged agony in this war.

(Prados 2006, 203)¹⁸

US culpability has been mitigated, however, in regard to certain covert operations in Poland, Albania and Cuba, where US long-term objectives were defeated by the compromise of its operations and communications by enemy intelligence. US officials were unaware, for example, that British intelligence officers Kim Philby and George Blake were actually Soviet agents (moles) who would succeed in betraying numerous espionage and covert action projects and cause the deaths of hundreds of Western agents (Pincher 1988, 24).¹⁹ The temptation to exploit voluntary agents for Realpolitik purposes must be considered as a plausible moral risk, though.

Other espionage agents are not entirely voluntary, raising a number of additional ethical concerns.

Deception and coercion in agent recruitment

When the CIA is unable to obtain voluntary agents, it sometimes “recruits” them, so to speak, through *deception*. In some cases, people who wouldn’t willingly work for the CIA are made unwittingly to do exactly that by passing information to a trusted friend or associate who happens to be in CIA employ but who presents himself as one with loyalties more congenial to the person being duped (Copeland 1978, 125–9; Felix [McCargar] 1988, 112). This method is sometimes called “false-flag” recruitment (Olson 2006, 55–6; Phillips 1982, 263–4; Epstein 1989, 89, 182–3),²⁰ since the recruiter claims to be someone he’s not. It’s essentially a con game, wherein one first ascertains the potential agent’s basic loyalties and core values in order to concoct a scheme to persuade him to provide sensitive information without upsetting his conscience or arousing his suspicions.

British spy Miles Copeland suggested in his Cold-War-era memoir, “If the prospective agent hates Americans”, for example, the recruiter “can tell him he is acting in behalf of the French – or the British, the Soviets, or some Senator or crusading newspaperman”, whatever his conscience is assessed as most likely to tolerate (Copeland 1978, 128–9).²¹ David Phillips, a former CIA officer, attested that “there are unsuspecting zealots around the world who are managed and paid as spies; they sell their countries’ secrets believing all the while they are helping ‘the good guys’” (Phillips 1982, 264).

Note that one’s opponent can also play this game; here’s Phillips again:

A Soviet KGB officer . . . might pose as a right-wing American in approaching a conservative U.S. government employee. He would attempt to persuade the American to report on the inner workings of his agency or department “to help my patriotic organization to be sure the Commies aren’t infiltrating our institutions”.

(Phillips 1982, 264)²²

Another example of deceptive recruitment was described by former CIA counterintelligence officer William Johnson:

Once . . . we found the KGB using a false Israeli flag; that is, pretending to represent the Israeli Service in recruiting Jewish refugees who had access to Allied secrets. At first, the recruited agents were asked to provide information from Allied files on Nazi war criminals, and then they were blackmailed to give Allied military information.

(Johnson 1986, 81)

More recently, former CIA officer James Olson published several fascinating and realistic examples of deception in agent recruitment, from classic false-flag approaches to scenarios in which CIA officers and their intermediaries operate for long periods of time under the cover of nongovernmental jobs in business, journalism and non-profit organizations (Olson 2006, 52–6, 72–6, 87–93, 194–7).²³ Presumably, credible cover jobs could enable CIA officers to recruit some agents via false-flag techniques.

A false-flag recruitment is odd from a moral perspective, since in one respect the agents thus engaged willingly provide sensitive information, probably knowing that they would be punished if their activities were exposed. But of course the voluntary nature of such action is only superficial, since if the agents knew to whom the information was actually being passed they would most likely not provide it.

Copeland asserted that agents recruited under false-flag premises might be treated more leniently than fully witting agents if caught by their own country's police or counterintelligence agency, if they sincerely believe that they've only provided information to an investigative journalist, for example (Copeland 1978, 106–7). One doubts, though, whether such a story would be believed.

But Copeland also related a more plausible illustration of how a false-flag scenario can be attractive to an intelligence agency. Apparently a CIA official in Prague in 1956 used one of his agents, a Soviet colonel, to organize a network of agents in Czech industries. These agents were told that they were to monitor Czech scientific establishments to detect instances in which the Czechs were concealing their inventions and their progress from the Soviets, and that this information would be forwarded to “a special section of the KGB”. In reality what they unwittingly provided – to the CIA – were details of Czech-Soviet exchanges of secret scientific information (Copeland 1978, 68–9).²⁴ Note that amid the somewhat comic tone to this case is an element of coercion: the Czech agents would have taken as deadly serious the fiction that the *KGB* was demanding their cooperation!

Two other general types of coercive recruitment have been mentioned in the literature.²⁵ In some cases, knowledge of an agent's potentially embarrassing or patently illegal activities is used to extort espionage service. Prospective agents might be confronted with proof of their past crimes and blackmailed into working as spies in exchange for their covert employer keeping such evidence from their own country's police. As former CIA officer Joseph Smith indicated, in many

cases the local police would already be aware of such crimes but would cooperate with CIA in not referring them for prosecution (Smith 1981, 115). Since this method closely resembles that of the FBI in coercing criminals into becoming informers, it might be regarded as less objectionable than some other methods of agent recruitment, though, as I'll argue later, there are ethical concerns regarding the agent's society that should not be ignored.

In other cases, embarrassing situations might be created for previously innocent potential agents, and the threat of exposure used to extort their compliance. One technique regarded by some writers as most effective, and which can be used in combination with a false-flag approach, is where an agent's conscience is "stretched" by the recruiter's careful counselling to gradually allow actions that he or she would previously have found unacceptable. Typically the recruiter develops a friendship or another ostensibly trustworthy relationship with someone who has access to sensitive information. Casual requests for seemingly innocuous data evolve subtly to more obviously illegal assignments, until the agent either makes a conscious decision to remain an informant, or continues out of fear of exposure (Copeland 1978, 127–8). Cooper and Redlinger suggested in *Making Spies*:

Those cultivating the spy will press favors upon him, without, in the initial stages, asking for anything in return. This is clearly a matter in which sensibilities must be catered to in order to avoid giving offense or having one's motives suspect. Reciprocity obliges most people to respond in kind; the trick is to escalate the exchange to the point where a more compromising engagement can be undertaken.

(Cooper and Redlinger 1986, 108)²⁶

Espionage activity that is initiated in a deceptive manner can thus at some point take on more obviously coercive characteristics. James Angleton reportedly described this method as "incremental entrapment in a subtle web of irresistible compromises" (Epstein 1989, 180).²⁷

The degree to which CIA employs blatantly coercive methods in its agent recruitment and handling²⁸ has been a topic of contention among former CIA officers. Arthur Jacobs argued that "there is rarely to be found any effective means of exercising absolute control [over an agent], even by such lurid devices as blackmail, exposure of offensive relationships or personal habits of the source" (Jacobs 1978).²⁹ James McCargar agreed, stressing that since the case officer is dependent upon the actions of the agent, this naturally inhibits the degree to which an agent can be dominated: "To this extent every agent is a free agent". He also argued that "compulsion is a very limited technique", since the agent thus "is in no frame of mind to exploit his own skills or possibilities to the fullest" (Felix [McCargar] 1988, 51, 56).³⁰ James Olson stated, "CIA case officers are taught during their training that blackmail rarely works and therefore should generally be avoided. This rationale, however, is more practical than moral" (Olson 2006, 49). Indeed, Jacobs, McCargar and Olson did not imply that coercive methods would be morally objectionable *if* they were *effective*.

But if CIA officials actually concluded that absolute control over an agent was impossible, this was not for lack of trying. For at least two decades the agency funded extensive experiments using mind-altering drugs, electroshock, hypnosis, sensory deprivation, and other techniques in an elusive quest to find foolproof ways to manipulate agents. Some of the motivation behind these efforts lay in fears that the Soviet Union and China had developed technical “brainwashing” methods that needed to be understood and countered by US intelligence. But sadly little consideration was given to the rights of the largely unwitting human subjects of CIA mind-control experiments (Marks 1979; 1991).

Even if agents cannot be completely controlled by their covert supervisors, it may be inferred that espionage agents almost by definition are regarded by their sponsors first as means to the end of collecting intelligence. The full range of habits, beliefs, virtues and vices making up the character of an individual agent are to the prudent espionage officer merely helps or hindrances to the production of useful intelligence for his or her superiors (Cooper and Redlinger 1986, 10, 19).

Of course, instrumentalist relationships are common to a wide variety of human endeavours, business negotiations being perhaps the most obvious. We have come to expect and tolerate such relationships (though perhaps not without regret) as a necessary concomitant of modern society. It is therefore the element of crude manipulation that can apparently be present in espionage which elicits our heightened ethical scrutiny.

William Hood wrote that an element of control is not simply desirable but imperative in agent recruitment:

No espionage service can tolerate the merest whiff of independence or reserve on the part of an agent. . . . With a new agent, the case officer’s first task is to maneuver him into a position where there is nothing that he can hold back – not the slightest scrap of information nor the most intimate detail of his personal life. Until this level of control has been achieved, the spy cannot be said to have been fully recruited.

(Hood 1982, 29)³¹

James Angleton, Hood’s former boss in counterintelligence, apparently held a similar view, according to Edward Epstein:

Whereas money, sex, ideology, and ambition provide the means for compromising targets, the lever used to convert a man into a mole tends to be blackmail. . . . Whatever lure is used, the point of the sting is to make it impossible for the recruit to explain his activities to his superiors. He is compromised, not so much by his original indiscretion, but for failing to report it.

(Epstein 1989, 183)

Note that Angleton here was referring to a special type of agent, the “mole” or penetration agent within an enemy’s intelligence service. Not all espionage agents would necessarily be compromised by failing to report certain activities to their employer, but an intelligence officer would (Olson 2006, 46–9).³²

E Drexel Godfrey Jr, a former CIA analyst, strongly criticized CIA methods of recruiting agents, stating that CIA officers are “painstakingly trained in techniques that will convert an acquaintance into a submissive tool . . . shred away his resistance and deflate his sense of self-worth” (Godfrey Jr. 1978, 631).³³ Somewhat less dramatically, James Olson claimed, “Case officers are trained to exploit other people’s weaknesses to draw them into espionage” (Olson 2006, 25).

Miles Copeland, expressing a more sanguine view, asserted that CIA uses coercion in agent recruitment “only when there is a good chance of converting it into positive motivation”:

As quickly as possible, the principal [an intermediary between officer and agent] must enable the agent to deceive himself into believing that he would have become an agent even had he not been caught with his pants down, and that what he is doing is justifiable on its own merits”.

(Copeland 1978, 150–1)

Moreover, Copeland said, the agent must be persuaded that the government employing him in espionage regards his safety as more important than any particular piece of information he might forward:

Maintaining such an attitude might occasionally mean passing up some item of tremendous importance, but in the long run it pays off because it keeps the agent feeling safe and happy and maintains his productivity over a long period of years.

(Copeland 1978, 130)

Another former CIA official, Howard Stone, admitted that CIA often recruits agents by bribery or blackmail. But believing that such methods often produce unreliable agents who only pretend to have access to important information, he hoped that CIA would try instead “to win over prominent foreign officials of sound moral character” (Ignatius 1979).³⁴ And former CIA operations officer Thomas Mulligan told me in 2015:

When I went through [CIA] training . . . there was a strict policy prohibition on using coercion, blackmail, or sexual exploitation in recruitment operations. . . . And I have no doubt that any case officer who relied on those tactics would be promptly disciplined and recalled from the field. I believe that part of the motivation for such a prohibition was moral, but of course there is a practical reason as well: If you’re running an agent on those grounds, you cannot expect the slightest bit of loyalty from him. . . . The best [officer]-agent relationships are grounded in mutual respect and a shared sense that the work being done together is important. Of course the [officer] must maintain control over the relationship. But that is fully compatible with the agent having a measure of autonomy.

(Thomas Mulligan, email message to author, October 19, 2015)³⁵

Another former CIA officer who served many years in Latin America told me in 1991 that *none* of his agent relations were based on blackmail or other coercion. He believed like Howard Stone that such methods invariably produced “servile” and unreliable agents who “don’t exercise good judgment”. In contrast, this officer said that his agents “produced for me because they knew I was reliable and they could count on me in a pinch. They would and did risk their lives for me”. He added, though, that different methods might be necessary in totalitarian countries where the stakes and pressures were greater (confidential interview with author, Autumn 1991). Hence, it seems likely that a CIA officer having qualms about deceptive or coercive recruiting methods would simply not be assigned to such countries, or would not remain there very long at least in an agent-recruiting capacity.

The disparate opinions expressed in the literature, supplemented by my interviews with former intelligence officers, lead me to believe that the degree of deception or coercion employed in agent recruitment and handling is a function of three factors: 1) the individual officer’s skills, personality and scruples; 2) pressure on the officer to obtain information (i.e. faster and more of it in a crisis) and 3) the frequency of “walk-in” or voluntary agents, which if plentiful reduce the need for deception or coercion to obtain needed information.

Of course, deception and coercion are morally suspect ways of treating rational adults, since they infringe their *prima facie* rights to privacy and freedom. On the face of it, it would seem ludicrous to think that a person could rationally will to be coerced into performing espionage, especially since there is theoretically no escape from the threat of blackmail. This recognition could lead persons to condemn coercive recruitment methods out of hand.

In cases where prospective agents’ prior perpetration of crimes mitigates their right to be free from *retributive* coercion, the issue of their consent loses some of its force. But this cannot be said to provide a “blank check” to a secret recruiter to coerce a criminal to engage in espionage.

However, if we imagine a prospective agent who works in a sensitive capacity for the government of a manifestly *tyrannical* state, there is another sense in which, since that government itself can’t rationally be willed by its oppressed citizens, neither can service to that government in ways that maintain its tyrannical nature be justified. But given the fact that opportunities to persuade citizens and government officials in tyrannical states that they ought to commit treason are sometimes quite limited, the potential justification of coerced recruitment of agents to achieve this becomes clearer.

Coercive recruitment of agents within a tyrannical state becomes even more acceptable as that state’s threat to other countries becomes more grave or imminent. The philosopher Sissela Bok claimed that “whenever it is right to resist an assault by force, it must then be allowable to do so by guile” (Bok 1989, 144); by extension, espionage can serve as an effective way to prevent a tyranny from launching an aggressive war or intimidating its neighbours. And the same would hold for espionage against terrorist organizations: especially since the 9–11 attacks, Americans are likely to support vigorous CIA efforts to penetrate such organizations with spies.³⁶

We need to be aware, though, of other moral implications of the relationship between an intelligence officer, his or her intermediary and the agent. Consider the following scenario:

An illustration

Imagine that a CIA officer, using both overt and covert sources of information, identifies a particular foreign citizen as one who probably has access or could obtain access to sensitive information desired by the US Government.³⁷ The prospective agent's movements are then monitored to discern any personal habits or foibles (like a gambling addiction) which could be exploited in the future.

Already, then, an issue of the prospective agent's right to privacy is raised. Law-abiding citizens of a democratic country would likely be outraged to find themselves being surveilled in this manner. Citizens of a police state might be less surprised and more apathetic, having experienced their rights violated on a regular basis. But this fact would not be enough in itself to justify an additional infringement: the burden of moral justification would rest with the intelligence agency conducting the surveillance.

A next step in this hypothetical scenario might be for the intelligence officer to arrange for an intermediary to meet the prospective agent in a familiar setting. The intermediary himself might be similar to the agent in terms of ethnicity and class so that their meeting would seem perfectly natural to the agent and others.³⁸

From this point the intermediary (guided by the intelligence officer) would take one or more of a variety of approaches, many of which were noted earlier in this chapter. If the prospect voices opinions critical of his government or sympathetic to the United States, a straightforward "pitch" might be made to work for US intelligence, though precautions would need to be taken to ensure that the individual was not planted by an opposing intelligence service. At least this approach entails little deception of the agent by the intermediary.

If the prospect were deemed unlikely to become a spy voluntarily, but has a history of criminal activity, or simply a personal habit that if exposed would be objectionable to his superiors or family, a "sting" could be set up to coerce his cooperation. We can even imagine a second intermediary telling the prospect that the first intermediary had been detained for questioning on suspicious activities possibly involving the prospect himself, and that the latter would be prudent to cooperate with the second intermediary. This variation on a "good cop/bad cop" routine would of course be entirely fictional. But it might be enough to induce the prospect to steal sensitive data or plant bugging devices, activities which would generate their own grounds for blackmail.

If the prospective agent were perceived to be immune to blackmail yet unlikely to volunteer to serve US intelligence, the intermediary might create a false-flag scenario, requesting increasingly sensitive information in return for seemingly innocuous favours or in the interest of serving some cause agreeable to the prospect. A false-flag approach in theory might be maintained indefinitely, but once the agent begins to provide secret data, the intermediary is able to suggest unpleasant consequences at any sign of the agent's reluctance or resistance.

Even if we acknowledge that these travesties of friendship might be justified under certain conditions, such as the tyrannical or threatening nature of the target state or terrorist organization, two additional concerns arise. First, we can imagine how the ability to recruit an agent coercively could easily generate its own imperative apart from the perceived value or gravity of the data he or she could credibly provide. In other words, the fact that the pool of prospective agents is theoretically very large could lead to coercive manipulation as a practice unconstrained by any consideration of proportionality. Recall Richard Bissell's statement that the CIA typically recruits agents "long before there [is] any reason to be certain whether [they] would be used or where or how or for what purpose" (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1975, 186).

An additional concern arising out of this discussion has to do with the fact that intelligence officers and their intermediaries must be trained to manipulate persons in calculated ways (though some likely have greater native ability in this skill than others). This recognition is shocking and disturbing to citizens in democracies, even though we are aware that other vital professions like the police and military must by necessity train their recruits in other unpleasant skills in order to be effective against criminals and enemy soldiers. Our concern in part is that such training may reinforce or result in the moral corruption of the trainee.³⁹

Comparisons with covert action

Some writers have noted some interesting similarities and differences between espionage and covert action.

Harry Rositzke argued that the kind of agent manipulation that frequently occurs in espionage and counterespionage operations may not apply to some types of covert action. Covert financial support for a political leader or dissident, for example, need not entail his or her coercion since it serves his or her interests (Rositzke 1988, 185–6). James McCargar expressed a similar opinion:

In a political operation the case officer must have arrived at a clear and workable accommodation of interests with the agent. Control by the case officer there must be, but not duplicity. The purposes of case officer and agent must have been presented with the maximum permissible clarity, and then a reconciliation of conflicts and limitations negotiated. In brief, the outstanding characteristic of the political case officer-agent relationship is that it must be an alliance, not a utilization of the agent by the case officer, as often occurs in intelligence.

(Felix [McCargar] 1988, 144–5)

But the fact that this state of affairs applied for a time to CIA relations with Panamanian dictator Manuel Noriega (Kempe 1989), among others, indicates that Rositzke's and McCargar's points do not dispel moral concern for the wider context of covert action. In other words, knowing that a covert action coincides with

the interests of particular foreign nationals is not sufficient to justify it ethically, since covert action may involve the violation of rights that ought to override those interests.

It is also likely that an intelligence officer would seek to “vet” (test the authenticity of) an agent of covert influence against the evidence supplied by informers or espionage agents, hence the need to use some method of agent recruitment and handling having one or more of the attendant moral concerns previously identified.

Since the “product” of a covert action agent is in some respects public (unlike the typical product of an espionage agent), it is perhaps more difficult to *deceive* a covert action agent than an espionage agent as to the real intentions of his or her secret employers. One can more easily imagine, though, a potential agent (such as a newspaper reporter or editorialist) being *coerced* through blackmail or other threats into engaging in covert action. Such considerations provide further qualification, then, to Rositzke’s and McCargar’s assertions of the voluntary participation of those agents.

Wider societal concerns

Another set of moral issues has to do with the subtle effects upon a society in which duplicity is engendered by espionage. The logical and practical extension of the relentless nurture of duplicity is either a Hobbesian state of nature or a totalitarian system where basic reciprocal trust between persons is utterly subverted.⁴⁰ Although it is unlikely that an intelligence agency by itself could produce this result in a foreign country (without an army of occupation or police powers to support it, that is), the fact remains that espionage has morally significant effects beyond those experienced by the agent alone. For example, feeding or exploiting an agent’s biases, fears or ideology in order to enhance his or her espionage productivity may contribute in some small way to wider social, ethnic or even international conflicts – to a greater extent if the agent is or becomes an influential leader. Undoubtedly many ethnic and religious animosities with ancient roots will continue to exist for generations, with or without the added variable of American espionage. But intentionally contributing additional fuel to old hatreds is irresponsible.

Of course, CIA agents no doubt can sometimes be recruited among persons with broader vision who seek to counteract violent hatred and those who would inflame it. Ideally the infiltrators of terrorist groups would do so out of repugnance towards their violence, and not because of blackmail or other coercion. Many infiltrators, though, would never be able to bring themselves knowingly to work for the CIA, hence the tactical advantage of a false-flag approach.

In penetrating a terrorist organization, though, a tension can arise between preserving innocent lives and maintaining intelligence sources. US intelligence reportedly had curious liaison contacts with PLO officials Abu Hassan (Ali Hassan Salameh) and Abu Iyad (Salah Khalaf), both of whom had planned Black September’s massacre of Israeli athletes at the 1972 Olympic Games in Munich, but

who apparently made a deal to protect Americans overseas from terrorist attacks in order to enhance PLO prestige with the United States (Ignatius 1983; Woodward 1987, 244–5; Randal 1991).⁴¹ The implication here is that PLO attacks on non-Americans would *not* encounter direct opposition by US intelligence. West German intelligence apparently had as an agent a Jordanian explosives expert who belonged to the group later blamed for the December 1988 bombing of a Pan Am jet over Lockerbie, Scotland, in which 270 people died (Engelberg 1989; Raviv and Melman 1990, 424–7).⁴² It's possible that the Germans did not exercise sufficient control over the agent, or that they waited too long to prevent the bombing, or that the agent simply didn't inform them of that particular plan. These examples suggest that in developing potentially productive intelligence relationships with members of terrorist organizations, a coldly utilitarian calculus would entail insufficient consideration of the rights and well-being of many innocent third parties.

Consider also the obstruction of justice involved in sheltering criminals who agree to become agents. An extreme example of the questionable moral nature of such relationships was the recruitment by US intelligence of a number of Nazi war criminals to engage in espionage and covert operations against the Soviet Union (Simpson 1988, chaps. 8–12).⁴³ Christopher Simpson quoted Harry Rositzke as telling him in a 1985 interview: “It was a visceral business of using any bastard as long as he was anti-Communist . . . [and] the eagerness or desire to enlist collaborators meant that sure, you didn't look at their credentials too closely” (Simpson 1988, 159). Simpson argued, however, that US intelligence actually did know about the war-crimes “credentials” of many of its post-war recruits, as did the British, French and Soviets, who also employed suspected and proven war criminals in intelligence roles (Simpson 1988, 73).⁴⁴ Simpson further showed that this practice became risky to US intelligence as well, when ex-Nazis threatened to publicize US covert operations in which they had participated unless the United States helped them to escape abroad to avoid prosecution for their wartime atrocities (Simpson 1988, 175).⁴⁵

In hindsight at least, it seems obvious that espionage and covert actions relying upon violent criminals as intelligence assets⁴⁶ bear a strong burden of moral justification, chiefly since the victims of their crimes cannot be assumed to give tacit consent to their shelter from prosecution, but also because they can pose a threat to the societies in which they are secretly sheltered.⁴⁷ Furthermore, in cases where perpetrators of mass murder (or even ordinary murder!) have sought refuge in intelligence work, it is difficult to see how the practice could be justified at all, even under the pressures that CIA officers felt in the early post-war years to quickly develop an underground network in the event of war with the Soviet Union.⁴⁸

To the Agency's credit, in 1995 under its Director John Deutch several guidelines were established to screen potential foreign agents regarding their involvement in human-rights abuses and criminal activities (Risen 1995).⁴⁹ Some clandestine service officers resented that change and became highly risk-averse in agent recruitment (Olson 2006, 84–5). But their reaction was misplaced, in my view: the new policy represented genuine moral progress.

Summing up

Let us now review the main ethical strengths and weaknesses of the espionage methods that have been described.

The use of human agents – voluntary and non-voluntary – is intended to provide information believed to be unobtainable through other methods. The risks inherent in all espionage activities suggest, though, that for the sake of the agent alone, efforts should be made to determine before the agent is recruited that the information needed cannot be ascertained by less problematic methods. In addition, since after an agent is recruited the agent-officer relationship takes on a life and momentum of its own, care must be taken to avoid situations where innocent third parties would be harmed or justice obstructed in the interest of preserving the agent's identity and continued service.

Recruiting voluntary agents has the advantage of involving no deception about the identity and general motives of the recruiter. Furthermore, a just cause can be served by intelligence officers and voluntary agents working together to undermine an unjust regime. But such agents usually deserve not to be deceived about the risks involved in the operations they are asked to carry out. Nor should the fact that their work is secret tempt their handlers to treat them as expendable, to allow them callously to be sacrificed to Realpolitik or the shifting winds of diplomacy.

The chief advantage of employing a false-flag approach or blackmail in certain situations is that intelligence-gathering objectives can be pursued even where foreign citizens are highly unlikely to serve voluntarily as CIA agents. But such methods raise very difficult ethical questions. False-flag methods by definition deceive the agent as to the identity of the recruiter, and thus hide from the agent the full risks inherent in his or her tasks as well as their true purposes. Blackmail is blatant coercion. It is difficult enough to justify against known criminals; all the more so when it arises out of the calculated entrapment of a previously innocent person who merely happens to have probable access to sensitive information desired by the CIA. Finally, to the extent that false-flag and blackmail tactics seek to "stretch" the agent's conscience, they can result in the moral corruption of the agent in addition to his or her victimization.

These primarily deontological and aretaic concerns about espionage are challenged, though, by the consequentialist reply that if one rules out an espionage source or method, one may thereby eliminate the possibility of knowing certain kinds of vital information. It's not difficult to construct hypothetical cases in which having particular information about the intentions of a tyrannical regime or a terrorist cell could mean the difference between life and death for many people, cases which would therefore question the validity of strict prohibitions on deceptive and coercive intelligence methods or the use of criminals as agents. Clandestine collection of intelligence using human agents will remain vital in penetrating hostile intelligence agencies (counterespionage), in monitoring the existence, movements, proliferation and elimination of weapons of mass destruction, and in monitoring and subverting international terrorism and narcotics trafficking.

An additional point needs to be made, however, concerning the meaning of moral justification in the present context. To say that a decision or action is morally justified does mean at least that it is morally permissible, and may also imply that it's the right or best decision or action, all things considered. But it does not necessarily mean that the outcome from such a decision is unequivocally good. It may be, for example, that coercive recruitment of an agent can be morally justified in a particular situation, given the dire consequences of not having the information that he or she can provide, say, plus a lack of morally acceptable alternatives. But since coercion involves an infringement of the agent's freedom and conceivably other basic rights, the external good that may result from the recruitment cannot do away with the fact that the agent – a human person with values, emotions, hopes and dreams, not merely an abstract “source”, “asset” or “penetration” – suffers real harm or is otherwise wronged in the process.

Notes

- 1 I'm grateful to Mitt Regan and Seumas Miller for allowing me to present this paper at a conference they hosted in June 2019 at St. Cross College, University of Oxford. The topic of ethics in espionage first drew my sustained attention back in 1985 in connection with my Ph.D. dissertation in Ethics and Society at the University of Chicago Divinity School. During the past three decades I've had several opportunities to publish my reflections on ethical issues in intelligence operations. Although many of the ends and means of intelligence collection have changed significantly in recent years, I'm persuaded that my earlier conclusions have held up surprisingly well, so I hope that my readers will forgive me for repeating many of my previous points in this essay. My doctoral dissertation was entitled *Covert Action: An Exploration of the Ethical Issues*, but contained a chapter on espionage. Some ideas from that treatise were later published as “‘Repugnant Philosophy’: Ethics, Espionage and Covert Action”, which was reprinted in *Ethics of Spying: A Reader for the Intelligence Professional*. Revised and expanded versions of my arguments subsequently appeared in my book *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation* (Perry 1993; 1995; 2006; 2009; 2016; Goldman 2006).
- 2 I also follow Frankena in using “teleological” as equivalent to “consequentialist”, but recognize that some philosophers use “teleological” as a synonym of virtue ethics, which Frankena labels “aretaic”. See, for example Orend (2006).
- 3 Here I'm indebted to W. David Ross, an important twentieth-century British philosopher, who proposed in *The Right and the Good* a mixed/pluralistic ethical theory that regarded *prima facie* consequentialist, nonconsequentialist and aretaic concerns as important to consider in making moral decisions (Ross 1930). For more of my perspectives on ethical reasoning, see the Chapter 1 of my book *Partly Cloudy*.
- 4 Similar points were made by John Langan in Langan (1983).
- 5 Although I mostly reflect a US perspective in this essay, I presume that most of the issues that I explore bear on the intelligence operations of other democracies as well.
- 6 Michael Walzer similarly argued in *Just and Unjust Wars*, “a state (or government) established against the will of its own people, ruling violently, may well forfeit its right to defend itself against a foreign invasion” (Walzer 1977, 82).
- 7 A “zero-sum” conflict is one in which one side's gain unavoidably results in the other side's loss.
- 8 Similar distinctions among types of consent were made in Gewirth (1986), Vandever (1986) and Hampton (1993). Former CIA case officer Thomas Mulligan claimed (in

- an email message to me on October 19, 2015) that my limiting criteria here (zero-sum conflict or hypothetical consent) are too narrow, and would preclude the US from spying on allies like Germany, for example, which he supports. That's an intriguing counterexample, but I stand by my approach.
- 9 Bissell's statement has some rather alarming ethical implications which will be discussed later in this article.
 - 10 McCargar asserted that in the vast majority of cases the motives of agents are mixed (Felix 1988, 61). Henry Crumpton narrates several "sanitized" stories of agents he recruited in Africa whose motives to spy were diverse (Crumpton 2012, chap. 3).
 - 11 See also Blum (1972, chap. 6) for support of the contention that defectors to the US (as opposed to defectors from) tend to be motivated more by ideological factors than financial inducements.
 - 12 See also Rositzke (1988, 69–71), Powers (1979, 127, 205) and Ranelagh (1987, 400–2).
 - 13 James Olson identified George Kisevalter as the CIA case officer who handled both Popov and Penkovsky, adding that "he was deeply attached emotionally to his two agents and had never gotten over their tragic ends" (Olson 2006, 232).
 - 14 Olson asks hypothetically whether South Korean agents about to be sent by the CIA into North Korea should be told that every previous mission had failed (Olson 2006, 138–9).
 - 15 Felix [McCargar], *Secret War*, 62–63. McCargar regarded that practice as "inept" but didn't specifically call it unethical.
 - 16 Similar claims were made by Phillips (1982, 331–2) and Marx (1988, 144) and a former CIA officer in a Fall 1991 confidential interview.
 - 17 See also Prados (2006, chaps. 2–4) and Powers (1979, 44, 403). On the Hungarian uprising of 1956, see Ambrose (1981, 235–40).
 - 18 Prados acknowledges elsewhere in Chapter 10 that Tibetan partisans achieved some impressive tactical victories against the People's Liberation Army before eventually (and inevitably) being overwhelmed.
 - 19 On Albania, see Bethell (1984).
 - 20 Phillips preceded his description of false-flag recruitment with this interesting comment: "Most intelligence officers who set out to persuade someone to become a traitor have to reach an accommodation of some sort with the code of ethics and morality they have inherited or adopted. Sometimes dirty tricks are involved in the recruiting of spies" (Phillips 1982, 263). Olson claims, "Both the CIA and FBI are very adept at false flag operations" (Olson 2006, 56).
 - 21 Copeland also asserted that "*most* spies really don't know which espionage service they are working for" (Copeland 1978, 129)! But that claim was judged to be ridiculous by three former CIA officers in separate confidential interviews with me.
 - 22 Ibid.
 - 23 According to *New York Times* reporter Mark Mazzetti, beginning in the 1970s "the CIA implemented a policy of not recruiting American journalists, clergy, or Peace Corps volunteers to spy for the agency, all of which had been routine up to that time", but that those rules "were not cast in stone", and were loosened significantly in counterterrorism efforts after the 9–11 attacks (Mazzetti 2013, 282).
 - 24 Copeland didn't actually use the term false flag, preferring to call unwitting agents "Willies" (Copeland 1978, 24). Another former CIA officer told me in a confidential interview that Copeland could not have had knowledge of the story of the Soviet colonel in Prague.
 - 25 Until recently I had seen no evidence that the CIA ever imitated the tactic of the Mafia, KGB or Viet Cong of threatening to kill persons or their families if they didn't agree to cooperate. Former CIA officer B Hugh Tovar in a letter to me dated February 25, 1992 said that any CIA officer who made such a threat "would have been fired outright". But violent threats allegedly made to CIA detainees after 9–11 were noted in *The Senate*

- Intelligence Committee Report on Torture* (Senate Select Committee on Intelligence 2014, 6).
- 26 Cooper and Redlinger, *Making Spies*, 108.
 - 27 It is not actually clear whether those were Angleton's words or Epstein's only. Epstein conducted numerous interviews with Angleton before the latter's death in 1987.
 - 28 Examples of coercion applied on informers by US federal and local law enforcement agencies are provided in Marx (1974, 414–15).
 - 29 The ineffectiveness of blackmail in agent recruiting was also suggested by former CIA director William Colby in an interview with me on September 14, 1991.
 - 30 I had the privilege of interviewing Jacobs and McCargar together circa 1991.
 - 31 But Thomas Mulligan in his October 19, 2015 email message to me characterized Hood's claims as "ludicrous".
 - 32 Olson, *Fair Play*, 46–49, imagines a Cuban intelligence officer working undercover at the United Nations who is discovered by US intelligence to be engaging in frequent homosexual encounters, which if exposed would at least get him fired and sent home. Should his cooperation be sought by means of a threat to expose his behaviour (Olson 2006, 46–9)? Olson claims (115), "The CIA and FBI do not use sexual entrapment for recruitment purposes", but that it's still widely used today by other nations' intelligence agencies (Olson 2006, 115).
 - 33 But Thomas Mulligan in his October 19, 2015 email message to me flatly denied that Godfrey's claim about CIA training was accurate.
 - 34 Ignatius offered his own opinion that agents recruited by the CIA "can be a rather scurvy lot" (Ignatius 1979). Incidentally, John Prados claims that Howard Stone was involved in the 1953 coup against Mossadegh in Iran and an unsuccessful coup attempt in Syria in 1957 (Prados 2006, 164).
 - 35 Thomas Mulligan, email message to the author, October 19, 2015.
 - 36 Craig Whitlock indicated that the CIA and its allied intelligence services had virtually no success in infiltrating human agents into Al-Qaeda or recruiting existing members to be informers (Whitlock 2008).
 - 37 A CIA process of identifying potentially valuable agents by carefully compiling and cross-checking information files was described in DeForest and Chanoff (1990).
 - 38 I have seen no evidence that the CIA ever kidnaps prospective agents, even in a false-flag scenario where its intermediaries could pretend to be the secret police of the agent's own country. That of course would be a highly "unnatural" way to contact a prospect. But note that this is distinct from cases of secret kidnappings or renditions of terrorist suspects for interrogation and incarceration.
 - 39 I explored in depth several ethical issues in intelligence interrogation in Chapter 11 of my book *Partly Cloudy* (Perry 2016). See also my article, "Some Unsettling Ethical Reflections on Interrogation" (Perry 2010), and my book reviews of Sanford Levinson, ed., *Torture: A Collection* (Perry 2005), and Michael Skerker, *An Ethics of Interrogation* (Perry 2011).
 - 40 On the all-too-real "mass atomization" of Soviet society, see Hannah Arendt, *The Origins of Totalitarianism* (Arendt 1973, chap. 10).
 - 41 Both men were assassinated, Salameh in 1979 by Israeli intelligence and Khalaf in 1991 by Abu Nidal's rival Palestinian group.
 - 42 Dan Raviv and Yossi Melman suggested that the Israelis had actually infiltrated the group implicated in the bombing and had warned the West Germans in advance. The Germans arrested 16 suspects but released 14 of them within two weeks. The bombing occurred six weeks after that (Raviv and Melman 1990, 424–7).
 - 43 The only major drawback I find in Simpson's analysis is his sanguine view of post-war Soviet capabilities and intentions. Perhaps that resulted in part from his inordinate reliance (evident in many of his footnotes) upon the opinions of disaffected former CIA analyst Victor Marchetti. But Simpson also exhibited a more general affection for revisionist views of the Cold War.

- 44 Rositzke mentioned that ethnic Russians, Balts, Ukrainians, Armenians and Georgians were recruited as agents for missions against the Soviet Union. He stressed their justified resentment against Soviet oppression, but didn't discuss how Nazi collaborators identified among them were handled (Rositzke 1988, 27–8, 166–73).
- 45 Simpson noted Miles Copeland's role in arranging for ex-Nazis to be brought to Cairo to serve as advisers to President Nasser's intelligence service (Simpson 1988, 251–2). In Copeland's memoir, he justified that project by claiming that the smuggled Germans were all bumbling and stupid – that is it was really a joke on Nasser – and that Mossad (Israeli foreign intelligence) used Nazis, too – implying that if the victims of Nazi crimes can justify such action, why should the U.S. deny itself useful assets? – both highly questionable and self-serving claims (Copeland 1978, 181).
- 46 Former CIA officer Justin O'Donnell told a Senate committee that he refused to accept an assignment from his boss Richard Bissell in 1960 to assassinate Congolese leader Patrice Lumumba. But O'Donnell nonetheless recruited a criminal whom he trusted (albeit “not a man of many scruples”) to assist him in the Congo; that same criminal was involved in scouting potential assassins for the CIA to use elsewhere under its “executive action” capability (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1975, 38–43, 181–7). That testimony was attributed in the Senate report to “Michael Mulroney”, who was later identified as Justin O'Donnell by John Prados in Prados (2006, 276). For allegations of CIA uses of organized crime figures, see McCoy (1972).
- 47 A notable case in which these concerns were implicitly affirmed was the US Drug Enforcement Agency's rejection of a Colombian drug cartel's offer to spy on leftist guerrillas in exchange for amnesty (Isikoff 1988).
- 48 Simpson quoted Franklin Lindsay, who in the early 1950s oversaw CIA paramilitary operations in Eastern Europe that apparently involved some former Nazi collaborators:

You have to remember that in those days even men such as George Kennan believed that there was a fifty-fifty chance of war with the Soviets within six months. . . . We were under tremendous pressure to do something, do anything to prepare for war.

(Simpson 1988, 159–60)

Rositzke reported that during a heated meeting at the Pentagon in 1949, an Army colonel banged his fist on the table and shouted, “I want an agent with a radio on every goddamn airfield between Berlin and the Urals.” That was, of course, before the advent of U-2 and satellite reconnaissance (Rositzke 1988, 21).

- 49 A year later the Intelligence Advisory Board reported that since 1984,

several CIA assets were credibly alleged to have ordered, planned or participated in serious human rights violations such as assassination, extrajudicial execution, torture or kidnapping while they were assets – and that the CIA was contemporaneously aware of many of the allegations.

(Associated Press 1996)

References

- Ambrose, Stephen E. 1981. *Ike's Spies: Eisenhower and the Espionage Establishment*. New York: Doubleday.
- Arendt, Hannah. 1973. *The Origins of Totalitarianism*. San Diego, CA: Harcourt Brace Jovanovich.
- Associated Press. 1996. “CIA Involved in Abuses, Report Says”. June 29.

- Bethell, Nicholas. 1984. *The Great Betrayal: The Untold Story of Kim Philby's Biggest Coup*. London: Hodder & Stoughton Ltd.
- Blum, Richard H. 1972. *Deceivers and Deceived: Observations on Confidence Men and Their Victims, Informants and Their Quarry, Political and Industrial Spies and Ordinary Citizen*. Springfield, IL: Charles C. Thomas.
- Bok, Sissela. 1989. *Lying: Moral Choice in Public and Private Life*. New York: Vintage/Random House.
- Carle, Glenn L. 2011. *The Interrogator: An Education*. New York: Nation Books.
- Cooper, H. H. A., and Lawrence J. Redlinger. 1986. *Making Spies: A Talent Spotters Handbook*. Boulder, CO: Paladin Pr.
- Copeland, Miles. 1978. *The Real Spy World*. London: Sphere.
- Crumpton, Henry A. 2012. *The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service*. New York: Penguin Press.
- DeForest, Orrin, and David Chanoff. 1990. *Slow Burn: The Rise and Bitter Fall of American Intelligence in Vietnam*. New York: Simon and Schuster.
- Engelberg, Stephen. 1989. "Bonn Had Informant in the Group Suspected in the Pan am Bombing". *New York Times*, May 23.
- Epstein, Edward J. 1989. *Deception: The Invisible War between the KGB and the CIA*. New York: Simon & Schuster.
- Felix, Christopher [McCargar, James]. 1963. *A Short Course in the Secret War*. New York: E.P. Dutton & Co.
- . 1988. *A Short Course in the Secret War*. New York: Dell.
- Frankena, William K. 1973. *Ethics*. Englewood Cliffs, NJ: Prentice-Hall.
- Gewirth, Alan. 1986. "Professional Ethics: The Separatist Thesis". *Ethics* 96 (2): 282–300.
- . 1988. "Ethical Universalism and Particularism". *The Journal of Philosophy* 85 (6): 283–302. <https://doi.org/10.2307/2026720>.
- Godfrey, Jr., E. Drexel. 1978. "Ethics and Intelligence". *Foreign Affairs*, April. www.foreignaffairs.com/articles/united-states/1978-04-01/ethics-and-intelligence.
- Goldman, Jan, ed. 2006. *Ethics of Spying: A Reader for the Intelligence Professional*. Lanham, MD: Scarecrow Press.
- Grodzins, Morton. 1956. *The Loyal and the Disloyal: Social Boundaries of Patriotism and Treason*. Cambridge: Cambridge University Press; Chicago: Chicago University Press.
- Hampton, Jean. 1993. "Contract and Consent". In *Companion to Contemporary Political Philosophy*, edited by Robert Goodin and Philip Pettit. 2nd edition, 379–93. Cambridge, MA: Blackwell Publishers.
- Hood, William. 1982. *Mole*. New York: Random House.
- . 1983. *Mole*. New York: Ballantine.
- Ignatius, David. 1979. "In from the Cold: A Former Master Spy Spins Intriguing Yarns of His Past Intrigue". *Wall Street Journal*, October 19.
- . 1983. "Mideast Intrigue: PLO Operative, Slain Reputedly by Israelis, Had Been Helping U.S.". *Wall Street Journal*, February 10.
- Isikoff, Michael. 1988. "Medellin Cartel Leaders Offered U.S. a Deal". *Washington Post*, July 20.
- Jacobs, Arthur. 1978. "Letter to the Editor". *Foreign Affairs*, July.
- Johnson, William R. 1986. "The Ambivalent Polygraph". *International Journal of Intelligence and Counterintelligence* 1 (3): 71–83. <https://doi.org/10.1080/08850608608435024>.
- Kempe, Frederick. 1989. "Ties That Bind: U.S. Taught Noriega to Spy, But the Pupil Had His Own Agenda". *Wall Street Journal*, October 18.

- Langan, John. 1983. "National Interest, Morality, and Intelligence". *Studies in Intelligence* 27 (3): 57–69.
- Le Carré, John [Cornwell, David John]. 1984. *The Little Drummer Girl*. New York: Bantam Books.
- Mangold, Tom. 1991. *Cold Warrior*. New York: Simon & Schuster Ltd.
- Marks, John. 1979. *Search for the "Manchurian Candidate": The CIA and Mind Control*. New York: Times Books.
- . 1991. *The Search for the "Manchurian Candidate": The CIA and Mind Control: The Secret History of the Behavioral Sciences*. New York: WW Norton & Company.
- Marx, Gary T. 1974. "Thoughts on a Neglected Category of Social Movement Participant: The Agent Provocateur and the Informant". *American Journal of Sociology* 80 (2): 402–42.
- . 1988. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.
- Mazzetti, Mark. 2013. *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth*. New York: Penguin Press.
- McCoy, Alfred W. 1972. *The Politics of Heroin in Southeast Asia*. 1st edition. New York: Harper & Row.
- Olson, James M. 2006. *Fair Play: The Moral Dilemmas of Spying*. Dulles, VA: Potomac Books, Inc.
- Orend, Brian. 2006. *Morality of War*. Peterborough, Ont: Broadview Press Ltd.
- Penkovsky, Oleg. 1965. *The Penkovsky Papers*. Translated by Peter Deriabin. New York: Doubleday.
- Perry, David L. 1993. "Covert Action: An Exploration of the Ethical Issues". PhD diss. Chicago: University of Chicago Divinity School.
- . 1995. "'Repugnant Philosophy': Ethics, Espionage, and Covert Action". *Journal of Conflict Studies* 15 (1): 92–115.
- . 2005. "Review of Sanford Levinson, *Torture: A Collection*". *Ethics & International Affairs* 19 (1): 119–20. <https://doi.org/10.1017/S089267940000366X>.
- . 2006. "Review of John Perry, *Torture: Religious Ethics and National Security*". *The Cresset: A Review of Literature, the Arts, and Public Affairs* 70 (1): 58–9.
- . 2009. *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation*. Lanham, MD: Rowman & Littlefield.
- . 2010. "Some Unsettling Ethical Reflections on Interrogation". *International Journal of Intelligence Ethics* 1 (1): 47–75.
- . 2011. "Review of Michael Skerker, *An Ethics of Interrogation*". *Journal of Military Ethics* 10 (4): 327–9. <https://doi.org/10.1080/15027570.2011.639157>.
- . 2016. *Partly Cloudy: Ethics in War, Espionage, Covert Action, and Interrogation*. 2nd edition, revised and expanded. Lanham, MD: Rowman & Littlefield.
- Phillips, David A. 1982. *The Night Watch*. Reprint edition. New York: Ballantine Books.
- Pincher, Chapman. 1987. *Traitors: The Anatomy of Treason: What Makes a Man Betray His Country?* New York: St. Martin's Press.
- . 1988. *Traitors*. New York: Penguin Books.
- Powers, Thomas. 1979. *The Man Who Kept the Secrets: Richard Helms & the CIA/by Thomas Powers*. New York: Knopf.
- Prados, John. 2006. *Safe for Democracy: The Secret Wars of the CIA*. Chicago: Ivan R. Dee, Publisher.
- Randal, Jonathan. 1991. "Document Suggests Abu Nidal Was Behind Slaying of Arafat Aide". *Washington Post*, July 23.

- Ranelagh, John. 1987. *The Agency: The Rise and Decline of the CIA*. New York: Simon & Schuster.
- Raviv, Dan, and Yossi Melman. 1990. *Every Spy a Prince: The Complete History of Israel's Intelligence Community*. Boston: Houghton Mifflin.
- Risen, James. 1995. "CIA to Issue Guidelines on Hiring Foreign Operatives". *Los Angeles Times*, June 20.
- Rositzke, Harry. 1988. *The CIA's Secret Operations: Espionage, Counterespionage, and Covert Action*. Boulder, CO: Westview.
- Ross, William D. 1930. *The Right and the Good*. Oxford: Clarendon Press.
- Senate Select Committee on Intelligence. 2014. *The Senate Intelligence Committee Report on Torture: Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*. Brooklyn, NY: Melville House.
- Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. 1975. *Alleged Assassination Plots Involving Foreign Leaders*, 94–465. Washington, DC: US Government Printing Office. www.intelligence.senate.gov/sites/default/files/94465.pdf.
- Simpson, Christopher. 1988. *Blowback: America's Recruitment of Nazis and Its Effects on the Cold War*. 1st edition. New York: Weidenfeld & Nicolson.
- Smith, Joseph Burkholder. 1981. *Portrait of a Cold Warrior by Joseph Burkholder Smith*. New York: Ballantine Books.
- Vandevver, Donald. 1986. *Paternalistic Intervention: The Moral Bounds on Benevolence*. 1st edition. Princeton, NJ: Princeton University Press.
- Walzer, Michael. 1977. *Just and Unjust Wars*. New York: Basic Books.
- Whitlock, Craig. 2008. "After a Decade at War with West, Al-Qaeda Still Impervious to Spies". *Washington Post*, March 20.
- Wines, Michael. 1991. "2 or 3 Agents Are Believed Killed after Rare U.S.-Syrian Contacts". *New York Times*, February 7.
- Woodward, Bob. 1987. *Veil: The Secret Wars of the CIA 1981–1987*. New York: Simon & Schuster.

5 The rights of foreign intelligence targets

Michael Skerker

Liberal states are dedicated to the protection of human rights but protecting the rights of their citizens may entail infringing upon or violating the rights of foreign citizens. This is what some call the liberal dilemma of intelligence collection (Omand and Phythian 2018; Gendron 2005, 418). The same is true for military operations, but in many cases, wars are avoidable, at least in principle, through deterrence and diplomatic actions. Yet intelligence gathering, by its very nature, must be ongoing, in part to forestall wars. If a state can build weapons of war with a reasonable hope that they will not be used and train military personnel with a reasonable hope they will not be deployed, the same is not true for intelligence-gathering equipment and personnel.¹

In what follows, I articulate a 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. This chapter focuses on signals intelligence, SIGINT, and image analysis intelligence, IMAGINT. The model ultimately cautions states to be conservative in their intelligence-gathering efforts. All states of a certain character are permitted to engage in the most rights-respecting, most efficacious techniques they have at their disposal. Given the range of technical abilities of different states, a state with discriminate, sophisticated means of intelligence gathering must consider if its citizens can tolerate the cruder, less discriminate retaliatory operations an adversary state might employ.

Foundation for a theory of just intelligence

This section develops the foundation of a cosmopolitan theory of just intelligence collection. I develop it in detail elsewhere (Skerker 2020b; 2019; 2016). In brief, people living in groups have collective moral responsibilities to protect and address other people's rights that can only be consistently and reliably met through coordinated action. Typically, these collective moral responsibilities are partially acquitted by creating and supporting institutions to address the relevant rights, like schools, hospitals, businesses, churches and militaries. These institutions are essentially outcome-oriented, set up to foster, create and protect the collective moral goods (e.g. health, education, security) that protect rights and fulfil morally important needs. Once these institutions exist, the collective moral responsibility of laypeople is partly met by supporting these institutions.

The professionals who work in morally vital institutions meet their collective moral responsibilities in part by adhering to their properly constituted professional norms. Since these institutions are created to acquit collective moral responsibilities, professionals have a moral – and not just a professional or legal – duty to comply with their professional imperatives to accomplish their institutions’ characteristic ends. The relevant duties are moral duties since actors’ norm-guided actions help their institutions meet, foster and protect people’s rights.

Professional norms are chiefly ends-oriented, directing the professional to take steps that bring about their institutions’ characteristic ends for their clients: education, justice, health, security etc. Professional norms are also constrained by deontological concerns reflecting *ex ante* rules winning the hypothetical consent of all affected by the professionals’ actions. These constraints specify how the institutional imperatives are to be met, guided by stakeholders’ presumed aversion to being grossly wronged in some areas while being assisted in others.²

Professional norms

Certain state agents have a professional duty to meet the collective moral right of security for their political entities, but this duty is too vague to be action-guiding. We can take advantage of the criterion of universalizability inherent in most schemes of rights and duties to further delineate relevant professional duties. We can consider if everyone affected by a potential tactic or norm (norms can be seen as rules for generating tactics)³ would endorse it for meeting their interests and protecting their rights. Those affected would include three stake-holding groups for any professional action in an adversarial field (like policing, soldiering, law, or intelligence): the professionals themselves, their “targets” and their clients. In the abstract, we can see that these groups would endorse tactics and norms striking an optimal balance between being practically efficacious and rights respecting for all concerned. Any member of the stake-holding groups can be expected to endorse professional norms and tactics that efficiently and reliably lead to the characteristic end of their professions like security, but in a way that minimizes rights violations along the way. This trade off can be expressed by the adage “the cure shouldn’t be worse than the disease”. The preferred moral framework I call the “security standard” identifies norms and tactics rationally worthy of consent by the three stake-holding groups. It endorses norms and tactics surviving a three-stage winnowing process. In the context of security-seeking professions, the standard 1) canvases locally feasible tactics aimed at securing an environment relatively free of rights violations or the threat thereof 2) isolates the most reliable, efficacious, proportional and efficient tactics of those locally feasible and 3) endorses the most rights-respecting among the tactics meeting the practical metrics of 2).

Before proceeding, let me address some potential methodological questions. Hypothetical consent is sometimes criticized for being inadequate to ground norms or obligations. I am not arguing that intelligence gathering norms are based on hypothetical consent. Rather, they are based on collective moral

responsibilities. The hypothetical consent of all stakeholders is modelled to delineate the contours of these norms. Hypothetical consent is also sometimes criticized as a theoretical flourish adding nothing to what a theorist happens to find compelling. A hypothetical consent model *is* apt for crafting norms for national security actors because the theorist cannot say ahead of time which kind of professional norms and tactics in the security sphere are best for all political entities in all times. There are two contingent variables affecting national security that have to be taken into account: available tactics and the current level of danger. The first element of the security standard canvasses locally feasible tactics. Best practices for certain kinds of intelligence operations will shift over time as technology improves, social science makes breakthroughs and tactical experience expands, so what is consent-worthy for being a state-of-the-art intelligence-gathering method one year may be outmoded years later. Agencies also develop insights at different paces, so state A's intelligence apparatus can be faulted for using relatively unreliable or ineffective techniques already abandoned by other states, provided that these better techniques are economically and technically feasible for state A. Thus, element 2 of the security standard seeks the most practically effective norms and tactics that are currently employed somewhere in the world, and demands, effectively, that our political entity practice the state of the art, or as close to it, as is technologically or economically possible for it (further, since the security standard endorses the best norms and tactics, it places constant pressure on state agents to refine their capabilities). A second reason that different norms and tactics might be consent-worthy in different states is that more aggressive security-seeking tactics or less deferential norms might be consent-worthy in times of great danger.

The clients of intelligence officers – the inhabitants of their state – have a positive right to security. Therefore, they can demand their agents deliver that security. Intelligence officers can model their clients' consent to the most efficacious norms and tactics to that end. Their concerns would not be limited to efficacy, but also take into account reliability and efficiency. Since any kind of professional action might also produce negative effects, proportionality is also important to consider. An intelligence officer has no rational grounds to think a generic client would endorse relatively ineffective, inefficient, unreliable and disproportionate norms and tactics when better ones exist. No doubt some techniques (or norms encompassing tactics and techniques) will be more efficient, but less reliable or more efficacious, but less proportionate etc. so we can imagine an overall net "value score" of these four practical elements answering the question "what norm or tactic works best". Still, the norm or tactic best conducting to security is not necessarily consent-worthy. Among a class of high-scoring norms or tactics, those that are the most rights-respecting are most worthy of consent on account of clients' duties to respect the rights of foreigners and their own intelligence professionals and because of clients' interests in being exposed to the least rights-infringing tactics on the part of foreign adversaries.

This rights-respecting element will itself be the product of an optimal balancing of the interests of the three-stakeholder groups. The client's positive right to

security will be largely met with practically efficacious norms and tactics that actually do conduce to protect security. These norms and tactics may have to be modified from the highest levels of efficacy or efficiency in deference to the rights of the targets as well as the state agents implementing them. While targets of given actions can also be the clients of the same actions when they are wielded by their own domestic intelligence agencies, qua target, their interest would be to be exposed to no intelligence collection. Barring that, their interest is in being exposed to the most minimal, necessary and discriminate types of collection, meaning that qua target, they would endorse the most reliable, effective, efficient and proportionate measures, infringing on as few as their rights as possible. Intelligence collectors should spend no more time or collect no more information than is necessary. When it comes to inter-state intelligence collection, it is in the interest of the client in one state to endorse the most minimal and discriminate actions targeting foreigners, because as we will see in the next section, she implicitly endorses those same tactics being used against herself by foreign intelligence agencies.

Regarding the third stake-holding group, state agents have a right not to be ordered to perform actions exposing themselves to wanton risk or threatening their long-term mental, moral and physical health (Skerker 2020a). For example, intelligence officers can probably never be ordered to have sexual relations with targets or to cultivate drug addiction in the course of undercover work.

Thus, acceptable norms and tactics may vary if we take into account rights and not merely the efficacy of the norms and tactics. They may also vary if the rights of all three stake-holding groups are taken into account as opposed to the rights of just one. Examples will be given in a later section. The triangulation of rights is in the interests of all since any given person might at some point occupy all stake-holding groups. A person might be a state agent for some span of her life; be targeted by a foreign intelligence agency and be the recipient of the security provided by other state agents.

Forfeiting, Waiving, and Ceding Rights

Just because an institutional actor has a duty to do something it does not mean she is not wronging her target/client in executing her duty in a norm-compliant way. For example, a doctor has a duty to preserve people's health and must adhere to certain norms and tactics balancing healthy outcomes with respect to patients' rights. Just the same, she may not examine someone in a non-emergency situation unless the patient consents. The patient's consent waives claim rights that would otherwise make it morally wrong for the doctor to touch or probe the patient's body. A previous section concluded that security standard-compliant norms and tactics will respect the rights of all three stake-holding groups involved with intelligence collection. We now need to discuss which rights these groups enjoy. We will focus on how targets and non-targets (whose information might be accidentally collected) might forfeit, waive or cede rights to adversary intelligence officers.

One temporarily forfeits certain rights when one acts unjustly and another party acting in self- or other-defence needs to materially infringe on those rights to halt the unjust action or threat. So, for example, an unprivileged irregular militant, bent on committing acts of terrorism, forfeits privacy rights to his operational communications if intelligence agencies need to intercept his communications in order to interrupt his plots.

Some intelligence targets like national security actors waive rights that would otherwise morally inhibit intelligence agencies from targeting them for collection. One might expressly waive a claim-right to another person, giving her a liberty-right to act in a way that would otherwise violate the rights of the person who ceded the right, as when a patient cedes a right to a doctor to touch his body. Service personnel arguably waive claim-rights against being attacked to future conventional enemies when they enlist in the armed forces, extending permission to enemy service personnel to try and attack them in war-time.⁴

Most non-targets of collateral intelligence collection do not waive their relevant rights. Some *cede* relevant rights though. Again, one can *waive* rights through express consent or tacit consent.⁵ Ceding rights can come as part of being duty bound. A duty to deliver X to Y means one cedes a claim-right for X to Y. One could not, for example, object if Y took proportionate means to seize X if one did not voluntarily do one's duty and deliver it. One might have a duty to deliver something to someone in the context of a particular practice like a game, but more often, one has duties outside of particular practices one voluntarily enters.

One owes a duty to uphold just institutions to the inhabitants of a state and directly expresses the duty to the government employees who are those inhabitants' agents. A duty to uphold just institutions means ceding claim-rights against state agents 1) when those agents are competently pursuing their professional obligations and duties and 2) when insisting on those rights would prevent state agents from serving their principals. This ceding of claim-rights gives the state agents liberty-rights in turn, creating the space for them to perform their norm-compliant actions without wronging the affected parties. So, for example, domestically, a person's duty to uphold just institutions means he cedes claim-rights against having his liberty curtailed by competent police hewing to due process protocols in the event that evidence implicates him of a crime. One does not cede claim-rights to professionals acting in violation of their professional norms or incompetently executing their norms.

The duty to support just institutions is not restricted to institutions of one's own state, but extends in different ways to foreign institutions. The duty to support just institutions is based on the duty to protect the rights of other human beings, a cosmopolitan duty which is unaffected by the nationality of the recipient. So, for example, one cedes claim- and liberty-rights to the state agents of a foreign state one visits as a tourist when insisting on those rights would prevent foreign agents from permissibly performing their duties to protect their own citizens, residents and guests (e.g. tourists).

Normally, the duty to support just institutions does not require one to do anything for state B when one is residing in state A.⁶ That said, one should usually

cooperate with foreign law enforcement officers if one can provide information about a crime committed abroad. This is an expression of the cosmopolitan duty to help protect other people's rights. The foreign law enforcement effort may also protect oneself in the case of international crime like drug trafficking or terrorism. This claim may not be too controversial. When it comes to another state's *adversarial* actions against one's own state, the duty to support just institutions owed foreigners even entails ceding certain claim-rights against foreign national security agents who are acting according to their professional duty. The scope of this rights-ceding is set, on the restrictive side, by the security standard, and on the permissive side, by 1) what is necessary for adversary agencies to keep their people safe and 2) what intelligence actions the rights-ceder can be modelled as accepting.⁷

On the restrictive side, inhabitants of one state can object to the actions of an adversary agency that fail the security standard, for example, if the agency is employing norms and tactics that are more unreliable, disproportionate, ineffective, inefficacious and rights infringing than alternatives the agency has at its disposal. Agencies cannot be criticized for using the best technology they can afford, even if it is less sophisticated than the technology used by the inhabitants of the targeted state. They can be criticized for failing to train in state-of-the-art tradecraft that is based on open-source information and not dependent on technology. Again, the duty to support just institutions does not justify the behaviour of corrupt or incompetent adversary agents.

On the permissive side, inhabitants of one state have a duty to support the just institutions of other states, which entails ceding the claim-rights necessary to create the moral permission for adversaries to keep their clients safe. At base, this permission will cover what are essentially investigative efforts to identify security threats. These actions include *diagnostic* collection efforts designed to anticipate threats.⁸ We will assume that intelligence gathering will involve *accidental* or foreseen but unintentional (i.e. *collateral*) collection on people who are not security risks to the collecting agency's state (e.g. caught in communication with the legitimate target). One cedes claim-rights against *accidental* collection, because if agencies cannot act where there is a risk of collecting or surveilling a mistakenly targeted person, they cannot act at all. It may seem odd to cede a claim-right against an accidental action since the party to which the right is ceded cannot intentionally perform an accidental action. What this ceding involves is really an acknowledgement that the agent would not be considered to have acted negligently when an agency accidentally collects on an innocent party. Civilians' duty to support just (foreign) institutions does not directly address *collateral* collection; this has to be justified via a waiver, discussed later. The ceding of rights associated with the duty to support just institutions is also not the main justification for *direct and sustained* targeting for collection because agencies should only be doing that against security threats to their states and those targets will have either waived or forfeited rights. Given what was just said about accidental collection, innocent parties are not wronged when an agency mistakenly targets them with direct collection efforts and then breaks off collection and purges the relevant data if and when the mistake is promptly understood.

Ceding certain claim-rights that enable foreign intelligence officers to engage in collective efforts that might accidentally or diagnostically collect the information of an innocent person is part of that person's duty to support just foreign institutions protecting foreigners' rights. The scope of adversary permissions can also be widened or restricted based on waivers inhabitants of particular states can be modelled as making. These waivers may also simply reiterate the minimal permissions based on the duty to support just institutions.

One waives certain claim-rights when one enters into a permissible, adversarial practice. For example, a boxer waives his right against being hit when he engages in a bout. This dynamic also applies if one's adversarial practice is mediated by an agent, as in a lawsuit. When one sues someone, one engages a lawyer to try to seize some of the defendant's property or limit her rights. One cannot begrudge the target of one's lawsuit hiring a lawyer to defend her interests in turn. The defendant might after all be in the right or the degree of her wrong-doing may be contestable. By contrast, one cedes no rights to the agent of a fully culpable wrong-doer if one hires an agent to protect one's rights and interests. A gangster may not hire a gunman to bolster his offense against the bodyguard of an innocent person whom the gangster threatened.

So a foreign state agent's actions are potentially justified indirectly, as a reciprocal entailment of a client consenting to his own agents' outward-facing actions. If the inhabitants of state A retained claim-rights against being collaterally, diagnostically or accidentally collected on, then intelligence agencies of state B could not permissibly engage in the same protective function inhabitants_A have a right to demand of (their own) agencies. This is to say that inhabitants_B could not have their moral right to security met to the same degree that inhabitants_A have their right met.

One cannot complain if one is targeted with the same collection tactics one wants one's own agencies to use against foreigners. Since all have the right to protection by their intelligence agencies, consent-worthy intelligence gathering norms and tactics, like consent-worthy legal norms, will be those that are acceptable to all sides equally. They have to be acceptable to one as a client or a target. Agency leaders can model their clients' consent to collection practices at two junctures. First, on the permissive side of the equation, they can ask, what action does securing national security against a particular adversary demand, given the current bilateral situation? Second, on the limiting side of the equation, they can ask, what kind of reciprocal response would clients tolerate? Answers to the second question may eliminate norms and tactics suggested by answers to the first question.

Unlike diagnostic and accidental collection, collateral collection is only justified via a waiver consequent to entering into an agent-mediated adversarial practice. Imagine that a bodyguard can only defend his principal by shooting at an unjust attacker in a way that endangers an innocent bystander. The bystander has a duty to try to rescue endangered innocent people, but not at the cost of her life. We have no grounds to say she would not be wronged if she is injured in the cross-fire. Put differently, the bodyguard is not permitted to fire away, with the thought

that the bystander has ceded claim-rights against being collaterally harmed. We *could* say principals have waived rights against being exposed to collateral harm if everyone had a bodyguard and bodyguards protected their principals against both unjust attackers and other bodyguards. By hiring a bodyguard, one would be entering into a quasi-adversarial, agent-mediated practice. By parity of reasoning, we can say that agency leaders can model their clients' waivers of rights against collateral collection if they also model them as endorsing their intelligence officers engaging in collection efforts that might collaterally collect on foreigners. The agents of such an agency act permissibly when they collect their innocent persons' communications as a side effect of targeting someone with whom the innocent person communicates. Agency leaders can model this consent if and so long as it is technologically impossible to only collect one half of a conversation or textual exchange.

The reflexivity of this model should encourage a conservative attitude towards intelligence collection. We must ask on behalf of the model consentor if she can consent to her state agents using tactics abroad that, via the principle of reciprocity, she must also permit foreign agents to use against her. As will be argued later, this reflexive question also applies to intelligence officers concerning the means and extent to which they are willing to be targeted or have their relatives targeted.

Just intelligence-gathering tactics

Using this reciprocal approach, the rule of thumb should be that security agencies should use the same collection tactics abroad on non-government agents that they use domestically. For example, if the security standard indicates that warrants issued by judges are necessary for a security service to intercept a particular domestic inhabitant's communications or that a domestic criminal suspect has to be warned about a right to remain silent in police interrogation, the same treatment should apply to a foreigner targeted by the security service. Let us now consider several considerations that will present caveats to that rule of thumb. These considerations will argue for an expansion of intelligence collection powers. The second half of this section will consider the rights of different intelligence targets and non-targets, which largely constrain intelligence activities.

Practical limitations on foreign agents acting abroad or the different nature of the target might suggest different tactics leading to greater infringements on the target's rights. Police may be able to conduct line-of-sight surveillance of suspects with undercover officers, whereas such intimate operations may not be feasible against certain foreign targets, particularly in harsh terrain or repressive countries. Long-distance imaging and SIGINT technology may lead to less discriminate operations than domestic operations (e.g. a satellite image can cover a huge footprint compared to what an undercover agent can see). To say this more privacy-infringing tactic is consent-worthy under the security standard is to say the model consentor permits her adversary's security agencies to attempt the same in her country.⁹ While this reciprocity is hard to imagine in some asymmetrical contexts – al-Qaeda operators shelter in the Federally Administered Tribal Area

(FATA), but anti-Pakistan government irregulars do not train in Vermont – there are plenty of peer state rivalries in which reciprocal scenarios are more likely.

A further disanalogy between foreign intelligence operations and domestic law enforcement presents an additional complication. By their nature, intelligence operations are prophylactic, dealing with prospective threats. An intelligence agency might not be adequately vigilant if it only gathered intelligence on known intelligence targets. To anticipate threats or discover new leads, intelligence agencies might wish to engage in bulk data interception and use automated searches to scan the content of the messages or scan the metadata for suspicious patterns or contacts between new numbers and known intelligence targets. Yet this kind of prospective action violates due process in that the target's privacy is infringed prior to evidence of wrong-doing. This form of collection can be made more sensitive to the targets' rights by automating the collection process so that a human analyst only reads or listens to an intercept if there is a high likelihood of its intelligence value, but this is still a significant departure from the standard balance of power between liberal state and citizen. We will need to consider if the security risks for inhabitants of one state are sufficiently grave that they can be modelled by agency leaders as endorsing the risk of being reciprocally targeted by adversary states' dragnet intelligence operations (more in the following).

A third qualification is that reciprocity is necessarily with respect to intelligence function rather than the technological expression of that function. An endorsement of intelligence agency_A's diagnostic collection including broad satellite coverage, selector-guided data intercepts and bulk data collection would permit adversary agency_B's similar diagnostic measures. Yet a wide range of concrete practices could be justified if the security standard permits security services to conduct foreign operations employing the most reliable, efficient, rights-respecting etc. tactics available to the service within a given function area. The best locally available tactics justified by the security service will vary depending on a given political entity's wealth, size, technological prowess and ingenuity. If the standard then effectively permits all security actors to "do their best", the standard allows situations in which, for example, wealthy country A's intelligence services can conduct very discriminate, sophisticated, targeted and automated intercepts of foreign intelligence target's communications – so that very few innocent people have their privacy infringed or violated – while also permitting poor country B's intelligence services to conduct relatively crude, indiscriminate intercepts that infringe on the privacy of far more innocent people. For example, the 2006 film *The Lives of Others* depicts 1980s era Stasi agents steaming open random East German citizens' letters in order to see if they contained any subversive content. This method of intercept is obviously far more invasive than an automated system that only saves communications with specific selectors for human analysis. So the leaders of technologically sophisticated agency_A, considering targeted intercepts of foreign expats_B on A's soil, would need to consider if their relatively backward adversary in state B will reciprocally respond by steaming open the mail or listening to all the phone conversations of expats_A in state B. Thus, intelligence collection activities fail the security standard in particular instances if one state's adversary's best

methods of intelligence collection are so crude as to be imagined to be intolerable to the inhabitants of the target state. In this case, intelligence officers would need to refrain from collecting from a certain state if they could anticipate that the state would retaliate by engaging in its crude collection methods (political entities with more sophisticated adversaries would not encounter this problem). That said, it is difficult to think of an example of SIGINT that would be so rights-infringing as to be intolerable for any state to suffer at the hands of its dangerous adversary if that was the price of garnering signals intelligence. One's tolerance of risk is influenced by the nature of the harm the risky activity forestalls. Crude forms of SIGINT might be intolerable if the reward for the risk was lower, such as if the target state did not pose a military threat to the collector state.

One might wonder if any states enjoy a unilateral right to collect against adversaries because of the illegitimate nature of the target government. As mentioned earlier, one can hire a bodyguard if threatened by a gangster, but the gangster does not have a right to hire extra gunmen in response. Since the security standard is indexed to the protection of negative liberty, it justifies traditional policing and national security actions of even some illiberal and/or autocratic states. While the security standard does not justify repressive actions aimed at a government's non-violent political or ideological opponents, it does justify the bread-and-butter responsibilities of a state aimed at protecting its inhabitants from street crime, piracy, terrorism and foreign military attack. I will follow John Rawls's usage referring to states that do this as well as provide internal law and order in a mostly egalitarian manner as "decent states" (I will refer to states, but it could also be the case that a political entity within an internationally recognized state might have significant autonomy and protect its inhabitants from external threats). Hence, Russia, China and Iran, for example, have the right to engage in foreign intelligence operations as a means of defending their people against foreign military attack and intelligence collection. The security actions autocratic states may legitimately engage in to protect their people also protect the autocratic regimes, which, in other moments, may repress their own people. Internal repression has to reach a high level to remove hypothetical consent to a state's national security operations. Under these conditions, foreign invasion would be rationally preferable to the perseverance of the repressive regime. The security standard does not justify the coercive actions of states with governments that largely neglect ordinary inhabitants and use power largely to benefit a ruling clique. Such governments are virtually indistinguishable from criminal gangs. I will refer to these as unjust states.

The security standard prefers the most rights-respecting out of the most practically efficacious tactics and norms that are locally feasible. We therefore have to consider the scope of intelligence targets' rights, applying the justifications for intelligence operations to specific categories of targets. In order to accomplish this aim, we have to consider both the target and the context for collection. Any SIGINT or IMAGINT operation will involve three major relevant variables: the collecting agency, the target and the agency with defensive jurisdiction over the target. Significantly, there are agencies with roughly equal technological abilities

with their adversaries; agencies with greater abilities than their adversaries and those with lesser abilities. There may also be situations where a target is in a failed or unjust state and has no intelligence agency acting on his behalf. In all the cases where a functioning and responsible agency exists, the collecting agency has to consider if the defending agency's retaliation or reciprocal actions are tolerable for the collecting agency's own citizens given the overall threat environment. This concern will likely be readily addressed in the affirmative if the collecting agency is technologically or operationally inferior to its adversary since there is a good likelihood that the adversary's relatively discriminate reciprocal response will be tolerable to the collecting agency's citizens (obviously, this would not be the case if both agencies were operating on a very crude level and one was only slightly more sophisticated than its rival). The situation facing inhabitants of failed and unjust states will be addressed at the end of this section.

I would suggest there are seven relevant categories of intelligence targets:

- 1 a positively identified foreign intelligence officer or service member
- 2 a suspected foreign intelligence or military agent (the latter might be non-uniformed)
- 3 a non-specific target, for example a random person collected against in dragnet fashion
- 4 a civilian of intelligence value, for example a politician, bureaucrat, engineer or scientist
- 5 the relative, lover, colleague or friend of 1–4
- 6 a positively identified unprivileged irregular, for example a member of a terrorist group
- 7 a suspected unprivileged irregular

People have rights to privacy which presumptively cover professional communications. Certainly, it is wrong for professors, doctors, accountants, priests etc. to hack each other's professional correspondence. Adversary military, privileged irregular combatant or intelligence personnel in decent states have a right to communicate their operational plans with colleagues since (according to the traditional post-Westphalian just war tradition) these professionals do nothing legally or morally wrong in pursuing national security goals. Yet since their adversaries have the same right to pursue the national security goals of their own political entities, those adversaries can engage in strategic behaviour such as intercepting their enemy's communications.¹⁰ National security actors waive their rights against having their operational communications intercepted when they join their organizations since they know the parameters of the profession include communication interceptions. Further, assuming that the operationally significant information collected regards state secrets, foreign security personnel do not suffer personal privacy violations when their communications are intercepted. The professional secrets are in a sense, state property, like military materiel. Waiving claim-rights against being targeted with collection efforts is not the same thing as waiving rights to the information, in which case it would be wrong for the agent

to attempt to conceal the information. Intelligence officers can take steps to safeguard their communications and resist intrusions. Waiving claim-rights against being targeted with collection efforts does not entail a requirement to volunteer the relevant information any more than waiving a claim-right against being struck in a boxing match means a boxer must refrain from ducking.

Intelligence agencies will often want to collect personal information about their state agent target. The recruitment of intelligence assets from within military and intelligence agencies sometimes occurs when recruiting agents identify vulnerabilities or dissatisfactions on the part of their targets. Further, many intelligence officers work undercover. One way to identify undercover agents is to closely monitor their communications and examine the documents associated with their “legends”. Certainly, intelligence officers know how their game is played, so voluntary entrance into the profession, where they are trained about information security and the professional perils of personal foibles, can be understood as amounting to a waiving of a claim-right against having their personal information being targeted by adversary collectors.

There is a greater separation between public and private for service personnel than for intelligence officers. Going to work for service personnel may mean physically deploying to a different country or to sea. Stateside service personnel conduct most of their professional work on bases in uniform using unique military matériel and using specially secured communication and data storage devices. So there is usually a physical and social separation between professional and personal lives. Unlike civilian intelligence officers, service members can readily do their jobs in most cases without intercepting their adversaries’ private communications or information. Further, in most cases, their job is overt; unlike many intelligence officers, they present themselves as service personnel while working. So the personal communication and data storage of service personnel per se are usually irrelevant to adversaries; it does not relate to national security and does not identify a service member’s true profession. Yet service members’ personal information can be turned into a vulnerability through their own indiscretions. Damaging information is of interest to adversary agencies as it can make service personnel vulnerable to recruitment.

I do not think that it is permissible as a matter of course for adversaries to target all the private communications of service personnel and hack all their personal data files looking for leverage. Militaries need to recruit relatively large number of people. Enlistees know of course that they will be physically vulnerable to enemies in the event of war (which statistically, they may well avoid during their time of service). Since intelligence collection is prophylactic, agencies would want to collect potential blackmail material against service personnel from potential future adversaries as soon as they enter the military. It seems unrealistic to think that many potential enlistees would be willing to enlist if they knew that all potential adversaries would be invading their privacy as a matter of course and that unlike intelligence officers, they would not have the advantage of clandestine identities to shield them from adversaries’ attention. So, unlike intelligence officers, who know how intelligence operations work and who have some protection in their

clandestine identities, it does not seem reasonable to think enlistees waive a right to all their personal information to foreign adversaries. Leaders of intelligence agencies would also have to consider the effect on military recruitment if this kind of information collection became the new normal, brought about in part through their universal collection of their adversary military's personal information.

Finally, like intelligence officers, privileged irregular militants engaging in guerrilla tactics typically hide in plain sight by presenting themselves as ordinary civilians when not engaged in operations. Since they dress as, and live among, non-combatant civilians, they cannot begrudge their conventional adversaries engaging in counter-insurgency to collect personal information and intercept communications on suspected targets in order to distinguish irregulars from non-combatants.

In 3) and 7) a variety of intelligence collection operations, including counter-insurgent operations, regularly produce false-positives, interdicting innocent people mistaken for militants. A clearly concerning case is where the communications of innocent people might be collected and analysed when their out of context remarks trigger automated collection or where intelligence operations wrongly indicate that a particular person is a foreign intelligence officer, intelligence asset or an irregular militant. In a domestic law enforcement context, rights-infringing investigations of suspects (who turn out to be innocent) can sometimes be justified. State agents tasked with investigative functions cannot only interact with guilty persons or people of intelligence value. Agents' mandate instead is to investigate suspects, people who might be innocent or might be guilty. Agents would not be meeting their protective duty if treating all suspects with the benign indifference they do apparently innocent people. Similarly, intelligence operations ill-serve the state if they are restricted to investigating known threats, to the exclusion of anticipating future threats. Investigations require some rights infringements like questioning, arrest, interrogation and searches. People in a just state, where state agents can be held accountable for bad behaviour, do not have their rights violated by security standard-compliant investigative actions since they can be modelled as consenting to security standard compliant norms and tactics aimed at protecting their rights. The case is more complicated in international settings since the intelligence collector is not necessarily acting to secure the community of which the target is a part and the target likely will not have the ability to identify or sue the intelligence agents who wrong her.

As an expression of their duty to support just institutions, inhabitants of one state cede claim-rights against having some of their information collected diagnostically by an adversary agency in order to ascertain if they are a security threat. This diagnostic level of collection would seem to be the minimal requirement of a duty to support just foreign security institutions. All people have a right to demand that their security agents identify looming threats. Ceding a right against diagnostic collection is a way to support this right enjoyed by foreigners. So, intelligence agencies may be justified – contingent on meeting the practical elements of the security standard – in conducting automated dragnet signal interception of civilian communications guided by selectors, in which all data from a particular

region is digitally scanned for certain security sensitive references prior to select communication being forwarded to a human analyst for consideration. Metadata recording and retention may also be justified for the same reason. Agencies might want to retain years' worth of big data in order to have a library to scan if current investigations highlight an old communication as being of significance. Agency leaders might model inhabitants of their states accepting the risk that their adversaries will store their old communications but never view them – unless the adversary finds evidence that a citizen is actually a spy or a terrorist – as a cost of their own agencies doing the same thing in a fraught security environment. Inhabitants of states without major security concerns could not be modelled as accepting this risk. The cost to civilians is steeper, and potentially less tolerable, if an adversary had very sloppy selection algorithms and so fed a large number of false-positive communications to human analysts. Still, even this cost is perhaps tolerable since the foreign analyst presumably reads an anonymized text or email. By contrast, the cost might be unbearable if the adversary's diagnostic efforts involved reading every written communication or listening to every conversation as a matter of course. Businesses might fear intercepted and stored communications more than individuals. Even if an agency is reasonably sure its rival does not engage in industrial espionage, it has to consider if domestic business actions would be harmed because of executives' fears that sensitive communications *could* be intercepted and misused or leaked.

A further point for agency leaders to consider on the subject of big data collection might relate more to the retention, rather than the collection, of the data. The cost to average citizens and businesses is greatly increased if intelligence agencies store their intercepted data on relatively insecure servers and then hackers steal the data and make it available in a searchable database. One might not worry much if one's online searches and texts are stored on an NSA or MSS server in some desert, never to be read unless one starts corresponding with jihadists, but worry very much if that information is available on a website prospective employers, spouses and divorce attorneys can search for a modest fee.

Due process protections can help make domestic criminal investigations security standard-compliant. People can demand to be protected from criminals and have crimes against them promptly solved, but innocent people also do not want to be regularly inconvenienced or frightened by ham-handed investigations and so would endorse checks on investigators by neutral arbiters to help ensure that investigations are warranted. Appealing to the reciprocal element of the security standard, inhabitants of one state would endorse due process style protections appropriate for domestic undercover work for foreign intelligence targets if their agencies needed to move beyond the diagnostic phase to target a particular person the initial diagnosis suggested was a threat. Graduated due process protections are important since the same standards inhabitants_A could be modelled as endorsing could guide collection efforts targeting them on behalf of inhabitants. Some due process protections involved in an overt domestic investigation such as those involving arrest and interrogation are not apt since the target will not initially, if ever, know he is an intelligence target. The key relevant protection is

the requirement of a warrant from a neutral court prior to engaging in collection against foreign civilian targets. Collectors would have to produce evidence that the desired target is a person of intelligence value. The court should view foreign intelligence targets as having the same privacy rights as domestic inhabitants, be it with respect to their physical person, their possessions, their communications or their data. This requirement would extend to targets who are suspected of being civilian intelligence officers operating outside security-sensitive areas like intelligence agency headquarters and embassies.

Intelligence agencies might also take an interest in politicians, diplomats and civilians working in sensitive industries. Their work product on their computers and work-related communications are fair game for interception if they pose a potential threat to other states. These professionals can be modelled as waiving claim-rights against having work-related communications and devices targeted (posing a risk of collaterally capturing personal communication) since they voluntarily took jobs where they pose indirect threats to adversaries or are part of a state's overall foreign policy establishment. Security training likely regularly reminds them of what is at stake in their communications. Moreover, they should choose to be scrupulous in separating personal from professional communication.

The harder question is whether they have ceded claim-rights to all their personal data. Intelligence agencies might very much want to gather embarrassing or incriminatory information against a politician, diplomat, or defence contractor in order to blackmail him or find out personal information about him in order to improve a recruiting officer's ability to develop rapport. I suggested earlier that the security standard would likely not permit targeting service personnel in this manner because the reciprocal cost is too high. Cost is relative, so it would be more accurate to say that the cost of inviting universal collection against one's own military usually outweighs the benefit of collecting against random service personnel. The benefit of collecting damaging information against select politicians, diplomats or weapons scientists is far greater. Further, the number of people targeted is relatively small. Politicians and diplomats can be trained about the risks of extracurricular indiscretions and provided with relatively secure devices. Politicians in democracies are also partially vetted during campaigns as their opponents try to identify and publicize any damaging information. In many cases, scandals foreign intelligence agencies might discover have already been revealed to voters.

Scientists and other researchers working very closely on weapons or intelligence gathering technology can perhaps be modelled as waiving claim-rights against having personal information targeted since they likely know or should know the tactics of adversary agencies and the importance those agencies place on the scientists' work. It seems a heavy cost to researchers working on more peripheral research, perhaps on defence or intelligence grants, if their funding comes with a risk that all their personal information will be potentially collected and exploited by foreign intelligence agencies. Here, leaders of agencies would have to think very carefully if the security environment warrants reciprocal invasions of domestic researchers' privacy.

Intentionally intercepting the communication or records of friends, relatives and lovers of all the aforementioned categories is fraught. To be clear, this tactic involves separate targeting of a target's familiars, not incidentally collecting against them in the course of intercepting the target's communications. Intelligence agencies may seek personal information that could be used to blackmail targets regarding their relatives' foibles or to reveal vulnerabilities or proclivities that intelligence officers might otherwise exploit in order to cultivate the person as a spy. Intelligence officers might also offer incentives to targets to help relatives in distress.

First, relatives of service members, intelligence officers, weapons researchers etc. have not waived rights in the role-based manner of their relatives. Have they forfeited their rights by being complicit in their relative's actions? One cannot help what career one's child, parent or sibling chooses, but what about a spouse? The spouse of a service member knows about his or her spouse's profession, but an intelligence officer might never reveal his true profession to his spouse or at least not until after they are married. Bearing in mind that reciprocal element of the security standard, it seems too high a bar to demand divorce as the price of avoiding being targeted for intelligence collection. Still appealing to this reciprocal element, intelligence officers have to consider if they are willing to have their own relatives targeted for intelligence collection prior to targeting their potential assets' relatives. Such targeting violates the targets' rights. Except perhaps in the most perilous security environments, it seems the reciprocal element would preclude targeting relatives.

Finally, an international criminal like a drug dealer, a pirate or an unprivileged irregular combatant,¹¹ whose operational communications are intercepted, does not have his moral rights violated wherever he is located because he lacks a right to contribute to criminal operations via those communications. However, since his identity is likely not overt, the collecting agency has to go through due process steps of getting a warrant prior to targeting him. Failure to do so would violate the target's rights even if he really was a criminal.

The foregoing argument assumes that targets live in decent states with functioning governments engaging in national security work on behalf of their inhabitants. Unprivileged irregulars and other types of criminals sheltering in failed or unjust states have no more of a right to secret operational communications than they do if they are operating in just states. Service personnel and intelligence officers serving unjust regimes are effectively serving criminal organizations and so, like ordinary criminals, forfeit a right to their operational communications. Defence contractors or weapon scientists in unjust states may be closer to criminals if they are knowingly colluding with an unjust regime. Those who are coerced by their repressive governments are wronged by being targeted for collection since they have not forfeited their rights through culpable collaboration. Agencies in other states need to appeal to the doctrine of double effect or lesser evil arguments in order to justify wronging these groups of people.

Service personnel, intelligence officers and defence contractors presumably are not present in failed states. People in failed or unjust states have a duty to support

just foreign institutions as a way of respecting foreigners' rights. This duty means ceding claim-rights against diagnostic and accidental collection, but not collateral collection. Collateral collection occurs when an agent foresees that collecting against a target will also capture information from a target's interlocutors even though they are not intelligence targets. My view is that minimal diagnostic collection meant to ascertain if one is a security threat is included in the duty to support just foreign institutions, but collateral collection is only justified via a waiver consequent to entering into an agent-mediated adversarial practice. A waiver of rights against collateral collection is entailed by a modelled endorsement of one's agents engaging in collection efforts collaterally collecting on foreigners. Agency leaders can model this consent if or so long as it is technologically impossible to only collect against one member of a conversation. Thus, this justification does not extend to non-targets in failed or unjust states because these people lack intelligence agents working on their behalf against foreign adversaries.

One might think that non-targets living in unjust states have a duty to help protect foreigners from the non-targets' unjust leaders. Yet non-complicit civilians in unjust states are like hostages, victims of their own leaders and potentially threatened by adversaries as well. Their duties cannot extend beyond those of non-targets living in just or decent states. They are wronged by collateral collection. Agencies would have to appeal to the doctrine of double effect or make a lesser evil argument to justify violating these people's rights.

Collateral collection *is* permissible if it will ultimately contribute to rudimentary law enforcement benefiting non-targets like the interdiction of terrorists or drug dealers in a failed or unjust state. In that case, innocent people in the target area can be modelled as ceding claim-rights to any agency that will act in the interest of their rights when local criminals are removed from the scene.

Notes

- 1 Gendron, Pfaff, Diderichsen and Vrist Ronn make the same point in rejecting direct application of just war theory to intelligence operations (Gendron 2005, 418; Pfaff 2006, 75; Diderichsen and Rønn 2017, 482).
- 2 Pfaff and Tiel also use a social contract framework (Pfaff and Tiel 2004, 4).
- 3 For example, an egalitarian norm will exclude certain tactics that focus only on certain ethnic groups.
- 4 I make an argument for this position in Chapter 7 of my *The Moral Status of Combatants: A New Theory*.
- 5 The latter can be effectuated by voluntarily entering into a practice involving certain well-known concessions on the parts of members. For example, one tacitly consents to abide by the rules of a game when one voluntarily begins playing, even if those rules might force one to suffer some harm or loss. When one loses a hand in poker, one cannot object that "I wasn't playing *that* sort of poker".
- 6 Though, for example, one ought not to subvert foreign elections by posting disinformation on the internet.
- 7 Pfaff and Tiel have similar ideas, but express their ideas in a terse manner that prompts many questions.

- 8 Pfaff and Tiel base the permission to engage in diagnostic collection on tacit consent. Their position is vulnerable to standard critiques of John Locke's famous account of political obligation based on tacit consent. Namely, one can ask how tacit consent obtains if citizens are never provided with the express terms of the "contract" and do not have meaningful refusal options.
- 9 The adversary agency's permission does not mean agencies in the target state are not permitted to oppose their actions.
- 10 See *An Ethics of Interrogation*, Chapter 7.
- 11 An irregular combatant is a combatant who uses guerrilla tactics and/or represents a non-state group (often then using guerrilla tactics). An unprivileged irregular is one who fails the criteria for moral and lawful belligerency: obeying a unified chain of command, carrying one's arms in the open, wearing identifying emblems, and obeying the laws and customs of war.

References

- Diderichsen, Adam, and Kira Vrist Rønn. 2017. "Intelligence by Consent: On the Inadequacy of Just War Theory as a Framework for Intelligence Ethics". *Intelligence and National Security* 32 (4): 479–93. <https://doi.org/10.1080/02684527.2016.1270622>.
- Gendron, Angela. 2005. "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage". *International Journal of Intelligence and CounterIntelligence* 18 (3): 398–434. <https://doi.org/10.1080/08850600590945399>.
- Omand, David, and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Illustrated edition. Washington, DC: Georgetown University Press.
- Pfaff, Tony. 2006. "Bungee Jumping off the Moral Highground". In *Ethics of Spying: A Reader for the Intelligence Professional*, edited by Jan Goldman, 66–103. Lanham, MD: Scarecrow Press.
- Pfaff, Tony, and Jeffrey R. Tiel. 2004. "The Ethics of Espionage". *Journal of Military Ethics* 3 (1): 1–15. <https://doi.org/10.1080/15027570310004447>.
- Skerker, Michael. 2016. "Moral Implications of Data-Mining, Key-Word Searches, and Targeted Electronic Surveillance". In *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley J. Strawser, 251–75. New York: Oxford University Press. www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190221072.001.0001/acprof-9780190221072.
- . 2019. "A Two Level Account of Executive Authority". In *Sovereignty and the New Executive Authority*, edited by Claire Finkelstein and Michael Skerker. New York, NY, USA: Oxford University Press.
- . 2020a. "What Can Be Asked of Interrogators?". In *Interrogation and Torture: Integrating Efficacy with Law and Morality*, edited by Steven J. Barela, Mark Fallon, Gloria Gaggioli, and Jens David Ohlin, 253–78. New York: Oxford University Press.
- . 2020b. *The Moral Status of Combatants: A New Theory of Just War*. 1st edition. Abingdon, Oxon; New York: Routledge.

6 Digital sleeper cells and the ethics of risk management

Kevin Macnish

Introduction

The advent of networked systems has brought with it new opportunities in intelligence, giving rise to a sub-species of “cyberintelligence”. One such opportunity is that of what I refer to here (for want of a better term) “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. There is limited written evidence of such cells existing, the most famous being that used on the Ivano-Frankivsk power network in 2015 (Lehman 2016), but anecdotal evidence suggests that the Ivano-Frankivsk case was not an anomaly.

Such new opportunities bring with them new risks, including ethical risks. This calls for intelligence ethics to expand to include cyberintelligence and with it the ethical debate to similarly expand. The problem, as I argue in the following, is that traditional ethical frameworks for intelligence, and particularly the notion of *jus ad intelligentia/in intelligentium*, are often insufficiently granular to provide ethical guidance in cases of uncertainty. Whereas traditional (analogue?) intelligence has centuries of case studies to draw on, the new ethical issues arising in cyberintelligence have no historical analogies.

In this chapter, I argue that a way forward in developing an ethics of cyberintelligence, at least insofar as consideration of proportionality is to play a role, is to consider likely reciprocity. I explore this through an analysis of the aforementioned digital sleeper cells. Following an introduction to some of the challenges facing intelligence ethics in the digital, networked age, I consider the nature and role of digital sleeper cells and how they are likely to be perceived by those using them and by those affected by them. I then suggest that the recently developed ethics of risk literature can inform and guide ethical intelligence activities through their ability to highlight complicating factors which may otherwise be overlooked.

It is important to note that in this chapter I am not suggesting that any current or former intelligence agencies are being cavalier in their use of digital sleeper cells. From private conversations, the impression given is that the use of these tools, at least in liberal democracies, is extremely limited and carefully controlled. While some may be willing to take such reassurances on trust, many will not, especially in light of intelligence scandals such as reportedly “sexed up” dossiers being used

by politicians to justify going to war (Herring and Robinson 2014; Humphreys 2005). Furthermore, while we may currently have morally trustworthy intelligence chiefs in post, it would be complacent to presume that this will always be the case. I am hence not writing in critique of any one state or agency, still less any individuals. I am, though, writing with an eye clearly on the future moral health of the intelligence community.

Intelligence ethics

There are a number of ways, theories and frameworks through which we can approach intelligence ethics. If intelligence is about finding out, or trying to find out, information that we do not already know, then intelligence ethics is about discovering this information in an ethical manner. As such, there are a number of standard normative frameworks that can be applied to intelligence ethics. I have argued elsewhere (Macnish 2017, 78–82) that, at the very least, we can think about intelligence ethics from a deontological perspective, a consequentialist perspective, a virtue ethics perspective or a reciprocity perspective. Each of these has its respective advocates and dissenters. However, I also believe that one of the most promising frameworks for understanding intelligence ethics is that of the just war tradition. This approach has been promoted by Michael Quinlan, David Omand, Ross Bellaby and myself at different times in the past (Bellaby 2014; Macnish 2017; Omand 2011; Quinlan 2007). The just war tradition carries the advantage of a combination of both deontological and consequential thinking, coupled with a rich tradition of philosophical reflection and case studies.

One challenge to using the just war tradition in thinking about intelligence ethics is that, while the aforementioned historical tradition is indeed rich and varied, it has only recently started to be applied to intelligence ethics. As such, there are far fewer cases or arguments from which to draw when one comes to specifically intelligence-related problems. The just war tradition is therefore a valuable framework through which to understand established ethical problems, but it is far weaker when it comes to determining what to do in scenarios with new and emerging technologies. For example, we can agree that there is strong rationale for thinking that any intelligence activity should be proportionate in terms of the harms that it risks when balanced against the benefits that it promises. However, proportionality is notoriously complex even in established war thinking. Take, for example, the sinking of the Argentinian light cruiser *ARA General Belgrano* in the Falklands crisis in 1982 (Rice and Gavshon 1984). The *Belgrano* was in international waters, sailing away from the Falkland Islands when it was torpedoed by HMS *Galahad*. From a tactical perspective the *Belgrano* posed no threat and so the sinking of the largest ship in the Argentine Navy appears to have been a disproportionate action, especially considering the 3000 lives that were lost when the ship sank. Yet from a strategic perspective, the *Belgrano* was able to protect the rest of the Argentine fleet from the British Navy. With the removal of this battleship, the British Navy was able to dominate the waters around the Falkland Islands, strengthening the British military presence significantly (Rice and

Gavshon 1984, 115–31). Hence we might say that the sinking of the *Belgrano* was disproportionate from a tactical perspective but proportionate from a strategic perspective.

If there are such challenges within traditional war discourse when it comes to determining proportionality, how much more difficult is this when thinking about new technologies used in intelligence? The challenge here is that the condition of proportionality frequently lacks sufficient granularity to be able to determine what is and is not a proportionate action in intelligence. We are therefore challenged to come out with ethical guidance in the face of a very broad brush framework. There are further problems in applying the just war tradition to intelligence, not least that the just war tradition is a predominantly Western tradition, rooted in a combination of classical philosophy and Judaeo-Christian ethics. As such, one wonders how such ethical precepts might be applied on a global level. There have been attempts to develop a truly global ethics in recent years, catalyzed by the international aspect of the internet and globalization (Brey 2007; Ess 2008; 2006; Küng and Kuschel 1993; Widdows 2014; 2016). While these concerns are hardly new in thinking about military ethics (we have, after all, experienced two world wars in the last 120 years) they do leave open concerns that what appears proportionate to western values may not appear to be proportionate when one's starting point is Buddhist or Taoist ethics.

Finally, there is the concern of the Collingridge dilemma (Kudina and Verbeek 2019; Liebert and Schmidt 2010). This states that we have an essential problem in determining the ethics of new and emerging technologies. We frequently do not know what the ethical problems with new technologies will be until those technologies have become embedded in society. The dilemma then arises because when the technology has been fully embedded in society, it is too late to restrict or even prevent the distribution of that technology. There have been several suggestions as to how to approach ethics of emerging technology,¹ but the problem remains that we will always be left in a position of some uncertainty as to the ethical implications of new technologies prior to their actual use in society.

If we bring these three concerns together (the lack of granularity in determining proportionality, the varying ethical assumptions across the globe and the empirical uncertainties of new technologies) then we discover some significant gaps in the application of just war thinking to intelligence ethics insofar as this concerns new and emerging technologies. In the face of these gaps I want to propose that a practical way forward is to consider what we believe will be the likely response of the spied upon party upon discovery of a particular act of espionage. This would fall within the traditional *jus in intelligentia* category of considering likely consequences without necessarily being consequentialist (Hurka 2005; Macnish 2016; 2015). Furthermore, my proposal is not that we determine our action on the basis of a likely response, but rather that we determine our tolerance threshold for such responses. That is, we should determine our behaviour on the basis of what we may reasonably trigger by our actions. Note that this is not a condition of reciprocity through which we may find that we are drawn into a vicious cycle of being forced to conduct unethical acts because our adversaries have committed

those acts. Rather, it is a matter of asking whether it is acceptable for us to do X if we have reasonable grounds to believe that X will trigger Y.

For example, if the act of arresting an intelligence officer from an adversarial state is reasonably believed to occasion a declaration of war from that state, then we may determine that the arrest of said officer would be a disproportionate act. If, on the other hand, the arrest is likely to occasion a reciprocal arrest of one of our intelligence officers in that state, then the act might well fall within our tolerance threshold of a reasonable price to pay for the action. At the same time, the context might be such in which the declaration of war may be appropriate for other reasons (and hence fall within our tolerance threshold), or indeed in which the arrest of one of our intelligence officers would fall outside our tolerance threshold. In the remainder of this chapter I will develop this thought of considering tolerance thresholds to the risky application of new technologies in intelligence (and specifically, cyber intelligence).

Cyber intelligence and digital sleeper cells

We may distinguish between security, counterintelligence and intelligence through a lens of active versus passive approaches to state security and economic well-being. Security is a matter of preventing attacks or espionage against the state through relatively passive means, while counterintelligence involves preventing attacks or espionage against the state through more active measures designed to reveal the intentions and abilities of adversaries. Intelligence itself is then about attacking adversaries in order to gather intelligence on their intentions and abilities. More kinetic active approaches such as *agents provocateurs* and sabotage, while not forming a part of intelligence collection in a strict sense, frequently fall within the purview of state intelligence agencies. That is, they are not, at least in times of peace, the appropriate domain for military action but are rather managed by state intelligence.

A similar continuum can be drawn when it comes to the online connected world of cyber. Cyber security is relatively passive, seeking to prevent attacks and espionage through the use of firewalls, monitoring and the development of highly secure systems. Cyber counterintelligence is the more active state of preventing attacks and espionage through the active gathering of intelligence about the terrorist or espionage intentions of adversaries. Cyber intelligence is therefore focused on attacking adversaries in order to gain intelligence on their broader intentions and abilities insofar as these have a bearing on the state. Acts of cyber sabotage, fake news generation and similar cyber activities once more fall beyond the traditional understanding of intelligence and yet are not clearly military activities when enacted during peacetime. As with the physical analogues of *agents provocateur* and sabotage, acts of cyber sabotage and active disinformation campaigns interfering with domestic activities of adversarial states are typically managed by state intelligence agencies.

One particular approach to cyber sabotage and cyber intelligence gathering is that of a digital sleeper cell. This is a form of malware which is inserted into

an adversary's computer network but which remains dormant until activated at some point in the future. The analogy is drawn with a sleeper cell in terms of intelligence collection, for instance when agents are inserted into a foreign country and live as regular citizens in that country for years, building networks of trust and allowing them to rise to positions of significance and importance before becoming active and returning information to their country of origin (Leuprecht, Szeman, and Skillicorn 2019). This is an approach which has reportedly been employed by China in infiltrating a number of US economic interests over the last 20 to 30 years as a means of gathering intellectual property on key technological developments (Fialka 1999, 18–40).

The digital sleeper cell is therefore distinct from more traditional forms of cyberattack such as worms, Trojan horses and phishing attacks. A digital sleeper cell may be used to insert one of these traditional forms of malware, but only when the sleeper cell is activated. Hence the Stuxnet virus developed by Israel and the United States and employed against the Iranian nuclear power system in 2011 was a virus which brought down that system but was not a digital sleeper cell as it became active as soon as it was placed in the system (Farwell and Rohozinski 2011; Langner 2011). Similarly, the WannaCry and notPetya attacks of more recent years were straightforward cyberattacks (Greenberg 2018; Marsh 2018; Mattei 2017; Mohurle and Patil 2017; Smart 2018). By contrast, the Black Energy virus used against the power grid in the Ivano-Frankivsk region of Ukraine in 2014 involved the use of a digital sleeper cell. In this case, the virus had lain dormant in the system for some time before it was triggered by various people, themselves subject to a spear phishing attack, clicking on macros in Microsoft Excel files (Lehman 2016).

Digital sleeper cells do not have to be used solely for the purpose of sabotage. They may, for instance, also be used in intelligence gathering activities. Such a cell may be inserted into a country's network but once more will remain dormant until active, at which point it will start returning information to the initiating organization. In the case of intelligence collection it is perhaps harder to see why one would not wish to begin the intelligence collection immediately. It may be the case that one wishes to have the potential for intelligence collection on a certain network without having the need or perhaps the capacity to deal with the intelligence that the network would reveal in the short term. However, the discovery of such a digital sleeper cell would likely occasion a similar response to the finding of an active intelligence gathering cyberattack. By contrast, a digital sleeper cell aimed at sabotage, if discovered, might occasion a less extreme response than the act of sabotage itself. The discovery of a digital sleeper cell is hence similar to the discovery of a "real threat". One may know in principle that there is a threat (what we may call a "mere threat"), but the discovery of actual means in place to enact the threat elevates it to a "real threat". A "real threat" poses a greater risk to the state than a "mere threat", but not as much risk as it would were the threat to be enacted. There are hence three levels of concern: "mere threats", "real threats" and "enacted threats". As these increase in terms of harm (from potential to actual), the severity of response is likely to increase also.

It is also worth noting that digital sleeper cells may or may not be anonymous. In the analogue equivalent of an espionage sleeper cell, the agents in that cell would not wish to reveal the intentions of the sending organization (i.e. that they are present purely for the purposes of economic espionage for their sending country). In the case of the digital sleeper cell, though, it may be that the sending organization desires that it is recognized as such after the act of sabotage has occurred. Through this, the sending organization might gain kudos within the intelligence community, gain the advantage of fear over adversaries and potential adversaries and show off to its political bosses about the efficacy of its operations. This was the case with the Black energy digital sleeper cell in Ukraine around which there seems to have been no question but that it had been developed and put in place by Russian intelligence (Lehman 2016).

It is therefore the task of state cyber security agencies to protect against the insertion of digital sleeper cells into sensitive state networks. These agencies are typically tasked also with the counterintelligence activity of locating digital sleeper cells, and frequently also with the development and placing of digital sleeper cells themselves in adversarial networks. As such, digital sleeper cells are becoming an active and pervasive means of low-level cyber conflict, a “real threat” within a domestic networked infrastructure. A key ethical concern with the use of digital sleeper cells, though, is that we do not know how they will be received upon discovery by the recipient state (Leuprecht, Szeman, and Skillicorn 2019). I have suggested, for example, that the discovery of a digital sleeper cell with the goal of triggering an act of sabotage might occasion a lesser response than the act of sabotage itself. However, this is not a given. It may well be that the recipient state chooses to interpret the presence of a sabotage-related digital sleeper cell as tantamount to the act of sabotage that it threatens. As Leuprecht et al. note:

because of the widespread lack of understanding of the operation of cyber and cyberphysical systems, the difficulty of distinguishing malice from incompetence when communication and computation systems malfunction, and the difficulty of assessing intent, the targets of [digital sleeper cells and other offensive threats] cannot easily judge the magnitude of the threat. There is at least the possibility that they will overreact, perhaps extremely. This could lead to retaliation at higher levels and so escalation, perhaps even spilling over into kinetic responses.

(Leuprecht, Szeman, and Skillicorn 2019, 400–1)

In this way, we are returned to the three problems raised earlier regarding the use of the just war framework for determining ethical actions in cyberspace. There is a lack of granularity in terms of determining whether a digital sleeper cell would be proportionate, based in part upon a lack of knowledge as to how the sleeper cell would be perceived by the recipient state and the challenge of the Collingridge dilemma that we will not know for certain the impact of the digital sleeper cell until it is activated.

For example, imagine that South Korea places a digital sleeper cell on a North Korean network. In this case, context is crucial. The likely North Korean response would probably differ depending on whether the network related to the Ministry of Defence, a munitions factory, a power network or a hospital. It seems that there are a number of potential responses that North Korea could take in this situation. It might decide that digital sleeper cells are what it does as well and therefore not worry overly about the situation. It might believe that its own digital sleeper cells are not obvious to the South Korean security services and try to gain diplomatic advantages by touting the cyber infiltration performed by South Korea in the international community. A third alternative is that the North Korean state could interpret the presence of the digital sleeper cell as a “real threat” against the target. A fourth alternative would be that the digital sleeper cell is seen as an attack on the target. Lastly, and the most extreme, would be to see the digital sleeper cell as an attack on the state itself. This might appear to be an extreme response. After all, it is tragic for a hospital to experience a cyberattack in the way that many British hospitals suffered through the WannaCry attack in 2017, but this was not seen as an attack on the state. However, it is not unfeasible to think of a scenario in which a liberal democracy employs digital voting software for a national election only to find such software has been infiltrated by a digital sleeper cell which threatens to sabotage the process by altering votes for particular candidates. In this latter case the attack may be seen as tantamount to one on the democratic foundations of the liberal state. Such an attack might then quite reasonably be interpreted as *casus belli* and lead to a kinetic military response (Smith 2018).

Furthermore, even thinking in these terms assumes a very high degree of knowledge regarding the recipient state’s networks and the potential for damage of whatever malware the digital sleeper cell will enact. It is worth remembering that the first worm was created in what was believed to be a secure networked environment of university computers by graduate student Robert Tappan Morris in 1988 (Branscomb 1990). What that student did not know was that at least one of the computers was attached to the broader network of computers linking universities at the time, leading to an FBI investigation. In a similar manner, it is not implausible that a Ministry of Defence computer network might at some point connect to a civilian hospital network, allowing any attack on the legitimate defence target to spread to a non-legitimate civilian target. In this way, the digital sleeper cell would form a part of an indiscriminate act of targeting, thus violating the principle of discrimination in the just war tradition.

The use of digital sleeper cells therefore raises a number of ethical issues from the outset. As Donald Rumsfeld once famously said in relation to the Iraq War, there are known unknowns and unknown unknowns (Daase and Kessler 2007; Pawson, Wong, and Owen 2011). In this case, the known unknowns include the likely response of the recipient state upon discovery of a digital sleeper cell. The unknown unknowns here involve the precise spread and impact of whatever malware the digital sleeper cell unleashes.

Cyber intelligence, ethics and risk

I have argued elsewhere that we should understand security as the inverse of risk. That is, the greater the things we value are put at risk (in terms of greater probability of harm, or greater harm), the less secure the situation in which we find ourselves and vice versa. Given the aforementioned continuum between security, counterintelligence and intelligence, intelligence activities (including sabotage) can reasonably be seen as acts of risk management in the national security and intelligence sphere. Cyber security (and, by extension, cyber counterintelligence and cyber intelligence) is a subcategory of this way of thinking. Cyber security is therefore a measure of risk insofar as that risk occurs in relation to the cyber domain, and cyber intelligence is a matter of risk management wherever intelligence and related activities take place in relation to the cyber domain. Of course, it is increasingly the case that for much of the world everything of significance is at least impacted by, if not reliant on, the cyber domain. As this tendency increases it will become less relevant to discuss “cyber” security and simply refer to “security”. Put another way, the context of security will likely soon be such that the vast majority of security is in some manner a matter of cybersecurity.

The benefit of defining security and intelligence in terms of risk is that this opens to discussion a vast discourse on the ethics of risk, which has been developed over the last 30 years by academics such as Sven Ove Hansson. The definition places risk as the central concern of intelligence and security activities, which in turn challenges us to think more carefully about what is meant by and what is implied by situations involving risk.

A standard definition of risk would involve a calculation of severity and probability. The more severe the harms which are threatened in a risky situation, the more risky that situation will be. Similarly, the greater the likelihood of harms occurring renders a risky situation more risky. Hence a low probability of a minor paper cut is a low risk. The high probability of losing one’s life is, by contrast, a high risk. There are then any number of intermediate positions involving the high probability of a minor harm (a high likelihood of a paper cut, for example) and a low probability of a major harm (a remote chance of death).

Through breaking down risk into its constituent terms of severity and probability we are then more able to see which ethical issues may arise through engagement in risky situations such as the placing of digital sleeper cells in conditions of epistemic uncertainty. For example, I have already suggested that we do not know what harm may arise through the employment of a digital sleeper cell in at least some contexts. We may have a reasonable idea as to what would happen if the digital sleeper cell were activated, although even then there is the problem of unforeseen network connections allowing for malware to travel between legitimate and illegitimate targets, but there is also the question as to what would happen if the digital sleeper cell were discovered before being activated. We are once more in the realm of the unknown unknowns in the cyber domain. Hence the calculation of (likely) harms is extremely complex, if not impossible.

Furthermore, there are additional problems in terms of the subjectivity of harm. Generally speaking, harms have both objective and subjective dimensions. It is, *ceteris paribus*, undoubtedly objectively harmful for a person to lose their hand. However, it is arguably worse for a concert pianist to lose her hand than for a philosopher to lose his. This may be exaggerated when it comes to harms arising to people of different cultures and societies. This was brought home to many in a recent Massachusetts Institute of Technology (MIT) experiment involving self-driving vehicles (Awad 2017; Ganesh 2017; Holstein and Dodig-Crnkovic 2018). Most research subjects in Europe and the United States, when placed in a dilemma in which a self-driving car needed to kill one of a number of people, opted for the car to kill an elderly person rather than a child. This was reversed when the same experiment was conducted with Chinese research subjects. There may be a number of reasons for this, not least a traditional reverence for the elderly in China, which has been absent from European and American culture for some time and issues of overpopulation in China, whereas many countries in Europe are experiencing population decline. The fact remains, though, that the harm of killing a child vis-à-vis the harm of killing an elderly person in at least this one scenario differed from a subjective perspective depending on whether the person asked was Chinese or European. As such, it is extremely difficult to measure the harms which might arise as a result of employing a digital sleeper cell in a state with radically different values from one's own.

There are further questions to be asked about the distribution of risk. It is frequently the case that the person making a risky decision will not be the same person who faces paying the costs of that decision (Wolff 2010). If I choose to go hang gliding, and sufficiently inform myself of the risks implicit in that, then I freely undertake to both experience the benefits of hang gliding (the joy of soaring through the air) and the costs of hang gliding (the chance of something going wrong leading to a fatal accident). This, though, is a very different situation from one in which I determine whether you should go hang gliding, in which case I make the decision while you bear the costs and benefits. Yet another alternative may be a situation in which I make a decision from which I stand to benefit but you stand to pay the costs. Such was the case, for example, when Ford decided not to recall their Pinto model in the 1970s even after the car was determined to be unsafe on the roads (Lütge 2018; Malloy and Lang 1993). In that instance, the senior management of Ford were almost certainly neither driving a Pinto themselves, nor were they making the information about the lack of safety of the Pinto available to the general public. The decision makers were therefore benefiting from the decision in terms of salaries arising from sales of the Pinto model (coupled with savings on not conducting a recall) while the general public, both drivers and passengers in Pinto cars and those on the road with them, stood to pay the costs arising from having unsafe vehicles on the roads. In the case of digital sleeper cells, we are almost certainly talking about a scenario far closer to that of the Ford Pinto than of my going hang gliding. The digital sleeper cell is put in place by one state which stands to benefit from the activation of that cell at some point in the future, while the recipient state gains nothing but bears the cost of any

sabotage that may occur. This distribution of the risk in using sleeper cells renders them, in and of themselves, a highly attractive approach to intelligence activities. The way in which that risk is balanced out is through the threat of reciprocal action on the part of the recipient state. However, as noted earlier, we frequently do not know what that reciprocal action will be and therefore are left in a position of uncertainty.

While these are relatively broad problems which come from looking at the ethics of risk, there are a number of very specific problems which occur in debates surrounding risky situations on a frequent basis and are nonetheless fallacious. These have been highlighted as fallacies of risk by Sven Ove Hansson (Hansson 2004). Of these, at least three seem to pertain particularly to problems in cyber intelligence and digital sleeper cells. The first is what Hanson calls the tuxedo fallacy (Hansson 2009, 426). This is essentially a critique that calculations of risk are often undertaken under conditions of extreme simplification, in the process of which complicating but important externalities are ignored. In this way, risk can be calculated with a seemingly mathematical certainty, just as one can be sure of the 1 in 38 probability of the ball on a roulette wheel landing on any particular number. However, Hanson's point is that quite clearly in real life we are not able to calculate probabilities with anything like the level of accuracy that we are in an ideal casino. We may be able to talk of more or less probability of a particular event occurring, but in many cases, it is relatively meaningless to talk of a 56% chance versus a 62% chance of a particular event unfolding. As such, we can talk about likelihoods in terms of particular states responding to the discovery of a digital sleeper cell within a network, but it is hard to say that the risk of placing a digital sleeper cell in the network pertaining to a Ministry of Defence, for example, would be numerically greater than the risk of placing the same digital sleeper cell in the network of the same state's Ministry of Foreign Affairs.

A second fallacy that Hanson raises is what he calls the "sheer size fallacy" (Hansson 2004, 353). This fallacy holds that if a prospective risk appears to be smaller than a currently accepted risk then the prospective risk is worth taking. There are several problems with this position, not least that the currently accepted risk might actually be unacceptably large but not recognized as such. For example, it is frequently argued that the risk of accidents occurring with self-driving vehicles is lower than the risk of accidents occurring with manually driven vehicles. The conclusion of this line of argument is therefore we have an imperative to get self-driving vehicles on the roads as soon as possible. While this may be true, it may also be the case that the risks of driving both manual and self-driving vehicles could be too high (i.e. above a threshold of acceptability to the majority in society). It also obscures the potential to reduce the risk self-driving vehicles further, permitting one to settle for a mere improvement on risk rather than seeking to achieve a significant or substantial improvement. The parallel here with digital sleeper cells is their apparently low-risk nature. Without considering potential or likely retaliatory measures, as suggested here, a digital sleeper cell appears attractive given that no agents' lives are risked and the potential for devastation is significant.

The third fallacy to consider here is what Hansson calls the “infallibility fallacy” (Hansson 2004, 359). This arises when experts and the public have differing attitudes to a course of action, leading to the conclusion that the public are wrong about the right course of action. The response of those guilty of the fallacy is typically that the public need to be better informed in order to come to the “right” conclusion. However, as Hansson points out, it may also be that the experts are wrong (as they have been on many occasions). He notes that

when the output of a risk analysis of a complex technology indicates a low level of risk, the possibility that this analysis was wrong may very well be a dominant part of the legitimate concerns that a rational decision maker can and should have with respect to the technology in question.

(Hansson 2004, 359)

In the case of intelligence activities, it is rare that the general public becomes aware of operations until 30 years or more after the event, unless there is a scandal. Rather than running all potential intelligence activities past the public for comment (even in the abstract), the “public” in intelligence cases is typically, at least in liberal democracies, represented by parliamentarians in committees that oversee the intelligence agencies. In this case, the fallacy would unfold as parliamentarians expressing concerns about a particular course of action (the use of digital sleeper cells either in the abstract or in a particular instance) and being told by the heads of the respective intelligence agencies (in this case, the experts) that they are simply wrong.

There is already a general lack of expertise in intelligence matters, which may be compounded by a tendency to hold the intelligence agencies somewhat in awe. This is then further compounded by a lack of expertise in cybersecurity (quite possibly shared by the head of the intelligence agency), which means they are likely to be swayed in favour of accepting operations proposed by the experts. Due to the composition of the accountability process, there is unlikely to be strong evidence to the contrary of what is being proposed, leading to an assumption that, as the fallacy states, the experts are right and the politicians wrong. This could once more lead to a more risk-prone scenario.

As Hansson notes, this fallacy can be overcome to some degree through education and politicians (and others) with oversight of intelligence activities have a duty to become as informed as possible within any reasonable confines of national security considerations. However, the responsibility does not (should not) lie with politicians alone, but with the intelligence agencies to present the alternatives as clearly and impartially as possible with the aim not of winning an agenda but of gaining a clear sense of direction from political masters. Furthermore, the mere awareness of the fallacy’s existence is a first step to countering its effects.

In summary, there are a number of benefits of seeing cybersecurity in terms of risk, not least in being able to draw on a growing body of literature dedicated to discussing the ethics of risk. Some of the challenges raised here in relation to digital sleeper cells have been problems of epistemic uncertainty, subjective elements

in calculating harms and the distribution of risk costs and benefits. In addition, there are at least three fallacies that Hansson suggests in relation to risk which have application to the deployment of digital sleeper cells and cyber intelligence in general. The three on which this chapter has focused have been the tuxedo fallacy, the sheer size fallacy and the infallibility fallacy. Each of these can have a significant impact on how risk is calculated and determined to be acceptable or not.

It is, once more, important to be clear that in raising these issues I am not directing criticism at any one state or intelligence agency, still less any individual. To the best of my knowledge, most western liberal democracies have accountability structures surrounding their intelligence agencies of varying degrees of robustness. Furthermore, those who reach significant positions of authority within those agencies tend to be conservative and risk-averse, often far more so than their political masters.² Nonetheless, while this is currently the case, it would be foolish to rely entirely on internal cultures of conservatism to ensure that only those who were generally risk-averse became the key decision makers in these organizations.

Conclusion and call to action

The realm of cyber intelligence, just as the realm of cyber security, is introducing new technologies and new techniques which carry ethical consequences. While we have developed ethical frameworks for approaching intelligence, my argument in this chapter has been that these frameworks, and particularly the just war tradition on which I have focused, lack the degree of granularity necessary for determining whether these new technologies are ethically acceptable in their application. In response to this, I suggested that we may add a consideration within the proportionality principle of *jus in intelligentium* to the effect that we consider the proportionality of a particular intelligence technique through the lens of the likely response that this technique will occasion if discovered by an adversary.

This approach is both plausible and helpful in determining at least one set of likely outcomes from the use of a new technology in intelligence. At the same time, the focus on the need to determine an adversary's reaction highlights how little we may know about the likelihood of that reaction. In many cases, we are operating blindfolded in a dark room, exacerbated by differences in ethical values on a global scale and a lack of knowledge sufficient to provide certainty as to the full extent of the potential damage of any malware inserted into a network by a digital sleeper cell.

I have also argued that intelligence and security are areas which involve risk management, which, as we have seen, introduces further ethical complications in terms of the determination of risk, its distribution and a number of fallacies which are frequently associated with it. Through approaching intelligence situations with the ethics of risk in mind, we may be better able to at the very least avoid or mitigate some of these fallacies and at the same time recognize the shortcomings of our own rational beliefs.

Ultimately, my concern in this chapter has been that if we compensate for a lack of granularity in, for example, proportionality conditions through determining

likely responses to the implementation of new technologies such as digital sleeper cells, then we will be confronted with our own significant epistemic uncertainties. There are, of course, means to respond to such uncertainties. The most obvious is perhaps that of international law. However, international law is itself at times very vague, and, like all laws, frequently lags behind technological innovation. The Tallinn Manual 2.0 has been a valuable contribution to determining the manner in which international law applies to cyber security and cyber intelligence operations between states. Yet Tallinn 2.0 runs into similar problems as the just war tradition. As with the just war tradition, it is at times insufficiently granular to provide clear guidance on the employment of novel technologies. The manual also evidences a lack of agreement between experts on key issues of applying international law to the cyber realm. Finally, as the manual itself makes clear in the introduction, it is no more than the views of a limited group of experts. The Tallinn Manual 2.0 is not legally binding and is intended as the start of the conversation rather than its conclusion.

Instead of encouraging further international law around cyber intelligence activities, more effort should therefore be placed into informal bilateral and multilateral agreements between operators.³ As Leuprecht et al. note,

there is an opportunity to constrain and shape the way that states engage in cyberwarfare in the future in the way the Law of Armed Conflict, the UN Charter, and the UN Declaration of Human Rights have done in the kinetic realm.

(Leuprecht, Szeman, and Skillicorn 2019)

While such informal agreements as I am proposing may lack the compelling nature of international law, through their informal nature, they can allow for respective intelligence agencies to be more open about what they do and do not wish to see happen as a result of cyber activities.

Notes

- 1 See for example Boenink, Swierstra, and Stemerding (2010), Brey (2017; 2012; 2011), Lucivero, Swierstra, and Boenink (2011), Palm and Hansson (2006) and Wright (2011).
- 2 One may think here of the reported instance when the then British Prime Minister asked his intelligence chiefs if they couldn't just assassinate Idi Amin, the Ugandan dictator. The response was said to be a polite, "We don't do that sort of thing". If that is genuinely reported then it reflects well, but is clearly not universal, as the CIA evidently were actively engaged in assassination attempts in the 1960s viz. at least Fidel Castro and Patrice Lumumba (Johnson 1992).
- 3 See for example Meyer (2011). Also see OSCE, *Decision 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1202 (March 10, 2016); United Nations, General Assembly, *Group of governmental experts on developments in the field of information and telecommunications in the context of international security*, A/70/150 (July 22, 2015); UN General Assembly, *Resolution adopted by the General Assembly*, Training 23, 1 (December 19, 2014).

References

- Awad, Edmond. 2017. "Moral Machines: Perception of Moral Judgment Made by Machines". PhD diss., Massachusetts Institute of Technology. <https://dspace.mit.edu/handle/1721.1/112532>.
- Bellaby, Ross W. 2014. *The Ethics of Intelligence: A New Framework*. London; New York: Routledge.
- Boenink, Marianne, Tsjalling Swierstra, and Dirk Stemerding. 2010. "Anticipating the Interaction between Technology and Morality: A Techno-Ethical Scenario Study of Experimenting with Humans in Bionanotechnology". *Studies in Ethics, Law, and Technology* 4 (2): 1–38. <https://doi.org/10.2202/1941-6008.1098>.
- Branscomb, Anne W. 1990. "Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime". *Rutgers Computer & Technology Law Journal* 16: 1.
- Brey, Philip. 2007. "Is Information Ethics Culture-Relative?". *International Journal of Technology and Human Interaction (IJTHI)* 3 (3): 12–24.
- . 2011. "Anticipatory Technology Ethics for Emerging IT". In *CEPE 2011: Crossing Boundaries*, 13–26. Milwaukee, WI: INSEIT.
- . 2012. "Anticipatory Ethics for Emerging Technologies". *NanoEthics* 6 (1): 1–13. <https://doi.org/10.1007/s11569-012-0141-7>.
- . 2017. "Ethics of Emerging Technologies". In *Ethics of Technology Methods and Approaches*, edited by Sven Ove Hansson, 175–91. London; New York: Rowman & Littlefield Publishers.
- Daase, Christopher, and Oliver Kessler. 2007. "Knowns and Unknowns in the 'War on Terror': Uncertainty and the Political Construction of Danger". *Security Dialogue* 38 (4): 411–34. <https://doi.org/10.1177/0967010607084994>.
- Ess, Charles. 2006. "Ethical Pluralism and Global Information Ethics". *Ethics and Information Technology* 8 (4): 215–26. <https://doi.org/10.1007/s10676-006-9113-3>.
- . 2008. "Culture and Global Networks: Hope for a Global Ethics". In *Information Technology and Moral Philosophy*, edited by M. J. van den Joven and J. Weckert, 195–225. Cambridge: Cambridge University Press.
- Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War". *Survival* 53 (1): 23–40. <https://doi.org/10.1080/00396338.2011.555586>.
- Fialka, John J. 1999. *War by Other Means: Economic Espionage in America*. New York: W. W. Norton & Company.
- Ganesh, Maya I. 2017. "Entanglement". *Machine Research* 6 (1): 76–87. <https://doi.org/10.7146/aprja.v6i1.116013>.
- Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History". *Wired*, August 22. www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
- Hansson, Sven O. 2004. "Fallacies of Risk". *Journal of Risk Research* 7 (3): 353–60. <https://doi.org/10.1080/1366987042000176262>.
- . 2009. "From the Casino to the Jungle". *Synthese* 168 (3): 423–32. <https://doi.org/10.1007/s11229-008-9444-1>.
- Herring, Eric, and Piers Robinson. 2014. "Deception and Britain's Road to War in Iraq". *International Journal of Contemporary Iraqi Studies* 8 (2–3): 213–32. https://doi.org/10.1386/ijcis.8.2-3.213_1.
- Holstein, Tobias, and Gordana Dodig-Crnkovic. 2018. "Avoiding the Intrinsic Unfairness of the Trolley Problem". In *Proceedings of the International Workshop on Software Fairness*, 32–7. FairWare '18. New York, NY: Association for Computing Machinery. <https://doi.org/10.1145/3194770.3194772>.

- Humphreys, James. 2005. "The Iraq Dossier and the Meaning of Spin". *Parliamentary Affairs* 58 (1): 156–70. <https://doi.org/10.1093/pa/psi013>.
- Hurka, Thomas. 2005. "Proportionality in the Morality of War". *Philosophy & Public Affairs* 33 (1): 34–66. <https://doi.org/10.1111/j.1088-4963.2005.00024.x>.
- Johnson, Boyd. 1992. "Executive Order 12,333: The Permissibility of an American Assassination of a Foreign Leader". *Cornell International Law Journal* 25 (2): 401–36.
- Kudina, Olya, and Peter-Paul Verbeek. 2019. "Ethics from Within: Google Glass, the Collingridge Dilemma, and the Mediated Value of Privacy". *Science, Technology, & Human Values* 44 (2): 291–314. <https://doi.org/10.1177/0162243918793711>.
- Küng, Hans, and Karl-Josef Kuschel. 1993. *A Global Ethic: The Declaration of the Parliament of the World's Religions*. New York: Continuum.
- Langner, Ralph. 2011. "Stuxnet: Dissecting a Cyberwarfare Weapon". *IEEE Security Privacy* 9 (3): 49–51. <https://doi.org/10.1109/MSP.2011.67>.
- Lehman, Gary. 2016. "Cyber-Attack against Ukrainian Power Plants Prykarpattiaoblenergo and Kyivoblenergo: Lessons Learned; Implementation Considered". <https://garylehman.net/wp-content/uploads/2016/01/Cyber-Attack-Against-Ukrainian-Power-Grid-Implications.pdf>.
- Leuprecht, Christian, Joseph Szeman, and David B. Skillicorn. 2019. "The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity". *Contemporary Security Policy* 40 (3): 382–407. <https://doi.org/10.1080/13523260.2019.1590960>.
- Liebert, Wolfgang, and Jan C. Schmidt. 2010. "Collingridge's Dilemma and Technoscience". *Poiesis & Praxis* 7 (1): 55–71. <https://doi.org/10.1007/s10202-010-0078-2>.
- Lucivero, Federica, Tsjalling Swierstra, and Marianne Boenink. 2011. "Assessing Expectations: Towards a Toolbox for an Ethics of Emerging Technologies". *Nanoethics* 5 (2): 129–41. <https://doi.org/10.1007/s11569-011-0119-x>.
- Lütge, Christoph. 2018. *Ford Pinto: Is Cost-Benefit Analysis Allowed in Ethical Decision Making?* London: SAGE. <https://doi.org/10.4135/9781526442093>.
- Macnish, Kevin. 2015. "An Eye for an Eye: Proportionality and Surveillance". *Ethical Theory and Moral Practice* 18 (3): 529–48. <https://doi.org/10.1007/s10677-014-9537-5>.
- . 2016. "Persons, Personhood and Proportionality: Building on a Just War Approach to Intelligence Ethics". In *Ethics and the Future of Spying: Technology, National Security and Intelligence Collection*, edited by Jai Gaillott and Warren Reed, 95–106. Abingdon, UK: Routledge.
- . 2017. *The Ethics of Surveillance: An Introduction*. London; New York: Routledge.
- Malloy, David C., and Donald L. Lang. 1993. "An Aristotelian Approach to Case Study Analysis". *Journal of Business Ethics* 12 (7): 511–16. <https://doi.org/10.1007/BF00872372>.
- Marsh, Sarah. 2018. "US Joins UK in Blaming Russia for NotPetya Cyber-Attack". *The Guardian*, February 15. www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine.
- Mattei, Tobias A. 2017. "Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack". *World Neurosurgery* 104 (August): 972–4. <https://doi.org/10.1016/j.wneu.2017.06.104>.
- Meyer, Paul. 2011. "Cyber-Security through Arms Control". *The RUSI Journal* 156 (2): 22–7. <https://doi.org/10.1080/03071847.2011.576471>.
- Mohurle, Savita, and Manisha Patil. 2017. "A Brief Study of Wannacry Threat: Ransomware Attack 2017". *International Journal of Advanced Research in Computer Science* 8 (5): 1938–40. <https://doi.org/10.26483/ijarcs.v8i5.4021>.
- Omand, David. 2011. *Securing the State*. London: C. Hurst & Co Publishers Ltd.

- Palm, Elin, and Sven O. Hansson. 2006. "The Case for Ethical Technology Assessment (ETA)". *Technological Forecasting and Social Change* 73 (5): 543–58. <https://doi.org/10.1016/j.techfore.2005.06.002>.
- Pawson, Ray, Geoff Wong, and Lesley Owen. 2011. "Known Knowns, Known Unknowns, Unknown Unknowns: The Predicament of Evidence-Based Policy". *American Journal of Evaluation* 32 (4): 518–46. <https://doi.org/10.1177/1098214011403831>.
- Quinlan, Michael. 2007. "Just Intelligence: Prolegomena to an Ethical Theory". *Intelligence and National Security* 22 (1): 1–13. <https://doi.org/10.1080/02684520701200715>.
- Rice, Desmond, and Arthur Gavshon. 1984. *The Sinking of the 'Belgrano'*. London: Martin Secker & Warburg Ltd.
- Smart, William. 2018. *Lessons Learned Review of the WannaCry Ransomware Cyber Attack*. London: NHS.
- Smith, Patrick T. 2018. "Cyberattacks as Casus Belli: A Sovereignty-Based Account". *Journal of Applied Philosophy* 35 (2): 222–41. <https://doi.org/10.1111/japp.12169>.
- Widdows, Heather. 2014. *Global Ethics: An Introduction*. Abingdon, UK: Routledge. <https://doi.org/10.4324/9781315711379>.
- . 2016. "Why and What Global Ethics?". In *Ethics in an Era of Globalization*, edited by M. S. Ronald Commers, Wim Vanderkerckhove, and An Verlinden. 1st edition, 95–112. London; New York: Routledge.
- Wolff, Jonathan. 2010. "Five Types of Risky Situation". *Law, Innovation and Technology* 2 (2): 151–63. <https://doi.org/10.5235/175799610794046177>.
- Wright, David. 2011. "A Framework for the Ethical Impact Assessment of Information Technology". *Ethics and Information Technology* 13 (3): 199–226. <https://doi.org/10.1007/s10676-010-9242-6>.

7 Intelligence sharing among coalition forces

Some legal and ethical challenges and potential solutions

David Letts

Introduction

Since the end of World War II there have been numerous examples of coalition operations involving two or more military forces, including some operations that have been held under the authority of the United Nations through the passing of a UN Security Council Resolution.¹ Other types of multinational operations, comprising both formal alliances that are set up under treaty arrangements, such as NATO,² and more informal coalitions that are typically established under ad hoc arrangements that deal with a specific issue or incident, such as the International Maritime Security Construct,³ have been a feature of military operations for centuries.⁴ Changes in the structure of alliances and coalitions have also been a regular occurrence, often driven by changes that occur in the political landscape of one or more partner State. There are also other types of cooperation that occur between military forces, such as routine participation in exercises and training activities, as well as exchange of personnel, staff meetings and high-level discussions between senior officials. Overall, these activities are all examples of two or more foreign militaries working together to achieve a common objective.

An integral aspect of these coalition operations is the collection, pooling and sharing of intelligence between the forces of the coalition states involved and such sharing often represents an indispensable element of the effective conduct of these operations. However, intelligence sharing among coalition forces can raise difficult questions of domestic and international laws. This is especially true in situations where one State contributes intelligence to a combined operational pool that is then used by all of the coalition partners as they pursue their individual goals. In such situations, there may be differences in legal and ethical perspectives on the use of the pooled intelligence even among liberal democratic states.

This chapter will initially identify what is meant by the term “intelligence” and then outline some of the mechanisms used by states to collate and pool their intelligence resources. The next part of the chapter will review two recent case studies where coalition states have relied on intelligence to undertake military operations and assess the implications that arise from these cases. The case studies will be supported by consideration of some hypothetical scenarios that illustrate the problems that arise for other coalition partners in circumstances where there is some

possibility that an operational partner state may use pooled intelligence to undertake an activity that does not correspond with the legal obligations that apply to the “providing” state.

Why is this analysis being undertaken? Reviewing some of the challenges involved in sharing intelligence among coalition partners can help to identify where the legal and ethical risks lie for coalition states so that conscious decisions regarding intelligence sharing can be included in the working methodology of shared intelligence agencies and the planning of such operations. The chapter will conclude with some suggestions that coalition states may want to consider so that concerns regarding the legal issues that arise from intelligence sharing between states can be adequately addressed.

What is “intelligence” and how is it used?

The collection of information to assist military commanders discharge their duties has been an element of warfare for as long as battles between opposing forces have been held. One way of describing the concept of intelligence is the approach used by the RAND Corporation who note that “military intelligence includes information on other countries’ military forces, plans, and operations gained through a variety of collection methods” (RAND Corporation n.d.). In its simplest form, the term “intelligence” refers to “information concerning an enemy or an area” that is then available for a commander to use (Watson n.d.). These days, collection of intelligence occurs from a wide variety of sources, including “satellites, ultramodern aircraft, electronic systems, human sources, cameras, imaging and electronic devices, and a host of other systems” which all combine so that information collection can be now undertaken on a scale that was not previously achievable (Watson n.d.).

The pooling and sharing of intelligence between the forces of states involved in a coalition is also a common feature of modern military operations, and this shared material is usually indispensable for the effective conduct of these operations. There are different methods used to establish intelligence sharing networks, with perhaps the most famous (or infamous?) being the “Five Eyes” network that is established under the UKUSA Agreement of 1946.⁵ The Five Eyes network originally only included the United Kingdom and the United States of America but by 1956 it had been expanded to include Canada, Australia and New Zealand.⁶

Other states have more recently established military intelligence sharing agreements but the volatility that can impact inter-state relations has meant that some of these arrangements have not been without a certain level of difficulty. For example, in August 2019 it was reported that the South Korean government had decided to give the necessary three months’ notice that the 2016 military intelligence agreement between Japan and South Korea would not be renewed due to “ongoing tensions over wartime history and trade”.⁷ However, at the last minute in November 2019 it was announced that a solution had been reached between the two states that allowed the agreement to be renewed “six hours before the agreement was to expire” (Tong-hyung 2019).

Another way in which intelligence is shared between states is through the creation of pooled resource centres, and again these may, or may not, be part of a formal alliance structure. An example of intelligence sharing as part of a formal alliance is the NATO Intelligence Fusion Centre (NIFC) that has been operating in the United Kingdom since December 2007 (NIFC n.d.). The NIFC's website identifies its mission as being the provision of "intelligence to warn of potential crisis and the support the planning and execution of NATO operations",⁸ More recently, in 2017 NATO reformed its headquarters organization by establishing a Joint Intelligence and Security Division with a mission to "initiate a broad series of reforms to improve the quality and utility of intelligence provided to NATO's most senior political and military leaders" (von Loringhoven 2019).

Intelligence centres that operate with pooled resources may also be focused on specific issues, and can be constructed in separate and distinct ways. Three examples of this occurring in the maritime domain are:

- The Singapore Information Fusion Centre (IFC) which is a permanent arrangement that was established in 2009 to provide regional maritime domain awareness and is hosted by the Republic of Singapore Navy. The IFC uses a network of International Liaison Officers (ILOs) from a range of different countries that collect open-source information in order to compile a range of products that contribute to maritime domain awareness in the IFC's area of interest (IFC 2019b). The IFC holds a "Shared Awareness Meeting" approximately every six months where information is provided regarding maritime security incidents that have occurred in the region during the previous six-month period. At the time of writing, 24 different states have contributed ILOs since the IFC's inception.⁹
- Combined Maritime Forces (CMF), which operates as a partnership of approximately 30 states at any one time, has three discrete missions related to maritime security in the middle east region: CTF 150 Maritime Security (outside the Gulf), CTF 151 Counter-Piracy and CTF 152 Gulf Maritime Security (CMF 2020). CMF's website describes the organization as a "coalition of the willing and does not proscribe a specific level of participation from any member nation" (CMF 2020). Nevertheless, CMF does have a headquarters in Bahrain where intelligence is shared – at least in the form of maritime domain awareness – and the CMF hosts a regular Shared Awareness and De-confliction (SHADE) conference where senior officials can discuss maritime issues and threats in CMF's area of operations.¹⁰
- The relatively open reporting and sharing of information that occurs with the IFC and CMF can be contrasted with United Kingdom Maritime Trade Operations (UKMTO), "a Royal Navy capability with the principal purpose of providing an information conduit between military which (includes/security forces) and the wider international maritime trade" (UKMTO n.d.). In relation to sharing information, UKMTO declares that it "shares relevant information with appropriate authorities within states in the region. All information received is strictly controlled in a secure information system and

recognises that the source and content of the information is often extremely sensitive” (UKTMO n.d.).

This section of the chapter has shown that intelligence can be collected and shared in a number of different ways, and these methods will vary according to the manner in which a coalition has been established and the type of intelligence being collated. In the case of the “Five Eyes”, the intention behind that coalition has always been to collect sensitive and highly classified intelligence, while other intelligence collection centres, such as the IFC in Singapore, are constructed to receive and disseminate open-source intelligence.

Regardless of whether intelligence being collected is open source or highly classified, the potential legal and ethical risks associated with its dissemination to, and use by, coalition partners should be properly understood. The next part of the chapter will examine some case studies to illustrate the problem.

Coalition operations – two case studies

Many military operations that have taken place in the past few decades have been characterized by the involvement of coalition forces: the 1999 NATO intervention in Serbia and subsequent deployment of peacekeeping forces in Kosovo; Afghanistan after 2001; Iraq after 2003, including operations against the Islamic State (ISIS) since 2010; the 2011 intervention in Libya; recent Saudi-led airstrikes in Yemen; and even the activities of the Combined Maritime Forces off the east coast of Africa and in the Gulf region that was mentioned in the previous section.

The previous sections of this chapter have identified that intelligence sharing in coalition operations, regardless of whether or not the laws of armed conflict apply, is now a regular and expected feature of these activities. However, in recent years there have also been numerous reported instances of intelligence sharing being one of the key reasons why states have engaged in conduct that has subsequently proved to be wrongful – or at least, perhaps, regrettable. Examples that will be briefly examined in this section of the chapter are the Iraq War in 2003 and the recently released *Report of the Government Inquiry into Operation Burnham and related matters* (Arnold 2020). In both of these incidents, intelligence available to the coalition forces played a key role for at least part of the legal justification that was provided for the operation. The issue that arises for consideration in this chapter is whether there is a resultant legal and ethical risk that intelligence provided by one coalition partner could be, or was, misused by another coalition partner to commit a violation of international law.

Iraq War 2003

Much has been written regarding the use of intelligence to inform the decision-making that preceded the entry of coalition forces into Iraq in 2003 and there are plenty of opinions about whether or not the use of military force at that time was legal from a *jus ad bellum* perspective.¹¹ However, assessing that question is not

the purpose of using this period as a case study in this chapter. Rather, the purpose is to make some remarks about the key pieces of intelligence that coalition forces relied upon, and assess whether legal consequences arise.

The central legal document relevant to this present assessment is United Nations Security Council (UNSC) Resolution 1441 which was adopted by a unanimous vote of 15–0 on November 8, 2002 (UNSCR n.d.). It is not necessary to delve too deeply into the text of UNSCR 1441 for this chapter, other than to mention the critical concept that is directly relevant to the intelligence assessment regarding Iraq, namely that it “has been and remains in material breach of its obligations under relevant resolutions”. Contentious arguments were then subsequently raised in relation to who had the legal authority to decide that military action should take place as a result of these “material breaches” but again, this question is beyond the present scope.¹²

In order to authorize military action, clearly there needed to be an assessment of whether sufficient evidence to support the claims of material breach existed. It is this point that provides the area of most concern for the topic of this chapter, as it has been noted that during “Security Council debates during the conflict, China, France, Germany and Russia were all unsatisfied that the US and UK allegations about Iraq’s weapons of mass destruction and support for terrorism had been substantiated” (Anton 2013). The primary reason for this dissatisfaction, of course, is that the United States and the United Kingdom (and Australia) did not share the intelligence that they supposedly relied upon in forming the opinion that military action against Iraq was necessary under one of the legal bases that were provided at the time.¹³ Additionally, it is noted that subsequent to the cessation of coalition military action in Iraq, it was found that neither weapons of mass destruction were held by Saddam’s regime nor were the supposed close terrorist links with Al-Qaeda ever proved.

The New Zealand Defence Force (NZDF) in Afghanistan: Operation Burnham

The second case study to briefly consider is *Operation Burnham* which was a New Zealand Special Air Service operation that took place in Afghanistan in August 2010. The reason this case study has been chosen is that it involved, *inter alia*, allegations that faulty intelligence had been used during the operation and this criticism, and others, were subject to a detailed and lengthy inquiry with the result being that publicly available information can be reviewed (Arnold 2020). The purpose of the inquiry was to examine a number of “allegations of wrongdoing by NZDF forces” during the operation including the killing of civilians in violation of the law of armed conflict, deliberate destruction of civilian houses and an alleged “cover-up” by the NZDF (Arnold 2020, 7–8).

As far as the purpose of this chapter is concerned, a number of aspects of the Operation Burnham Report are relevant.¹⁴ First, the Report contains a detailed analysis of the intelligence assessment that was relied upon to undertake the NZ Special Forces’ raid that was the subject of the inquiry. The report’s assessment

of the intelligence raised by, and shared with, the NZDF was that it was largely accurate and could be reasonably relied upon (Arnold 2020, 189, 197). Next, the Report addresses the situation of NZDF being aware of the possibility that handing over a detainee to Afghan authorities may result in that person being tortured (i.e. that the NZDF had intelligence to that effect) and then looks at the issues that arise. The Report stated that:

the core obligations fall into three broad categories: preventive obligations, conduct obligations and response obligations. States need to do all they can to prevent torture, not commit it or be complicit in it, not return or transfer people to places where they face a real risk of torture, and respond swiftly and effectively if torture may have, or has, occurred.

(Arnold 2020, 302)

The final point regarding the Report is its conclusion that significant mistakes were made by the NZDF in relation to events that took place while the force was deployed to Afghanistan, including a failure to adequately deal with the transfer of a detainee to Afghan custody despite a real risk of torture existing. Additionally, “NZDF and other New Zealand agencies did not respond as they should have when they learnt of the possibility that he had been tortured” (Arnold 2020, 385).

The salient point from this case study is that intelligence can be used, or misused, in a variety of ways. In a situation like that faced by the NZDF on operations in Afghanistan the collection and use of shared intelligence to inform a combat mission was found to be quite appropriate. However, the Report also found that there was a lack of adequate action taken in relation to credible intelligence that a detainee was likely to be tortured and that proper consideration of that likelihood created a legal responsibility to prevent the detainee’s transfer to Afghan authorities in those circumstances (Arnold 2020, 315–16). The potential consequences that arise from such transfers will be dealt with later.

The applicable legal frameworks

The legal framework governing intelligence sharing among coalition partners can be influenced by a number of overlapping regimes and comment regarding the main legal frameworks will now be provided.

The law of state responsibility

Under the general international law principle of state responsibility, states can be responsible for internationally wrongful conduct attributable to them, normally because such conduct is committed by the state’s own organs and agents.¹⁵ A number of rules, however, allow for state responsibility to arise in connection to the wrongful act of another state. The most relevant of these rules in relation to sharing intelligence among coalition partners is codified in Article 16 of the

International Law Commission's (ILC) *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (ASRs):

Aid or assistance in the commission of an internationally wrongful act

A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if:

- (a) that State does so with knowledge of the circumstances of the internationally wrongful act; and
 - (b) the act would be internationally wrongful if committed by that State
- (International Law Commission 2001a, 65)

This rule, however, is subject to a number of limiting elements, as explained by the ILC's commentary:

Article 16 limits the scope of responsibility for aid or assistance in three ways. First, the relevant State organ or agency providing aid or assistance must be aware of the circumstances making the conduct of the assisted State internationally wrongful; secondly, the aid or assistance must be given with a view to facilitating the commission of that act, and must actually do so; and thirdly, the completed act must be such that it would have been wrongful had it been committed by the assisting State itself.

(International Law Commission 2001b, 66)

Of particular relevance here are the requirements of knowledge by the assisting state and the parity of obligations on the part of the assisting and the assisted state, both of which are more complex than it might appear at first glance. Similarly, the scope of the rule appears to be limited to aid and assistance provided by one state to another, and therefore if that approach is taken it would not apply to assistance provided by states to non-state actors. However, in the *Bosnian Genocide case* the International Court of Justice not only affirmed the customary status of Article 16 but also applied it by analogy to assistance provided by a state to a non-state actor, albeit in the specific context of state responsibility for complicity in relation to the crime of genocide.¹⁶

Therefore, despite some questions regarding limitations, which exist about the breadth of Article 16's scope, there is potential for coalition states to be attributed some level of responsibility for aiding or assisting a third state's internationally wrongful act through the provision of intelligence. While normally the assisting state would only be responsible for its own (now wrongful) act of providing assistance, it may also be that in some cases the assisting state will share in the responsibility of the assisted state for committing the principal wrong.

Responsibility of international organizations

In addition to state responsibility, the possibility also exists that if a coalition military operation takes place under the umbrella of an international organization,

such as the UN or NATO, the organization itself might accrue responsibility as an international legal person for aiding and assisting a state or another organization in the commission of an internationally wrongful act. The provision of intelligence, that was then used to enable a violation of international law, could easily assist with the commission of such an act. However, the ICJ has made it clear that any such responsibility for an organization will not be of a criminal nature, but arises as a matter of its “obligations and responsibilities under international law”.¹⁷

Further, in 2011 the ILC concluded its project on the responsibility of international organizations and Article 14 of the ILC’s draft articles is an equivalent rule to Article 16 in the articles on state responsibility (International Law Commission 2011). Whether the ILC’s work accurately reflects customary law is a difficult question, but in any case there is support for considering that “the notion of the responsibility of international organizations presupposes, naturally, that international organizations are considered separate actors in their own right, with their own legal personality and moral agency” (Klabbers 2017, 1136). One obvious difficulty in attributing responsibility to international organizations is that they are not normally parties to the relevant International Humanitarian Law (IHL) and human rights treaties, thus requiring an exploration of whether they are bound by similar obligations under customary international law – a task that is, unfortunately, beyond the scope of this chapter.

International Humanitarian Law

While IHL¹⁸ does not specifically regulate the collection or sharing of intelligence, it does impose some primary obligations on states with respect to the conduct of other states. These primary rules operate in addition to the secondary rules of state responsibility under general international law. Most importantly, under Common Article 1 of the four Geneva Conventions of 1949, all “High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances”.¹⁹

In the words of the authoritative Pictet Commentary of 1960, Article 1 of Geneva Convention (III), this overarching obligation:

applies to the respect of each individual State for the Convention, but that is not all: in the event of a Power failing to fulfil its obligations, each of the other Contracting Parties (neutral, allied or enemy) should endeavour to bring it back to an attitude of respect for the Convention. The proper working of the system of protection provided by the Convention demands in fact that the States which are parties to it should not be content merely to apply its provisions themselves, but should do everything in their power to ensure that it is respected universally.

Parallel obligations exist under customary IHL. For example, Rule 139 of the ICRC Customary IHL Study provides that “[e]ach party to the conflict must respect and ensure respect for international humanitarian law by its armed forces

and other persons or groups acting in fact on its instructions, or under its direction or control” (ICRC n.d.). Rule 144 stipulates that “States may not encourage violations of international humanitarian law by parties to an armed conflict. They must exert their influence, to the degree possible, to stop violations of international humanitarian law” (ICRC n.d.).

It is therefore at the very least arguable that a state which shares intelligence with another state (and possibly a non-state actor) in the course of a coalition military operation can violate these rules. If that state does so in the knowledge that the other state (or non-state actor) is engaged in serious violations of IHL, such as war crimes, or that there is real risk that such violations might occur, then legal responsibility would arise.

International human rights law

The applicability of human rights treaties extraterritorially and in times of armed conflict is a matter of both complexity and controversy. Judicial authority and academic literature on the topic are voluminous and somewhat confusing. It is however beyond dispute that there is an increasing trend towards applying human rights law to such situations, and it seems unlikely that this trend will reverse itself in the future. Some partners in coalition military operations, such as the United States and Australia, are subjected to less exacting scrutiny of their compliance with the relevant human rights treaties than other states, such as those in Europe or the United Kingdom, which have accepted the compulsory jurisdiction of the European Court of Human Rights (ECtHR).²⁰ Even so, because of the close relationships of cooperation in coalition operations, it is inevitable that the increased level of scrutiny by the ECtHR will have ripple effects even on non-European coalition partner states.

Importantly, just like the Geneva Conventions, human rights treaties impose both negative and positive obligations on states’ party. These obligations not only require respect for the provisions themselves, but also oblige states to ensure they are not complicit in violations by third parties, as well as exercising due diligence to prevent and suppress violations by third parties against individuals within the state’s jurisdiction. Close scrutiny of the way in which states have met these obligations has occurred, and one recent example is the *Report into Detainee Mistreatment and Rendition 2001–2010* released by the United Kingdom’s Intelligence and Security Committee of Parliament in 2018. In relation to intelligence sharing, the Report found that British “Agencies shared an unprecedented amount of intelligence with foreign liaison services to facilitate the capture of detainees . . . [but] . . . the Agencies failed to consider whether it was appropriate to pass intelligence where mistreatment of detainees was known or reasonably suspected” (Grieve 2018, 3).

Scrutiny of the outcome from intelligence sharing is only likely to escalate as more information enters the public domain via freedom of information requests, publication of information on the internet, formal public inquiry processes like the UK inquiry mentioned earlier, and through the cross-referencing and linking of different sets of national information releases that analysis of the compiled

data permits. Similarly, intelligence operations generally have been subjected to increased public scrutiny after the “Snowden revelations” of the electronic surveillance capabilities of agencies such as the National Security Agency (NSA) and Government Communications Headquarters (GCHQ) were made public in 2014 (BBC News 2014). This has in turn provoked much litigation, as well as important activities within the UN system, including the adoption of a number of resolutions on the right to privacy in the digital age by the UN General Assembly.²¹

It is simply inevitable that intelligence sharing in coalition military operations will increasingly become a live issue before both domestic courts and international institutions applying human rights law. Accordingly, some serious thinking is required to understand how human rights standards might apply to such extraordinary situations, beyond simply rejecting their applicability outright – a strategy that has been previously known to backfire.

Other areas of uncertainty

Legal uncertainty can arise due to other legal regimes that could potentially impact on partner use of shared intelligence. For example, international or domestic criminal law could be relevant if lethal targeting operations are conducted by a coalition partner following the provision of shared intelligence. Again using the United Kingdom as an example, in 2016 the UK Parliament’s Joint Committee on Human Rights examined the “Government’s policy on the use of drones for targeted killing” (Joint Committee on Human Rights 2016). Issues that were canvassed by the Committee included assessing whether “those involved in implementing the Government’s policy . . . are . . . running the risk of criminal prosecution for murder or complicity in murder” (Joint Committee on Human Rights 2016, 24). The Committee had particular concern about the provision of intelligence to a partner that then prosecutes a lethal strike against an individual whose status as a lawful military target under the applicable legal regime is contested. The Committee noted that the:

possibility of criminal prosecution for complicity in murder also arises for all those UK personnel who have a role in assisting or facilitating the use of lethal force by coalition allies, such as the US, which has a much wider approach to the use of lethal force outside of armed conflict. Such assistance might take the form of logistical support (for example, permitting US jets to use UK airbases), or the provision of intelligence about targets gathered by UK surveillance and reconnaissance.

(Joint Committee on Human Rights 2016, 24)

It should also be noted that while a potential charge of complicity could be a matter of individual criminal responsibility at the micro level, it could also elevate to state responsibility for an internationally wrongful act at the macro level.

Uncertainty as to the status of an individual could also arise due to differing national legal interpretations on the issues of civilians taking a direct part

in hostilities.²² For example, in Australia's case, membership of an organized armed group could be enough to warrant the lethal targeting of an individual in a non-international armed conflict.²³ However, a coalition partner may not have the same legal opinion, and therefore sharing intelligence with Australian forces may lead to a kinetic operation resulting in the death of an individual where the legality of that death is not agreed. A further risk potentially arises for those states that are party to the International Criminal Court.²⁴

Potential solutions

The potential legal issues associated with intelligence sharing are many and varied, so it is not possible to provide a simple, cohesive set of solutions that would cover every conceivable eventuality. Rather, it is necessary to contemplate how a few selected initiatives might contribute to overcoming the challenges that are created by the issues identified in this chapter.

One step along the way has already occurred with the creation of the Five Eyes Intelligence Oversight and Review Council (FIORC) in 2017. The FIORC has the stated aim, *inter alia*, of creating a forum where Council members can:

exchange views on subjects of mutual interest and concern, compare best practices in review and oversight methodology, explore areas where cooperation on reviews and the sharing of results is permitted where appropriate, encourage transparency to the largest extent possible to enhance public trust; and maintain contact with political offices, oversight and review committees, and non-Five Eyes countries as appropriate.

(Five Eyes Intelligence Oversight and Review Council 2017)

The fact that this Council exists at all, in an area that is notoriously reluctant to shed too much light on its activities, is testament to the progress that has been made in recent years towards transparency and accountability in relation to intelligence activities.

Other potential solutions include the production of guidelines and policy recommendations for organizations such as NATO and its partner state armed forces that would enable them to engage in effective intelligence sharing in the modern battlespace, while ensuring that this is done in compliance with applicable legal frameworks. These guidelines should result in simplifying the decision-making processes for the military legal advisers and their operational commanders, which would go a long way towards improving legal certainty and providing improved situational awareness and intelligence analysis. This, in turn, should result in better operational outcomes for those involved in coalition operations.

A final point here is to note the role played by various civil society interest groups and the press who routinely subject the activities of armed forces to rigorous scrutiny. There have been many occasions when reports of violations of applicable legal standards have emerged through the work of such interest groups and the press and it is not expected that any change in the focus of these entities will

occur. In fact, the important oversight function of external bodies was explicitly recognized in the Operation Burnham Report as being able to “provide a platform to enhance public understanding of complex legal and operational issues, and to identify good (or bad) practice in a fair, independent and impartial manner” (Arnold 2020, 370). The Report observed that military forces can be unable to do this without external assistance due to:

what we regard as failings of culture at the upper echelons of NZDF – confirmation bias, lack of objectivity and rigour in scrutinising “facts”, unnecessary defensiveness coupled with an unwillingness to acknowledge error, failure to follow up inconvenient information, and non-compliance with the disciplines and obligations inherent in the principles of ministerial control of the military and ministerial responsibility to Parliament.

(Arnold 2020, 379)

This criticism is not just applicable to the NZDF; it can easily be applied to other military forces when assessing their response to allegations of unlawful activity.

Conclusion

Intelligence sharing by coalition forces is a necessary element of many activities undertaken by modern military forces. Coalition operations may be increasingly frequent in a polycentric international order in which no single state is dominant. The use of intelligence can not only provide coalition forces with a distinct battlespace advantage but also raise legal and ethical questions for states and military commanders if shared intelligence is used in a manner that is inconsistent with a range of existing legal obligations that reflect different ethical perspectives. This chapter has described how issues can arise even among liberal democracies with a common political and ethical heritage. Even more pressing concerns will arise in coalitions comprised of states with more diverse sets of values.

Clarifying the applicable legal frameworks that accompany sharing of intelligence is a task that needs further work, and achieving this will help to delineate between what is permissible and those practices that are prohibited, as well as outline any zones of constructive ambiguity. This chapter has attempted to highlight some of the legal considerations that apply to intelligence sharing by coalition partners. It is really only a starting point on a journey, however, that has many miles yet to run. States and their armed forces, the United Nations and other international organizations such as NATO must devote sufficient attention to the topic in order to foster the detailed academic and military consideration that is needed to satisfactorily address the issue in a satisfactory way.

Postscript

The impetus for writing on this topic originated from a paper produced by The Royal Institute of International Affairs (Chatham House) in November 2016²⁵ and

a subsequent Workshop on Intelligence Sharing in Multinational Military Operations that was convened at the University of Nottingham in January 2018.²⁶ The author is very grateful to all those involved in both of these activities for their valuable and thoughtful contributions, but responsibility for the opinions in this chapter rests with the author alone.

Notes

- 1 An early example is UN Security Council Resolution 84 of June 25, 1950 which authorized military operations in Korea, while a more recent example is UN Security Council Resolution 1973 of March 17, 2011 which *inter alia* enforced an arms embargo, imposed a no-fly zone and strengthened the sanctions regime in relation to Libya.
- 2 NATO is formally known as the North Atlantic Treaty Organization and was established in 1949 pursuant to the *North Atlantic Treaty* 34 UNTS 243.
- 3 The International Maritime Security Construct (IMSC) is a coalition currently comprising eight nations (Albania, Australia, Bahrain, Kingdom of Saudi Arabia, Lithuania, United Arab Emirates, United Kingdom and United States of America) that was formed in 2019 to support maritime security in the Gulf region. See IMSC Public Affairs (2020) for further details about the IMSC and “Australia Joins International Maritime Security Construct in the Gulf” (n.d.), a press release from the Australian Prime Minister announcing Australia’s involvement in the IMSC.
- 4 In this chapter, the term “coalition operations” will be used for convenience to describe the various types of multinational operations, regardless of whether the states involved are part of a formal alliance or some other more informal coalition; the term “partner operations” can also be sometimes used to describe situations when military forces are working together. One analysis of the distinction that may be drawn between a “coalition” and a “wartime alliance” can be found in Weitsman (2010).
- 5 Details of the 1946 UKUSA Agreement which was a “top secret, post-war arrangement for sharing intelligence between the United States and the UK” can now be obtained from the UK National Archives after the files that relate to the Agreement were publicly released in June 2010 (The National Archives 2010).
- 6 Details of the UKUSA agreement were made public in June 2010 after FOI requests were lodged in the UK and the USA (Norton-Taylor 2010).
- 7 In the period prior to the deadline for the termination of the agreement, calls were made for the two parties to resolve their differences and ensure that the agreement continued to operate (Harold 2019).
- 8 <https://web.archive.org/web/20200128162530/http://web.ifc.bices.org/about.htm>
- 9 See IFC (2019a).
- 10 The 45th SHADE was held in Bahrain in November 2019 and although the 46th SHADE was scheduled to be held in April 2020, it has been delayed until November 3–5, 2020.
- 11 Compare, for example, the contrasting positions on this topic taken by O Corten Y Dinstein (Corten 2010; Dinstein 2011).
- 12 See generally Simpson (2005) and Iwanek (2010).
- 13 The two main legal arguments were that action was, in fact, authorized under existing UNSC Resolutions and/or it was necessary to respond in self-defence to the threat posed by Iraq. Previous references to the works of Corten, Dinstein, Simpson, Iwanek and Anton, provide details of critical assessments of the legality of these arguments (Corten 2010; Dinstein 2011; Iwanek 2010; Anton 2013).
- 14 The Operation Burnham Report comprises 12 Chapters and 2 Appendixes and covers a far greater breadth of topics than is possible, or necessary, to address in this chapter.
- 15 See generally Rothwell et al. (2014, chap. 8).

- 16 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, [2007], ICJ Rep, paras 420–421.
- 17 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, [2007], ICJ Rep, para 170.
- 18 The term International Humanitarian Law (IHL) is widely used, but the body of law it encompasses is also known as the law of armed conflict (LOAC) or the law of war. IHL is sometimes narrowly construed to refer to the law that protects victims of armed conflict. For one explanation of this law, see ICRC (2004).
- 19 Article 1 is identical in each of the four Geneva Conventions of 1949: *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* 75 UNTS 31 (GC I); *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea* (GC II) 75 UNTS 85; *Geneva Convention Relative to the Treatment of Prisoners of War* (GC III) 75 UNTS 135; *Geneva Convention Relative to the Protection of Civilian Persons in Times of War* (GC IV) 75 UNTS 287.
- 20 The United Kingdom's departure from the European Union did not result in the UK ceasing to be a member of the European Court of Human Rights (Cowell 2021).
- 21 UN General Assembly Resolution 71/199, *The right to privacy in the digital age*, A/RES/71/199 (December 19, 2016).
- 22 Agreement on what constitutes "direct participation in hostilities" is widely contested with many states critical of the approach adopted by the ICRC as set out in Melzer (2009). See generally McLaughlin (2019).
- 23 Clarifying the position for members of the Australian Defence Force, the *Criminal Code Amendment (War Crimes) Act 2016* included membership of an organized armed group within the category of what constitutes a lawful target.
- 24 *Rome Statute of the International Criminal Court*, July 17, 1998, 2187 UNTS 3.
- 25 See Moynihan (2016).
- 26 This Workshop, conducted under the "Chatham House Rule" involved a number of government practitioners, academics and representatives from international organizations and NGOs, was co-organized by the University of Nottingham's International Law and Security Centre and the ANU College of Law's Centre for Military and Security Law.

References

- Anton, Donald K. 2013. "International Law and the 2003 Invasion of Iraq Revisited", Revised Version of a Paper Delivered on 30 April 2013 at ANU Asia-Pacific College of Diplomacy Seminar". *The Invasion of Iraq: Canadian and Australian Perspectives*, ANU College of Law Research Paper No. 14–19.
- Arnold, Terence. 2020. *Report of the Government Inquiry into Operation Burnham and Related Matters*. Auckland: New Zealand Government. www.operationburnham.inquiry.govt.nz/assets/IOB-Files/Report-of-the-Government-Inquiry-into-Operation-Burnham-print-version.pdf.
- "Australia Joins International Maritime Security Construct in the Gulf". n.d. *Pm.Gov.Au*. Accessed December 16, 2020. www.pm.gov.au/media/australia-joins-international-maritime-security-construct-gulf.
- BBC News. 2014. "Edward Snowden: Leaks That Exposed US Spy Programme". *BBC News*, January 17. www.bbc.com/news/world-us-canada-23123964.
- CMF. 2020. "Combined Maritime Forces (CMF)". *Combined Maritime Forces (CMF)*. Accessed December 16, 2020. <https://combinedmaritimeforces.com/>.

- Corten, Olivier. 2010. *The Law against War: The Prohibition on the Use of Force in Contemporary International Law*. Oxford; Portland, OR: Hart Publishing.
- Cowell, Frederick. 2021. "The Brexit Deal Locks the UK into Continued Strasbourg Human Rights Court Membership". *LSE Brexit Reality* (blog). Accessed March 20, 2021. <https://blogs.lse.ac.uk/brexit/2021/01/17/the-brexit-deal-locks-the-uk-into-continued-strasbourg-human-rights-court-membership/>.
- Dinstein, Yoram. 2011. *War, Aggression and Self-Defence*. 5th edition. New York: Cambridge University Press.
- Five Eyes Intelligence Oversight and Review Council. 2017. "Charter of the Five Eyes Intelligence Oversight and Review Council". Accessed December 16, 2020. www.dni.gov/files/ICIG/Documents/Partnerships/FIORC/Signed%20FIORC%20Charter%20with%20Line.pdf.
- Grieve, Dominic. 2018. *Detainee Mistreatment and Rendition: 2001–2010*. London: HMSO. <https://isc.independent.gov.uk/wp-content/uploads/2021/01/20180628-HC1113-Report-Detainee-Mistreatment-and-Rendition-2001-10.pdf>.
- Harold, Scott W. 2019. "South Korea Should Consider Sticking with Intelligence-Sharing Pact with Japan". *The RAND Blog* (blog). November 5. www.rand.org/blog/2019/11/south-korea-should-consider-sticking-with-intelligence.html.
- ICRC. n.d. "Customary IHL: Rule 139: Respect for International Humanitarian Law". Accessed December 16, 2020. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule139.
- . n.d. "Customary IHL: Rule 144: Ensuring Respect for International Humanitarian Law Erga Omnes". Accessed December 16, 2020. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule144.
- . 2004. "What Is International Humanitarian Law?". Accessed December 16, 2020. www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf.
- IFC. 2019a. "Information Fusion Centre". Accessed December 16, 2020. www.ifc.org.sg/ifc2web/app_pages/User/common/commonIndexv5.cshtml.
- . 2019b. *MARSEC Situation in IFC AOI 2019*. Singapore: IFC. www.ifc.org.sg/ifc2web/Publications/Annual%20Report/2019/AOI%20Document%202019.pdf.
- IMSC Public Affairs. 2020. "IMSC Holds Virtual Change of Command Ceremony". *U.S. Central Command*, April 30. Accessed December 16, 2020. www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/2176451/imsc-holds-virtual-change-of-command-ceremony/.
- International Law Commission. 2001a. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. New York: United Nations. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
- . 2001b. *Year Book of the International Law Commission 2001 Volume II Part Two*. New York: United Nations. https://legal.un.org/ilc/publications/yearbooks/english/ilc_2001_v2_p2.pdf.
- . 2011. *Draft Articles on the Responsibility of International Organizations 2011*. New York: United Nations. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_11_2011.pdf.
- Iwanek, Tomasz. 2010. "The 2003 Invasion of Iraq: How the System Failed". *Journal of Conflict and Security Law* 15 (1): 89–116. <https://doi.org/10.1093/jcs/krp024>.
- Joint Committee on Human Rights. 2016. *The Government's Policy on the Use of Targeted Killing: Second Report of Session 2015–16*. London: HMSO. <https://publications.parliament.uk/pa/jt201516/jtselect/jtrights/574/574.pdf>.

- Klabbers, Jan. 2017. "Reflections on Role Responsibility: The Responsibility of International Organizations for Failing to Act". *European Journal of International Law* 28 (4): 1133–61. <https://doi.org/10.1093/ejil/chx068>.
- McLaughlin, R. 2019. "Organised Armed Groups and Direct Participation in Hostilities". In *Military Law in Australia*, edited by Robin Creyke, Dale Stephens, and Peter Sutherland. Alexandria: The Federation Press.
- Melzer, Nils. 2009. *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*. Geneva: ICRC. www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf.
- Moynihan, Harriet. 2016. *Aiding and Assisting: Challenges in Armed Conflict and Counterterrorism*. Chatham House Report, November 2016. <https://www.chathamhouse.org/sites/default/files/publications/research/2016-11-11-aiding-assisting-challenges-armed-conflict-moynihan.pdf>.
- The National Archives. 2010. "Newly Released GCHQ Files: UKUSA Agreement". *The National Archives*. Accessed December 16, 2020. www.nationalarchives.gov.uk/ukusa/.
- NIFC. n.d. "NATO Intelligence Fusion Centre (NIFC)". Accessed December 16, 2020. <http://web.ifc.bices.org/>.
- Norton-Taylor, Richard. 2010. "Not So Secret: Deal at the Heart of UK-US Intelligence". *The Guardian*, June 24, sec. US News. www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.
- RAND Corporation. n.d. "Military Intelligence". Accessed December 16, 2020. www.rand.org/topics/military-intelligence.html.
- Rothwell, Donald, Stuart Kaye, Afshin Akhtarkhavari, and Ruth Davis. 2014. *International Law: Cases and Materials with Australian Perspectives*. 2nd edition. Port Melbourne, VIC, Australia; New York: Cambridge University Press.
- Simpson, Gerry. 2005. "The War in Iraq and International Law". *Melbourne Journal of International Law* 6 (1): 167.
- Tong-hyung, Kim. 2019. "South Korea Will Keeps Its Military Intelligence Pact With Japan: For Now". *The Diplomat*, November 23. <https://thediplomat.com/2019/11/south-korea-will-keeps-its-military-intelligence-pact-with-japan-for-now/>.
- UKTMO. n.d. "About UKTMO". Accessed December 16, 2020. www.ukmto.org/about-ukmto.
- UNSCR. n.d. "Security Council Resolution 1441: UNSCR". Accessed December 16, 2020. <http://unscr.com/en/resolutions/1441>.
- von Loringhoven, Arndt Freytag. 2019. "A New Era for NATO Intelligence". *NATO Review*, October 29. www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html.
- Watson, Bruce W. n.d. "Intelligence | Military Science". *Encyclopedia Britannica*. Accessed December 16, 2020. www.britannica.com/topic/intelligence-military.
- Weitsman, Patricia. 2010. "Wartime Alliances versus Coalition Warfare: How Institutional Structure Matters in the Multilateral Prosecution of Wars". *Strategic Studies Quarterly* 4 (January): 29–53.

Part III

**Bulk data collection
and analysis**



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

8 Privacy, bulk collection and “operational utility”

Tom Sorell

The Snowden revelations in 2013 concerned the large-scale secret collection of normally private personal communications data for counter-terrorism purposes. Both the American NSA and the British GCHQ were implicated. It is widely believed that the privacy rights of large numbers of entirely innocent US and UK citizens were violated or at least significantly limited by bulk collection. In earlier work, I have expressed scepticism about privacy-based criticisms of bulk collection for counter-terrorism (Sorell 2018). But even if these criticisms are accepted, is bulk collection nonetheless legitimate *on balance* – because of its operational utility for the security services, and the overriding importance of the purposes that the security services serve? David Anderson’s report of the Bulk Powers review in the United Kingdom suggests as much, provided bulk collection complies with strong legal safeguards (Anderson 2016).

I think it is hard to mount a uniformly compelling operational utility argument, because purposes other than counter-terrorism are pursued by the security services with the help of bulk collection. For example, the Intelligence Services Act 1994, section 1(2) says that apart from the interests of national security and the prevention and detection of serious crime, the Secret Intelligence Service may act “in the interests of the economic well-being of the United Kingdom”. The phrase “interests of the economic well-being of the United Kingdom” is open to a disturbingly wide range of interpretations. It might be taken to include the cybersecurity interests of very large companies headquartered or merely located in the United Kingdom (PwC 2017; Zetter 2010), or intellectual property interests of UK companies that are targets of foreign government or foreign company espionage. Do these interests justify (morally justify) government acquisition and analysis of large personal data sets? In my view the answer to this question is “No”, unless there is a clear and significant benefit to UK citizens in general from the cybersecurity of the large companies in question. Even when relevant “economic interests” are confined to those “also relevant to the interests of national security”, as required by the Investigatory Powers Act (2016) section 204 (3a), the legitimacy of intelligence service action to promote or protect these interests is disputable. In particular, it is disputable when the action in question involves bulk collection.

For example, domestic manufacturers of weapons and military equipment are economically important to the United Kingdom and also important to UK security in some sense; it does not follow that intelligence services can legitimately act in the interests of those companies by directly supplying them commercially useful information obtained by bulk collection. Yet electronic interception for these purposes has taken place (Dover 2007), possibly assisted by acquisition of bulk personal data sets.

Other purposes that bulk collection serves include the recruitment by the United Kingdom of intelligence agents abroad. Is *this* purpose not at the very least morally ambiguous, given the mortal dangers faced by agents in some countries, and the moral dubiousness of treachery when agents are recruited to act against their own country's interests? The answer appears to be "Yes". Counter-terrorism and other purposes closely allied to life-saving are *differentially* compelling as grounds for bulk collection if bulk collection is effective. Counter-terrorism is unsurprisingly emphasized in the case studies favouring the use of bulk collection in the Bulk Powers report. But it is unclear what proportion of uses of bulk collection are for counter-terrorism, and so the utility of bulk collection may not have the justificatory power that Anderson's report implies it has.

The rest of this chapter falls into three parts. In the first, I go into some of the privacy objections to bulk collection, and why even some of the more sophisticated of these do not appear to me to engage with the mechanics of bulk collection. Then I consider the Anderson Bulk Powers report. It concedes that bulk collection is privacy-violating, but maintains that the right to privacy can be limited by the right to security, and that bulk collection can be effective for ensuring security, as illustrated by the case studies in his report. Since the purposes served in the case studies are not exhaustive of the purposes to which bulk collection is put, the question arises whether the remaining purposes legitimately limit personal privacy. If the answer is "No", there may be an argument for limiting the purpose of bulk collection to more or less uncontroversial security concerns, where being uncontroversial depends on probable prevention of large-scale injury or loss of life, rather than the pursuit of ill-defined "national economic advantage" or even strategic advantage. The subsequent sections deal with these remaining purposes. A final section draws conclusions.

Bulk Collection and Privacy

As I use the term, "bulk collection" refers to obtaining large personal data sets containing the information of, for the most part, entirely law-abiding persons. To illustrate, data sets composed of the names and addresses of bank account or credit card holders might be of interest to investigations of fraud or money-laundering or organized crime even if few people whose names are included have anything to do with those offences. Location data for people's telephones forms another relevant kind of data set, even if few of the telephones in question belong to persons of interest to the security services. In the same way, the names of passengers on airline flights between certain destinations might be collected, though

the majority of passengers concerned are travelling for entirely innocent reasons. Data concerning telephone or email exchanges is a further example.

After the Snowden disclosures, the bulk collection of communications data in the United States and the United Kingdom was widely condemned as a large-scale violation of the privacy of those whose data was collected (Shorrocks 2013; Lyon 2014). The US legal understanding of *whose* privacy matters has changed since 2013, when Snowden first publicized the activities of the US National Security Agency. Before the disclosures, American law normally prohibited the collection of content from conversations between “US persons”, but treated communications between foreigners or between US persons and foreigners, especially “agents of a foreign power”, as fair game for purposes like counter-terrorism. In other words, the content of emails and other communications between US persons was normally out of bounds, but the content of emails and other communications between foreigners was not, if the purpose of collecting content was a legally recognized purpose of intelligence service activity. In the intermediate case of communications between US persons and foreigners, content collection was not necessarily ruled out, and might be permitted if the foreigners were employed by a foreign government. As for US persons’ communications, although their *content* was normally out of bounds, their meta-data might be collected for purposes like counter-terrorism. Meta-data is information about email or telephone exchanges apart from their content. It might include the time an email arrived, the route it took through the internet to or from a particular IP address, how big the email was and what address it was sent to.

The American government’s view before and even immediately after the Snowden disclosures was that US persons’ communication data privacy matters more than the communication data privacy of foreigners, and that the collection of mere meta-data rather than content either does not rise to the threshold of a privacy violation at all, or at least counts as a relatively minor intrusion. After the passage of the USA FREEDOM Act in 2015, two things changed. First, bulk collection of US persons’ meta-data was supposed to be discontinued. Second:

the policy of the United States [was] that the privacy and civil liberties of everyone in the world must be taken into account when agencies collect signals intelligence.

(Edgar 2017, 4)

In the United Kingdom, the Snowden disclosures also led to an official reconsideration of bulk collection by the intelligence services. David Anderson, a lawyer appointed as Independent Reviewer of Terrorism Legislation in the United Kingdom, issued influential reports successfully recommending law reform in the area of UK government access to communications data. These recommendations resulted in the Investigative Powers Act (2016), which introduced a regime of judicial oversight of warranting of targeted interception, bulk collection and “equipment interference” (hacking or malware installation). Anderson also conducted a review in 2016 of the actual security benefits of bulk collection, based on a mix of secret and publicly summarized case studies which the UK intelligence

services made available to him. This is the Bulk Powers Review that gives rise to this chapter.

The Conclusion of the Review concedes that bulk collection results in the storage and analysis without consent of large amounts of personal data. Under European law and international human rights treaties, this is an intrusion into privacy even if the data is not the content of messages, even if it is not “sensitive” or “protected” data to do with for example health, sexuality or religion, and even if it is not humanly inspected, but only held and processed by IT systems. The fact that bulk collection is invasive does not, however, mean it is impermissible. Anderson writes:

international human rights instruments are pragmatic enough to recognise that intrusions into individual privacy will often be justified in the public interest. The privacy right may be overridden, where it is proportionate to do so, in the interests of national security, safety and the prevention of disorder or crime.

(Anderson 2016, 119)

And, Anderson goes on, these are the interests promoted by bulk collection as used by the Intelligence services in the Review case studies.

Each of the case studies is said to represent a success, small or large, against serious crime or threats to national security. They all involve intrusions, however technical, into the rights [to a private life and personal data]. But as they also illustrate, the benefits of successful operations are not simply measurable in a dry tally of operational gains. Individually and cumulatively, they change lives for the better.

(Anderson 2016, 120)

At this point, several questions arise. First, granted that bulk collection violates a right to privacy, are the interests that it arguably serves weighty enough to override that right? Some of Anderson’s illustrations – I come to them in a moment – might suggest the answer “No”. Second, even if the interests that Anderson lists *are* overriding, do they exhaust the interests pursued by the intelligence services through bulk collection? Here the answer is a clear “No”, since uses of bulk collection listed by the Intelligence services themselves for the Review include the pursuit of economic well-being and recruitment to MI6. These interests are *not* necessarily overriding, as I go on to argue.

A further question, and one that is perhaps more fundamental than the questions about overridingness just raised, can be put by asking whether privacy is satisfactorily understood in European or human rights law. In particular, it can be asked whether a loss of privacy or intrusion takes place when, as European law provides, someone loses *control* of his or her data (without consent) (De Hert 2008).

It is clear that one can lose control of information against one’s will without losing privacy, as when one’s diary is lost under a tonne of rubble after an earthquake. In this case, no loss of privacy has occurred because, though the diary is out of its

owner’s control, it is not readily accessible to an interested reader. Even if it came to be in someone’s control, say, because someone excavating the rubble comes across it, it does not divulge any information until someone actually reads the diary and takes in its contents. Until information is extracted and understood, there is no loss of privacy. But now suppose someone does read the diary. Even then it may be of no interest to the reader so that he or she disregards and forgets the diary’s contents. If there is a loss of privacy at all, it is limited and temporary.

In view of cases like these, I favour a more restricted understanding of loss of privacy: namely when sensitive information – not just any old information – about someone (a) comes to the *attention* of someone else without the data subject’s consent; (b) is grasped and remembered by that second person, and (c) the information is not normatively public. To take the last part of this formulation first, it seems clear that some information about oneself *ought* (morally ought) to be public – in the sense of being available for some time on the public record – whether one likes it or not – for example, the fact that a court has passed a sentence against one, or that one holds a public office, or that one has signed a petition, or that one is a qualified doctor. These are legitimately public pieces of information even though they are personal, because the institutions they are associated with are partly public-facing.

For example, the fact that someone has been sentenced to a crime should be on the public record because justice, as the saying goes, must not only be done but also be *seen* to be done. This is the effect of having public trial proceedings in due process-respecting jurisdictions, and records of verdicts and sentences. If the proceedings are normatively public, why is not a record of the proceedings normatively public? Again, certification bodies assure the public that identified people have the training to do certain potentially dangerous things, such as administering medical treatment, and where the certifications are missing, people should beware. Publicity in the case where certifications are missing or fraudulent is therefore obligatory. If it is discovered by an official or a patient that Smith is not a qualified or competent cosmetic surgeon, that fact needs to be made public, notwithstanding the fact that it is personal information about Smith. If a trial proceeds to a sentence before the eyes of anyone who wants to visit the public gallery of the court, then it is on the public record and ought to be available to members of the public who are not able to get into the public gallery.

Coming now to privacy and *attention*, it seems clear that this is what makes the difference between sensitive information being merely available for sharing and information actually being shared. Privacy is violated when availability of information turns into possession of information, that is, someone’s taking in information intended not to be shared. Although mere availability facilitates possession of private information, it is not sufficient for loss of privacy, unless there is a reasonable probability that availability turns into possession. To return to the diary under a tonne of rubble, it is in some sense available to any excavator, but it is not likely to come into anyone’s possession, because of the difficulty of excavation.

Finally, let us turn to sensitivity. Not every piece of personal information is sensitive. A person’s shoe size or hair colour or the fact that they like chocolate ice

cream does not normally rise to the threshold for sensitivity, because there is no clear connection between that information coming into someone else's possession and probable loss of status or disadvantage or harm to the person the information concerns. Some kinds of information are conventionally protected against disclosure whether intended to be shared or not, because they so engage prurience, idle curiosity, prejudices, malice or other kinds of threats to the status of the data subject, that he or she should have the last word about disclosure.

In previous (sometimes joint) papers (Sorell 2018; Guelke and Sorell 2016), I have tried to give some indication of the range of sensitive information by reference to zones of privacy. These zones include the human body, the human mind (understood as the locus of one's fundamental beliefs and emotional attachments) and the home. Targeted surveillance using cameras, bugs and telephone taps penetrates many of these zones and is therefore often highly intrusive, as it gives surveillance agents access (visual or auditory) that is willingly extended by the surveillance target only to intimates, including access to unguarded expression of information that is not normally divulged to everyone. When cameras or taps or direct inspection are used, information normally classified as "sensitive" such as health information, or information about deep convictions, or about intimates, is extracted from secret observation of the body, secret listening in on people speaking their mind, or secret searches of a home. Again, targeted secret surveillance often bypasses triggers for voluntary concealment of one's body, or guarded or coded disclosure.

By contrast with targeted surveillance by means of bugs or taps, bulk collection does not necessarily penetrate the zones of body, mind or home. In particular, bulk collection of telephone meta-data – the staple of NSA work – is relatively unintrusive. It is not in itself a penetration of private zones, though it may lead to such a violation for example in a case where analytics of bulk collected data identifies someone as a suspect who merits targeted surveillance, say because he is in frequent email communication with a known jihadist.

Although bulk collection is not necessarily a privacy violation, other things are often wrong with it: for example, its secrecy (Sorell 2018; Lucas 2014), its eluding legal oversight and its supporting a far greater volume of searches and analyses than intelligence services are able to take in or act upon, so that it self-defeatingly produces acute information overload.

Doubts about bulk collection as a privacy violation are rarely heard from those writing on the ethics of intelligence.¹ But this may be because examples used by these writers are out of keeping with the way most bulk collection works. For example, Isaac Taylor writes:

the privacy at stake when data collection is being carried out is what we can call informational privacy. The interest here is in not having certain pieces of personal information revealed to others under certain circumstances. Yet, even with this narrowing of the issue, the interest at stake is difficult to identify. I might have an interest in various people not having access to my medical records, but the reasons why I might want to keep those records private from one group of people (potential employers, say) might be very

different from the reasons I want to keep them hidden from another group (like co-workers).

(Taylor 2017, 329)

This passage makes it sound, first, as if bulk collection homes in on “sensitive” information, namely content from health or employment data bases, and as if this content might somehow come through bulk collection to the attention of people personally known to the data subjects (employers, co-workers) to whom they are sure they do not want to disclose this information. But this way of thinking misses the facts that (a) it is not nosy colleagues or bosses but machines with no human curiosity who are collecting the relevant data,² (b) counter-terrorism is the purpose of the collection, (c) connections with personal information depend on queries happening to excavate a name from a mountain of data and (d) meta-data rather than content is what has mainly been collected in cases emphasized post-Snowden: telephone meta-data at that. The latter point is worth making because a lot of personal communications meta-data, such as what number reaches a particular named person at a given address, has long been available in public telephone directories available to everyone – without anyone thinking that it is an invasion of privacy.

Operational Utility and Agent Recruitment

So far, I have argued that machine-collected communications meta-data is not particularly intrusive. Even if it were, its being useful for counter-terrorism would normally justify the invasion of privacy. I now consider uses of bulk collection by the intelligence services for purposes *other* than counter-terrorism. The Bulk Powers review report itself calls attention to the role that bulk collection by GCHQ plays in the identification of possible agents for recruitment as Secret Intelligence Service agents (Anderson 2016, 153). Again, the Intelligence Services Act 1994, section 2, authorizes activity by the SIS for pursuing the economic advantage of the United Kingdom. Are these uses of bulk collection unobjectionable? In this section I consider recruitment of foreign agents; in the next I turn to secret service action in the interest of national economic advantage.

The SIS in the United Kingdom recruits agents both at home and abroad.³ Some recruitment is open and consists in part of inviting applications from university graduates, in much the way mainstream employers in the United Kingdom might. This form of recruitment would not normally require bulk collection, and there is reason to think that applicants who go through it get full information about the risks they run, as well as reasoned assessments of their aptitude for the work. In this way, both potential employees and the agencies decide to work together with their eyes open about what will be involved.

Matters stand differently where the agents to be recruited are from abroad and are identified, possibly with the aid of bulk collection, and approached secretly. There are good reasons why people should not (morally should not) act as secret agents for foreign powers, and these are also reasons why foreign powers should not try to recruit such agents, including with the help of bulk collection. Some

of these reasons are drawn from the moral character of the foreign powers doing the recruiting, and some are drawn from the character of the jurisdiction against whose interests a recruited agent would act.

If the power for which the prospective agent would operate is illiberal and undemocratic, perhaps even unapologetically authoritarian, then it has questionable domestic legitimacy; and the ground for its pursuing its own interests at the expense of another country's, still less another liberal democratic country's, seems weak. In a sense there is little reason for even a citizen of such a jurisdiction to promote its official interests abroad, since that country's official interests are often detached from those of its citizens. But, by the same token, there is even less reason for a foreigner to act against their own country's interests in the service of that sort of recruiting country's interests.

It is possible that agents do not see the interests they oppose or promote as strictly national ones, but instead as class interests or ideological interests with global constituencies. Perhaps agents for communist countries saw things this way in the closing stages of World War II and immediately afterwards. This does not make talk of betrayal of one's country or colleagues inappropriate. Kim Philby's information for the Russians compromised many UK agents. In particular, many of those sent to Eastern Europe were killed immediately after being deployed (Bethell 1994). Philby betrayed UK agents, and therefore in some sense the United Kingdom, even if Philby was setting out to advance the interests of an international proletariat.

So much for agents of illiberal powers, such as the former Soviet Union or Russia in our own day. There are further reasons why citizens or residents of liberal democratic countries should not be the agents of foreign powers – even if the foreign power is liberal and democratic itself. These are reasons drawn from the character of the agent's home jurisdiction. Quite apart from the existence of legitimate local laws against espionage – their legitimacy is by itself a reason for prospective agents to respect those laws – targets of recruitment in these jurisdictions benefit from local liberal democratic protections and probably enjoy economic opportunities for which they should be grateful. The minimal expression of such gratitude is to be law-abiding. Acting as an agent of a foreign power not only shows ingratitude: it also renders the agent an *adversary* of the local jurisdiction whose freedoms benefit him or her. The agent is rendered an adversary without necessarily having a grievance against that jurisdiction (he or she may simply want the money paid to an agent). So the betrayal can seem (morally) gratuitous. It can seem gratuitous even if the recruiting country has the same moral character as the local jurisdiction.

What about the recruitment of agents by liberal democratic countries from illiberal and undemocratic countries that systematically oppose the recruiting country? In particular, what are we to say about prospective agents who, while they are citizens or residents of a certain illiberal and undemocratic regime, deplore its illiberality and lack of democracy? In this case the citizens or residents may not benefit much from citizenship, and acting for the foreign power might contribute to the removal of a regime facing both domestic *and* foreign opposition for its illiberal and undemocratic ways. Here the case for internal resistance or even rebellion might

double as a case for accepting foreign assistance for a pro-democratic movement. Might it not also function as a justification for co-operation as an intelligence agent with a foreign power interested in, among other things, local democratization?

No. Intelligence agents respond to demands for information from a foreign jurisdiction. The foreign jurisdiction may itself be democratic, but *its* demos is not that of the agent’s country. Its interests are not likely to be the same as those that would be pursued by a local demos after a regime change. So the idea that a local citizen interested in democratization might choose for that reason to become an intelligence agent for a foreign democracy seems ill-grounded. A person interested in democratization might look to external sources for funds, for example a would-be political party intending to operate in a democracy, but only by risking the impression of a party being directed from another jurisdiction. If, to avoid this impression, the money was secretly outsourced, that would undercut another norm of democracy – transparency – without cancelling the risk of undue foreign influence. In any case, if the choice of sources of funds were between an intelligence service and almost any other institution – an NGO, a private foundation, an international governmental organization – it is hard to see why the intelligence service would be preferred: it is too closely tied to the interests of a particular country rather than an interest in democratization. From many points of view, then, the promotion of liberal democracy does not seem to be an appropriate purpose of a foreign intelligence service, even the intelligence service of a democratic country.

The reasons for citizens of illiberal, non-democratic countries not to become agents of other country’s intelligence services do not stop there. I have left out the obvious consideration that traitors in countries without due process are in mortal danger if discovered. They are likely to put not only themselves but also their families at risk. Even if their betrayal has been discovered, punished and officially acknowledged by all concerned through a public prisoner exchange and relocation to the country of their intelligence handlers, the agents are not necessarily safe, as the recent poisoning of Sergei Skripal by the KGB in Salisbury shows (Dejevsky 2019).

Even when the jurisdiction betrayed by an intelligence agent is sinister or worse, as in the case of Skripal, the fact remains that the agent is a traitor, and so is intelligibly an object of hatred of his countrymen and not only his country’s officials. Especially where someone has acted enthusiastically as an intelligence agent for his own country before acting as an agent for another, the fact of his ending up in the pay of a human rights-respecting government does not confer on him much moral credit or put in a more favourable light his previous work for the illiberal government’s intelligence service. In this respect, Skripal at his best was less estimable than a dissenter-turned-foreign-intelligence-agent.

Whether recruited at home or abroad; whether he or she acts for a liberal or an authoritarian regime, an agent accepts to lead a compartmentalized life, part secret, part open to his or her intimates. The role inevitably involves systematic deception of various audiences, some professionally hostile, others harmless, others positively supporting and loving. It also involves casually breaking confidences, and posing on demand as a holder of a variety of political views. David Cornwell

(AKA John Le Carré, the celebrated author of spy novels) was recruited while still a student at Oxford to work for MI5, and conscientiously infiltrated both left- and right-wing clubs. He was not above reporting the activities of close friends (Sisman 2015, chap. 6). This rather seedy behaviour appears only to have served the purpose of ingratiating himself with his handlers. The same casual betrayal of friends is associated with top-echelon spies. When Kim Philby's status as a Russian agent was conclusively established by MI6, he was not summarily arrested, but told privately in Beirut by an old friend and MI6 colleague, Nick Elliot, that the game was up (Macintyre 2015, chap. 14). This humane gesture was supposed to have led to a gentlemanly surrender by Philby after taking the opportunity of saying goodbye to his family. Instead, Philby promptly absconded and was next heard of in Moscow. Absconding was both a personal betrayal of the friend *and* an abandonment of his family, who were left with the shame of their relation to him and the embarrassment of being seen by others as possibly complicit.

Operational Utility and National Economic Advantage

I have been arguing that the use of bulk collection for prospective agent recruitment abroad is morally questionable, because prospective agent recruitment abroad is itself morally questionable. Agent recruitment from one's *own* citizenry for intelligence work abroad is morally justifiable, but it is presumably often possible *without* bulk collection. I now turn to a third purpose of bulk collection, namely pursuing national economic advantage. Unlike bulk collection for counter-terrorism or for the purpose of acting against serious and organized crime, bulk collection for national economic advantage is not readily connected to defence from life-threatening attack or even defence against other non-lethal harms, and it is notable that all of the bulk collection success stories presented to the Anderson review come from defensive activity.

In addition to its departure from self-defence, bulk collection for economic advantage seems to make countries who are otherwise military and intelligence allies into adversaries, at least temporarily. For example, France and the United Kingdom share intelligence about terrorists and people traffickers, but they have been, and will probably again be, competitors in procurement processes for military equipment in the Middle East and South Asia. In the context of competitive procurement, timely intelligence about discounts offered by France for large orders of military equipment are clearly of the utmost value to the United Kingdom (or UK companies bidding for contracts), and obtaining this intelligence is certainly within the remit of the SIS. Bulk acquisition has a role in identifying which officials in countries buying the equipment would have received price information, and which email accounts might therefore be worth penetrating. The same methods might also reveal who is in a position to be successfully bribed (SIS agents have exemptions from prosecutions under recent bribery law in England and Wales) (Horder 2011).

Espionage for economic advantage against competitors (as opposed to fully fledged adversaries) is a by-product of the end of the Cold War.⁴ It takes at least two forms: the direct supply of intelligence information by a country's intelligence

services to firms from that country, and espionage in the service of the home government’s economic policy. The second kind of activity might consist of equipment interference at laboratories or companies in a competitor nation. This sort of activity has relatively recently been agreed to be out of bounds by the G20, and by the United Kingdom in respect of China (Foreign & Commonwealth Office UK 2015). The first kind of activity has long been informally outlawed in the United States (Rascoff 2016), but not in the United Kingdom.

Dover documents a case in relation to UK arms manufacturers from around 2005. He highlights the process of a manufacturer’s being introduced to foreign procurement officials by a local UK Defence Attaché, supported by a now defunct UK government body, the Defence Export Services Organization (DESO), and several intelligence services:

Having received first indications marketing and been introduced to agents and procurement officials the manufacturer takes steps to provide them with a corporate presentation. Information on these officials and agents will have been collated locally by embassy officials *and might also have been subject to general or centralised information trawls by MI6, DIS and GCHQ* [my emphasis] – depending on the character and positioning of the person in question (interview 05IS; interview 24IS; Scott, 1996, C2.26). These presentations are discreet and are held without publicity. The DA [Defence Attaché] will nearly always be in attendance at these presentations, as a representative of the UK government, and will often be in full dress uniform (interview 24IS). This emphasizes the UK government’s backing of the product and also allows the DA to pass on convincing accounts of how the equipment has been successfully used by the UK’s armed forces (interview 24IS; interview 18IS).
(Dover 2007, 695)

A subsequent intervention might consist of an embassy reception held to underline UK government support for the proposed sale. At this stage, too, the intelligence services sometimes made a contribution:

The primary motivation for hosting such an event is to give the manufacturers an overt ‘kitemark’ [mark of trust] of British government support. Such events also serve an information-gathering purpose – in soft terms as a means by which to network locally and illuminate matrices of influence and business. Of course, such ‘soft’ methods do not preclude the use of central intelligence assets – such as GCHQ to intercept communications or with human intelligence to reveal negotiating positions within rival companies or the client government, although this occurs only in a few notable cases (interview 05IS; interview 27IS).

(Dover 2007, 696)

Dover does not emphasize *automated* evidence trawls; he is interested in “stovepiping” – the supply of intelligence – whether electronic or not, humanly

gathered or not – direct to officials of a company seeking a sale, as opposed to officials in government. His discussion nevertheless illustrates what sometimes happens when the intelligence services act “in the interests of the economic well-being of the United Kingdom”.

Now for the central question: “What, if anything, is morally wrong with what Dover describes?” First, and most obviously, it is not immediately clear that promoting sales of a UK company always contributes much to the well-being of the United Kingdom as a whole. Whether it does depend on for example how much UK tax the company pays, how many UK citizens it employs and how well it pays them. Supporting a UK arms manufacturer raises further issues. For one thing, arms sales have traditionally been associated with corrupt payments of “commission” or other euphemistically labelled charges (Gilby 2014). Again, it matters what type of customer is buying. Is it a liberal democratic regime that is constrained in its resort to force? Or is it an authoritarian government that is not above using its weapons against its own or other civilians, for example in a proxy war? When these questions are pressed in the case of sales to Saudi Arabia – highly relevant at the time Dover carried out his research – it is not clear that moral justification for intelligence service assistance for arms deals is very strong if it exists at all.

It might be thought that while intelligence service pursuit of UK economic well-being in general is perhaps open to the criticisms made in the last paragraph, intelligence service pursuit of UK economic well-being through bulk collection is not, at least when it is lawful. Under the Investigatory Powers Act (2016) section 204 (3a), bulk collection for national economic well-being is permitted only where it is “also relevant to the interests of national security”. Not every company seeking to sell goods or services in foreign procurement exercises will contribute to national economic well-being as well as having relevance to national security. So, clause 3a does seem to work in some cases to limit what the intelligence services can do. Unfortunately, this is not its effect in the problematic area of arms. Supporting big UK arms manufacturers is arguably always “relevant” to the interests of national security, in the sense that sales (even to dubious regimes) finance research that leads to innovation in military technology that undoubtedly helps to protect the United Kingdom. So, if the “relevance” clause was intended to limit economically motivated bulk collection to unproblematic cases, it does not seem to go far enough.

Perhaps the cases that the “relevance” clause most uncontroversially applies to are those in which the intelligence services assist in monitoring and responding to cyberattacks on UK companies. Here the purpose of bulk collection, for example of email meta-data for attack attribution, is defensive, and the beneficiaries are a very large range of organizations in both the public and private sectors of the United Kingdom. In the past, cyberattacks have been directed at UK communication companies with large customer bases as well as the National Health Service: in the latter case, the connection between preventing those attacks and increasing UK *economic* well-being is obscure. Other kinds of well-being are relevant instead. Protecting these seems more urgent morally than in the case where the interests of UK arms makers are assumed without argument to line up with UK interests.

The UK National Cyber Security Centre (NCSC) is a branch of GCHQ. As its 2019 Annual Report makes clear, it has developed a number of software tools for companies and public sector organizations to use in routine cybersecurity, and it has devised special safeguards for government networks that it is adapting for the NHS to prevent attacks like the WannaCry ransomware exploit in 2015 against the National Health Service. The NCSC Annual Report for 2019 gives examples of tools it has developed:

- the NCSC “Internet Weather Centre”, which will aim to draw on multiple data sources to enable full understanding of the United Kingdom’s digital landscape
- the Infrastructure Check service: a web-based tool to help public sector and critical national infrastructure providers scan their internet connected infrastructure for vulnerabilities
- Breach Check: a web-based tool to help government and private sector organizations check whether employee email addresses have been compromised in a data breach

(National Cyber Security Centre 2019)

At least the first of these three tools seems to involve bulk collection, and this time for cybersecurity and economic purposes that seem reasonable. The reason is that the tools are defensive, and are partly used to defend public institutions. The use of these or other tools to give the UK or UK companies is less strongly justified at first sight, because the question of who benefits from UK economic advantage and to what extent, needs to be specified first.

Conclusion

I have been arguing that the best case for the moral justifiability of bulk collection is where bulk collection clearly contributes to counter-terrorism. Anderson’s claim that bulk collection of this kind is privacy-violating, but that privacy violations are a price worth paying for the prevention of terror attacks, concedes too much to privacy concerns. According to me, the simple collection and machine processing of personal information that never comes to personal attention, and that does not lead to targeted surveillance, is not by itself a privacy violation. The personal information of the average citizen in the United Kingdom, though held in data bases, is no more likely to receive attention than the diary under tons of rubble after an earthquake. It is simply too disconnected from the electronic travel, communication and financial transaction profiles of people who are reasonable targets. What is more, the information is not typically “sensitive” in senses I tried to elaborate in the first section. Typical personal information is protected not only by the law but also by judicial interventions in the authorization of bulk collection; it is also protected by the sheer amount of data and the sheer number of data analytics exercises that are needed to provide actionable intelligence.

Not every goal pursued by the UK intelligence services is as closely connected to the protection of lives as counter-terrorism. Agent recruitment is not. The pursuit of greater UK economic well-being is not. On the contrary, these purposes are arguably morally questionable in many cases. Foreign agent recruitment is an invitation to treason with all the attendant risks to the welfare and life of the agent and his or her family. The pursuit of UK economic well-being is conducted by the SIS under a regime that permits bribes and perhaps encourages “stove-piping” and the over-identification of state interests with the interests of economically important UK companies. Bulk collection in the service of these morally questionable purposes is itself morally questionable – whatever its operational utility.

Notes

- 1 An exception is Macnish (2018).
- 2 Of course, it is possible that people with access to data sets captured through bulk collection are personally interested in the addresses and financial records of particular people, but this fact is a reason for their not being employees of institutions that compile and analyze the data bases for counter-terrorism. It is not a reason for abolishing the data bases or for not building them in the first place. There have been cases of security service misuse of bulk data bases, including out of noisyness or simple convenience but no one suggests these are very numerous (Bowcott and Norton-Taylor 2016).
- 3 Not every intelligence service recruits foreign agents. The CSIS in Canada apparently does not.
- 4 See Porteous (1996; 1995).

References

- Anderson, David. 2016. *Report of the Bulk Powers Review*. London: HMSO.
- Bethell, Nicholas. 1994. “Profits and Losses of Treachery: Victims of Kim Philby’s Betrayals Are”. *The Independent*, September 6. www.independent.co.uk/voices/profits-and-losses-of-treachery-victims-of-kim-philbys-betrayals-are-staking-a-claim-to-the-cash-1447065.html.
- Bowcott, Owen, and Richard Norton-Taylor. 2016. “UK Spy Agencies Have Collected Bulk Personal Data since 1990s, Files Show”. *The Guardian*, April 20. www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s.
- De Hert, Paul. 2008. “Identity Management of E-ID, Privacy and Security in Europe: A Human Rights View”. *Information Security Technical Report* 13 (2): 71–5. <https://doi.org/10.1016/j.istr.2008.07.001>.
- Dejevsky, Mary. 2019. “Opinion: There Are Still Questions about the Skripal Poisoning That No One Wants to Answer”. *The Independent*, 4 March. www.independent.co.uk/voices/skripal-poisoning-salisbury-attack-yulia-russia-novichok-putin-a8807191.html.
- Dover, Robert. 2007. “For Queen and Company: The Role of Intelligence in the UK’s Arms Trade”. *Political Studies* 55 (4): 683–708. <https://doi.org/10.1111/j.1467-9248.2007.00669.x>.
- Edgar, Timothy H. 2017. *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, DC: Brookings Institution Press.

- Foreign & Commonwealth Office UK. 2015. “UK-China Joint Statement 2015”. *GOV.UK*, October 22. www.gov.uk/government/news/uk-china-joint-statement-2015.
- Gilby, Nicholas. 2014. *Deception in High Places: A History of Bribery in Britain’s Arms Trade*. Illustrated edition. London: Pluto Press.
- Guelke, John, and Tom Sorell. 2016. “Violations of Privacy and Law: The Case of Stalking”. *Law, Ethics and Philosophy* 2016 (4): 32–60.
- Horder, Jeremy. 2011. “On Her Majesty’s Commercial Service: Bribery, Public Officials and the UK Intelligence Services”. *The Modern Law Review* 74 (6): 911–31.
- Lucas, George R. 2014. “NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden”. *Ethics & International Affairs* 28 (1): 29–38. <https://doi.org/10.1017/S0892679413000488>.
- Lyon, David. 2014. “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique”. *Big Data & Society* 1 (2): 2053951714541861. <https://doi.org/10.1177/2053951714541861>.
- Macintyre, Ben. 2015. *A Spy among Friends: Philby and the Great Betrayal*. London: Bloomsbury Paperbacks.
- Macnish, Kevin. 2018. “Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World”. *Journal of Applied Philosophy* 35 (2): 417–32. <https://doi.org/10.1111/japp.12219>.
- National Cyber Security Centre. 2019. *Annual Review 2019*. London: HMSO. www.ncsc.gov.uk/files/NCSC_Annual%20Review_2019%20FINAL%20double%20pages%20V2.pdf.
- Porteous, Samuel D. 1995. “Economic/Commercial Interests and the World’s Intelligence Services: A Canadian Perspective”. *International Journal of Intelligence and Counter Intelligence* 8: 275–306.
- . 1996. “Looking Out for Economic Interests: An Increased Role for Intelligence”. *Washington Quarterly* 19: 191–204.
- PwC. 2017. *Operation Cloud Hopper*. PwC. www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.
- Rascoff, Samuel. 2016. “The Norm against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections”. *The University of Chicago Law Review* 83 (December): 249–69.
- Shorrock, Tim. 2013. “A Modern-Day Stasi State”. June 11. www.thenation.com/article/archive/modern-day-stasi-state/.
- Sisman, Adam. 2015. *John Le Carré: The Biography*. 1st edition. London; Oxford; New York; New Delhi; Sydney: Bloomsbury Publishing.
- Sorell, Tom. 2018. “Bulk Collection, Intrusion and Domination”. In *Philosophy and Public Policy*, edited by Andrew I. Cohen, 39–60. London; New York: Rowman & Littlefield Publishers.
- Taylor, Isaac. 2017. “Data Collection, Counterterrorism and the Right to Privacy”. *Politics, Philosophy & Economics* 16 (3): 326–46. <https://doi.org/10.1177/1470594X17715249>.
- Zetter, Kim. 2010. “Google Hack Attack Was Ultra Sophisticated, New Details Show”. *Wired*, January 1. www.wired.com/2010/01/operation-aurora/.

9 Surveillance, intelligence and ethics in a COVID-19 world

Jessica Davis

Introduction

In the initial weeks and months of the COVID-19 pandemic, states grasped at any possible tools to help them battle the economic, health and human impacts of the disease. The severity of the crisis led states to use, or consider using, any tools at their disposal, including those that had previously only been used for national security applications. The pandemic struck at a time when personal technology (such as smartphones) and surveillance technology uses were at an all-time high and states looked to both of these types of technology to stop the spread of the virus. The use of intelligence and surveillance tools that were once largely purview of security, intelligence and law enforcement being used for pandemic surveillance represents the lengths that many states have been willing to take to stop the spread and limit the damage (Davis 2020).

States leveraged personal technologies primarily for contact tracing purposes, or to provide notifications to users of possible exposure to COVID-19. However, some states sought to use tools developed for national security purposes (such as counter-terrorism or counter-espionage), which often exploit personal technology data, to help contain the virus. Other surveillance technologies, such as closed-circuit cameras and facial recognition software, were also deployed to combat the virus. The use of these tools and techniques, once largely the purview of security, intelligence and law enforcement, represented the extraordinary lengths that many states took to stop the infection. These efforts involved collecting data on citizens from cell phones, financial transactions and social media intelligence and combined it with or exploited it for health data, raising significant concerns about privacy and civil liberties.

The nature of the pandemic has in part driven this reliance, or at least turn, to technology and national security surveillance techniques. Traditional contact tracing works well when transmission requires sustained, intimate contact, but when transmission can occur through limited exposure and the virus can be spread by asymptomatic people, traditional models of health surveillance may fall short (Berman, Fowler, and Roberts 2020). In the first six months of the pandemic, however, the disease has proven largely impervious to these efforts. Many of these technologies were envisioned to be used in a targeted way, as a means of

tracing close contacts and the source of infection. In many cases, the ability to trace specific cases has proven only partially successful due to the widespread infection rates many countries experienced.

Of course, public health surveillance and national security surveillance are two distinct paradigms with different values and governing norms (Berman, Fowler, and Roberts 2020, 1). For the purposes of this chapter, I will make a distinction between the two by using the terms *national security surveillance* to describe technologies and techniques of surveillance usually associated with law enforcement, intelligence, and security services, and *health surveillance* to refer to more traditional modes of the collection of health, infection and pandemic-related information. National security surveillance and public health surveillance also have very different purposes and applications, differences that have an impact on any discussion of intelligence, ethics and surveillance during a pandemic. Health surveillance is cooperative, minimizes data collection and limits subsequent use (Berman, Fowler, and Roberts 2020, 1). National security surveillance operates coercively, maximizes data collection, and in some countries, there are few limits on use of lawfully collected data (Berman, Fowler, and Roberts 2020, 1). In these two forms of surveillance, the role of consent, scope of collection and subsequent use are all different and differently restricted (Berman, Fowler, and Roberts 2020, 19).

This chapter will look at the surveillance methods used by states in an effort to stop the pandemic and discuss the ethical implications of those efforts, drawing on literature in the field of ethics of surveillance and bio-surveillance. This analysis will be structured on two frameworks for the ethical collection and use of intelligence by Bellaby and Omand (Omand 2006; Bellaby 2012).

National security surveillance in the first six months of the pandemic

In the first six months of the pandemic, a number of states discussed the possibility of exploiting national security surveillance tools to fight the pandemic. In most cases, states opted to forgo these efforts due to a host of practical, privacy, legal and technological challenges. However, to curb the spread of COVID-19 some countries have been moving to implement technologies to monitor and surveil their citizens and provide early warning of infection and spread. Indeed, the policy response to the COVID-19 pandemic has been to categorize and compare a mix of policy tools that have been deployed by governments, some of which have been national security surveillance tools. In almost every country, the COVID-19 pandemic has seen an unprecedented use of technology (The Soufan Center 2020; Dunlop, Ongaro, and Baker 2020; Berman, Fowler, and Roberts 2020, 1).

In a survey of 56 countries conducted between March and August 2020, 45 (80%) were using technology to track COVID-19 outbreaks. Of those 45 countries, another 18 (40%) were using national security surveillance technology to track infected individuals, individuals required to self-quarantine, or to surveil their population writ large for signs of infection or compliance with local regulations, illustrated in Figure 9.1.

USE OF TECHNOLOGY FOR COVID19 SURVEILLANCE

- No technology used
- Use of technology (personal)
- Use of national security surveillance technology

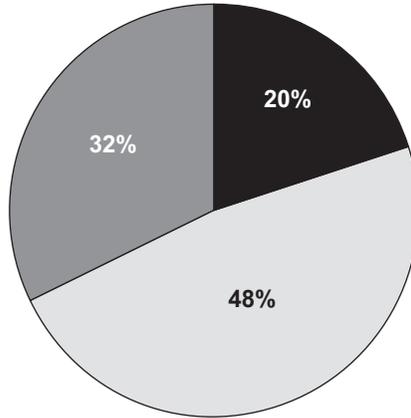


Figure 9.1 Use of technology for COVID-19 surveillance.

These technologies primarily involved facial recognition and closed-circuit cameras, location monitoring, financial transaction and social media intelligence and other (unspecified) tools that were developed to combat terrorism but that had been re-deployed to combat the pandemic. For example, in the United States, Army technology developed to combat terrorism was deployed to help monitor the spread of COVID-19. The Army used social media, news media, blogs and government sources to create actionable data to be used for force protection, including information about COVID-19 derived from all of these sources (Brading 2020).

In another example, in March 2020, Israel invoked emergency powers to use cell phone tracking data to retrace the movements of those believed to be infected and to implement quarantines. The data had previously been acquired by the Israeli Security Agency (colloquially known as Shin Bet) for counter-terrorism purposes. The disclosure of the programme raised concerns that it violated the privacy of Israeli citizens and that granting of emergency powers would open the door to future abuses (Sachs and Huggard 2020). The utility of these surveillance tools during the COVID-19 pandemic is questionable, as in September 2020, Israel announced that it was undertaking another three weeks of lockdown (at least) due to rising infection rates (BBC News 2020b).

Israel was not alone in deploying existing national security surveillance tools for pandemic surveillance. In Pakistan, a secret surveillance system that was used to track terrorist suspects by the Inter-Services Intelligence Directorate (ISI) (Pakistan's primary intelligence service) was deployed to combat the pandemic. While few details have been released regarding its actual application for pandemic surveillance, the system has geo-fencing and telco-tracking mechanisms and allows for the monitoring of confirmed patients and potential virus carriers. The system is also reported to track movements and be able to listen to private phone conversations as part of its efforts to monitor possible symptoms (Shairani 2020).

While counter-terrorism tracking programmes have been deployed in at least two countries, other states have deployed national security surveillance tools more selectively in their bid to stop the spread of the virus. For instance, South Korea used mobile technology against the outbreak to facilitate contact tracing – people who tested positive for the virus were asked to describe their recent movements, and the state facilitated this process by using Global Position System (GPS) phone tracking, surveillance camera records and credit card transactions (McCurry 2020). For its part, Hong Kong opted for physical location monitors in the form of wristbands that linked to smartphones to provide location-tracking services to help enforce quarantine requirements for new arrivals (Sharwood 2020).

The use of closed-circuit cameras and facial recognition software was also deployed in the early stages of the pandemic. These efforts were aimed at detecting possible signs of infection and to detect compliance with quarantine or regulatory requirements. In China, facial recognition technologies that can detect elevated temperatures in a crowd were deployed and cameras were used to flag and identify citizens not wearing a mask. These surveillance activities were described by the state as part of a response during an “extraordinary time” that requires extraordinary measures (Kuo 2020). However, Chinese citizens noted that the same justification was used in deploying other surveillance technologies in advance of the Olympics, technologies that have since become a permanent feature in China (Kuo 2020). In Russia, closed-circuit cameras were used to enforce lockdown while in France, surveillance cameras were used to check adherence to rules (BBC News 2020; Rosemain 2020). As part of a three-month experiment, artificial intelligence-powered technology checked for adherence to local rules in place during the pandemic, such as wearing masks and adhering to physical distancing requirements (Rosemain 2020).

The use of national security surveillance technologies and tools for pandemic surveillance has been relatively constrained to a small number of countries. Many other states have adopted personal technologies like applications installed on smart phones for pandemic surveillance, monitoring and alerts, but for the most part these applications have been limited in scope and have privacy protections in place. While many states initially considered using more invasive and targeted measures for pandemic surveillance, privacy, legal and regulatory and practical constraints have limited this practice. In essence, while the tools of national

security appealed during the initial phase of the pandemic, the actual nature of how the virus spreads, along with the rate of infection, also worked to preclude the use of national security surveillance technologies.

Thinking ethically about national security surveillance during the pandemic

Times of crises and emergencies often lead states to consider or implement legislation, regulation and practices that they otherwise would not in the name of national security. Even though there are almost certainly critics of these practices, in many cases, public support is often on the side of governments implementing these changes in the name of national security. States of emergency may also stifle or silence critiques of these practices. However, the COVID-19 pandemic is relatively unique in terms of national and international emergencies: it is far lengthier than most, which creates space for critique and re-considering practices adopted early during the pandemic. It also allows for the consideration of best practices for the duration of the pandemic and future emergencies.

Intelligence studies have furnished us with two very useful frameworks for investigating the ethics of the practice of intelligence, which is a collection of activities such as information gathering, exploitation, all-source analysis and covert action (Herman 2013). Omand's framework calls for intelligence to be collected and analysed using six main principles:

- 1 sufficient sustainable cause
- 2 integrity of motive
- 3 proportionate methods
- 4 right authority
- 5 a reasonable prospect of success and
- 6 recourse to secret intelligence as a last resort

(Omand 2006, 618–19)

Bellaby's framework has similar elements and a few key differences. Bellaby argues that the practice of intelligence should be conducted along six principles as well:

- 1 just cause
- 2 legitimate authority
- 3 intention (intelligence should be used for the intended purpose)
- 4 proportionality (the harm caused outweighed by gains)
- 5 as a last resort and
- 6 targets should be discriminate (between legitimate and illegitimate)

(Bellaby 2012, 109)

Both frameworks have significant overlap in the principles they espouse, including just or sufficient cause, proportionality, intentionality, legitimate authority and

turning to intelligence as a last resort. They differ in that Omand also includes the proposition that intelligence activities should only be undertaken when they have a reasonable prospect of success, while Bellaby proposes that targets of intelligence collection should be discriminate, in that some targets are legitimate, while others are illegitimate. For instance, it could be argued that mass surveillance breaches this principle because it does not discriminate between targets – everyone is a target of the intelligence collection mechanism.

In terms of using intelligence and surveillance during the COVID-19 pandemic, the cause can certainly be justified or found to be sufficient. As of September 2020, at least a million people had died worldwide from the virus, and millions of others had fallen ill, some with effects lasting in excess of six months and the economic effects of the pandemic have also proven significant (Yong 2020). These simple measures only scratch the surface of the pain and suffering that COVID-19 has caused. As such, using intelligence and national security surveillance to combat the pandemic could certainly be justified and be found proportionate as well in many societies. The proportionality question, however, is an essentially contested one and one that will differ from society to society depending on the importance that is placed on privacy.

The question of the legitimacy of authority of using intelligence and national security surveillance tools and techniques for pandemic surveillance is an interesting one and one that has already been breached. In the Israeli case, the legal foundation for the data set was for counter-terrorism and could not easily be transferred to pandemic surveillance. This lack of just authority resulted in a ban on the use of some of these tools until new laws are passed (BBC News 2020a). In Pakistan's case, the lack of legitimate authority does not seem to have stopped the ISI from employing its tools and techniques, a clear violation of the ethical principles of intelligence.

In the context of a global pandemic, the idea that intelligence and national security surveillance could be used as a last resort is an interesting one. Many tools exist that could facilitate contact tracing and population monitoring other than those employed by national security and intelligence agencies. In fact, most states have chosen to employ those tools rather than use their more contested tools for pandemic surveillance. However, if a vaccine for the virus proves illusive or only partially effective, states may increasingly be tempted to employ these tools and they may in fact be justifiable as a last resort.

The differences between the two ethical frameworks presented here are also worth considering. Omand argues that intelligence should only be undertaken when it has a reasonable prospect of success. In the case of COVID-19, early results from surveillance practices have demonstrated (particularly in the case of Israel) that the deployment of national security surveillance has not been successful. This is largely the result of the specific nature of the virus – it is easily transmitted and can be transmitted by asymptomatic people. For its part, most national security surveillance systems are targeted surveillance systems, most easily deployed and most useful against a set number of targets. Surveilling an entire population for possible signs of infection is something better left to health surveillance technologies and techniques.

Finally, Bellaby argues that targets of surveillance and intelligence practices need to be discriminate, meaning that there needs to be a difference between legitimate and illegitimate targets. In many of the cases of national security surveillance deployed against COVID-19, this distinction has not been made. Instead, these tools have been deployed in the faint hope that they can provide some assistance for states fighting the pandemic. They have failed to distinguish between legitimate and illegitimate targets. However, this principle is perhaps of use in the future, if the scenario described earlier (no vaccine, or a minimally effective vaccine), and in a situation where a state has low levels of virus transmission. In that case, then some of the national security surveillance tools (such as enhanced location monitoring) could prove useful for reducing the spread of the virus and enforcing quarantine. In this instance, it would be critical to differentiate between legitimate targets of surveillance (perhaps those suspected of infection and unwilling to comply with quarantine) and those not (healthy or quarantine-abiding individuals).

In addition to this framework, I also propose that in the case of health surveillance (particularly when done by national security agencies, or using national security surveillance tools and techniques), that transparency is a critical element. The authority for national security agencies to collect and use data – and the use of techniques and methods should not come as a surprise to citizens of democratic state. In the current case, the enemy is a virus, not an adaptive adversary, so the need for secrecy about specific methods may exist, but actual collection and use of information should be transparent and open to democratic debate (Davis 2020). Civil liberties should not be abandoned quickly or easily, even in the face of a global pandemic. Instead, any sacrifices made should be done by considering the ethics of the proposed action and balancing the welfare of individuals and the population writ large.

Consistency of use is another critical consideration. Indeed, in talking about the use of intelligence for counter-terrorism, Omand notes that there are worries over the wider uses to which information derived from information technology might be put (Omand 2006, 616). While all the propositions proposed in these frameworks are important, the consistency of use of data is one of the most important propositions in terms of ensuring ethical use of intelligence collected to combat the pandemic. Data must be used in a manner consistent with how and why it was collected (Davis 2020). These concerns should be central during the pandemic and any discussion of using national security surveillance. Consideration needs to be given to what will happen to the information, how long it will be retained for, who will maintain (and have access to) the data and its ultimate destruction. Information collected for public health can result in stigma, embarrassment and discrimination (Berman, Fowler, and Roberts 2020, 24). Discrimination based on health status is a very real concern and one that will only grow if an effective vaccine is not found.

A particular problem with using national security surveillance for pandemic surveillance is the aggregation problem. While an individual piece of information

is not useful, in aggregate, they reveal intimate details of life (Berman, Fowler, and Roberts 2020, 23). One single data point is not that useful; but a comprehensive record of what a person purchased over a sufficient period of time will reveal intimate life details (the whole adds up to more than sum of its parts) (Berman, Fowler, and Roberts 2020, 23). The aggregation problem needs to be part of the ethical framework for considering the use of national security surveillance tools and techniques for pandemic surveillance.

In considering the use of national security intelligence practices for pandemic surveillance, states should consider the elements of Omand and Bellaby's frameworks. They need to balance just or sufficient cause, proportionality, intentionality, legitimate authority and turning to intelligence as a last resort. An ethical framework also needs to consider the prospect of success, as well as the discrimination of targets of surveillance. In addition to these considerations, any use of national security surveillance tools should be done in a transparent manner, with any subsequent data being used consistently within its purpose (the reason why it was collected) and in consideration of the aggregation problem.

Conclusion

The news is not all bad from a privacy and intelligence perspective. In some ways, modern technology has made health surveillance and reporting more private and real time than traditional methods of contact tracing and exposure notification. In some cases, no personal data is collected (e.g. in Germany, Canada and Vietnam) and a positive exposure results in a notification, rather than it being traced back to an individual contact, which has the obvious impact of informing a third party of the health status of an infected individual. In addition, concern over the expansion of national security surveillance has chilled uptake of disease tracking technologies in the United States (Berman, Fowler, and Roberts 2020, 1), and likely many other countries as well. When considering information sharing, Maxwell also raises questions about the legitimacy of state access to the private data of citizens in pursuit of the public good (Maxwell 2020).

When national security surveillance techniques are combined with health information, there is a strong potential for harms. On their own, national surveillance techniques certainly have risks, and the same can be said for health information. Combining these together creates greater potential for harms due to the sensitive nature of the information being collected, the intrusive means being proposed and the possibility of the information being used for a purpose other than just pandemic surveillance. It raises a host of potential issues including the involvement of national security agencies in health surveillance (where many of the proposed tools, techniques and analytic capabilities reside), information management, control, access and destruction and limits and sunset clauses on any of this proposed activity.

Surveillance systems are necessary to track (and eventually stop) the spread of infectious diseases, but those same systems can be used in discriminatory ways,

such as by limiting freedom of movement and speech (Youde 2012, 83). This is true when national security surveillance tools are used and there are additional risks and vulnerabilities. The international community has a moral and international legal obligation to track the spread of the outbreak of an infectious disease and use any data collected in this process to benefit the general population (Youde 2012, 83).

It is not sufficient to simply ask IF something is legal; we should ask whether it should be and under what circumstances (Davis 2020). This is especially true in the case of pandemic surveillance, or really any extraordinary measures put in place in a time of crisis. We also need to acknowledge that it may be difficult or impossible to roll back or limit powers once in place and that sunset clauses and benchmarks are only a start (Davis 2020).

In the far past, pandemics transformed international politics but in more recent pasts, their effect on the international system has been more muted. Drezner argues that COVID-19's effects in this regard will be minimal (Drezner 2020, 14), although one area that may change is tolerance for surveillance. There has not been a widespread uproar about the use of national security surveillance technologies or tools, or other kinds of surveillance, by citizens, which implies that many may be willing to trade some aspects of privacy for the promise of increased security. Of course, the risk is that these technologies become a permanent feature of life (The Soufan Center 2020), even after the pandemic is over and COVID-19 spread is under control. Indeed, surveillance may, for some people, be preferable to movement restrictions, mask protocols and physical distancing requirements.

At the same time, in considering the prospect of national security surveillance for the COVID-19 pandemic, it is critical to remember the limitations of these tools and technologies. The "promise" of national security surveillance for the pandemic may have fallen short. National security surveillance involves tools and techniques that are largely targeted means of surveillance. While this has been of little use in the early stages of the pandemic, as the pandemic spreads, and perhaps comes more under control, these targeted measures may have more appeal and utility and may have particular appeal if a vaccine is not forthcoming or turns out to be minimally effective.

It is also important to remember the enduring nature of emergency powers. Indeed, parallels can be drawn between the first six months of the global pandemic and the era immediately following the terrorist attacks of September 11, 2001, 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. As we consider what, if any, national security surveillance tools and techniques should be deployed to combat the global pandemic, we would be wise to remember that privacy and civil liberties are hard-won rights, and yet are easily surrendered for the promise of economic prosperity, physical health and freedom of movement. The pandemic may yet force us to choose between these things.

References

- BBC News. 2020. "Russia Uses Facial Recognition to Tackle Virus". *BBC News*, April 3. www.bbc.com/news/av/world-europe-52157131.
- . 2020a. "Coronavirus: Israeli Court Bans Lawless Contact Tracing". *BBC News*, April 27. www.bbc.com/news/technology-52439145.
- . 2020b. "Coronavirus: Israel to Impose Three-Week National Lockdown". *BBC News*, September 13. www.bbc.com/news/world-middle-east-54134869.
- Bellaby, Ross. 2012. "What's the Harm? The Ethics of Intelligence Collection". *Intelligence and National Security* 27 (1): 93–117. <https://doi.org/10.1080/02684527.2012.621600>.
- Berman, Emily, Leah Fowler, and Jessica L. Roberts. 2020. "COVID-19 Surveillance". SSRN Scholarly Paper ID 3666300. Rochester, NY: Social Science Research Network. <https://doi.org/10.2139/ssrn.3666300>.
- Brading, Thomas. 2020. "Army Anti-Terrorism Technology Helps Pinpoint COVID-19 Cases". *US Department of Defense* (blog). May 13. www.defense.gov/Explore/News/Article/Article/2185429/army-anti-terrorism-technology-helps-pinpoint-covid-19-cases/.
- Davis, Jessica. 2020. "Intelligence, Surveillance, and Ethics in a Pandemic". *Just Security*, March 31. www.justsecurity.org/69384/intelligence-surveillance-and-ethics-in-a-pandemic/.
- Drezner, Daniel W. 2020. "The Song Remains the Same: International Relations after COVID-19". *International Organization*, 1–18. <https://doi.org/10.1017/S0020818320000351>.
- Dunlop, Claire A., Edoardo Ongaro, and Keith Baker. 2020. "Researching COVID-19: A Research Agenda for Public Policy and Administration Scholars". *Public Policy and Administration* 35 (4): 365–83. <https://doi.org/10.1177/0952076720939631>.
- Herman, Michael. 2013. *Intelligence Services in the Information Age*. Abingdon, UK: Routledge. <https://doi.org/10.4324/9780203479667>.
- Kuo, Lily. 2020. "The New Normal: China's Excessive Coronavirus Public Monitoring Could Be Here to Stay". *The Guardian*, March 9. www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.
- Maxwell, Nick J. 2020. "Information Sharing in the Era of Coronavirus Tracing Apps: A New Context for Fighting Financial Crime?". *RUSI* (blog). August 11. <https://rusi.org/commentary/information-sharing-era-coronavirus-tracing-apps>.
- McCurry, Justin. 2020. "Test, Trace, Contain: How South Korea Flattened Its Coronavirus Curve". *The Guardian*, April 23. www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve.
- Omand, David. 2006. "Ethical Guidelines in Using Secret Intelligence for Public Security". *Cambridge Review of International Affairs* 19 (4): 613–28. <https://doi.org/10.1080/09557570601003338>.
- Rosemain, Mathieu. 2020. "French Watchdog Warns against COVID-19 Smart Surveillance". *Reuters*, June 17. www.reuters.com/article/us-health-coronavirus-france-privacy-idUSKBN23O2T7.
- Sachs, Natan, and Kevin Huggard. 2020. "Technosurveillance Mission Creep in Israel's COVID-19 Response". *Brookings* (blog). June 9. www.brookings.edu/techstream/technosurveillance-mission-creep-in-israels-covid-19-response/.
- Shairani, Kaukab Tahir. 2020. "Will Pakistan's Mass Surveillance Strategy Outlive the Pandemic?". *The Diplomat*, June 5. <https://thediplomat.com/2020/06/will-pakistans-mass-surveillance-strategy-outlive-the-pandemic/>.

- Sharwood, Simon. 2020. "Hong Kong Makes Wearable Trackers Mandatory for New Arrivals, Checks in with 'Surprise Calls' Too". *The Register*, March 19. www.theregister.com/2020/03/19/hong_kong_wearable_trackers_mandatory/.
- The Soufan Center. 2020. "IntelBrief: Will COVID-19 Usher in the Era of the Surveillance Industrial Complex?". *The Soufan Center* (blog). May 8. <https://thesoufancenter.org/intelbrief-will-covid-19-usher-in-the-era-of-the-surveillance-industrial-complex/>.
- Yong, Ed. 2020. [etc.] "Long-Haulers Are Redefining COVID-19". *The Atlantic*, August 19. www.theatlantic.com/health/archive/2020/08/long-haulers-covid-19-recognition-support-groups-symptoms/615382/.
- Youde, Jeremy. 2012. "Biosurveillance, Human Rights, and the Zombie Plague". *Global Change, Peace & Security* 24 (1): 83–93. <https://doi.org/10.1080/14781158.2012.641278>.

Part IV

Covert operations



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

10 Ethics and covert action

The “Third Option” in American foreign policy

Loch Johnson

Covert action as an instrument of American foreign policy

Covert action (CA) has been defined by a former high-level practitioner as “influencing people, organizations, and events in other countries secretly, using a variety of inducements and pressures while attempting to conceal sponsorship” (Bissell, Pudlo, and Lewis 1996, 207). Put simply, this hidden approach to foreign policy consists of government attempts to shape events and conditions overseas through the use of propaganda, political and economic programmes, as well as paramilitary operations (PM “ops” or warlike activities).

The aspiration is to channel the currents of history in a direction favourable to the United States. Former Secretary of State Henry Kissinger stated the case for the Third Option: “We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot operate”.¹ Thus, the purpose of covert action is to give the world a secret nudge – or even a shove – in a pro-American direction. This chapter examines the range of covert actions adopted by the United States, and explores their pros -and cons.²

Covert action as a government process

With sensitivity to ethical implications, this section addresses the legal foundations of covert action in the United States, along with its decision-making procedures and degree of accountability.

The legal foundations

The United States has resorted to covert actions since the nation’s earliest days. President Thomas Jefferson, for example, ordered paramilitary operations (PM ops) against the Barbary Pirates (Wallace 1975). Not until enactment of the National Security Act of 1947, though, which created the modern American intelligence establishment, did covert action have a formal, legal underpinning. That landmark law provided boilerplate language for the newly minted Central Intelligence Agency (CIA, known by insiders as “the Agency”) that allowed it to engage

not only in intelligence collection and analysis, its main charge, but to pursue as well “such other functions and duties related to intelligence affecting the national security as the President or National Security Council may direct”.

The Truman Administration turned to this spongy wording (supplemented by executive orders) for authority to launch a series of covert actions around the world, crafted mainly to shore up Western defences against a perceived rising Soviet threat. Since the CIA enjoyed access to unvouchered funds as a result of its sensitive activities, the agency became all the more attractive as an organization to carry out clandestine operations beyond the prying eyes of Washington’s media corps and inquisitive lawmakers (US Department of State 2019, 35).

In 1974, as the CIA was in the throes of controversy over domestic spying and the agency’s secret manipulation of elections in Chile (as directed by the Nixon White House), the government finally addressed the subject of covert action specifically in a statute. The Hughes-Ryan Act, passed in the waning days of that year, still lacked a robust definition of covert action; nevertheless, the new law was revolutionary in its reach. Henceforth, the CIA (or any other organization assigned a CA task) had to seek formal White House authority, with the president required to “find” that a proposed covert action was important to the nation and should proceed – a so-called findings process. Gone were the days of “plausible deniability” when the nation’s chief executive could claim ignorance about a CA endeavour that became public and proved embarrassing. More sweeping still, the president was required to report all CA approvals to the appropriate oversight committees in Congress. Suddenly, dramatically, lawmakers were now in the loop for the Third Option. The Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) would now receive regular briefings on presidential findings within two days of their approval by the president.

Lawmakers further tightened the legal screws on covert action six years later with passage of the Intelligence Oversight Act of 1980. In another revolutionary move, this law mandated *prior notice* to SSCI and HPSCI on all covert actions approved by the president. No more two-day delays were allowed, as had been the case under Hughes-Ryan and which often made it too late for lawmakers to object. From now on, members of Congress had an opportunity to offer their critiques *before* operations were launched – perhaps managing to close the barnyard door (if necessary) before the CA horse had bolted out.

By virtue of this chance for genuine debate within the secure confines SSCI and HPSCI, lawmakers could skewer (if necessary) untoward proposals – even threaten budgetary retaliation should the executive branch ignore suggested modifications offered by the congressional Intelligence Committees. The 1980 statute did not expressly require legislative approval of covert actions; however, it did establish a setting that permitted lawmakers to weigh in. Congress holds the power of the purse; as a result, the opposition of SSCI and HPSCI members could not be taken lightly by the White House, whether the criticism was just verbal or followed by a formal (if technically non-binding) vote against a specific covert action.

Subsequently, in the aftermath of the Iran-*contra* scandal involving covert actions during the Reagan Administration (the 1980s), Congress at last placed into law a formal definition of the Third Option, by way of the Intelligence Oversight Act of 1991. This statute continues to stand as the current legal foundation for America's secret interventions abroad. The definition states that covert action is "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly". The name of the CA game was, in a word, *influence*. The law also emphasized that, in times of emergency, the president had to provide advanced reporting just to eight leading members of Congress, four in each party (the "Gang of Eight"). Within two days of a presidential finding, however, the full memberships of SSCI and HPSCI were supposed to be briefed – a rule not always honoured by the executive branch in recent years.

What ethical ramifications emerge from this set of intelligence laws³? An important aspect of such considerations in a democracy is the extent to which government officials and agencies act in a manner faithful to a nation's constitutional framework. From this point of view, an ethical evaluation of covert action carried out by the United States rests on one's interpretation of the Constitution. Almost all of America's leading legal authorities, along with most of its political scientists, understand this document to have established co-equal executive and legislative branches of government. "Ambition would be made to counter ambition" was the prescription advocated by James Madison, the leading drafter of the Constitution in 1787 (*Federalist Papers, No. 51*). The nation's founders gave to Congress, whose duties are outlined in Article I of the Constitution, strong authority to curb executive power, extending from a tight grip by lawmakers on spending authority to their right to authorize war – and even impeach and remove a sitting president from office.

From this vantage point, the intelligence laws in the modern era as they relate to covert action display a moral goodness; they establish, for the first time in world history, a muscular legislative branch able to monitor the nation's proposed secret interventions around the globe. However belatedly, the bedrock principles of representative democracy as expressed in the Constitution had been brought into the invisible side of America's government.

If, however, one believes that Article II of the Constitution, which addresses presidential authority, has a superior status over Article I, and that it grants unfettered authority to the White House when it comes to national security affairs, then the CA statutes enacted from 1974 to 1991 are morally bankrupt, because they hobble (so critics allege) the ability of a president to protect the United States from foreign threats and internal subversion. The congressional checks and balances in the sensitive domain of intelligence place (according to this pro-Article II perspective) an undue burden on the executive branch in its struggle against global terrorism and other dangers. The survival of democracy – the ultimate moral good – is held hostage to a perverted doctrine of "the separation of powers" in the federal government; giving Congress a role in domestic affairs, say,

agriculture or health care, is sensible, but certainly not when the very survival of the nation is at stake in a hostile and uncertain world. So goes the argument of Article II devotees.

This unrestrained pro-presidency point of view had been roundly rejected by drafters at the Constitutional Convention in 1787; and, in the modern era, it was crushed again by America's painful experiences from the mid-1960s to the mid-1970s with presidential excesses during the Vietnam War, the Watergate scandal and revelations of the CIA spying at home. James Madison, George Washington, Lord Acton, Justice Brandeis, J William Fulbright – the list goes on of those wise counsels over the years who understood the risks of power concentrated in the hands of the president.

In contrast, Richard Nixon, Henry Kissinger, Dick Cheney and legal scholar John Yoo, as well as Donald J Trump and his Attorney General William “Bill” Barr (to mention a few), rejected the notion that Madison's anti-power moral imperative lies at the heart of the American Republic.⁴ As a result, they contributed to the subversion of the most basic ethical principle that undergirds democracy: freedom from autocracy. They routinely stiff-armed a role for Congress in international affairs, as though the value of executive branch efficiency surpassed the need for congressional restraints on the possible abuse of power. They turned their backs on the central motivating goal of the constitutional founders: no more King George III's ruling over America – or any future tyrants.

The history of intelligence law and covert action is, from the perspective offered in this chapter, an impressive unfolding of measures designed to improve the chances that the United States will test and temper executive branch initiatives with at least some degree of debate within SSCI and HPSCI over proposed “special activities”. The disquieting alternative is to rely solely on only two elected officials, the president and vice president, along with CIA bureaucrats, to make these important judgements on behalf of the American people. That approach produced, among other examples, the Bay of Pigs fiasco in 1961; the dubious CIA assassination plots against foreign leaders in the 1960s; the domestic spy scandals revealed in the mid-1970s and the *Iran-contra* affair in the mid-1980s.

Decision-making for covert action

Statutes related to intelligence have attempted to “democratize” CA procedures in recent years, bringing lawmakers into the picture just as the founders broadly advocated at the Constitutional Convention. These efforts also display a moral goodness that allows basic democratic values to enter into the practice of choosing what covert actions, if any, the United States should pursue – primarily, a meaningful role for representatives of the people in Congress.

In the years leading up to the Hughes-Ryan Act in 1974, the democratic principles of representative government – the heart of moral goodness in an open society – had been largely abandoned when it came to intelligence matters. The spy power would be an exception to the normal, constitutional interactions between Congress and the executive in other policy domains. For example, the

Church Committee, which in 1975 investigated intelligence practices in America, reported that only 14% of covert actions carried out by the United States from 1961 to 1975 had been approved by the National Security Council (NSC) (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1976, 56–7).

On those occasions when the president and vice president were in the “witting circle”, rarely were members of Congress informed – including those who served on the small subcommittees in both chambers that dealt with CIA budgets. In post-Hughes-Ryan days, however, the moral foundations of CA decision-making have been more in harmony with the intent of the Constitution. A handful of senators and representatives, supported by expert aides, now review key intelligence initiatives. As the law has evolved since 1974 to strengthen democratic procedures – within the necessary limits of protecting legitimate national security secrets, which obviously prohibit debate in the full legislative chambers on delicate CIA activities – so have covert-action decisions become more open to legislative review (chiefly via SSCI and HPSCI) and, therefore, more ethically defensible in an open society.

Covert action and accountability

As with covert action innovations in US law and decision-making procedures, so, too, has intelligence accountability moved in a direction of a higher ethical standing, at least as that concept is defined in a democracy as supporting significant checks on unbridled executive power – in this case, secret power. With regard to CAs, their shaping and review have gone from the sole domain of bureaucratic specialists and their managers in the executive branch, with occasional course corrections from the White House, to serious question-and-answer sessions within the inner sanctums of SSCI and HPSCI on the merits of specific covert action findings authorized by the president.

As for the canard that CA as a policy option has been ruined by the new laws and procedures since Hughes-Ryan and the Church Committee, because lawmakers are unable to keep a secret and leak information about findings to the media, the evidence since the creation of SSCI and HPSCI simply does not support that claim – which is expressed mainly by those who long for a return to the “good old days” of Article II supremacy, when the CIA operated with minimal supervision even from the White House, let alone the Congress. Since the mid-1970s, almost all of the top intelligence leaders (DCIs, and after that office was abolished in 2004, Directors of the CIA or D/CIAs) have endorsed the new and more rigorous forms of intelligence accountability, with William J. Casey, architect of the *Iran-contra* affair, the exception.

The covert action process and democratic principles

Process, that is, the procedures established by the Constitution and law for decision-making and accountability, is the essence of democracy, because it determines

whether or not elected officials beyond the White House and the executive branch agencies are included in the determination of covert action policies. As Treverton has observed with respect to the Iran-*contra* scandal, in which lawmakers were completely bypassed by the Reagan White House in its pursuit of covert actions: “Excluding Congress also excluded one more ‘political scrub,’ one more source of advice about what range the American people would find acceptable” (Treverton 1990, 43). Ethical covert actions depend on an ethical CA process, based on honouring the shared-power prescripts of the Constitution.

Covert action in practice

In tandem with the question of CA process is the critical matter of practice: the actual implementation of the Third Option overseas. What kinds of covert actions have America embraced, how well have they succeeded and how have they stacked up ethically? An examination of these operational dimensions requires another set of criteria beyond, but related to, the democratic principles expressed in the Constitution. This chapter looks next at the scope of covert actions over the years; though in abbreviated form since space constraints prohibit a more exhaustive presentation. The guiding question is: to what degree have America’s CAs reflected a commitment to an ethical foreign policy?

From 1947 to 2020, the scope of US covert actions has been wide. They may be divided into four categories, according to their focus and methodology. By far the most extensively used form has been secret propaganda, or what the CIA refers to – in one of its more creative euphemisms – as “perception enhancement”.

CA as propaganda

In this approach, the CIA has disseminated around the globe what it calls “perspectives” on world affairs, that is, secret media insertions that shine a favourable light on the United States, while portraying its adversaries in dark tones. The messages have been, in most instances, placed into foreign media channels – newspapers, magazines, television and more recently social media – by CIA foreign agents known inside the agency as “media assets”.

Into hundreds of media outlets around the globe, the CIA pumped roughly 70 to 80 insertions per day during the Cold War (1947–1991). This approach seems to have helped in the *coups* against the leaders of Iran in 1953 and Guatemala in 1954, for instance; further, according to CIA officials, the agency assisted significantly in the aftermath of World War II in buttressing fledgling democracies across the latitudes against secret media assaults concocted by the Soviet Union – early examples of the internal manipulation in democratic societies for which Russia became infamous in the United States after its meddling in the 2016 and 2020 presidential elections (Roosevelt 1979; Wise and Ross 1964). In its efforts first to defeat, then when he was elected anyway (in a free and open contest during the 1970s), to topple the President of Chile, Salvador Allende, the CIA expended millions of dollars in propaganda operations.

The agency also ran its own radio stations in different parts of the world, such as Radio Free Europe, to propagate messages worldwide; and smuggled anti-communist books and magazines into Russia, Eastern Europe and other communist countries (Johnson 1989, 22–4). The CIA has gone so far as to encourage its copious media contacts inside the United States to write negative reviews and commentary about books critical of the agency, and positive evaluations of pro-CIA publications; or to attack investigating congressional committees – a disquieting illustration of how on occasion the Langley propaganda machine has been turned against an American audience in an attempt to marginalize critics (Wise 1976).

Recently, the CIA promulgated a steady drumbeat of favourable and similarly worded media coverage inside the United States on the subject of its torture practices against suspected terrorists in the wake of the 9/11 attacks. Current and former intelligence officers appeared up on multiple television and radio talk shows, as well as sending out choreographed emails and twitters, and giving speeches that tried to defend the agency’s “enhanced interrogation” methods (Johnson 2018, 201–2). Controversial, too, has been the dilemma of “blowback”, whereby CIA propaganda insertions abroad waft back in this media-compressed world to influence American citizens at home.

Political covert action

The CIA’s early efforts to thwart communist takeovers in countries around the globe included not just propaganda but also support to pro-Western (or at least independent) political organizations and individuals. British Intelligence – MI6 – has an expression that captures the attempts of spy agencies to influence political events abroad through the judicious dispersal of money: “King George’s cavalry”, a euphemism for “cold cash to the rescue” – a sure way to influence some people.

The CIA paid money secretly to advance its well-known 1953 and 1954 *coups* (Iran and Guatemala), and supported the Christian Democratic Party in Italy from 1948 throughout the 1960s in its electoral competitions against the Italian Communist Party (supported just as vigorously and secretly by Russian rubles dispensed by the KGB). Neither superpower thought it wise to make its cash interventions openly for fear that the Italian voters would balk at supporting candidates who seemed to be dancing on the strings of an outside power.

Should the United States pay brides to modern-day politicians in other countries, in return for their support of US global initiatives? Critics maintain that the United States would be considered more honourable around the world if, unlike Russia, it refused to use secret political operations – or any other form of covert action – against fellow democratic states. This is a rule already followed by Washington officials with respect to members of the “Five Eyes” intelligence alliance – the spy services of the United States, the United Kingdom, Australia, Canada and New Zealand. Should this principle be extended to all free nations?

Economic covert action

In the economic sphere CAs can become particularly nasty. They often skate across the boundary of ethical propriety, as with proposals to contaminate foreign food supplies; crop and livestock destruction; the incitement of labour strikes and mining harbours to discourage shipping, as well as blowing up electrical power lines and oil depots – favourite operations carried out in Nicaragua during the *contra* segment of the Iran-*contra* affair.

In addition, the CIA (and no doubt the KGB as well) has counterfeited foreign currency to trigger inflationary pressures in a target country; depressed the world price of certain agricultural products vital to the economies of adversary nations – especially devastating in one-crop economies; contaminated oil supplies; cultivated parasites that might be useful for the ruination of crops overseas; diluted pesticides bought in the international marketplace by nations hostile to the United States and attempted environmental alterations via cloud-seeding in the skies over enemy territory.

Here the negative moral implications scream out and such initiatives deserve severe condemnation, especially food, livestock and environmental tampering. As with all covert actions, the Golden Rule provides a North Star: do unto others as you would have them do unto you. Imagine posing the question to an American citizen: would you find any of these operations fair play if aimed at the United States? Few CAs would qualify for a “yes” answer.

Paramilitary operations

Within the realm of PM ops, one confronts the most dangerous, extreme and controversial forms of covert action. They are the responsibility of the CIA’s Special Operations Group (SOG), located in the Special Activities Division of the Directorate for Operations (DO). The SOG’s officers are recruited (“sheep-dipped”, in the odd phrase) from the US military for the most part. The activities they pursue can range from supplying weapons to allies overseas, such as Stinger missiles to the *mujahideen* in the agency’s 1980s struggle against a Soviet army occupying Afghanistan, to managing full-scale “covert” wars – as if anything large in scope could stay covert long. Journalists have amusingly labelled this latter phenomenon “overt-covert action”.

The most significant change in the conduct of paramilitary activities by the agency in recent years has been the adoption of drone attacks against suspected terrorists. Drones, such as the Predator and the Reaper, feature Hellfire missiles nestled beneath their wings that can quickly incinerate targets below, making this most lethal form of covert action in the CIA’s contemporary arsenal. First employed by the second Bush Administration, then (in higher numbers) by the Obama Administration, President Donald J. Trump further escalated their use. Each of these administrations turned to drone warfare not only on authorized battlefields, as in Iraq and Afghanistan, but also in such far-flung locales as Somalia, Yemen and the Maghreb. While some within the DO view the drone as the most

effective form of covert action yet devised, others – including an agency director, John Brennan, a former analyst – see this approach as a troubling departure from Langley’s basic mandate as an analytic organization, not a combat unit. Disturbing, too, has been the “collateral damage” caused by CIA drones, including members of a wedding party in Pakistan mistakenly identified as a terrorist gathering.

Another controversy revolves around whether suspected terrorists should be assassinated by drones, or merely identified by these aircraft for later capture on the ground by US Special Forces for trial in a court of law. One suspect targeted for death was an American citizen, Anwar al-Alaki, who left the United States for Yemen and became a popular radio personality spouting anti-American rhetoric – perhaps driven to radicalism by ham-handed FBI surveillance against him when he lived in the DC area working as a Muslim cleric (Shane 2015). Disputes have arisen, as well, over the target list generated in the Department of Justice (DoJ) and the White House, based on Intelligence Community and Department of Defense (DoD) recommendations. A couple of attorneys in the DoJ are reportedly assigned to establish the kill list, which the White House then approves or disapproves. Critics maintain that this decision is too important for such a limited form of review; as a supplement, they argue, there should be a warrant process (like those provided for national security wiretaps in the United States since 1978), accompanied by reporting to SSCI and HPSCI before the drones take flight on their deadly missions.

Finally, secret cyberwarfare has become a household word and common practice among nations. As Russian manipulation of US elections attests, its potential is unsettling, to say the least – not to mention the possibility of cyberattacks against America’s energy grid, stock exchange, hospitals, schools, air-traffic control and nuclear reactors. Quite properly the United States is ramping up its cyber-defenses – and, as a stand-by, its offenses as well.

CA practice as it relates to process and principles

Covert actions might be thought of as secret intelligence interventions that lie along a continuum marked by Red Zones at either end, like a football field, with most operations taking place on the green expanse between these zones.

The red zone of the ludicrous

One can envision a Red Zone on the south end of the field that encompasses proposed CA initiatives that can only be described as Vaudevillian in nature: so comical, were they not seriously proposed, as to require a quick dismissal by any official with an ounce of good sense. An example of a South Red Zone candidate was the CIA’s proposal to rid Cuba of Fidel Castro, in an operation known as “Elimination by Illumination”. The plan was to spread the word through media assets in Cuba and leaflets dropped over the island that the Second Coming of Christ – the arch anti-communist – was imminent and spelled the end of Fidel Castro, the anti-Christ in democracy’s passion play. An American submarine

would surface off the coast of Cuba and shoot star shells into the midnight skies: the manifestation of Christ's arrival. The people of Cuba would then supposedly rise up against Castro. When this idea was run by the Kennedy Administration at a meeting of the National Security Council (NSC), a chorus of snickers quickly quashed the madcap scheme.

Into this Are-You-Kidding Zone should have fallen, as well, such other CIA initiatives against Castro as sending him exploding cigars and sprinkling depilatory powder in his boots at night to make his charismatic beard drop out. Neither worked. Each of these proposals made it through the CA decision process, which in these instances did not involve formal NSC review – and certainly no legislative oversight.

The red zone of the extreme

At the other end of the CA “football field” – the North Red Zone – are a set of operations that are so repugnant and contrary to American values that they should be automatically denied as well. Here are the most extreme forms of covert action that, one would hope, the US officials would eschew reflexively on moral grounds.⁵ Hypothetically, one can envision these possibilities: using CA methods to disperse chemical and biological agents against a foreign adversary; bringing about major environmental alterations that would harm an enemy or engaging in significant economic dislocations incurred by crop and livestock destruction.

America has never engaged in such practices, although any nation with an advanced CA capability could and, on a couple of occasions at least, government planners in Washington proposed such measures during the Kennedy years. In one instance, the CIA considered undermining Cuban-Soviet relations by lacing sugar exported from Havana to Moscow with a bitter (though harmless) chemical substance, rendering it unpalatable. Discovering this initiative by way of a leak to the White House, a senior NSC aide intervened and had the 14,125 bags of sugar destroyed before they were shipped to the Soviet Union (Wicker et al. 1966).

Another scheme – more chilling – with the codename Operation Square Dance was the product of someone's fertile mind in the Department of Defense, trying to edge the military into the covert action game during the 1960s. This plan envisioned the destruction of the Cuban economy, and the resulting demise of Fidel Castro, by dropping from aircraft onto the island late at night batches of a parasite known as Bunga. This pest craves sugar cane, Cuba's main crop. The overheated DoD planner suggested further that the attack could be “exacerbated and exploited by such measures as spreading hoof-and-mouth disease among draft animals, controlling rainfall by cloud seeding, mining cane fields, burning cane, and directing other acts of conventional sabotage against the cane milling and transportation system”. An exasperated National Security Adviser (and former dean at Harvard University), McGeorge Bundy, rejected the proposal out of hand as beneath the dignity of any civilized nation (Johnson 2017, 92–3).

One does not have to be Immanuel Kant (“Do not evil, though the world shall parish”) to comprehend that some CA activities have no connection – even

remotely – to what the United States stands for. Extreme proposals of the North Red Zone variety ought to be readily recognized and dismissed out of hand.

The middle kingdom

In between the ludicrous and the extreme lie the bulk of CA initiatives. How useful have they been down through the years? Opinions on this question vary widely. On the side of scepticism is a proposal from national security expert Morton Halperin to ban covert actions altogether (Johnson 2019); and Senator Frank Church's lukewarm acceptance of the Third Option, but only in rare cases to thwart terrorists or help friends in narrow circumstances (such as preventing a communist takeover in Portugal in the 1980s) (Church 1976). At the other end of the spectrum, one can find unbridled support for this approach from DCI William J. Casey of the Reagan Administration, an architect of the Iran-*contra* affair, and academician Roy Godson (Godson 1981).

In between are those who accept the need for at least a CA standby capability, for use in emergencies; those who would endorse this means periodically – but only under certain conditions, including most importantly the presence of executive and legislative accountability; and those who recommend an embrace of every arrow in the foreign policy quiver, especially when the United States is at war against another country or a terrorist organization. Two of the most thoughtful policymakers who appeared before the Church Committee to testify on covert action, former Secretaries of Defense Clark Clifford and Cy Vance, argued in favour of retaining a CA capability, but strictly as a last resort when diplomacy had failed and fighting an overt war was too risky and expensive (Johnson 1985, 147–8).

Officers in the DO and their seventh-floor leaders at the agency often point with a special pride to a number of covert actions. High on this list are the CIA's successes soon after the Cold War began in thwarting communist party takeovers in Italy, Greece and Turkey, as well as nations in Asia, Latin America and Africa. Agency officers also view the Iran *coup* of 1954 and the Guatemala *coup* the next year as feathers in their caps. They then skip forwards – quickly over the Bay of Pigs paramilitary fiasco in 1961 – to the agency's secret war in Laos, which lasted from 1962 to 1968 (Prados 2006; Colby and Forbath 1978). In this instance, the CIA played an important role in keeping communist guerrillas preoccupied with civil war in that nation, rather than have them cross the border into South Vietnam and attack American troops.

Another highlight, from the vantage point of the front porch at Langley, Virginia (CIA Headquarters), was support for the *mujahideen* during the Reagan years, helping the Taliban repel the Soviet Army from Afghanistan. A high mark, too, was the agency's response in the wake of 9/11, when DO officers assisted the US military drive the Taliban out of power, after these erstwhile American allies turned against the United States and provided a safe haven for Osama bin Laden (OBL), the Al-Qaeda leader (Coll 2019). Most recent on the list of positive outcomes is the elimination of OBL in 2011, after a decade spent searching for him.

On the assassination front more generally, some at Langley view the capacity of drones to strike down future “9/11” perpetrators as a significant contribution to America’s safety. Some agencies have also found merit in the agency’s propaganda programmes as a way to counter the active disinformation machines of Russia, North Korea, Iran and other nations markedly hostile towards the United States.

Critics of the Third Option are quick to respond, though, that the Marshall Plan, the Truman Doctrine and the placement of American soldiers permanently in Europe and Japan were of much greater importance in thwarting communism worldwide than the Third Option, which played a part only at the margins. The Iran *coup*, they point out further, eventually led to an uprising against America’s puppet, the shah (king), along with a discrediting of the United States that lingers in Iran. Moreover, they argue, Guatemala has continued to endure extreme poverty in the years since the CIA intervened; Langley may have aided the United Fruit Company in its desire to extract bananas more cheaply from Guatemala, but did nothing to help the people of that desperately poor nation. As for Laos, when the PM operations ended in 1968, the agency’s local allies – the Hmung – were decimated by communist forces; and, though the *mujahideen* were successful against the Soviet Army in Afghanistan during the 1980s (thanks in part to CIA-provided Stinger missiles and other sophisticated arms), the Taliban soon turned against the United States and befriended Al-Qaeda as it planned the 9/11 attacks against the United States.

Even critics of covert action usually grant some merit to the agency’s role in routing the Taliban in Afghanistan after 9/11, but they point to bin Laden’s escape for a decade and, even more significantly, the Taliban’s ongoing military operations against the United States today in Afghanistan. On the death of bin Laden, most Americans were pleased about that joint military/CIA operation, although some would have preferred to see him captured and tried in court for his terrorist activities. Critics are generally critical of the agency’s drone programme, labeling it indiscriminate, highly unpopular abroad even with those in the Middle East who favour the United States and likely to result in drone retaliations directed against Americans and their homeland.

Joining a recent director of the CIA, John Brennan, in expressing dismay that the CIA has become a killing machine instead of focusing on its core mandate of intelligence collection-and-analysis is a key congressional overseer, Senator Angus King (I, Maine). He chastises the executive branch for being “the prosecutor, the judge, the jury, and the executioner all in one” when it comes to drone attacks – a development that he sees as “very contrary to the traditions and the laws of this country” (Greenberg 2016, 15). Finally, critics well remember the Bay of Pigs disaster, along with – the lowest point in the modern history of covert action – the deeply troubling abuse of the government’s secret powers during the Iran-*contra* affair (Byrne 2014).

Evaluating the merits and the ethics of covert action

On the positive side, covert action seems to have been useful in its PM forms as a supplement to overt US warfare (as in Korea and Vietnam), along with America’s

struggles against global terrorism. Also, the roll-back of the Taliban after 9/11 was a shining example of how the CIA and the military can work together in emergencies to defeat America's foes.

Less convincing has been the excessive use of drone assassinations, along with the periodic lack of coordination between CIA and DoD drone attacks. Critics make a strong case that, outside of an authorized battlefield, drone warfare should be prohibited altogether. So should assassinations. Despite these widespread reservations about murder-by-drone, in January of 2020, President Trump ordered the death of Qassem Soleimani while this high-ranking Iranian leader and head of the Islamic Revolutionary Guards Corps Quds Force was visiting in Iraq. This decision was an unfortunate use of a US Reaper drone, extending this method of killing to a government official and inviting similar retaliations against US officials by Tehran's secret agents. Outside of official battlefields, killing is *ipso facto* immoral – with the exceptions of immediate self-defence or the careful targeting of terrorist groups proven to have murdered US citizens.

This Trump-ordered hit invites an international free-for-all among state and non-state assassins, whether at the controls of a drone, wielding a poison-tipped umbrella, or wearing a suicide vest. The end result could be international chaos, with outcomes unlikely to benefit the United States – mainly a crumbling world order that would surely endanger America's own leaders. After all, government officials in the democracies live in fishbowls and are comparatively easy targets. As well, assassinations seldom achieve their ostensible goal of bringing peace to a region; and they mostly fail in execution, as the more than 30 plots by the CIA against Fidel Castro testify (Turner 2005).

As for covert actions overall, based on the historical record, one should be sceptical about any claim that the vast majority of such operations have protected and advanced America's global interests. Among the knowledgeable and thoughtful sceptics is former Director of National Intelligence (DNI) Admiral Dennis Blair, who has observed: "if we'd have done none of them we would probably be better off, and certainly no worse off than we are today" (Mazetti 2013, 80). One of the top leaders on the Church Committee, Senator Walter "Fritz" Mondale (D, Minnesota), concluded that past covert actions have been characterized by "high political costs and generally meager benefits" (Johnson 1985, 224). In brief, covert action has had occasional success and should be kept in reserve, but with the caveat that this method should be resorted to only in emergency situations, most notably as a PM supplement in times of authorized overt warfare or to stymie terrorist activities aimed at the United States and its allies.

While the future is too unpredictable to construct precise and binding rules in perpetuity regarding the proper use of these secret initiatives, some sensible rules of the road have emerged over the years as the United States gained experience in world affairs. A starting place is to acknowledge that PMs in support of authorized overt warfare make sense, as long as they stay out of the Red Zones. William H Webster, DCI from 1987–91, has offered additional benchmarks for deciding on the merits of a proposed covert action. As CIA chief, he demanded answers from

the DO to a series of thoughtful questions before he would approve a covert action (Johnson 2011, 281):

- is it legal (that is, does it follow the approval and reporting rules laid out by Hughes-Ryan and the Oversight laws of 1980 and 1991)?
- is it consistent with American foreign policy and, if not, why not?
- is it consistent with American values?
- if it becomes public, will it make sense to the American people – what is sometimes referred to as the *New York Times* test?

Most important, though, is the vital ingredient discussed at the beginning of this chapter: the pride of place that *process* must claim in any true democracy. The glory of an open society is debate, and the precious gift given to the American people by the founders was a system of government designed to require debate among the branches of government. Sole executive authority was anathema to their philosophy, and, indeed, to the wisest philosophers throughout history. Debate – held within the confines of the CIA (experts) and the NSC (elected officials and experts), along with the SSCI and HPSCI (elected officials and experts) – is the *sine quo non* for elevating the chances of foreign policy success while, at the same time, retaining a high moral standing in America’s use of the Third Option.

Further, the United States should always be mindful of a Fourth Option: leading by example – doing the right thing that others, at home and abroad, will respect and admire; acting with a dignity and patience befitting the world’s oldest and strongest democracy; staying within the white lines of law and propriety; keeping the high moral ground by pursuing a principled foreign policy. “If America has a service to perform in the world – and I believe it has”, observed the chairman of the Senate Foreign Relations Committee in the 1960s, J William Fulbright, D-Arkansas, “it is in large part the service of its own example”.⁶ Exploding cigars, poisoned dart guns, foreign crop and livestock destruction, mining distant harbours, the use of torture – these are not the kind of activities that America has valued since its founding. On the contrary, the United States is the nation that supported the Marshall Plan, that sends hospital ships around the world to aid the unwell, that responds to hurricane disasters wherever they may strike, that champions human rights in the international arena.

Two of America’s finest diplomats have reached similar conclusions. “When we mine harbors in Nicaragua, we fuzz the difference between ourselves and the Soviet Union”, lamented George Ball during the Cold War (Ball 1984, 37). “We act out of character, which no great power can do without diminishing itself”. More recently, a former US Ambassador to Mexico with 31 years of service at the Department of State, Roberta Jacobson rues the abandonment of the moral high ground that America once enjoyed. “The loss of those principles makes us ‘like everyone else’ in a world where ‘everyone does it’”, she concludes (Jacobson 2019), adding that this loss “makes us less safe, less prosperous, and less of an example”.

In contrast to these views, Mike Pompeo, a recent agency director who went on to become Secretary of State in the Trump Administration, recommended a rather different approach to world affairs. “The CIA, to be successful”, he advised, “must be aggressive, vicious, unforgiving, relentless” (Mogelson 2019, 43). He seemed to be channelling his hyper-realist predecessor at State, Henry Kissinger, who believed that morality is something best left for Sunday morning church gatherings, not for use as a guide in the Machiavellian world of international relations. In response to State Department officials who were advocating more US attention to global human rights, Secretary Kissinger reportedly observed, “The State Department is made up of people who have a vocation for the ministry. Because there were not enough churches for them, they went into the Department of State” (Rohter 2003, 7).

Which of these pathways should America follow? That question is for US citizens and their representatives in Washington to resolve. This chapter suggests, though, that the United States has much work ahead if it wishes to restore its moral leadership in the world, becoming again the beacon of hope and democracy that it once was during the early years of the Cold War. Adopting a more discriminating approach to covert action would be a worthy place to begin.

Notes

- 1 Remarks delivered by Kissinger on “Evening News”, *NBC Television Network*, January 13, 1978.
- 2 It would be easy, and entirely wrong, to misconstrue the remarks presented here as an attack on the CIA. Over a 100 agency officers have given their lives for the United States as paramilitary operatives and in other intelligence-related duties abroad. I admire and respect the service given to the nation by its intelligence officers; I am only trying here to evaluate objectively the merits of covert action as an arm of American foreign policy.
- 3 On the importance of morality in the conduct of intelligence activities, see Omand and Pythian, who write: “ethical issues should not be left to the intelligence community to assess alone within that secret world” (Omand and Pythian 2018, 198).
- 4 “Bill’s view on the separation of powers was not overlapping authority keeping all branches in check, but keeping the other branches neutralized, leaving a robust executive power to rule”, observes law professor Douglas Kmiec, who preceded Barr as head of the Office of Legal Counsel in the Department of Justice (Bazelon 2019, 4).
- 5 For a “ladder of escalation” of CAs, rising from modest to extreme proposals, see Johnson (1992).
- 6 112 *Cong. Rec.* 10808 (1966).

References

- Ball, George. 1984. “Should the CIA Fight Secret Wars?” *Harper’s*, September 1984, 34–44.
- Bazelon, Emily. 2019. “Who Is Bill Barr?” *The New York Times*, October 26. www.nytimes.com/interactive/2019/10/26/opinion/william-barr-trump.html.
- Bissell, Richard M., Frances T. Pudlo, and Jonathan E. Lewis. 1996. *Reflections of a Cold Warrior: From Yalta to the Bay of Pigs*. 1st edition. New Haven: Yale University Press.
- Byrne, Malcolm. 2014. *Iran-Contra: Reagan’s Scandal and the Unchecked Abuse of Presidential Power*. 1st edition. Lawrence, Kansas: University Press of Kansas.

- Church, Frank. 1976. "Covert Action: Swampland of American Foreign Policy". *Bulletin of the Atomic Scientists* 32 (2): 7–11. <https://doi.org/10.1080/00963402.1976.11455562>.
- Colby, William, and Peter Forbath. 1978. *Honorable Men: My Life in the CIA*. New York: Simon & Schuster.
- Coll, Steve. 2019. *Directorate S: The C.I.A. and America's Secret Wars in Afghanistan and Pakistan, 2001–2016*. New York: Penguin.
- Godson, Roy, ed. 1981. *Intelligence Requirements for the 1980's: Covert Action*. Washington, DC: National Strategy Information Center.
- Greenberg, Karen J. 2016. "Rethinking How We Try Terrorists". *The American Scholar*, June 6. <https://theamericanscholar.org/rethinking-how-we-try-terrorists/>.
- Jacobson, Roberta. 2019. "What Trump and Corruption Cost Us". *The New York Times*, October 14.
- Johnson, Boyd. 1992. "Executive Order 12,333: The Permissibility of an American Assassination of a Foreign Leader". *Cornell International Law Journal* 25 (2): 401–36.
- Johnson, Loch K. 1985. *A Season of Inquiry: The Senate Intelligence Investigation*. Lexington: University Press of Kentucky.
- . 1989. *America's Secret Power: C.I.A. in a Democratic Society*. 1st edition. New York: Oxford University Press Inc.
- . 2011. *The Threat on the Horizon: An Inside Account of America's Search for Security after the Cold War*. Oxford; New York: Oxford University Press.
- . 2017. *National Security Intelligence*. 2nd edition. Cambridge, UK ; Malden, MA: Polity.
- . 2018. *Spy Watching: Intelligence Accountability in the United States*. New York, NY: OUP USA.
- . 2019. "Witness Testimony from the Church Committee Hearings on Covert Action, 1975". *Intelligence and National Security* 34 (6): 899–913. <https://doi.org/10.1080/02684527.2019.1606884>.
- Mazzetti, Mark. 2013. *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth*. New York: Penguin Press.
- Mogelson, Luke. 2019. "The Shattered Afghan Dream of Peace". *The New Yorker*, October 28. www.newyorker.com/magazine/2019/10/28/the-shattered-afghan-dream-of-peace.
- Omand, David, and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Washington, DC: Georgetown University Press.
- Prados, John. 2006. *Safe for Democracy: The Secret Wars of the CIA*. Chicago: Ivan R. Dee, Publisher.
- Rohter, Larry. 2003. "Word for Word/Kissinger on Pinochet; The Human Rights Crowd Gives Realpolitik the Jitters". *The New York Times*, December 28. www.nytimes.com/2003/12/28/weekinreview/word-for-word-kissinger-pinochet-human-rights-crowd-gives-realpolitik-jitters.html.
- Roosevelt, Kermit. 1979. *Countercoup: The Struggle for the Control of Iran*. New York: McGraw-Hill.
- Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. 1976. "Final Report". 94–755. Washington, DC: US Government Printing Office. www.intelligence.senate.gov/sites/default/files/94755_II.pdf.
- Shane, Scott. 2015. *Objective Troy: A Terrorist, a President, and the Rise of the Drone*. New York: Tim Duggan Books.
- Treverton, Gregory F. 1990. "Intelligence: Welcome to the American Government". In *A Question of Balance: The President, The Congress and Foreign Policy*, edited by Thomas Mann, 70–108. Washington, DC: Brookings Institution Press.

- Turner, Stansfield. 2005. *Burn Before Reading: Presidents, CIA Directors, and Secret Intelligence*. New York: Hyperion.
- US Department of State. 2019. *Foreign Relations of the United States, 1977–1980, Volume XIX, South Asia*. Washington, DC: US Government Publishing Office. <https://history.state.gov/historicaldocuments/frus1977-80v19/comp1>.
- Wallace, Robert. 1975. “The Barbary Wars”. *The Smithsonian*, January 1975.
- Wicker, Tom, et al. 1966. “C.I.A. Operations: A Plot Scuttle”. *New York Times*, April 28.
- Wise, David. 1976. *The American Police State: The Government against the People*. New York: Random House USA Inc.
- Wise, David, and Thomas B. Ross. 1964. *The Invisible Government*. 1st edition. New York: Random House.

11 Jus ad vim

War, peace and the ethical status of the in-between

Nicholas Melgaard and David Whetham

A good crisis

“Never let a good crisis go to waste” has been attributed to different political leaders at different times, in different political circumstances. The difficulty in crediting this aphorism is probably evidence of its near universal applicability. Opportunistic coercive activity that falls through the cracks between war and peace, is the subject of this chapter. Political actors can use significant events within or between countries to circumvent normal barriers. While attention is focused on a major issue elsewhere, it creates opportunities for action in areas that would normally have a much higher transaction cost for getting involved. The world looks left; some cunning political actor moves right.

The COVID-19 pandemic has been one such unwasted crisis. Russia and possibly China seem to have done just this with the recent coronavirus pandemic.¹ Reports quickly spread of the large-scale, coordinated state-supported effort to amplify division, spread misinformation, undermine trust in national and international responses (Rankin 2020). A campaign began by simply amplifying the disinformation that an open society was perfectly capable of creating itself. But this was then developed into a focused attempt to hack the labs creating a vaccine for information about its storage and distribution protocols (Corera 2020). The direct goal might not have been the loss of life. Still, the entirely predictable effect of such actions will be the undermining of public confidence in a necessary health initiative. The indirect result could certainly be an increase in deaths.

Oscar Jonsson (2019) argues convincingly that the Russian government sees war and peace not as binary states but as a spectrum, with information warfare now being capable of achieving political goals commensurate with war (Jonsson 2019). With this in mind, Gary Corn (2020) discusses in a recent article how Russia hates to waste a crisis (Corn 2020). He summarises, “Information operations are a key component of Russia’s strategy for confronting Western democracies, and covert deception and disinformation form the core of its active campaigns”. Yet another modern actor to whom our ancient aphorism could credibly be credited.

The sowing of controlled chaos, promotion of dissension and disorder: these are not incidental effects, but rather consciously deployed instruments aimed at the weakening of trust within society and the undermining of its domestic institutions.

They target the faith and confidence between societies, and the international institutions that have supported the cooperation that has underpinned the flourishing of the West since the end of World War II. Russia's actions aren't about defeating the West. The intention is to weaken it and level the playing field. Perhaps then, Global Russia will be able to reassert itself.

An important question then arises. Brutal as it is, we have an appropriate ethical framework for dealing with the traditional means of warfare. The just war tradition, a constantly evolving body of thought seeking to enable structured ethical discussion at the very extremes of human behaviour, has been developing since antiquity. But we have next to no specific ethical framework to deal with this other kind of subversive political activity. What rules should govern a response to dishonest coercive opportunism? In this case, we might ask what level of sub-war threshold political activity we are willing to find "acceptable", or at least, what do we recognize as falling short of an "armed attack", permitting us to cross the threshold into war ourselves as a response? If not war, what is the appropriate response to information- and communication-based threats? What are we morally permitted actually to do?

Why does it matter?

It would be a mistake to consider the Just War a purely Western Tradition. Still, in the form it is most often framed, it is a synthesis of classical Greco-Roman and later Christian values (Johnson 1981). It also embraces a way of thinking that results in a "common language for discussing and debating the rights and wrongs of conflict" (Whetham 2010, 65). The just war tradition provides guidance on what is acceptable, and (most importantly) not acceptable, even in times of war. It states that there should be limits on when the use of force can be considered legitimate (the *jus ad bellum*), and that there should also be limits on what and whom that force can be directed against (the *jus in bello*).

Fundamentally, this way of thinking assumes that there is a difference between the situation of war and the situation of peace. This is very important to the present discussion. The "declaration by a legitimate authority" is considered so important, not just because of the need to ensure one has the right to wage war, but the declaration element signifies a political community's move from one understanding of context to another. The new context permits one to do things that one would otherwise not be allowed to do. This includes, of course, the deliberate taking of human life as an extension of the idea of collective self-defence. This is the apex of ethical discussion in armed conflict; the reason why some things are allowed in war that would be unthinkable in peace. The *ad bellum* determination means that such acts can be engaged with on behalf of one's community. The fact that plans to do this can be premeditated and formulated in advance shows the difference between this and the peace-time actions of a police officer responding to a call out and forced to draw their weapon when the bank robber turns out to be armed. One might be permitted to arrest someone in peacetime, but one is not supposed to set

out with the intention of killing them before one even leaves the police station. Not so in war.

At least the police officer knows the context she is operating in. In the same way, military staff officers planning a military operation are generally clear whether their planning assumptions are based in the context of an international armed conflict, non-international armed conflict or some kind of peace support mission in which the use of lethal force is still generally considered as an available option. But where do state-sponsored hostile information operations that can result in indirect harm, or even death, sit in this understanding? Robert Gates, US Secretary of Defense, describes (2009) this ambiguity very unambiguously: “the categories of warfare are blurring and no longer fit into neat, tidy boxes” (Gates 2009).

So what are our options? As much as we would like to see “the West” as ethically principled, this is naturally an area in which our own state wishes to act as well. Of course, it must do, and not only in a purely defensive role. The fact that such measures are technically “non-violent” and less immediately risky than “boots on the ground” must count towards their attractiveness.

The first option is that we can choose to apply the exceptional permissions afforded by a state of war by acting as if we are in a state of constant conflict, with everything that goes along with this. The second is that we can limit our responses to the peacetime model of permissible action and address the threats as criminal activities rather than as acts of war.² This latter response has some credibility, at least in terms of providing a clear framework to the problem. One should expect the police to deal with such threats, gather evidence and hand it over to the prosecutors to make the decision to charge in a court or not. In the case of actors not based in the same territory where harmful actions have taken place (where a domestic court is not suitable), issues are raised through diplomatic channels and demands made for the relevant jurisdiction to prosecute those responsible. In the case of disinformation, this could either be dealt with as an “incitement to xxx” type charge, or perhaps as a civil defamation case, dealt with through the civil courts (with the risk of damages being payable if the issue is found to be proved on the balance of probabilities).³ Of course, this sort of thing takes a great deal of time. The results may simply be ignored. Or foreign jurisdictions able to act might simply decide not to.⁴ It might then be up to the politicians to choose what to do through diplomatic channels, with powerful states being able to mobilize international public opinion in the form of collective political or economic sanctions. Or they may not. What is certain is that while it is possible that something on this range of actions might conceivably act as a deterrent to the behaviour occurring in the first place, being unable to respond in kind, or even threaten to do so because one would be breaking the same laws, makes deterrence lack a large element of its necessary credibility.

Countering such behaviour within one’s own peacetime rules will possibly therefore be inadequate. Peacetime laws are supposed to protect people from harm, not give them permission to harm others. Special permissions are needed to allow harm to be inflicted. Self-defence can justify inadvertently hurting a mugger

who is assaulting an old lady, for example. But extending the idea of self-defence to permit such activity in a third-party state is effectively moving the framework of understanding from the individual-based rights and permissions of peacetime, to the collective self-defence ideas inherent in wartime.

To see such behaviours as causing harms commensurate with armed conflict, thus warranting a war-like response, certainly carries with it a better chance of deterrence. But is it really war? Thomas Rid (2012) prefers to see this kind of “sub-war” activity as “neither crime nor war, but rather in the same category as subversion, spying or sabotage, existing somewhere on the spectrum between apolitical crime at one end and genuine war at the other” (Rid 2012, 7). This seems to echo the understanding (or at least practice) of the Russian state. If the traditional binary – war versus peace – conception is no longer appropriate, and one chooses to try and understand contemporary conflict as more like a spectrum of activity, how does this help us answer the question regarding what we are actually morally permitted to do on this spectrum?

Jus ad vim

There is a view that the “consensus behind just war theory is slowly beginning to wane and the relevance of the theory gradually eroding”. Jai Galliot (2019) comments that due in part to the changing means of political control, many “have begun to find that there is a limit to the extent to which the traditional principles and usual rules of war found in just war theory . . . can be stretched to cover modern conflict”. Such a range of conflicts includes the very different environments of Vietnam, Afghanistan, Iraq, Libya and Syria. Galliot focuses on a discussion of “kinetic” (violent) force in periods of ill-defined, fluid armed conflict, yet the idea is the same for political, information-based action. Such cases, Galliot observes “tend to focus on individual rather than categories of people and involve the employment of emerging military technologies”, they are “somewhat resistant to moral evaluation within the state-centric framework of the traditional just war theory” (Galliot 2019, 3–4). When the subject of power becomes so individualized, the traditional context-based justification of wartime behaviour becomes very difficult to sustain.

Still, the reasons why such ideas of *jus ad vim* have taken hold are not difficult to understand. According to Brunstetter and Braun in their highly influential paper in 2013 responding to the outlining of the idea by Michael Walzer, *jus ad vim* activity is just “nominally easier to justify”. *Ad vim* measures require less of a commitment from politicians and statesmen than measures that clearly fall above the war threshold, but still permit you to do more than in the domestic peacetime context (Brunstetter and Braun 2013, 88). It has been popular because there is a gap in the ethical market for clear and consistent scaffolding to provide structure to decision-making below the threshold of traditionally understood armed conflict, whether this is a raid, surgical strike, drone attack or subversive information campaign.

Rather than accepting that all legitimate warlike actions can be justified because one’s political community have determined that the *ad bellum* criteria have been

satisfied (i.e. one's state is now at war), *ad vim* requires that each specific non-peaceful act is assessed against the *ad bellum* criteria on its own merits. Does the specific act have a just cause related to an injury or harm received or threatened; does the individual or institution carrying out the act have sufficient authority and have they declared why they are responding in such a way; is it the real reason why one is seeking to act, that is does the actor have the appropriate intention; is the response proportionate to the injury suffered or threatened; will the action have a reasonable prospect of being successful and finally, has everything else that might work within the normal range of actions (domestic law, diplomatic sanctions etc.) already been attempted?

If these criteria can be met, the act itself may be permitted, but how is one to carry it out? If one were to accept this new category, the next natural step would be just applying the ethical framework for activity *in bello* to such sub-threshold behaviour. *In bello* rules already specify who and what may be made the object of attack and to what extent. While the spectrum of activity is potentially broad and can cover everything from kinetic attacks through to non-physical information operations aimed at shaping actions or perceptions, in theory at least, the same *in bello* rules could apply, supplementing the *ad bellum* principles so they are taken all together for each act. In that respect, "changing weapon systems does not change the moral demands on those operating the systems" (Skerker 2021). The rights of those being targeted, and those who will be affected even if not directly targeted, still need to be taken into account.

However, simply transferring the existing rules from a state of declared war is not as viable as it at first might sound. For example, Brunstetter and Braun (2013) argue that the principle of "last resort" simply does not make sense transferred from an *ad bellum* to an *ad vim* context because it is war itself that is the last resort rather than the type of behaviours that fit here – these are the steps that are being tried before the last resort of war itself (Brunstetter and Braun 2013, 97). They are also concerned that the principle of proportionality may inadvertently permit escalation – something that goes against the very reason why politicians may choose to act in this area in the first place. One of the attractions for operating in this area is precisely because the actions do not cross the war threshold or pitch one's country into a state of armed conflict. If this consideration is ignored, then action taken may very quickly escalate resulting in open hostilities (Brunstetter and Braun 2013, 98). The point for policy makers is to be able to act and respond in this area within an ethical framework that can guide appropriate behaviour, without resulting in the kind of large-scale harms that war almost inevitably involves.

Brunstetter and Braun ask, "what would a theory of *jus ad vim* that counters the shortcomings of the *jus ad bellum* framework in this context look like?" (Brunstetter and Braun 2013, 88). These revised principles for *jus ad vim* and *in bello* can also then be used for other "non-kinetic" means as well (Lupton 2019). Their solution is to "recalibrate" *jus ad bellum* criteria by adding a new principle, the probability of escalation. Their argument is that a similar set of rules should be employed in sub-threshold conflict, but with the addition that the

risk of escalation ought to be minimized. This is a completely understandable step to take. Given sub-threshold conflict remains outside the boundaries of all-out war, the potential for a crisis to develop is a key consideration, whereas this might cease to be relevant if and when a situation of all-out war has already been accepted. However, for the reasons that we set out in the following, we think this recalibration does not solve things in the way intended.

***Jus ad vim*, categories and shifting contexts**

Our first concern is that such an articulation is incomplete. Avoiding escalation alone surely does not imply moral equity. For example, if I am a vastly superior state, I could probably guarantee that the other weaker state I am bullying will be too fearful to retaliate, at least directly. Therefore, while there may be proxy actors or tools that can provide an element of deterrence, there may in fact be very little chance of escalation from their side. This surely does not mean that I am more justified in this behaviour.

More generally, the issue with Brunstetter and Braun's argument is that it implies that everything is ok so long as the situation does not escalate. They accept that escalation is not always a worse course of action, and increased coercion is not always immoral, but argue that ensuring that any *ad vim* action does not lead to the outbreak of war is "essential" (Brunstetter and Braun 2013, 99). We believe this represents fundamentally a frustrating aversion to confrontation for its own sake, and an unwillingness to accept that confrontation in one form or another might actually be more ethically viable than its alternatives. War is, after all, permitted as a last resort in the just war tradition only when the evil it is seeking to avert or turn back is genuinely considered to be worse than that of war itself. Without this acceptance that war may sometimes be (although admittedly rarely) the least-worse option, we see the "pacifism by other means" argument often levelled against modern revisionism apply in a similar way. If there is a starting prejudice against confrontation in any circumstances, then the inertia of any variation of Just War theory built on its foundations will always drag it towards pacifist inactivity. While attempting to prevent escalation may indeed be entirely appropriate, prudent and ethical in many or even most situations, when considering the importance of deterring harmful behaviours, to have a principle that prohibits acts that might lead to escalation seems the equivalent of publicly ruling out ground troops from a planned military intervention.⁵ An act that demonstrates a lack of resolve and signals a lack of willingness to back up one's actions with the necessary commitment to be able to see it through is likely to be shrugged off by any opponent who is willing to bear the stated limited costs one is willing to impose.

We believe that this problem comes from seeing *jus ad vim* as an attempt to provide a new category of moral decision-making in the ambiguous murky world that sits below the threshold of all-out war, but above peace. We use the terms "below", "above", "threshold", "phase" to talk about these forms of war. But we might just as easily use "outside" or similar, as the principle is that these cases do not share

the agreed upon context of being in a state of war. The concept of *jus ad vim* suggests that measures such as surgical strikes, limited force, information campaigns and other forms of limited coercion fall into a third category. As such, they are subject to rules that are different to those that pertain in either peace or war.

Our issue with this is that it is trying to solve the difficulty of switching between categories by creating another category. For “category” we might also read “context”. The problem is not that the contexts or categories we use to judge certain behaviours have ceased to be “fit for purpose” (to use a military expression). The problem is our insistence on judging behaviour based on contexts and categories. Any such moral theory will be doomed to failure as real world circumstances inevitably develop. Indeed, our reluctance to accept a new threshold as a solution to tired and irrelevant old thresholds is in large part due to why such measures are so frequently employed. It is precisely because they fall outside the recognized social conditions of “war” that surgical strikes, or COVID-related misinformation for that matter, have become so popular. A whole set of expectations and legal parameters exist on either side of this line. Valerie Morkevicius and Danielle Lupton (2019) comment that: “one reason just war principles may be subject to political abuse is that the concept of war itself is treated as a binary concept by contemporary just war thinkers” (Lupton 2019, 36). As Jonsson argues earlier, the challenge that we are faced with today is that our competitors do not recognize that line, or have deliberately circumvented where we have chosen to draw our own lines. New categories will simply inspire a new wave of the same kind of creative categorization that got us to this discussion in the first place.

Rephrasing the challenge

The alternative to drawing category distinctions is to accept that contemporary conflict can be better understood as a spectrum. Along with Rid (above), and apparently, conforming with “the Russian way of war”, Morkevicius and Lupton find that “the insights from the field of international relations make it clear that war, as it is traditionally understood, is actually a location on a broader continuum of political violence” (Lupton 2019, 52). This would suggest that a sliding scale of what you are permitted to do along a spectrum would be more useful for determining the appropriate ethical guidance (Garraway 2008).

The Just War framework “is about exceptions”, providing a structure for figuring out when you can do things you are not otherwise allowed to do.⁶ The “exceptions” of wartime behaviour are justified by reference to a change in context: between war and peace. When one’s political community determines that this status has changed, it means that previously prohibited acts can now be entertained. The declaration of war is a community’s articulation and recognition of a new and exceptional context. As such it is a social construct rather than an objective point that can be definitely observed.⁷

But as we have already seen, its principles are useful beyond this very specific context as well. When applied to situations where the political community has not accepted the change from peace to war, the *ad bellum* rules remain useful for

determining when exceptions can be made, and if they can, the *in bello* rules can still guide us into what we may do, or how far it is permissible to go. Do they need any help? We have already rejected the anti-escalation consideration earlier. Is that because we believe the combination of the two sets of criteria are genuinely sufficient on their own? We think that this may indeed be the case. Given the extremely long pedigree of the testing of those criteria, and the way they embrace a combination of absolute deontological requirements, while demanding considerations of both consequential and prudential factors, we believe it may simply be a matter of emphasis rather than the creation of new criteria.

Rather than being a “state-centric framework”, no longer appropriate for an age of non-state and sub-state actors (Galliot 2019, 3–4), we would argue that the just war tradition predates the modern, state-based system by some two thousand years.⁸ Its criteria have evolved over that time and have been applied to the wars of nation-states just as they were applied to the conflicts of city states, principedoms and empires in the middle ages.⁹ While the way we need to apply them must adapt to the changing character of war, we hold that the overlapping criteria remain remarkably robust for determining when an exception may be made in many different situations, not just war.

The greatest challenge is not the criteria themselves, but that they have evolved over several millennia to give us a framework for determining these exceptions and in the process been given the collective title of “the just war tradition”. But that does not mean that the criteria are only useful in that context – the same types of reasoning can be applied to any situation in which one is seeking to do something normally prohibited. It could therefore be usefully thought of as a “Just Exception Tradition”.

Take for example a “citizen’s arrest”. Normally, one cannot hold another person against their will, but there are certain exceptional instances where one can reasonably curtail someone’s liberty. In the United Kingdom, detaining someone against their will is itself a criminal offence, but the right to do this has been in common law for centuries under certain circumstances.¹⁰ While we are less interested in the legal articulation, the key thing here is the ethical principles that underpin this long understanding of when it is permissible (but never required) to break one rule in order to uphold another. There is a seriousness threshold that must be considered (just cause leading to delegated authority to act). You must also believe at the time (right intention) that it is not reasonably practicable for a police officer to perform this task (last resort), and that the action is genuinely necessary to prevent (reasonable prospect of success) a specific person (discrimination): causing physical injury to themselves or any other person; suffering physical injury; causing loss of or damage to property or making off before a constable can assume responsibility for them (macro proportionality).¹¹ Anyone attempting such an arrest must inform the subject why they are being held (declaration) and what they are suspected of (the just cause again). Obviously, one can’t use more force to do this than is considered reasonable in the circumstances (proportionality): “So, one can physically restrain a thief, but one cannot rape him; read his diary; or prevent him from voting” (Skerker 2021). One can find oneself in

serious trouble if the exceptional criteria are not met – for example, you could be found guilty of false imprisonment, and/or assault.

What are the contextual factors that need to be taken into account when seeking to defend the state and its citizens against hostile intervention? All of the Just War criteria overlap and must be considered as a whole rather than as an individual checklist, and while this is a subject that needs much further attention, here we look at two criteria in particular as they have already been discussed earlier – last resort and proportionality – as well as the role of discrimination and intention.

We think that, just as the other criteria need to be understood in context, the last resort criterion does still make sense even if one is not determining if the threshold to declare war has been crossed. War itself is the last resort when one is thinking about the former, but in this case, we are actually asking if there are any measures that don't require exceptions to be made that might work but haven't yet been tried. For example, Walzer prudently suggests that nonlethal policing actions, akin to what must be undertaken in zones of peace, should be prioritized first (Walzer 2007, 482). Only if these have not worked should the exception be made to permit the type of actions normally prohibited in peacetime. This is necessary precisely because the blanket permissions granted by a state of war do not exist.

While Brunstetter and Braun (and many others) are uncomfortable with the traditional criteria of proportionality, which can be seen as a “nebulous and indeterminate constraint” (Brunstetter and Braun 2013, 98), we think that it can still be extremely valuable. In war we know that what is at stake is a significant factor in determining what is justifiable. While some things remain forbidden regardless of context, there are some things that will change as the stakes get higher. For example, in a war of national survival, it may be permissible to cause more harm to those who have not made themselves liable to harm – that is non-combatants – as a foreseeable but undesired side effect of one's actions directed towards your state's survival, than if one were engaged in a very limited peace enforcement mission in which the aim is to get humanitarian assistance to those in desperate need. In such a situation, it would seem

inappropriate and even perverse to move the burden of risk on to that same population, accepting a high degree of collateral damage, for example, in an effort to minimize one's own casualties when the very purpose of being there is to protect those people who are now being put at additional risk.

(Whetham 2010, 83)

We agree with Brunstetter and Braun that, on the whole, discrimination must be applied in an even stricter sense than at the *ad bellum* level. But, this is to do with where on the conflict spectrum this activity is likely to be placed – what is at stake – rather than because it is happening in a different category of activity. Returning to the sliding scale/spectrum understanding of conflict mentioned earlier, this may require the sacrificing of individual rights to protect even more people, even if there is no declared state of war. For example, averting a nuclear

terrorist threat against a whole city might require some civilians to be put at risk of harm or even death. This may be true regardless of whether it takes place during declared hostilities or not. To prohibit the exception because the category is wrong is to fail the test of protecting one's people. As such, the spectrum is what is important, not the artificial category. This also has implications for the application of proportionality at the *in bello* level.

Finally, we agree with Brunstetter and Braun about the essential importance of intention. We think the emphasis here is of particular importance for the way that the *in bello* criteria of discrimination and proportionality are to be understood in this different context. We accept (as did the medieval scholars who debated these ideas 1000 years before us) that intention shapes the moral and physical quality of action, so there is a direct link between intention and the normal *in bello* criteria limiting who may be intentionally harmed and to what extent.¹² Right intention must be directed towards upholding the rights of the Other (Skerker 2021).

Directing an information attack against an agent of a hostile state causes no problems in wartime, and an exception can easily be justified if the stakes are sufficiently high outside of wartime. Creating a martyr by manipulating the social media of a regular civilian with no direct connection to the hostile acts being perpetrated by their state, in order to get that person arrested or killed (so their cause can be highlighted and used as a way to manipulate public opinion and ultimately change their government's policy) would be to go far beyond what was permitted. While one could perhaps justify the *in bello* considerations in terms of "it's not us doing the bad things to them – it's their state", this would be using the targeted person as simply a means to an end. One cannot escape moral responsibility by claiming that the result was foreseeable but unintended if the suffering is a required and intended part of the effect one is seeking.

In a broader sense though, right intention shapes more than the relationship with a specific target. Intentions do matter, and the idea of returning to the status quo ante bellum is very different from aspiring to return to something more positive. War must not be characterized as a return to anything. It seems almost impossible to make moral arguments if this is the case.

Our point in essence is that war and conflict must be justified as an activity towards an eventual improvement if it is to be justified at all. Simply restoring the ante-bellum conditions that led to the outbreak of war is a rather depressing justification for all the suffering and bloodshed it would involve. The belief that things cannot gradually get better is at once a belief in the inevitability of war, and at once a belief that we have no power to prevent it. The premise that war arises as an aggregate of human decision-making seems indisputable, however complex a social phenomenon the origins of a given war might be. The idea that we exercise choice to go to war, and can choose how we behave whilst fighting is surely the most basic premise of the just war tradition. Any form of moral discussion requires this. To claim that war is inevitable, but also concede that war is fundamentally a result of choices (and thus subject to moral discussion), is a totally incompatible pair of beliefs to hold. One must admit that a given conflict rests on human choices, we have some relevant moral agency, war is not inevitable, and

therefore things can indeed improve. Any moral decision-making in the context of conflict must at least acknowledge the possibility of things improving over time.

As such, just as acts of perfidy are prohibited because they undermine the essential faith in the rules themselves (Whetham 2009, 6), actions that destroy the foundations of knowledge or damage the long-term social cohesion even of a currently hostile state cannot be justified. It is impossible to see how this type of action, even if successful in undermining the will of an adversary, can actually lead to a better situation in the long run when the situation is viewed as a whole. In the same way, the just war tradition has long accepted that while it is acceptable to take the food or crops necessary for the subsistence of troops, it is never justified to destroy the means of making any more. For example, Deuteronomy (20:10, 19) forbids the destruction of fruit-bearing trees. “Condemning the civil population to starvation was hardly a way of promoting long-term reconciliation” (Whetham 2010, 69).

Conclusion

Let us return to the case of “sub-threshold behaviour”. We might ask whether act of political subversion, such as undermining another country’s COVID response, was indeed an act of war. The transmission of information was being deliberately obscured and undermined by an external actor. However, the question of whether this counted as an “act of war” merely serves to buy into an episodic, context-based set of justifications that are clearly not relevant anymore. It is not that there is a different and more satisfying answer to the question of when the balance tips over into a state of war, from a state of peace; the entire convention of justifying behaviour according to contexts and states is unviable.

Those who say this unacceptably blurs the distinction between war and peace are, unfortunately, disconnected from the current reality on the ground. One cannot simply lament that the reality doesn’t fit the socially constructed theory so, therefore, reality must change. It is up to a state or representative political community to determine if it is in a declared state of war or not, but the fact that harms can be deliberately committed against it without that state wishing to make such a declaration does not mean that it is only able to act using the tools of peacetime. Creating a new category between peace and war is one way of doing this, but for the reasons that we have set out earlier, we do not think this new category really solves the problem without creating new ones. Instead, we suggest that actions that go beyond the normally permitted may be justified as exceptions if they can satisfy the *ad bellum* and *in bello* reasoning we are already familiar with, with a special emphasis placed upon the intention criteria when considering the full ramifications of the proposed act.

In practice, our Just War position would focus less on consequentialist-based arguments aimed at working within one context or shifting to another. The value of declarations of war and victory parades in such cases serves to demarcate these shifts in context. Without them we are left with the *ad vim* problems mentioned earlier. Instead, the moral foundations of our position rest on a faith in the possibility of gradual progress towards peace. If this is not accepted as a possibility,

it becomes hard to have any moral discussion relating to armed conflict. Once this is taken as a foundational premise, individual actions are justified deontologically if they represent activity in the service of this progress.

When faced with political or information-based subversion, the discussion of whether this fits into the neat categories of war, peace or a third category is a moot point. Not even traditionally understood wartime behaviour fits into the neat categories of war and peace anymore. Nothing is solved or rescued simply by adding an intervening level. We might ask instead whether information-based attacks represent a credible source of harm, and whether they can be met with similar measures in response according to a framework within which deontological concerns based on an appreciation of human rights are respected. The answer to the first is “yes, absolutely”. To the second, “yes maybe”. Much more thinking is required in this area. While the reasoning inherent in the just war tradition may be a useful guide in a much wider range of situations than initially presumed, and can assist us with that necessary thinking, the discussion of *jus ad vim* must not be a discussion of how we continue to prop obsolete ideas up, but rather to assess the foundations upon which they are grounded.

Notes

- 1 For example, Rankin (2020) and The Soufan Centre (2020).
- 2 Of course this works both ways, and we would either have to limit our own responses to the area of legally permissible activity, ignore the rules ourselves or create some kind of legal fiction behind which we can hide – a move that makes taking the moral high ground rather awkward.
- 3 The balance of probabilities rather than beyond reasonable doubt is the bar in civil cases, at least in the UK.
- 4 We can't help thinking about the South African diplomats in *Lethal Weapon*, invoking “diplomatic immunity” each time they are about to be apprehended.
- 5 We are thinking of Kosovo in 1999 here, but there are other supposedly straightforward conflicts that were hampered by early declarations of red lines for domestic audiences that signalled limited commitment to adversaries at the same time.
- 6 A similar argument is made by Lucas (2015).
- 7 We accept that there may be situations in which a political community or state is objectively being attacked, such as when it has been subject to a surprise nuclear strike, even when it does not know from where the attack has come. This raises an interesting situation in which a state might be at war, but not sure whom it is at war with. See Whetham (2016).
- 8 If one takes that starting position to be the familiar 1648 Treaty of Westphalia.
- 9 See Whetham (2009).
- 10 The current laws are set out in Section 24A of the Police and Criminal Evidence (PACE) Act 1984.
- 11 In the UK, such an offence needs to be of a seriousness that carries a potential prison sentence of over 6 months imprisonment.
- 12 See Chapter 2 of Whetham (2009).

References

- Brunstetter, Daniel, and Megan Braun. 2013. “From Jus ad Bellum to Jus ad Vim: Recalibrating Our Understanding of the Moral Use of Force”. *Ethics & International Affairs* 27 (1).

- Corera, Gordon. 2020. "Coronavirus: Hackers Targeted Covid Vaccine Supply 'Cold Chain'". *BBC*, December 3. Accessed February 1, 2021. www.bbc.co.uk/news/technology-55165552.
- Corn, Gary. 2020. "Coronavirus Disinformation and the Need for States to Shore Up International Law". *Lawfare*, February 4. Accessed February 2, 2021. www.lawfareblog.com/coronavirus-disinformation-and-need-states-shore-international-law.
- Galliot, Jai. 2019. *Force Short of War in Modern Conflict*. Edinburgh: Edinburgh University Press.
- Garraway, Charles. 2008. "The Relevance of Jus Post Bellum: A Practitioner's Perspective". In *Jus Post Bellum: Towards a Law of Transition From Conflict to Peace*, edited by Carsten Stahn and Jaan K. Kelffner. The Hague: Asser Press.
- Gates, Robert M. 2009. "A Balanced Strategy: Reprogramming the Pentagon for a New Age". *Foreign Affairs*, January/February. Accessed February 1, 2021. www.foreignaffairs.com/articles/united-states/2009-01-01/balanced-strategy.
- Johnson, James T. 1981. *The Just War Tradition and the Restraint of War*. Princeton: Princeton University Press.
- Jonsson, Oscar. 2019. *The Russian Understanding of War: Blurring the Lines between War and Peace*. Washington, DC: Georgetown University Press.
- Lucas, George R., and David Whetham. 2015. "The Relevance of the Just War Tradition to Cyber Warfare". In *Cyber Warfare: A Multidisciplinary Analysis*, edited by James Green. Abingdon: Routledge.
- Lupton, Danielle, and Valerie Morkevicius. 2019. "The Fog of War: Violence, Coercion and Jus ad Vim". In *Jus Ad Vim*, edited by Jai Galliot. Edinburgh: Edinburgh University Press.
- Rankin, Jennifer. 2020. "Russian Media Spreading COVID Disinformation". *The Guardian*, March 18. Accessed February 1, 2021. www.theguardian.com/world/2020/mar/18/russian-media-spreading-covid-19-disinformation.
- Rid, Thomas. 2012. "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35 (1).
- Skerker, Michael. 2021. "The Rights of Foreign Targets in Cyber Operations". In *Cyber Warfare Ethics: A Handbook for Military Professionals*, edited by Michael Skerker and David Whetham. Havant: Howgate.
- The Soufan Centre. 2020. "Russia Exploits Coronavirus as New Opportunity to Spread Disinformation". Accessed February 2, 2021. <https://thesoufancenter.org/intelbrief-russia-exploits-coronavirus-as-new-opportunity-to-spread-disinformation/>.
- Walzer, Michael. 2007. "On Fighting Terrorism Justly". *International Relations* 21.
- Whetham, David. 2009. *Just Wars and Moral Victories: Surprise, Deception and the Normative Framework of European War in the Later Middle Ages*. Leiden: Brill.
- . 2010. "The Just War Tradition: A Pragmatic Compromise". In *Ethics, Law and Military Operations*, edited by David Whetham. Basingstoke: Palgrave Macmillan.
- . 2016. "'Are We Fighting Yet?' Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War?". *The Monist* (99).

Part V

Accountability



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

12 Reaching the inflection point

The Hughes-Ryan Amendment and intelligence oversight

Genevieve Lester and Frank Leith Jones

Introduction

Public acceptance of intelligence operations in a democracy requires trust in the government, including an acknowledgement of the government's right to withhold information from the public. Such trust requires at least some mechanism for oversight of such operations to ensure democratic accountability. The development of intelligence oversight in the United States has been driven by the executive-legislative relationship. The Hughes-Ryan Amendment to the Foreign Assistance Act of 1974 marked a distinct change in the conduct of intelligence oversight in the United States. The amendment affected foreign policy, covert action and presidential plausible deniability. It was the first sign the relationship between the executive and legislative branches was about to undergo a significant change regarding intelligence.

Public acceptance of intelligence operations in a democracy requires trust in the government, including an acknowledgement of the government's right to withhold information from the public. The constitution explicitly laid the groundwork for executive-legislative cooperation and competition in the area of foreign policy, but the relationship between the two branches regarding intelligence has developed largely in response to a changing threat environment and lawmakers' decisions regarding their oversight responsibilities. These two factors have created a state of tension, as the executive has ultimate control over the intelligence function, but Congress asserts oversight authority authorized through its constitutional prerogatives, and by the will of the public in bestowing its trust in their elected officials.

While scholars argue that there was some intelligence oversight in the early Cold War, it is generally held that prior to the Hughes-Ryan Amendment, oversight was a grudging responsibility (Barrett 2005; Marshall 2003). In the words of Senator Leverett Saltonstall, "The difficulty in connection with asking questions and obtaining information is that we might obtain information which I personally would rather not have, unless it was essential for me as a Member of Congress to

The views expressed in this chapter are those of the authors and do not necessarily reflect those of the US Army War College, the US Army or Department of Defense.

DOI: 10.4324/9781003164197-18

have it” (Stuart 2008, 271). Or in the self-exculpatory words of Director of Central Intelligence (DCI) William Colby in 1976:

The old tradition was that you don’t ask. It was a consensus that intelligence was apart from the rules . . . that was the reason we did step over the line in a few cases, largely because no one was watching. No one was there to say, ‘Don’t do that’.

(Johnson 2018, 104)

Some literature on intelligence oversight implies that the public, acting in response to the abuses described on the front page of the *New York Times*, catalysed the passage of Hughes-Ryan. This chapter, however, points to a series of congressional inflection points to explain why this amendment – the first serious intrusion on executive authority over covert action – took place when it did. It describes the political context of the amendment, how and why it was introduced and passed when it was, and then what the outcome was of this legislation, which challenged the concept of plausible deniability. It also explains why the shift that occurred, while definitive, was limited in scope, and introduces an analytical framework to help clarify how congressional activity can impact intelligence operations, an almost purely executive branch function.

Analytical framework

This chapter integrates three strands to offer a more robust way of understanding the passage of Hughes-Ryan. The first strand is the oppositional relationship of institutional development, whereby friction between the executive and legislative branches of government leads to institutional development (Lester 2015).¹ As Whittington and Carpenter argue: “[S]ustained conflict between legislative and executive actors lies at the center of institutional change in American political development” (Whittington and Carpenter 2003, 509). This conflict had already begun well before the Hughes-Ryan Amendment as Congress began to reassert its role in US foreign policy in the aftermath of the Vietnam War.

A second strand considers congressional behaviour regarding foreign policy, particularly after direct US involvement in the Vietnam War ended in 1973 and the foreign policy consensus that had existed since the beginning of the Cold War began to erode (Scott and Carter 2002, 153, 156). In 1974, that erosion was not yet evident because the full revelation of CIA abuses had not come to light. At that point, a less assertive Congress was still in play on foreign policy issues. Congress was “cooperating with the president to achieve foreign policy goals over which there is substantial consensus”, namely, countering the threat of communist expansionism (Scott and Carter 2002, 164, 165). The communist threat in the Western hemisphere was particularly worrisome to Congress and the executive branch since the Castro regime had seized control of Cuba. The election of Salvador Allende, a socialist backed by a coalition of left-wing political parties in Chile, was the precipitating event for US action to bring down

his government through a successful coup in September 1973, led by General Augusto Pinochet.

A third strand investigates what slows the process of institutional change. In the case of change in Congress, process and rules, as well as powerful individuals whose interests align with the status quo can and are incentivized to act to obstruct change. “The institutional drag hypothesis” posits that “institutions through their inertia and rigidity retard” change or structural innovation, but there are other related factors, such as the seniority system, where “loyalty to the congressional institution is *the* [emphasis in the original] necessary leadership trait” (Meeus and Oerlemans 2005, 64). As one commentator noted regarding Congress,

For generations, the House was a secretive, hierarchical, tradition-bound institution that gave little regard or influence to newcomers. Power was concentrated so assiduously in the handful of committee chairs that even the elected leadership hesitated to challenge the old men with the gavel.

(Lawrence 2018)

In this chapter’s discussion of the passage of the Hughes-Ryan Amendment, the three strands of the framework explain how, when and why the amendment passed. Individual action occurred within the context of inter-branch friction, which both supports and inhibits development. We see policy entrepreneurs acting within this context with the intention of advancing their agendas, while both institutional drag and the behavioural norms tied to maintenance of the status quo slow change. Ultimately, against the odds, progressive activity was successful. While the Hughes-Ryan Amendment was rather small in scope, it had an outsized impact on oversight, laying the foundation for the later development and institutionalization of intelligence oversight.

US policy and Chile

In March 1972, columnist Jack Anderson uncovered information about communications between the Nixon administration and the International Telephone and Telegraph Corporation (IT&T) regarding the company’s interest in financially supporting potential attempts to prevent the inauguration of the democratically elected Chilean president, Salvador Allende. Anderson claimed he had documents that showed the CIA planned to disrupt the Chilean economy to the point where a military coup would occur (New York Times 1972).

In response, the Senate formed a subcommittee in May 1972 to determine whether there had been an attempt to plot Allende’s downfall, questioning whether CIA had been involved and focusing on the broader issue of how multinational corporations may have sought to influence US foreign policy generally. The CIA attempted to have the issue of IT&T’s involvement transferred to the Senate’s Armed Services Committee, where it believed the issue would be protected from scrutiny (Subcommittee on Multinational Corporations 1973, 193). In September 1973, after the Chilean military had overthrown the Allende government, Senator

Edward Kennedy (D-MA), joined by Senator James Abourezk (D-SD), pushed for constraints on US support to the government of General Augusto Pinochet. They asked for a resolution denying Chile foreign aid, and requested that hearings be held regarding the junta's known human rights abuses (Johnson 2005, 197). Rumours began to circulate in the US and international press that the CIA had been involved in the coup (Time 1973, 38, 45, 46; Paterson 1987). With the Nixon administration under fire over the Watergate scandal, the balance of power between the two branches was shifting in favour of Congress, particularly to the liberal members who launched what was referred to as an "oversight revolution" (Paterson 1987, 161).

On April 22, 1974, Congressman Lucien Nedzi (D-MI), chairman of the House Armed Services Committee's Special Subcommittee on Intelligence, held a closed session on US covert operations in Chile with DCI Colby, testifying. Colby informed Nedzi and the Armed Services Committee's chief counsel, the only other person present, about the political actions that the CIA had taken against the socialist government of late President Allende. Off the record, Colby informed Nedzi that CIA involvement comprised other activities, including plans to help foment a coup. Colby, however, assured Nedzi that the CIA had nothing to do with the September 1973 military coup that brought down the Allende government and led to the leader's death. The CIA's plans for a coup had ended when the Chilean military opposed it. Further, Colby informed Nedzi that his testimony was available to all subcommittee members if they were interested in reviewing it. Nedzi made it known confidentially that the transcript would be made available to any member of the House who wanted to examine it as was allowable under House rules (Miller 1974; Prados 2003, 291; Snider 2008, 273).

Representative Michael Harrington, a Massachusetts Democrat and member of the House Foreign Affairs Committee, was the only congressman to request permission to review the classified transcript. In June, Nedzi granted him access, after discussing the request with the Armed Services Committee chairman and obtaining Colby's consent. Surprisingly, Colby stated that Nedzi could act as he saw fit, as he viewed the matter as an internal congressional affair. Harrington was appalled at what he read in the transcript. Subsequently, in a lengthy July 18 letter to Thomas Morgan (D-PA), chairman of the House Foreign Affairs Committee, and J William Fulbright (D-AR), chairman of the Senate Foreign Relation Committee, Harrington outlined Colby's testimony and requested a comprehensive investigation into the US role in the overthrow of the Allende government. His appeal to Morgan proved futile, although Senator Fulbright responded that he appreciated Harrington's exasperation. The Senate, Fulbright admitted, "at least has been unwilling to exercise control over the CIA" (one estimate is that more 150 such proposals had been rejected by Congress in the past) (Miller 1974). He believed a potential solution was the establishment of a joint congressional committee with authority to "exercise control" of the agency. He also offered to work with Harrington on proposed legislation (Miller 1974; O'Leary 1974b).

Undaunted, Harrington persisted in his efforts to bring attention to the Nixon administration's Chile policy, and to the more immediate problem of congressional

oversight of CIA covert operations. The same month, he introduced two bills aimed at strengthening congressional oversight of the CIA. One of the bills Harrington introduced called for the establishment of a “15-member House Committee on Intelligence Operations”. The committee would meet monthly to review intelligence operations and require members of the Foreign Affairs Committee to participate. Harrington contended that the House Armed Services Committee’s five-member panel was not conducting adequate oversight of the CIA’s activities (New York Times 1974a).

One month later President Nixon resigned over the Watergate scandal, and Vice President Ford was confronted with an ugly fact when on the same day he pardoned Nixon – September 8 – *New York Times* journalist Seymour Hersh claimed that US officials may have misled Congress when they claimed that the CIA was not involved in the overthrow of Allende (Hersh 1974a; New York Times 1974b; Wicker 1974).

Hersh based his reporting on the letters Harrington sent to Morgan and Fulbright, in which the Massachusetts’ legislator described Colby’s testimony in an “account from memory” (Wicker 1974). Harrington had informed Morgan that Colby testified that the Nixon administration had spent \$8 million in covert activities directed against Allende. In particular, \$500,000 was approved in 1969 and 1970 to help Allende’s political opponents, and \$350,000 went to bribing members of the Chilean Congress to vote against certifying Allende’s election. Later, another \$5 million was approved for “destabilization” activities in Chile, and in 1973, \$1.5 million was furnished to assist anti-Allende candidates for municipal offices (Wicker 1974). Hersh also quoted Colby testifying that the Nixon administration, to include Secretary of State Henry Kissinger, spent these funds for covert activities in Chile between 1970 and 1973. Colby stressed that the agency had no role in the military coup that deposed Allende (New York Times 1974b; Wicker 1974).

Hersh’s reporting ignited a firestorm. The next day, Harrington called for a public hearing into the CIA’s covert operations. He stated he would formally request the Foreign Affairs Committee to call for Kissinger and Colby to testify on the matter. Harrington complained that senior members of Congress were unwilling to investigate, fearing Kissinger (Hersh 1974b). Fulbright turned down Harrington’s call for an investigation, telling him that there was “no useful purpose” in his committee re-examining US policy towards Chile (Hersh 1974b). Morgan, on the other hand, vowed to take up the issue (Miller 1974). Some House members blamed Harrington for leaking the information to the newspapers, which he denied.

Harrington did admit that with the authorization of Nedzi, he had read Colby’s classified testimony transcript in June and characterized it as “the most direct, unambiguous and to the point I’ve ever seen”. His reaction to the information was one of “profound shock” (Hersh 1974b). Representative Donald M Fraser (D-MN), chairman of a House Foreign Affairs Committee subcommittee, felt similarly, “The executive branch had deceived the Congress as well as the public with respect to its involvement in the overthrow of the Allende regime” (Stern 1974a).

Shortly thereafter, an undisclosed source stated that the CIA had censored a book by two former intelligence officials that included detailed information about the agency's activities to prevent Allende from assuming the presidency in 1970. The rationale for the censorship was "national security concerns". According to the source, the authors quoted Kissinger as saying, "I don't see why we need to stand by and watch a country go Communist due to the irresponsibility of its own people", at a June 1970 meeting of the interagency "40 Committee", which was responsible for reviewing and authorizing CIA covert activities overseas, prior to presidential approval. Kissinger, the committee chair, refused to comment on these reports, but he told the Senate Foreign Relations Committee that the CIA had nothing to do with the coup "to the best of his knowledge and belief". Other government witnesses, such as the former US ambassador to Chile, denied any attempts to subvert members of the Chilean Congress (Hersh 1974d; Wicker 1974; O'Leary 1974a; Prados 2003, 290–1).

While Fulbright was disinclined to hold hearings, his Idaho colleague, Democratic Senator Frank Church, chairman of a Foreign Relations subcommittee, had no aversion to deeper scrutiny. Church believed executive branch officials had deceived Congress, as they had done with the Vietnam War, and promised to refer disingenuous testimony to the Department of Justice for investigation into potential perjury, claiming that he was "incensed" by the recent allegations. Subcommittee staff members were poring over the hearing transcripts to determine which officials may have lied under oath about CIA covert activities. Church believed there had been a serious attempt to at least mislead Congress, stating he would request Colby's April 1974 testimony before the House Armed Services Committee's subcommittee on intelligence as anonymous officials confirmed that this classified testimony included specific information about the cash payments the CIA made and their purpose. He intended to request Fulbright conduct a full committee hearing and review the "propriety" of clandestine activities against constitutionally elected leaders (Hersh 1974e; Mills 1974).

The State Department was now in the crosshairs, but also committed to supporting the senior officials who had testified before both chambers in previous hearings. However, Senator Kennedy, chair of a Judiciary Committee subcommittee, supported a complete investigation of the inconsistencies that existed in Nixon administration officials' testimony concerning US intervention into Chilean politics. He claimed that State Department officials had lied on at least three occasions in statements before Congress regarding US endeavours in Chile (Stern 1974a; Hersh 1974c; Mills 1974). He followed with a letter to Kissinger asking him on what basis were the CIA activities implemented without notifying Congress since the executive branch shared with it the conduct of US foreign policy (Stern 1974b; Mills 1974).

This line of discussion broadened to questions regarding what constituted the appropriate role of government's covert incursions in the activities of foreign, sovereign nations. Further, there were rumblings about reopening Kissinger's confirmation hearings as secretary of state. Once again, he was being accused of lying – as when he had misled senators regarding wiretaps on journalists and some

members of the administration. However, as one unnamed official pointed out to Hersh, if covert activities directed against a foreign government are approved, then high-ranking officials have to “lie about them. Lies are part of the business” (Wicker 1974). Tom Wicker, a *New York Times* columnist, disparaged that argument as misguided. He questioned whether the United States had “any legal or moral right to conduct covert operations abroad”, and whether any administration had “the constitutional authority to order . . . money spent for clandestine warfare against the legitimate government of a sovereign country”. These issues necessitated “full and open debate” because “gangster schemes of bribery, violence and even assassination are being carried out, in the name of the great American people” (Wicker 1974).

On September 13, Colby appeared on a panel at a conference in Washington, DC, where he told the attendees that the National Security Council had authorized the operations and the CIA had kept the chairmen or members of the appropriate committees in Congress informed. Harrington, a fellow panellist, challenged Colby on this point as did Abourezk. Abourezk was unconvinced that the CIA was providing Congress sufficient and current information about its covert operations. Both lawmakers called for the agency to undergo more intensive oversight, to which Colby expressed concern as to whether Congress could be relied upon to keep classified information safe, given recent leaks (Hersh 1974f).

Kissinger did not escape the furore unscathed. Hersh, citing anonymous former administration and current congressional officials, wrote that Kissinger had been the impetus for the economic sanctions that the United States imposed on Chile after Allende’s election, thereby preventing the Chilean government from obtaining loans from the World Bank, the Export-Import Bank and private banks. The Nixon administration had denied that it took such retaliatory steps, but Hersh reported that Kissinger controlled this step as well as the covert activities (Hersh 1974g; Goodsell 1974).

Hersh kept up the pressure. His next article informed readers that the CIA spent the last 18 months of Allende’s presidency sowing strife by secretly funding striking labour union members and trade groups to undermine the Chilean economy. Meanwhile, Kissinger had been called to testify before the Senate Foreign Relations Committee in closed session the same day. Kissinger emphasized that the covert activities were not intended to subvert the Allende government. The funds had been used to strengthen opposition parties and news media from threats by the Allende government, a position Ford similarly proclaimed at a news conference. Hersh also reported that Colby’s claims that the agency had briefed Congress had been confirmed. Colby had briefed the Senate Foreign Relations Committee’s subcommittee on Western Hemisphere Affairs and the House Armed Services Committee’s Subcommittee on Intelligence (Hersh 1974i; Miller 1974). The same day, Church’s subcommittee staff members provided Church with a memorandum recommending perjury charges against Richard Helms, the former DCI who apparently had not been truthful in prior testimony about CIA involvement in Chile. The report accused Kissinger of deceit in his testimony about the “scope and objective of CIA operations in Chile”. Three other high-ranking US

government officials involved in Latin American affairs were cited for misleading testimony (Miller 1974; Hersh 1974c).

In early October, Abourezk introduced an amendment to the foreign aid bill that would have stopped all CIA covert operations, which he likened to an “arm of the government conducting a secret war without either the approval of Congress or the knowledge of the American people” (Washington Post 1974a). Abourezk was allegedly “under no illusion” that his amendment would pass. However, he had forced the issue to be debated when many lawmakers had “traditionally averted their eyes” (Washington Post 1974b). His amendment was defeated 68 to 17.²

At this point, Senator Harold E Hughes (D-IA) introduced an amendment (amendment 1948 to S. 3394) to the Foreign Assistance Act of 1961 (sec. 662) on the Senate floor with the following language: “No funds may be expended by the Central Intelligence Agency for operations in foreign countries, other than those intended solely for obtaining necessary intelligence, unless the President makes specified findings and reports to specified Congressional committees”(US Department of State 2014, XLII).³ The amendment required the president to give explicit approval through a presidential finding for each action and state that this action was important to national security (US Department of State 2014, XLII).⁴

The amendment carried on a voice vote the same day. Hughes was particularly satisfied with the outcome, arguing it was a step towards a degree of control over intelligence operations overseas. The CIA did not respond officially to this amendment’s passage, but one anonymous official viewed the legislation as “unprecedented” and said that if it was enacted, “it would put a ‘condition’ not on the C.I.A. but on the President’s right to order clandestine activities” (Hersh 1974j).

Given the new attitude on the Hill, the administration agreed to have the CIA brief the House Foreign Affairs Committee on all the agency’s operations that could affect US foreign relations. This development resulted from a meeting a week earlier between Ford, Colby, Kissinger and House and Senate leaders. In the future, according to Nedzi, “any matters involving the CIA which affects foreign policy – including 40 Committee decisions – will be related to the House Foreign Affairs Committee”. He intimated that these briefings would occur before a covert operation began. Nedzi said that these briefings were similar to the ones that his subcommittee had been receiving since he had been chairman. Harrington, however, viewed the announcement as insufficient. The step, he grouched, “only contributes to the illusion of oversight; it doesn’t solve the problems as they are”. Further, the change would not lead to comprehensive investigatory hearings on US policy towards the Allende government and potential administration lying, which he had been pressing Morgan to undertake (Hersh 1974h; 1974j; Miller 1974).

The Senate’s actions on the foreign aid bill (S. 3394) included more than just concerns about the CIA’s activities and it was recommitted to the Foreign Relations Committee for further consideration (Raiford 1976). Nonetheless, the Senate action forced the House to confront the issue as part of the conference committee’s action on the Senate resolution. Representative Leo Ryan (D-CA) introduced an amendment

in a House Foreign Affairs Committee meeting on October 9, 1974. Similar in language to Hughes' amendment, Ryan's amendment specifically included the House Foreign Affairs Committee as an oversight body. Ryan's amendment, which he viewed as a step towards improved oversight within the committee's jurisdiction, was modified slightly by a floor amendment. Subsequently, it became part of the House version of the foreign aid bill (H.R. 17234), and was reported in the House at the end of October (Raiford 1976; Johnson 2005, 219).⁵

By December, the Senate had reported its foreign aid bill and its version passed in the Senate on December 4. The House followed a week later when it considered S. 3394 and passed the bill in place of its version. The conference committee completed its work on December 17, and the Foreign Assistance Act of 1974 included a modification of Ryan's amendment language. The Senate voted in favour of the Conference Report that day and the House followed a day later. President Ford signed the bill into law as Public Law 93-559 on December 30 (Raiford 1976; Kaiser 1978).⁶ The final language placed the following limitation on intelligence activities indicating that no appropriated funds could be spent by the CIA for operations overseas other than for activities needed for obtaining intelligence, and could only be done so when the president found that US national security necessitated such an operation. The president was also obligated to report that operation in a timely fashion to designated committees, which now included the Senate Foreign Relations Committee and the House Foreign Affairs Committee (Select Committee on Intelligence 1994).⁷

Analysis

In the police patrol/fire alarm model that has customarily been used to analyze congressional oversight, the Hughes-Ryan amendment could be understood to be an example of the fire alarm (McCubbins and Schwartz 1984).⁸ The model defines police patrol as driven by congressional interest in agency activities; this model assumes that Congress will discover and remedy any infractions. The police patrol is also – as the name reflects – intended to play a deterrent role. In contrast, fire alarm oversight involves Congress responding to the call to investigate an issue that has been brought forward, generally, by interest groups or other external observers (McCubbins and Schwartz 1984). Extending that metaphor, what happens when the patrols are largely perfunctory and the alarm sounds but no one responds?

This model does not accurately explain the events that led to the passage of the Hughes-Ryan amendment. Instead, this chapter offers an alternative explanation using the three strands mentioned previously. In this case, Harrington does pull the fire alarm, but the method he uses, his letters to the chairmen of the foreign affairs committees, are silent alarms. He does not make the letters' contents known for several months and only when they are leaked to the *New York Times* and the *Washington Post*. Until this disclosure occurs, his communications have no impact on the two chairmen: neither holds hearings in response. In fact, Morgan does not react to Harrington's letter and Fulbright underscores that the

likelihood of hearings or a change in jurisdiction regarding CIA oversight is pointless based on his past experience. Thus, there is no rush on Morgan or Fulbright's part to sound further alarms until the public revelation occurs.

The fire alarm or police patrol metaphor also does not fit as this model assumes that Congress, both chambers, is moved to act. That is not valid in this instance. The hearings held in the aftermath of the newspaper stories were token and more concerned about the leaks than the CIA covert operations (Miller 1974). To understand this reluctance requires more than counting the number of hearings or other quantitative methods; it demands attention be paid to the internal politics of the two chambers and the important members with a stake in the outcome.⁹ Institutional drag – our third strand – the unwillingness of an institution to change or innovate, can be understood as a means by which individuals or groups, such as committees, “lose their original vision of service to people, and become instead of self-serving mechanisms first of all” (Maxwell 1978, 120). Moreover, institutional drag is abetted by long and deeply held traditions and constituencies.

Values and norms (loyalty to an institution as an example) are involved as well, and in view of the powerful, no “upstart” is going to tamper with institutional practices. These factors are not dismissed quickly, but take intensive and continual initiative and attention to overcome (Mount Jr. 1990, 32). As one ethicist has pointed out,

An example of the dangers of institutional drag is the temptation for us to devote total loyalty to an institution, especially when the institution stands for noble ideals and becomes the chief or only definer of a person's identity. In such cases, loyalty to the institution becomes idolatrous. The institution is vested with the god-like prerogative of what is good and right.

(Mount Jr. 1990, 32)

Some of the most powerful members of the House and Senate, committee chairmen, were in danger of losing power by ceding control to other committees.

By June 1974, Fulbright is in his final few months as a senator. He has lost the Democratic primary to a challenger, former Arkansas government Dale Bumpers, who will ultimately win the general election. Fulbright is a lame duck with waning power (Binder 1974; Gwertzman 1974). Fulbright was equally demoralized about any attempt to rein in CIA covert activities by Congress. Senator John Stennis (D-MS) was another obstacle as chairman of the Senate Armed Services Committee and more importantly, chairman of the CIA subcommittee. The disclosures in the newspapers surprised and embarrassed him publicly and were solid evidence that he had not been conducting rigorous oversight of the agency (Stern 1974c; Paterson 1987, 162; Congressional Quarterly 1975, 538). Additionally, he preferred the arrangement in place whereby only his committee and the Appropriations Committee were cognizant of CIA activities and budgets. Adding the Foreign Relations Committee, with its liberal members, was outrageous to him and signalled a potential diminution of his power.

When Stennis assumed chairmanship of the Armed Services Committee in 1972, he conducted the subcommittee's activities differently from his predecessor, Richard Russell. Russell had occasionally invited senior Foreign Relations Committee members to attend CIA oversight sessions. When Stennis became the chairman, he stopped inviting his Foreign Relations Committee colleagues and oversight sessions became rare. The floor debate regarding Hughes' amendment shows clearly his attempts to thwart the passage of the amendment (Washington Post 1974a; Snider 2008, 32–3).¹⁰ The CIA knew it had allies in Stennis and Henry "Scoop" Jackson, another senior Armed Services Committee member, whom the agency preferred lead the Senate investigation into the CIA's relationship with IT&T in order to produce a result advantageous to the agency (Johnson 2005, 196).

Senator Church could have played a more prominent role in this issue, but he did not. Likely his run for re-election to the Senate monopolized his time. His seniority on the Foreign Relations Committee was such that he would have been stymied in using the committee to further a reform agenda. In fact, his relationship with Fulbright was now strained and publicly evident because of their disagreement over how to handle the Chile inquiry (Miller 1974). There were sufficient senators with clout that could push reforms, such as Edward Kennedy, Walter Mondale (D-MN), Howard Baker (R-TN) and the so-called new internationalists, such as Abourezk, but they were not members of the committees involved in the jurisdictional wrestling match (Johnson 2004, 10; Paterson 1987, 162; Miller 1974).¹¹ Mike Mansfield, the Senate majority leader, did allow amendments to the foreign aid bill, which provided Abourezk and Hughes a means of promoting increased oversight that would not require the expenditure of political capital. The timing of disclosures proved beneficial as reformers could offer amendments to the foreign aid bill, already under fire because of other issues. Thus, in the Senate, Hughes used a floor amendment with compromise language, not a committee bill, to advance enhanced CIA oversight.

The situation in the House is similar to that of the Senate. The chairman of the House Armed Services Committee, F Edward Hébert (D-LA), did not conduct hearings into the CIA covert operations, but instead held hearings regarding the leak of classified material and Harrington's involvement. Nedzi, like Stennis, was embarrassed by the newspaper articles, but did not conduct hearings. The Foreign Affairs Committee, of which Harrington was a member, took little action. In fact, when Harrington raised concerns about CIA involvement in Chile in light of the IT&T incident, the chairman of the Western Hemisphere subcommittee, Dante Fascell (D-FL), stated he did not intend to hold hearings (Miller 1974). In response, Congressman Leo Ryan fashioned language acceptable to them as an amendment to the foreign aid bill, essentially mirroring the Hughes amendment, ensuring its passage in the House. The Hughes-Ryan amendment was not only a compromise but it was also a warning sign that the "Senate barons" were losing control of their power (Snider 2008, 32–3).

With respect to the first strand, influential congressmen believed the president had complete autonomy regarding intelligence operations. Given that stance, there

was minimal challenge to executive authority when it came to the issue of covert action. Senator Carl Hayden, the Appropriations Committee chairman, held that congressional intrusion into intelligence activities “would tend to impinge upon the constitutional authority and responsibility of the President in the conduct of foreign affairs” (Whittington and Carpenter 2003, 505). Russell had told his colleagues that “we must take some matters on faith”, in beseeching his colleagues not to strengthen oversight requirements (Whittington and Carpenter 2003, 505).

Consequently, the second strand occurred: “Congress did not develop the institutional capacity to set its own policy interests or to ensure that the intelligence agencies adhered to those concerns”. In essence, Congress acquiesced to presidential leadership in this issue area. The oversight subcommittees faded “into near inactivity during most of the postwar period”. Members who may have objected to executive decision-making without consulting the relevant committees “were simply kept in the dark” (Whittington and Carpenter 2003, 505). Harrington’s complaint is indicative of this concern about “autonomous executive power” and “presidential hegemony” (Whittington and Carpenter 2003, 505).

Conclusion

While major change in terms of covert action and accountability was stymied by the forces described earlier, the Hughes-Ryan Amendment contributed a change that had a serious impact on the relationship between covert action and accountability. By requiring the president to notify Congress in the form of a presidential finding when a covert action was being planned, presidents were forced to acknowledge their role in covert activity and thus plausible deniability – the ability of the president to deny awareness of these types of activities – was at an end. In the words of intelligence scholar, Loch Johnson: “The objective of plausible deniability was to brush away footprints in a covert operation to prevent anyone from following the tracks back to the United States and particularly to the Oval Office” (Johnson 1985, 58). Those “tracks” would now be visible.

Other events would also spur the major reforms that Harrington envisioned. As noted earlier, Watergate was a catalyst, followed by Ford’s pardon of Nixon and the December 1974 revelations in the newspapers about the CIA’s domestic spying activities and attempted assassinations of foreign leaders. The November 1974 mid-term elections, another result of the Ford pardon, brought in a new class of members in both chambers, reformers that sought to wrest power from the committee leaders and begin a period where subcommittee chairs were in control. Even more importantly, Senate and House leaders could no longer avoid a full investigation into CIA activities, especially covert action.

While the Hughes-Ryan Amendment itself was rather limited, it not only ensured presidential responsibility for covert action, but it also broadened congressional activity in this executive-dominated arena. The notification requirement provided the basis for a framework of legislative oversight that would develop over subsequent decades. Lastly, the legislation empowered Congress, ultimately through the establishment of permanent committees a few years later, to share the

control – and responsibility for intelligence operations – a significant shift in the oppositional relationship between the two branches of government. While factors distinctive to the United States shaped the form of the legislation, Hughes-Ryan has broader significance as a milestone that marked a greater demand for transparency from the intelligence community that has only intensified in the succeeding years.

Notes

- 1 For an early discussion of this dynamic, see Whittington and Carpenter (2003).
- 2 120 Cong. Rec. 33482.
- 3 Foreign Assistance Act, Pub. L. No. 93–559 (1974).
- 4 120 Cong. Rec. 33487–33491.
- 5 See also 120 Cong. Rec. 39165–39165–39166.
- 6 120 Cong. Rec. 39165–39165–39166. See also Kaiser (1978).
- 7 Foreign Assistance Act, Pub. L. No. 93–559, 88 Stat., 22 USC 4222. See also Select Committee on Intelligence (1994, 4).
- 8 See also Deering (2003) and Johnson (2005).
- 9 This has been a common approach to gauging the efficacy of oversight. See Aberbach (1989) for a seminal text using this methodology.
- 10 120 Cong. Rec. 33489–33490.
- 11 120 Cong. Rec. 33491. See also Johnson (2005, 190–241) and Snider (2008, 33).

References

- Aberbach, Joel D. 1989. *Keeping a Watchful Eye: The Politics of Congressional Oversight*. 1st edition. Washington, DC: Brookings Institution Press.
- Barrett, David M. 2005. *The CIA and Congress: The Untold Story from Truman to Kennedy*. Lawrence, Kan: University Press of Kansas.
- Binder, David. 1974. “Little Difficulty in Senate Is Seen Over Confirmation of Kissinger as Secretary”. *New York Times*, August 23.
- Congressional Quarterly. 1975. *Congressional Quarterly, Almanac, 93rd Congress, 2nd Session, 1974*. Washington, DC: Congressional Quarterly Inc.
- Deering, Christopher J. 2003. “Alarms and Patrols: Legislative Oversight in Foreign and Defense Policy”. In *Congress and the Politics of Foreign Policy*, edited by Colton C. Campbell, Nicol C. Rae, and John F. Stack Jr., 1st edition, 112–38. Upper Saddle River, NJ: Pearson.
- Goodsell, James Nelson. 1974. “Chilean Generals Unfazed by Report of CIA Aid in Allende Ouster”. *Christian Science Monitor*, September 11.
- Gwertzman, Bernard. 1974. “Fulbright Sees Kissinger as Détente Foes Target”. *New York Times*, July 16.
- Hersh, Seymour M. 1974a. “C.I.A. Chief Tells House of \$8 Million Campaign against Allende in ’70–73”. *New York Times*, September 8.
- . 1974b. “Hearings Urged on C.I.A.’s Role in Chile”. *New York Times*, September 9.
- . 1974c. “State Department Backs Reports of a Hands-Off Policy”. *New York Times*, September 10.
- . 1974d. “Censored Matter in Book about C.I.A. Said to Have Related Chile Activities”. *New York Times*, September 11.
- . 1974e. “Senator Church to Press C.I.A. Issue”. *New York Times*, September 12.

- . 1974f. “C.I.A. Chief Says Covert Activities Are Not Vital”. *New York Times*, September 14.
- . 1974g. “Kissinger Called Chile Strategist”. *New York Times*, September 15.
- . 1974h. “Ford to Brief Five on C.I.A. Activities”. *New York Times*, September 19.
- . 1974i. “C.I.A. Is Linked to Strikes in Chile That Beset Allende”. *New York Times*, September 20.
- . 1974j. “Senate Shelves Foreign Aid Bill in Ford Victory”. *New York Times*, October 3.
- Johnson, Loch K. 1985. *A Season of Inquiry: The Senate Intelligence Investigation*. Lexington: University Press of Kentucky.
- . 2004. “Congressional Supervision of America’s Secret Agencies: The Experience and Legacy of the Church Committee”. *Public Administration Review* 64 (1): 3–14.
- . 2005. “Accountability and America’s Secret Foreign Policy: Keeping a Legislative Eye on the Central Intelligence Agency”. *Foreign Policy Analysis* 1 (1): 99–120. <https://doi.org/10.1111/j.1743-8594.2005.00005.x>.
- . 2018. *Spy Watching: Intelligence Accountability in the United States*. New York, NY, USA: Oxford University Press.
- Johnson, Robert David. 2005. *Congress and the Cold War*. New York: Cambridge University Press.
- Kaiser, Frederick M. 1978. *Legislative History of the Senate Select Committee on Intelligence*. Washington, DC: Congressional Research Service. <https://fas.org/sgp/crs/intel/ssci-leghist.pdf>.
- Lawrence, John A. 2018. “How the ‘Watergate Babies’ Broke American Politics”. *Politico Magazine*, May 26. <https://politi.co/2sgy8vF>.
- Lester, Genevieve. 2015. *When Should State Secrets Stay Secret?: Accountability, Democratic Governance, and Intelligence*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9781107337015>.
- Marshall, Bryan W. 2003. “Presidential Success in the Realm of Foreign Affairs: Institutional Reform and the Role of House Committees”. *Social Science Quarterly* 84 (3): 685–703.
- Maxwell, Grant. 1978. “Faith Experiences in Transition among Canadian Catholics”. In *Religion and Ethnicity*, edited by Harold Coward and Leslie Kawamura. Waterloo, Ont: Wilfrid Laurier University Press.
- McCubbins, Mathew D., and Thomas Schwartz. 1984. “Congressional Oversight Overlooked: Police Patrols versus Fire Alarms”. *American Journal of Political Science* 28 (1): 165–79. <https://doi.org/10.2307/2110792>.
- Meeus, Marius, and Leon Oerlemans. 2005. “National Innovation Systems”. In *Innovation and Institutions: A Multidisciplinary Review of the Study of Innovation Systems*, edited by Steven Casper and Frans van Waarden. Cheltenham: Edward Elgar Publishing Ltd.
- Miller, Judith. 1974. “Criminal Negligence: Congress, Chile, and the CIA”. *The Progressive*, November 1974. www.cia.gov/library/readingroom/docs/CIA-RDP79-00957A000100090005-5.pdf.
- Mills, Dean. 1974. “Study Looks for U.S. Lies about Allende”. *Baltimore Sun*, September 13.
- Mount, Jr., Eric. 1990. *Professional Ethics in Context: Institutions, Images and Empathy*. 1st edition. Louisville, KY: Westminster/John Knox Press.
- New York Times. 1972. “I.T.T. Said to Seek Chile Coup in ’70”. *New York Times*, March 22.
- . 1974a. “House Gets Bills to Extend Congress’ Control of C.I.A.”. *New York Times*, July 16.
- . 1974b. “Mr. Ford Is in Residence”. *New York Times*, September 8.

- O' Leary, Jeremiah. 1974a. "Kissinger Supervised Anti-Allende Moves". *Washington Star*, September 9.
- . 1974b. "Plot to Beat Allende Laid to CIA". *Washington Star*, September 12.
- Paterson, Thomas G. 1987. "Oversight or Afterview?: Congress, the CIA, and Covert Actions since 1947". In *Congress and United States Foreign Policy: Controlling the Use of Force in the Nuclear Age*, edited by Michael Barnhart. Albany: State University of New York Press.
- Prados, John. 2003. *Lost Crusader: The Secret Wars of CIA Director William Colby*. 1st edition. New York, USA: Oxford University Press.
- Raiford, William Newby. 1976. *To Create a Senate Select Committee on Intelligence: A Legislative History of Senate Resolution 400*. Washington, DC: Congressional Research Service. <https://fas.org/sgp/crs/intel/76-149.pdf>.
- Scott, James M., and Ralph G. Carter. 2002. "Acting on the Hill: Congressional Assertiveness in U.S. Foreign Policy". *Congress & the Presidency* 29 (2): 151–69. <https://doi.org/10.1080/07343460209507732>.
- Select Committee on Intelligence. 1994. *Legislative Oversight of Intelligence Act Ives: The U.S. Experience*. Washington, DC: US Government Printing Office. www.intelligence.senate.gov/sites/default/files/10388.pdf.
- Snider, L. Britt. 2008. *The Agency and the Hill: CIA's Relationship with Congress, 1946–2004*. Washington, DC: Center for the Study of Intelligence.
- Stern, Laurence. 1974a. "U.S. Again Denies Anti-Allende Policy". *Washington Post*, September 10.
- . 1974b. "CIA Chief Colby Facing Confrontation on Chile Operations". *Washington Post*, September 12.
- . 1974c. "Disclosure of CIA Chile Role 'Surprises' Overseers on Hill". *Washington Post*, September 13.
- Stuart, Douglas T. 2008. *Creating the National Security State: A History of the Law That Transformed America*. Princeton, NJ: Princeton University Press.
- Subcommittee on Multinational Corporations. 1973. *The International Telephone and Telegraph Company and Chile, 1970–1971*. Washington, DC: US Government Publishing Office.
- Time. 1973. "The Bloody End of a Marxist Dream". *Time*, September 24.
- US Department of State. 2014. *Foreign Relations of the United States, 1969–1976, Volume XXI, Chile, 1969–1973*. Washington, DC: US Government Printing Office. <https://history.state.gov/historicaldocuments/frus1969-76v21/notes>.
- Washington Post. 1974a. "The 'Covert Operations' Debate". *Washington Post*, October 7.
- . 1974b. "The Senate and the CIA". *Washington Post*, October 7.
- Whittington, Keith E., and Daniel P. Carpenter. 2003. "Executive Power in American Institutional Development". *Perspectives on Politics* 1 (3): 495–513. <https://doi.org/10.1017/S1537592703000367>.
- Wicker, Tom. 1974. "Secret War in Chile". *New York Times*, September 13.

13 Congressional oversight of US intelligence activities

Mary B. DeRosa

Introduction

The United States Constitution assigns to Congress the responsibility to oversee activities of the executive branch, both to enhance the quality of decision-making and to ensure democratic accountability of the executive. The work of US intelligence agencies is essential for national security and necessarily shrouded in secrecy. These characteristics make skilled external oversight crucial to prevent abuse and enhance the quality and credibility of intelligence activities, but they also make that oversight unusually difficult. US history is riddled with intelligence scandals and oversight failures. Congress has learned from these experiences and has crafted a credible oversight structure and process. But challenges remain for congressional overseers. This chapter examines these challenges, how they affect congressional oversight of intelligence, and Congress's efforts to ensure accountability for US intelligence activities.

History of congressional oversight and reforms

Early oversight and the Church Committee

The United States Government has engaged in intelligence collection and covert action since its earliest days. Congressional oversight of intelligence activities, however, has a relatively short history. It was not until the late 1940s, with the creation of the Central Intelligence Agency (CIA), that the US House of Representatives and Senate created entities – subcommittees of their Armed Services committees – with responsibility for intelligence oversight.¹

Congressional overseers in this early period exhibited a tendency common to oversight through the years: a cyclical interest that ramps up in response to public attention or perceived agency failure, but rarely persists past the crisis. Loch Johnson describes this pattern, which he calls his “shock theory” of intelligence oversight:

[After some pivotal event that leads to reform] At first, members of Congress keep a close eye on the spy organizations to assure the new rules are honored.

Before long, though, the interest and attention span of lawmakers begin to wane and the intelligence agencies are treated with a sense of benign neglect on Capitol Hill.

Inevitably the unwatched agencies go astray and shocked overseers “shake themselves out of their lassitude, rally to investigate what went wrong, and attempt to set the spy agencies back on a proper track . . . but only for a while before dropping off again” (Johnson 2018, 18).

A watershed in congressional oversight came in late 1974 after journalist Seymour Hersh published a lengthy article in the *New York Times* revealing significant illegal domestic activities by the CIA, including wiretaps, break-ins, mail openings, infiltration of domestic political organizations and the existence of files on 10,000 Americans involved in the anti-war movement (Snider 2008, 33). In the wake of these revelations, the Senate voted overwhelmingly to establish a select committee, chaired by Senator Frank Church, to investigate Intelligence Community activities (Snider 2008, 37–9).²

The Church Committee’s investigation lasted 15 months and was the “most exhaustive look at our government’s (or any government’s) secret intelligence agencies” (Schwartz Jr. 2007, 19). The Committee investigated domestic and foreign intelligence activities and its revelations were earthshaking. Its final report described massive efforts by the Federal Bureau of Investigation (FBI), CIA, National Security Agency (NSA) and other intelligence organizations to spy on, harass, disrupt and undermine US organizations and citizens because of their political views and lawful speech and activities. In its reporting on foreign activities, the Committee revealed assassination plots, election meddling and coup attempts, among other morally questionable and often flawed and counterproductive covert action (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1975; 1976a; 1976b; Snider 2008, 275–8).

In his transmittal letter for Book II of the Committee’s report, Committee Chairman Senator Church gave this description of the greatest lesson from the investigation:

The root cause of the excesses which our record amply demonstrates has been failure to apply the wisdom of the constitutional system of checks and balances to intelligence activities The founding fathers foresaw excess as the inevitable consequence of granting any part of the government unchecked power. This has been demonstrated in the intelligence field where, too often, constitutional principles are subordinated to a pragmatic course of permitting desired ends to dictate and justify improper means.

Our recommendations are designed to place intelligence activities within the constitutional scheme for controlling government power (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1976b, III).

Post-Church Committee reforms

The Church Committee revelations and other concerns that surfaced during that period led to a number of significant reforms to intelligence oversight. In the years since, there have been additional changes to structure and process.

In response to one of the Church Committee's key recommendations, within a year after the report's release the Senate and the House established "select" committees³ – the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) – with responsibility for oversight of intelligence and authorization of appropriations for intelligence activities.

Beyond structure, Congress also focused on ensuring a greater flow of information to the Congress from the Intelligence Community. In October 1980, Congress passed what is known as the Intelligence Oversight Act of 1980, which imposed consequential reporting requirements that continue to this day. The Act required that the intelligence agency leaders keep the intelligence committees "fully and currently informed" of intelligence activities, including "any significant anticipated intelligence activity", and "report in a timely fashion" any illegal activities or significant intelligence failures.⁴ In 1991, Congress shifted these notification responsibilities to the president.⁵ It imposed similar requirements on the Director of National Intelligence (DNI), when that position was created in 2004.

Congress also passed significant additional reforms to processes for covert action and electronic surveillance. In 1974 Congress passed what is known as the Hughes-Ryan Amendment in response to concerns about the covert activities that the CIA conducted in Chile, intended to thwart the election of Salvador Allende. The Hughes-Ryan Amendment, for the first time, formalized the process for approval and oversight of one important, and often perilous, type of intelligence activity: covert action, which is operational activity intended to "influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly". Hughes-Ryan required that the CIA must obtain the president's approval to conduct covert action and that the president must "find" that the activities are "important to the national security of the United States". The president must report this "Finding" to Congress (Ford 2006, 24–5). Congress amended these reporting requirements further in 1981 and again in 1991 to require covert action reports to the intelligence committees "as soon as possible" and "before the initiation of the covert action". If the president "determines it is essential to limit prior notice to meet extraordinary circumstances affecting vital interests of the United States", he may inform a smaller group of eight members of Congress. This has become known as "Gang of Eight" reporting (Ford 2006).⁶

The Church Committee subject that generated perhaps the greatest outrage was its extensive chronicling of domestic electronic surveillance by intelligence agencies. The Committee found that wiretapping of US citizens with no judicial warrant had been rampant (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1976b). In response, in

1978 Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA), which sets out a process for seeking a warrant from a specially constituted court to conduct surveillance within the US for the purposes of foreign intelligence. FISA's procedures guide the conduct of all electronic surveillance for foreign intelligence purposes in the United States. The FISA Amendments Act, passed in 2008, amended FISA to establish a process for some broader "programmatic surveillance" of foreign targets outside of the United States without individualized suspicion.

Congressional oversight tools

Hearings, briefings and legislation

The Intelligence Committees conduct virtually all of their work in classified settings. Their standard information gathering tools are hearings (open and closed), formal briefings, statutorily required reports, ad hoc information requests, and informal interactions. Legislation also plays a key, if indirect, role in oversight. The executive branch fears the impact of what it believes is ill-considered legislation. Often it will increase its interaction with the committees hoping to head off or change proposed legislation, or it will take corrective action itself in an attempt to persuade members that legislation is unnecessary.

The most important legislation for the intelligence committees is the annual Intelligence Authorization Act. Heather Molino, a former HPSCI staff director, described this bill as the committee's key tool for oversight of the Intelligence Community (Bahar et al. 2018). Although the congressional appropriations committees decide on funding for the agencies, Senate and House rules require that all intelligence appropriations be authorized separately and the intelligence committees have that responsibility. In producing authorization legislation, committee members and staff delve in minute detail into intelligence agency programmes, offices, activities and personnel to determine what may be funded, what is prohibited and other important details of how agencies will conduct their activities and interact with the committees. Thus, the legislation is a source of great influence and leverage for the committees. At least this is the case in theory. In fact, the intelligence committees have struggled over the last two decades to produce authorization legislation that can pass the Congress. When there is no authorization legislation, Congress inserts language into the National Defense Authorization Act (NDAA) that provides a blanket authorization for all amounts appropriated for national intelligence. The uncertainty about passage of this annual legislation reduces the effectiveness of intelligence committee oversight.

Investigations

Congressional investigations are a longstanding and critical tool of oversight. They usually arise from incidents of perceived failure or abuse or some other high-profile systemic concern. Congressional intelligence committees have used

this tool regularly over the years. Recent examples include the SSCI's lengthy investigation of the Bush Administration's detention and interrogation practices, HPSCI's investigation of the 2012 attacks on US diplomatic facilities in Benghazi, Libya and both committees' investigations of Russia's interference in the 2016 election. For some significant investigations of intelligence issues, however, Congress has created special committees in each chamber – such as with the investigation of the Iran-Contra affair in 1986–87 – or joint committees involving both chambers – such as the congressional investigation following the 9/11 attacks. Investigations tend to be more public and more adversarial than other tools of oversight. They are a key mechanism for developing an understanding of complex facts to uncover abuse, monitor the implementation of policy and inform the public. They also can serve as the basis for development of legislation and reforms.

Committee staff

Staff on the intelligence committees plays an outsized role in oversight. Both intelligence committees now have majority and minority staffs. The tradition in both the House and Senate has been to avoid partisanship and the staffs have usually worked together, although this tradition breaks down on occasion.⁷

Committee members delegate to their staff much of the day-to-day oversight of the Intelligence Community. Staff conduct the initial fact-finding and analysis that result in hearings, reports and legislation. Although members provide the vision and broad goals for this work, and they become intensely involved on certain issues, it is the staff that develops the information and expertise. Many professional staff members on both committees have worked previously in the Intelligence Community and are familiar with the offices and personnel. The staff engage with personnel in intelligence agencies more frequently and in more depth than staff of most other congressional committees.

Dynamics

Types of oversight

Much of the academic literature on congressional oversight identifies two dichotomous approaches. In the most influential article on the subject, political scientists Matthew McCubbins and Thomas Schwartz describe two categories of oversight: “police patrol” and “fire alarm”. With police patrol oversight Congress takes the initiative to review the activities of the overseen entity with the goal of finding and fixing potential problems. Police patrol oversight is active and centralized, in that the overseers themselves are responsible for uncovering concerns. Fire alarm oversight is initially more passive on the part of the overseers; it relies primarily on outside observers to identify existing problems or abuses and raise concerns to which Congress will respond. Police patrol is the more time- and resource-intensive of the two forms in this model (McCubbins and Schwartz 1984).

Other experts have identified “active” and “reactive”, “anticipatory” and “post-hoc”, and “institutional” and “investigative” as the most important distinctions between forms of congressional oversight (Nolan 2007, 116–17; Schwartz Jr. 2007, 23). The categories tend to line up. The first of the two terms – police patrol, active, anticipatory and institutional – describe oversight that uses hearings, briefings, formal and informal information requests, and legislation to stay on top of the agencies, understand their business and identify problems before they arise. The second terms – fire alarm, reactive, post-hoc and investigative – describe a form of oversight that reacts to discovery, usually from an outside source, of a failure or abuse and then investigates what happened and draws conclusions about fault and possible reforms.

McCubbins and Schwartz identified fire alarm as the most common form of oversight in Congress. Members of Congress prefer it, they argue, because it is cost-effective and its more decentralized approach is a better fit with the incentives for legislators than the more hands-on police patrol model. Other experts, however, have found that that police patrol oversight is more prevalent in Congress than McCubbins and Schwartz suggest. They attribute this to a change in the incentives for legislators since the mid-1970s because of a greater public interest, post-Watergate and Church Committee, in assuring that government programmes operate competently and consistent with law (Johnson 2018, 37–8).

Congress uses both forms of oversight with the Intelligence Community but is less effective at each than in other areas because of the unique challenges of intelligence oversight. Police patrol, as McCubbins and Schwartz noted, is a time and resource-intensive form of oversight. It becomes even more costly with intelligence because, as discussed in the following, relevant information is far more difficult to acquire, there are cumbersome restrictions on where it can be reviewed and with whom it can be discussed, and legislators, for a variety of reasons, lack the incentive to devote time and energy to these activities. As a result, although the intelligence committees do engage regularly in this proactive type of oversight, it is largely the responsibility of the professional committee staffs, with limited focus from members unless the issues are high profile (Johnson 2018, 209–48).

Fire alarm oversight is less effective with intelligence because there are fewer sources for alarms. McCubbins and Schwartz anticipated outside observers and interest groups who would act as watchdogs, keeping an eye on agency activities and alerting lawmakers to problems. In the intelligence world, because of the secrecy of the programmes involved, there are far fewer outside observers capable of raising alarms. Journalists play this role at times, usually based on leaked classified information.

Secrecy, expertise and capture

The most significant difference between oversight of intelligence and almost any other field is the difficulty congressional overseers experience acquiring and using information. Obtaining information is a challenge for all congressional oversight; the departments and agencies have greater expertise and knowledge

about the matters being overseen and legislators have to work hard to know the right questions to ask. But no other discipline involves the information constraints that exist for intelligence. Although the intelligence agencies share a significant amount of information with Congress, most relevant information is extremely sensitive and the agencies appropriately take measures to protect it from release. Moreover, unlike in other areas there are very few sources to which the overseers can look for information on intelligence other than the agencies they are reviewing. The resulting dynamic affects the legislators' ability to develop expertise and undermines effective oversight.

The executive branch has an expansive view of the president's legal authority to control classified national security information. The US Justice Department's Office of Legal Counsel has explained that the President has "ultimate and unimpeded authority over the collection, retention and dissemination of intelligence and other national security information in the executive branch", including for dissemination to Congress (Christopher H Schroeder, Memorandum opinion for the General Counsel Central Intelligence Agency, November 26, 1996).⁸ Congress and some experts dispute this legal analysis and the US courts have never resolved these differences (Cumming 2010, 3; Fisher 2008, 221). In practice, Congress has largely acquiesced in the view that the president is the "owner" of intelligence and is able to control access to information and operational details under some circumstances. Legislators consider the statutory reporting requirements, discussed earlier, to be a critical counterbalance; in particular the requirement that the president keep Congress, through its intelligence committees, "fully and currently informed of all intelligence activity" (Cumming 2010, 1–2). That requirement is vague, however. The executive branch has never interpreted this obligation to require provision of *all* intelligence to Congress. Congress asserts that right but has never sought to enforce it.

The branches have never developed a written set of rules for what the Intelligence Community must share (Kibbe 2010, 33). As a result, they rely on norms and historical understandings about what Congress may demand and conflicts are common. If Congress is not satisfied with what it receives, its realistic recourse is to criticize the administration publicly and use its leverage over appropriations, legislation and nominations to force the executive's hands. The effectiveness of these tools depends on whether the president feels Congress's actions can hurt him politically.

Even when Intelligence Community personnel agree to provide information in hearings or briefings, they often are selective in what they share. As James Baker explains, "[m]embers see only part of the picture, and then only that part of the picture contained in executive talking points that have survived layers of editing and that are designed to fend off policy or partisan attack" (Baker 2007, 132). Loch Johnson provides many examples from his own experience and that of others when the Intelligence Community provided obscure or incomplete information to intelligence committee questioners. He quotes former Senator William Cohen during a SSCI hearing about an intelligence controversy involving a CIA

asset in Guatemala who was implicated in various human rights violations: “if you asked the wrong question of the Agency you never got the right answer”, he complained and “If you asked the right question, you got only half the right answer” (Johnson 2018, 157).

Sometimes the process breaks down entirely. This was the case with the Iran-Contra scandal during the Reagan Administration in the mid-1980s. Members of the Reagan National Security Council and CIA secretly sold arms to Iran in exchange for Iran’s assistance in obtaining the release of US hostages in Lebanon. This sale violated the Arms Export Control Act. The NSC staff then created a private organization, outside of government, and funnelled some of the proceeds from the arms sale to that organization for its use in supporting the Contras, a Nicaraguan rebel organization. This too violated the law. Congress had enacted a series of measures, known as the Boland Amendments, that restricted US assistance to the Contras. One of these amendments specifically prohibited the use of funds to support the Contras.

The Reagan Administration reported neither of these operations to Congress. Indeed, when members of Congress specifically asked the National Security Advisor and his deputy about rumours of operations involving Nicaragua, the officials did not reveal the work of the private organization they had created (Johnson 2018, 147–8). This is despite notification requirements for intelligence activities and specifically for covert action. Iran-Contra is perhaps the most egregious violation by the executive branch of its post-Church obligations to notify Congress (the affair included many other serious violations of law as well). It is an example of the dangers of a notification system that must rely, to some degree, on the good faith of the president and those who work for him.

Secrecy poses other problems for members of Congress in their efforts to oversee the Intelligence Community. For example, members face difficulty in accessing intelligence that the Intelligence Community has provided. To read classified intelligence, they must go to a Sensitive Compartmented Information Facility (SCIF), a windowless vaulted space usually located in the intelligence committee’s office space. They may only read the materials there and, if notes are permitted, they must also be stored in the SCIF.

The use of limited briefings to inform some members about particularly sensitive covert actions or other sensitive intelligence programmes is another concern. The National Security Act permits the president to limit congressional notification of a covert action where he “determines it is essential to limit prior notice to meet extraordinary circumstances affecting vital interests of the United States”. In that case, the president is only obligated to inform the House and Senate majority and minority leaders and the chairs and ranking minority member of the House and Senate intelligence committees. In addition to these statutory “Gang of Eight” notifications for covert actions, there is a longstanding practice of “Gang of Four” notifications – to the chairs and ranking minority members of the intelligence committees – for some particularly sensitive intelligence activities that are not covert actions. When these limited notifications occur, members may not discuss what they have heard beyond the limited group that has been briefed, which

sometimes does not include even senior staff. This poses a hardship because these members rely on their staff for expertise and guidance.

Without being able to discuss the matter with staff, lawyers or any colleagues other than the few who had also been briefed, members of Congress have few avenues to raise concerns or take corrective action. Nonetheless, the executive branch may use the briefings to suggest approval. In response to public and congressional anger after a controversial programme leaked to the press, George W Bush Administration officials repeatedly cited severely limited congressional briefings – and the lack of subsequent congressional action – as proof that Congress had approved of their actions. Thus, as Kathleen Clark has argued, the briefings serve little or no oversight purpose and allow the executive branch to inoculate itself against later criticism for controversial programs (Clark 2012; Decker 2006, 300–1). Since the Bush Administration, the intelligence committees have pushed back much harder against limited briefings.

These constraints on the flow of information affect the quality and effectiveness of oversight in a number of ways. First, the inability to share or discuss the information they have robs lawmakers of traditional avenues for effective oversight. In the case of limited briefings, members can only raise objections with the executive branch and other briefed members. They cannot use the information to persuade colleagues to use leverage to address the concern – for example to pass legislation or cut funding (Kibbe 2010, 37). It is difficult to convince other lawmakers to take action when you are not able to explain why. Even if the briefing is not limited, the classified nature of the information prevents discussing it publicly, which often is the only effective way that individual legislators can bring attention to an issue.

Moreover, a number of factors make it difficult for lawmakers to develop expertise on complex intelligence matters. It is rare for any member of Congress to come into the job with experience in the intelligence community, so they must develop expertise on the job, which can take many years. Term limits for committee members have contributed to this problem. In this complex area, members often will just be getting up to speed when it is their time to leave the committee. The Senate no longer imposes term limits on SSCI members for this reason, but HPSCI members are limited to six years on the committee. The difficulty for members of obtaining and accessing information, and their inability at times to rely on staff expertise, makes learning the issues particularly time-consuming. Thus, lawmakers often are unable to develop expertise on complex intelligence matters. Or, more accurately, they are unwilling to take the time that developing that expertise would require.

Finally, when lawmakers do endeavour to develop expertise, they have few if any sources of relevant information other than the agencies they oversee and are unable to reach out to colleagues or others to debate or discuss the tough issues involved. As a result, they tend to give the views of the Intelligence Community significant, perhaps undue, weight. “Capture” – the loss of objectivity and distance – of overseers by the entities they oversee is always a concern in Congress. This is particularly true when the stakes for the country are high, as they

are when national security is involved. Capture is a significant risk with intelligence oversight. As Oregon Senator Ron Wyden described the problem, the Intelligence Community “sweeps in” and explains “[w]ell, these are tough issues”, and “only one point of view gets conveyed”. He says the committee members can “get caught up in the culture that makes you, in effect, something more like an ambassador [for the Intelligence Community] than a vigorous overseer” (Johnson 2018, 185).

To be sure, legislators come in many varieties and not all are subject to capture by the Intelligence Community. Loch Johnson describes the varying roles of intelligence committee members over the years. There are “ostriches”, who trust the intelligence community and pay little attention to committee matters; “cheerleaders”, who are outspoken defenders of the intelligence community; at the other extreme there are the consistently negative and mistrustful “lemon suckers”, and finally there are the “guardians” – the type most suited to effective oversight – who combine respect for the intelligence agencies with distance and the ability to criticize when necessary (Johnson 2018, 278–88). The dynamics of intelligence oversight tends to encourage ostriches and cheerleaders.

Incentives

The nature of intelligence oversight also affects the incentives for lawmakers to serve on the intelligence committees and to devote time to these issues if they do. A study in the 1970s of individual members of Congress found the three primary goals for legislators that guide the activities they choose to pursue: (1) reelection, (2) power and influence within the chamber and (3) good public policy. Legislators prioritize these in different ways (Nolan 2007, 124–5). Membership on one of the intelligence committees only reliably helps with the third goal.

Service on the intelligence committees produces little tangible benefit to a lawmaker’s constituents. It does not benefit local businesses, assist with infrastructure, improve the economy or address any day-to-day local concerns. It is possible, depending on what is happening in the world and the interests of constituents in a particular district, that an intelligence role will enhance a legislator’s reputation for seriousness among constituents. It is difficult for a committee member to capitalize on that role, however, because they cannot discuss their work publicly. Power within the Congress comes from many things, but a significant public profile and the ability to deliver something of use for fellow members, either politically or legislatively, are useful in pursuing influence among colleagues. Intelligence committee work typically produces neither of these things.

As a result, this is the situation intelligence committee members face: they have to work harder to obtain the information they need to do their job, they have difficulty developing expertise because of access restrictions and a lack of non-Intelligence Community sources of expertise, they lack sufficient leverage to produce positive oversight results, they get little or no press attention for the work they do, which rarely helps them get reelected, and they stand a good chance of being blamed for Intelligence Community failures if they occur. It is no wonder

that legislators either to avoid work on the intelligence committees or, if they cannot do that, do not prioritize their intelligence work.

Partisanship

A relatively recent phenomenon – the rise of partisanship on the intelligence committees – has had a significant impact on congressional oversight of intelligence. Avoiding partisanship was a key goal when Congress created the intelligence committee structure. This was, for example, the reason they were established as select committees, whose members would be chosen by leaders, rather than through the more political process used for standing committees. For most of their history, the committee leaders have respected this intent and avoided partisanship in their conduct of committee business. There were some breakdowns over the years, over the Reagan Administration policy towards the Contras, for example, and nominations for Director of Central Intelligence in the administrations of George HW Bush and Bill Clinton (Kibbe 2010, 39–40). But the committees largely returned to their bipartisan nature afterwards.

During the George W Bush Administration partisan relationships on the committees began to fray again, largely over committee Democrats' desire to investigate intelligence failures in the run-up to the Iraq War (Kibbe 2010, 40). The partisan breakdown of the committees continued through the Obama and Trump Administrations. During the Trump Administration, partisan rancour over investigation of the Russian interference with the 2016 election and, later, the impeachment of President Trump, caused the HPSCI to become largely dysfunctional.

Partisanship undermines effective oversight in many ways. It has interfered with the ability to pass intelligence authorization legislation, which is perhaps the single most important committee function. It also makes responsible investigation of intelligence failures and abuses less likely. More subtly, partisanship alters the focus of overseers. They become more interested in pursuing issues that can harm the other party or avoiding those that will harm their own. These interests crowd out focus on the crucial, complex, long-term problems of intelligence oversight.

Jurisdictional issues

When the House and Senate created the intelligence committees, the idea was that they would be the primary sources of oversight for the Intelligence Community. Their ability to control the authorization of appropriations would be their strongest oversight weapon. Some quirks of congressional structure, however, undermine the intelligence committees' authority considerably. One committee in each house of Congress is responsible for the appropriation of the entire executive branch budget. This means the committees with the power to authorize appropriations cannot assure that their carefully considered budget judgements will find their way into the final appropriation legislation. This is the same for all authorizing committees, but it has proven to be a particular problem for the intelligence committees because of another historical practice.

The intelligence budget has always been classified and housed in a classified section of the much larger defence appropriation. The purpose is to prevent adversaries from discovering intelligence capabilities by analyzing the intelligence budget. This means that the intelligence budget, unlike most key appropriations, does not have its own subcommittee. Instead, the Defense Subcommittees of the appropriations committees also handle the intelligence budget. Since 2009, at the recommendation of the 9/11 Commission, the Director of National Intelligence has declassified and released the “top line” budget number for the National Intelligence Program (NIP). This means it is no longer necessary to bury the top line number in the defence budget, which addresses one of the key reasons for combining the appropriations. Nonetheless, the structure remains and the subcommittee that considers the much larger defence appropriation has intelligence as a side duty (Kibbe 2010, 30).

That does not mean that the appropriators have no views on intelligence matters. It is not unusual for the appropriations committee to fund less than the authorizers have recommended or – potentially more problematic – fund programmes that the intelligence committees have specifically declined to authorize (Kibbe 2010, 31–2). Appropriators sit much higher in the congressional power hierarchy than the intelligence committees. Thus, despite the intelligence authorizers’ greater expertise and attention to intelligence issues, the appropriators usually win these battles, when they occur.

Additional observations on effectiveness of oversight

Structural weaknesses

The dynamics discussed earlier combine to pose hardships for congressional intelligence oversight that are greater than in other areas. Some of these problems are fixable, or at least could be alleviated. There have been proposals for decades to improve the strength of intelligence oversight by restructuring committee responsibilities in the House and Senate, whether by creating a joint House-Senate intelligence committee – the most ambitious and least realistic proposal – combining authorization and appropriation responsibilities in each chamber or, most modestly, creating stand-alone intelligence subcommittees on the appropriations committees (National Commission on Terrorist Attacks on the United States 2004).⁹

The purpose of each of these proposals is to boost the power and leverage of intelligence overseers. But Congress so far has proven incapable of structural reform. As the 9/11 Commission noted, “Few things are more difficult to change in Washington than congressional committee jurisdiction and prerogatives. To a member, these assignments are almost as important as the map of his or her congressional district” (National Commission on Terrorist Attacks on the United States 2004, 419). Powerful committee chairs, particularly on the appropriations committees, are unwilling to give up turf and there is no real constituency among other members for the change. The 9/11 Commission recognized this fact when it

said its structural recommendations for Congress, including the merging of intelligence authorization and appropriation responsibilities, were among its most important, but also the least likely to be implemented (National Commission on Terrorist Attacks on the United States 2004, 419).

The value of statutory requirements

Some of Congress's greatest successes have come when it weathered executive branch opposition and imposed process and notification requirements by statute. The executive branch resists statutory obligations out of a concern that they will reduce the President's flexibility on national security issues. Nonetheless, Congress has at times managed to capitalize on the right political environment – usually after a major intelligence scandal or failure – to get it done.

An example of such a success is the regulation of covert action. The Hughes-Ryan Amendment and subsequent reforms transformed covert action from chaotic and virtually ungoverned to a careful, deliberative process that is taken seriously within the executive branch and reliably communicated to intelligence committee overseers. One of the most important aspects of the reforms was the requirement for presidential sign-off on any covert action programme. This requirement recognizes that no matter how effective external oversight is, it can never succeed without strong oversight within the entities carrying out the activities. By requiring the president to be involved, Congress created an incentive for the bureaucracy to professionalize itself, both to protect the president from embarrassment and to protect the agencies from presidential wrath. One of the Church Committee's observations about the covert operations they reviewed was that they often had few "fingerprints" on them. There was no record of who approved or designed them, so nobody could be held accountable. Particularly in an area like covert action that is prone to abuse, it is critical to have awareness – and accountability – at the top. By imposing statutory process requirements, Congress assured this accountability exists with covert action.

Another example of effective obligations imposed by statute are the notification requirements imposed with the Intelligence Oversight Act of 1980 and subsequent legislation. These acts require the Intelligence Community to keep the committees "fully and currently informed" of intelligence activities, including "any significant anticipated intelligence activity" and any illegal activities or significant intelligence failures. Despite their vagueness and the difficulties that remain for the intelligence committees in getting information from the executive branch, these requirements have had a major, positive impact on the information flow.

The executive branch prefers to be guided in its interactions with Congress by norms and informal understandings. These norms are often effective, but they can also fall away if a president does not respect norms and does not fear political repercussions for violating them. With statutory obligations, agencies may look for ways to skirt them or interpret them narrowly, but they are unlikely simply to ignore them. Thus, it is in Congress's institutional interests to capitalize on the rare opportunities it has to impose oversight requirements through legislation.

Investigation successes and failures

Investigations are one of the most powerful tools for congressional oversight. The history of their use for in intelligence oversight is spotty, however, with some shining successes and many disappointments. The Church Committee, one of the most thorough and influential congressional investigations on any subject, is the gold standard.

Another recent success – messier and more modest – was the SSCI investigation of the CIA’s detention and interrogation programme. This investigation began in 2009 as a bipartisan effort, with the minority Republicans supporting the Democratic majority. The investigation process was not smooth. There were many disagreements between the agency and the committee staff, some extremely bitter and public. The Republicans eventually withdrew their support for the inquiry, which was approved on a partisan vote – only one Republican senator voted with all of the Democrats. But in 2012 the committee completed a 7000-page report and in 2014, after a sometimes painful process, obtained the Obama Administration’s final approval to release a redacted version of the 500-page executive summary. The published official report of the SSCI investigation provides a clear and disturbing picture of the CIA’s activities and treatment of detainees in the post-9/11 period (Senate Select Committee on Intelligence 2015). Although the CIA disputes the accuracy of parts of the report, the investigation has provided a public historical record that otherwise might not have existed of a dark episode in the history of US intelligence.

Other recent intelligence investigations have had more mixed results. The SSCI investigation of Russian interference in the 2016 election, for example, produced five bipartisan volumes of reports that, although they did not receive as much attention as they deserved, were well-regarded. A HPSCI Investigation of the same subject, on the other hand, resulted in a partisan melt-down that left the committee largely dysfunctional.

It is impossible to account for all of the circumstances that make some investigations succeed while others fail or never get off the ground. One similarity between the Church Committee and SSCI Torture investigations that might be relevant is that they both were charged with reviewing past actions that posed little political threat to the administration in power. In both cases the CIA opposed the efforts vigorously, but the executive branch political leadership was more forthcoming, if reluctantly.

Conclusion

An effective, responsible intelligence community guided by law with internal checks and a sense of accountability to the public is an important and realistic goal in the United States. Key to achieving that goal is strong external oversight from Congress. The intelligence community will always be “chiefly concerned with achieving the objectives of the president, whatever they might be. Because of this, it is sometimes tempted to downplay the risk and accentuate the gain” of

intelligence activities (Snider 2008, 307). Congress's relative distance from the role of planning and carrying out the activities allows it to be a needed dispassionate voice that corrects for this inherent bias.

Congressional oversight of intelligence has come a long way since its early days and Congress can point to many successes along the way. Nonetheless, inherent challenges of overseeing intelligence and the idiosyncrasies of congressional structure and incentives assure that this oversight will be inconsistent and flawed. Congressional oversight in the United States will remain, to paraphrase Winston Churchill, the worst form of oversight other than all the others we have tried.

Notes

- 1 Prior to formation of these subcommittees, what minimal oversight there was came from congressional defence committees (Snider 2008, 3).
- 2 The House followed suit in February and established a select committee, chaired first by Rep. Lucien Nedzi and later by Rep. Otis Pike. The House Committee proved to be less effective than its Senate counterpart and never officially published a final report (Snider 2008, 275–8).
- 3 In an effort to discourage partisanship in this sensitive area, the committees were established as “select” committees, for which party leaders would appoint the members, rather than going through the party caucuses, as happens with typical standing committees.
- 4 Intelligence Authorization Act for Fiscal Year 1981 (Intelligence Oversight Act 1980), §501(a) (1980).
- 5 Intelligence Authorization Act for Fiscal Year 1991, Pub. L. No. 102–88 (1991).
- 6 Intelligence Authorization Act for Fiscal Year 1981 (Intelligence Oversight Act 1980) Pub. L. No. 96–450 (1980); Intelligence Authorization Act for Fiscal Year 1991, Pub. L. No. 102–88 (1991); National Security Act of 1947, USC 50, §§3001 et. seq. (1947).
- 7 During its investigation of Russian election interference, relations between the majority and minority deteriorated to the point that the Republican committee majority reportedly planned to erect a physical barrier to separate the majority and minority staffs. The plan was abandoned (Grazis 2018).
- 8 See https://fas.org/sgp/othergov/olc_nuccio.html
- 9 Indeed, Senate leadership took the step to order the creation of such a subcommittee but has never implemented the change.

References

- Bahar, Michael, Michael Geoffroy, Matthew R. A. Heiman, and Heather Molino. 2018. “The Role of Congressional Intelligence Committees”. *Teleforum*, April 18. <https://fed-soc.org/events/the-role-of-congressional-intelligence-committees>.
- Baker, James E. 2007. *In the Common Defense: National Security Law for Perilous Times*. 1st edition. Cambridge; New York: Cambridge University Press.
- Clark, Kathleen. 2012. “Congressional Access to Intelligence Information: The Appearance of a Check on Executive Power”. SSRN Scholarly Paper ID 2112081. Rochester, NY: Social Science Research Network. <https://doi.org/10.2139/ssrn.2112081>.
- Cumming, Alfred. 2010. *Congress as a Consumer of Intelligence Information*. Washington, DC: Congressional Research Service. <https://fas.org/sgp/crs/intel/R40136.pdf>.
- Decker, Brian. 2006. “‘The War of Information’: The Foreign Intelligence Surveillance Act, Hamdan V. Rumsfeld, and the President’s Warrantless Wiretapping Program”. *University of Pennsylvania Journal of Constitutional Law* 9 (1): 291–356.

- Fisher, Louis. 2008. "Congressional Access to National Security Information". *Harvard Journal on Legislation* 45 (1): 219–35.
- Ford, Christopher M. 2006. "Intelligence Demands in a Democratic State: Congressional Intelligence Oversight". *Tulane Law Review* 81 (3): 721–76.
- Grazis, Olivia Victoria. 2018. "House Intel Committee Plan to Build Physical Wall Is Shelved". *CBS News*, March 8. www.cbsnews.com/news/house-intelligence-committee-physical-wall-plan-shelved/.
- Johnson, Loch K. 2018. *Spy Watching: Intelligence Accountability in the United States*. New York, NY, USA: Oxford University Press.
- Kibbe, Jennifer. 2010. "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?". *Intelligence and National Security* 25 (1): 24–49. <https://doi.org/10.1080/02684521003588104>.
- McCubbins, Mathew D., and Thomas Schwartz. 1984. "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms". *American Journal of Political Science* 28 (1): 165–79. <https://doi.org/10.2307/2110792>.
- National Commission on Terrorist Attacks on the United States. 2004. *The 9/11 Commission Report*. Washington, DC: US Government Printing Office. www.9-11commission.gov/report/911Report.pdf.
- Nolan, Cynthia. 2007. "More Perfect Oversight: Intelligence Oversight and Reform". In *Strategic Intelligence: Intelligence and the Quest for Security*, edited by Loch K. Johnson. Westport, CT: Praeger Publishers Inc.
- Schwartz, Jr., Frederick. 2007. "Intelligence Oversight: The Church Committee". In *Strategic Intelligence: Intelligence and the Quest for Security*, edited by Loch K. Johnson. Westport, CT: Praeger Publishers Inc.
- Senate Select Committee on Intelligence. 2015. *The Senate Intelligence Committee Report on Torture: Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*. 1st edition. New York: Skyhorse Publishing.
- Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. 1975. *Alleged Assassination Plots Involving Foreign Leaders*, 94–465. Washington, DC: US Government Printing Office. www.intelligence.senate.gov/sites/default/files/94465.pdf.
- . 1976a. *Foreign and Military Intelligence, Book I*, 94–755. Washington, DC: US Government Printing Office.
- . 1976b. *Intelligence Activities and the Rights of Americans Book II*, 94–755. Washington, DC: US Government Printing Office. www.intelligence.senate.gov/sites/default/files/94755_II.pdf.
- Snider, L. Britt. 2008. *The Agency and the Hill: CIA's Relationship with Congress, 1946–2004*. Washington, DC: Center for the Study of Intelligence.

14 Accountability for covert action in the United States and the United Kingdom

*Mitt Regan and Michele Poole*¹

States sometimes decide to conduct activities against adversaries without acknowledging their involvement in them. The decision to engage in such covert action creates a fundamental tension between the need for a state to fulfil its national security responsibilities and the principle that citizens in a liberal democracy should be informed about actions taken in their name so they can hold government accountable them (Lester 2015). Both the United States (US) and the United Kingdom (UK) have engaged in covert action for quite some time (Daugherty 2004; Cormac 2018). This chapter examines how each manages this tension. It reveals that, even as they accept the importance of accountability, liberal democracies may define the concept differently and use different mechanisms to provide it.

Definition of covert action

United States

The National Security Act of 1947² established the Central Intelligence Agency (CIA) and charged it with collection of foreign intelligence and the performance of “such other functions and duties related to intelligence affecting the national security as the National Security Council may from time to time direct”.³ The latter function was the basis for the agency’s involvement in covert action until such operations were explicitly authorized by statute in 1991 (Snider 2008, 140).

Congress codified the definition of covert action in the 1991 Intelligence Authorization Act. That defines covert action as “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly”.⁴ The statute provides that covert action does not include intelligence collection, and traditional diplomatic, military and law enforcement activities.

This definition distinguishes covert action from clandestine activities, which often are carried out by military units, especially Special Operations Forces. The distinction between intelligence collection and covert action ostensibly is that the

former involves passive information gathering, while the latter involves operations designed to affect the environment. The line is not a sharp one, however. Covert action can generate considerable intelligence even if that is not its primary goal and such operations obviously rely on accurate intelligence in order to be effective.

United Kingdom

Unlike the US, the UK has no statutory definition of covert action. Military doctrine describes covert action as operations “planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor” (Cormac 2018, 5). A recent report by the Intelligence and Security Committee of Parliament, a body discussed in more detail in the following, distinguishes between intelligence “coverage” and “effects”, with covert action falling within the latter category. As the report describes,

Intelligence coverage is the collection of information (or acquisition of information from allied intelligence services) by the Agencies and Defence Intelligence. Intelligence effects describe the Agencies’ and Defence Intelligence’s engagement in activities that have real-life outcomes.

(Intelligence and Security Committee of Parliament 2020, 26)

The Secret Intelligence Services or MI6 has described its work as including “using covert contacts overseas to shape developments and exploit opportunities in the UK’s interest” (Cormac 2018, 5) and leaked documents indicate that the Government Communications Headquarters (GCHQ), which has primary responsibility for signals intelligence, has its own “‘online covert action’ programme” (Cormac 2014).

Unlike the US, the UK does not formally or publicly distinguish between covert and clandestine action, nor between covert action and intelligence gathering. In contrast to the CIA, MI6 does not have its own paramilitary assets and so must work closely with UK Special Forces (UKSF). Indeed, UKSF are regarded as an asset that may be utilized by any agency when necessary. UK covert action thus consists of activities the US would consider clandestine military operations not subject to its covert action statute. Similarly, UK agencies do not have the resources that would enable them to clearly distinguish intelligence collection and covert action. This contrasts with the CIA, which has separate offices responsible for intelligence and operations.

The absence of sharp distinctions also is consistent with the UK’s emphasis on secrecy as essential to operational effectiveness. Both law and custom reflect a UK tradition in which government is provided considerable deference and flexibility in matters of national security (Cormac 2018, 5). As the discussion below describes, a broad conception of covert action creates challenges for any effort by Parliament to exercise effective oversight of this activity.

Responsibility for covert action

United States

Executive Order 12,333 provides that “[n]o agency except the Central Intelligence Agency . . . may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective”. The Directorate of Operations in the CIA oversees the Special Activities Center (SAC), which is responsible for conducting covert action. Within the SAC are the Special Operations Group (SAC/SOG), responsible for covert paramilitary operations, and the Political Action Group (SAC/PAG), responsible for covert political action, and psychological, economic and cyber operations (Harper 2015). SAC/SOG is largely comprised of former and current US Special Operations Forces. When active duty service members conduct covert action, they typically do so under the legal authority of the CIA Director, such as occurred in the operation that resulted in the death of Osama bin Laden.

The National Security Agency (NSA) was established by President Truman in 1952 to provide unified control over communications intelligence activities (Homeland Security Digital Library 1952). The mission of the NSA has expanded beyond the collection of communications intelligence to include offensive cyber operations, which almost certainly include covert action. In 2010 US Cyber Command (CYBERCOM) was created under the command of the then director of the National Security Agency. Its mission is to “direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners”.

A component of the military available to assist in covert action is US Special Operations Forces (SOF). US Special Operations Command (SOCOM) oversees SOF from the Army, Air Force, Navy and Marines, as well as a Joint Special Operations Command (JSOC), which is itself comprised of units from each of the services. SOCOM reports directly to the Secretary of Defense and the President. JSOC’s primary mission is to train and conduct special operations missions in support of traditional military operations, but elements of the force are sometimes placed under the legal authority of the CIA for the conduct of covert operations.

The National Security Council (NSC) serves as an important mechanism to coordinate covert action, based on its responsibility to “advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security”. The National Security Act of 1947 placed the CIA under the National Security Council and the NSC works to coordinate covert action across relevant government agencies.

Finally, the exception for traditional military activities under the covert action statute means that the military may conduct some covert operations that are not subject to the requirements of the statute. Recent legislation established that, in addition to kinetic activity, this exception includes cyber and information operations. As the discussion below describes, such activities are subject to separate requirements that resemble those in the covert action statute.

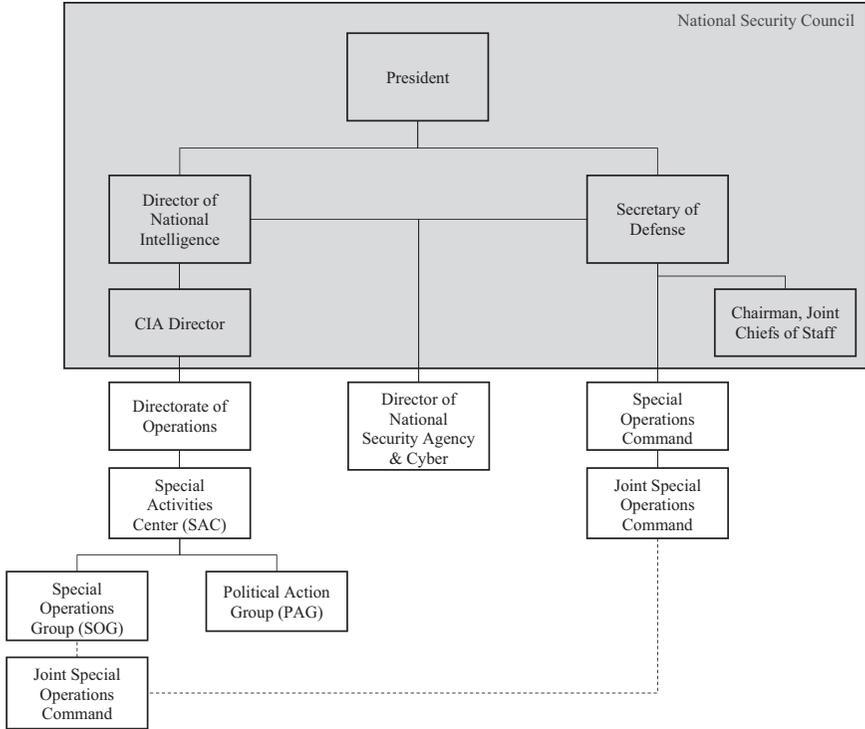


Figure 14.1 US components with responsibility for covert action.

Figure 14.1 depicts the elements of the US government with responsibility for covert action operations.

United Kingdom

As far as is possible to discern, UK covert action is not solely, or even mainly, the preserve of one agency. The Secret Intelligence Service (MI6) and/or the Government Communications Headquarters (GCHQ), which is responsible for signals intelligence, are the most likely agencies to undertake it. The Security Service (MI5) theoretically could do so but this is much less likely given its domestic remit. Covert action also has allegedly been conducted by other entities such as the Research, Information and Communications Unit (RICU), the UK’s specialist strategic communications unit that conducts counter-jihadist propaganda. Covert action by the UK thus is decentralized, dependent on the resources and needs of various agencies with respect to particular operations. Equally or even more important are the needs of various offices such as the Foreign and Commonwealth Office (FCO). Traditionally, the FCO has had the responsibility of officially

signing off on covert action, but it is unclear how much it has been involved in initiating it.

The lack of a single agency with primary responsibility for covert action not only reflects practical considerations, but is also consistent with the UK tradition of providing minimal information about the responsibilities of its intelligence and security agencies. For example, in 1924, 15 years after MI5 was created, the British Foreign Secretary declared during Parliamentary debate,

It is the essence of a Secret Service that it must be secret, and if you once begin disclosure it is perfectly obvious to me as to Hon. Members opposite that there is no longer any Secret Service and that you must do without it.

(Andrew 2009, 753)

This philosophy persisted until late in the twentieth century and did not change until judicial decisions and scandal prompted reforms. In 1987, in a case involving Sweden, the European Court of Human Rights ruled that privacy provisions of the European Convention on Human Rights required that infringement on human rights “must have some basis in domestic law . . . [and] the law in question must be accessible to the individual concerned and its consequences for him must also be foreseeable” (Andrew 2009, 758). The Security Service Act of 1989 then explicitly incorporated MI5 into British law as a statutory domestic security service. Its most significant responsibility is

the protection of national security, and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.

The impetus for comparable legislation regarding MI6 and GCHQ was the 1992 trial of three businessmen prosecuted in the Matrix Churchill scandal for illegal arms sales to Iraq. The trial revealed that MI6 had been aware of and advised the defendants on the sales and had been using the intelligence provided by one of them. The trial collapsed as a result and the Intelligence Services Act (ISA) of 1994 was passed in the midst of the three-year judiciary inquiry of the scandal (Gill 2007, 20). ISA formally established the Secret Intelligence Service (SIS), or MI6, as the UK foreign intelligence service and the GCHQ as its signals intelligence agency.

Two elements of the UK’s uniformed military services conduct or support covert action – Defence Intelligence (DI) and UK Special Forces (UKSF). DI is a component of the Ministry of Defence (MoD) and conducts all-source intelligence analysis “providing intelligence products and advice to policy, deployment and research decisions”. It provides support to planning and execution of covert action operations and benefits from intelligence collected during them.

Since 1987 UK Special Forces have existed as a separate directorate in the Ministry of Defence comprised of components from the British Army and Royal

Navy, later expanded to include the Royal Air Force. UK Special Forces conducts “short notice high risk operations in support of UK interests” under Joint Forces Command (Joint Forces Command n.d.). They are funded through the Ministry of Defence, but are considered a national asset for covert action, with a subset of UKSF serving the Secret Intelligence Service (Cormac 2018, 9). UK Special Forces is the last remaining government organization on which the government refuses to comment. There is an absolute exemption for UKSF under the Freedom of Information Act 2000 and it is government policy “not to comment, and to dissuade others from commenting or speculating, about the operational activities of Special Forces because of the security implications” (Directorate of Special Forces n.d.).

Finally, in 2010, Prime Minister David Cameron created the National Security Council (NSC) as a Cabinet committee to coordinate the government’s work on national security, including the management of covert action (Cormac, Goodman, and Holman 2016, 15). The NSC is chaired by the Prime Minister, includes ten other Ministerial members, and can draw upon other senior government officials like the Chief of the SIS or Director of GCHQ, if their presence is relevant to the issues before the council (Devanny and Harris 2014, 24). It is supported by a secretariat of approximately 200 officials led by a National Security Adviser (NSA) (Devanny and Harris 2014, 25, 27). Operations that require inter-department cooperation are likely to be reviewed by the NSC. Certain MI6 operations involving the FCO, however, are more likely to be reviewed by the Foreign Secretary, who will be the dominant cabinet figure overseeing such operations.

Regulation and oversight of covert action

United States

US conduct of covert action is subject to a detailed set of regulatory requirements that are designed to further both rigorous internal Executive branch review and informed oversight by Congress. From the creation of the CIA in 1947 through the mid-1970s, covert action was relatively unregulated and not explicitly subject to Congressional oversight. This changed as a result of hearings in the House and Senate in 1975. These produced evidence suggesting some CIA connection to events that resulted in the attempted or successful assassination of foreign leaders (Weiner 2008). They also revealed extensive surveillance of persons within the United States based on political beliefs and perceived national security risks (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities 1976; 1975). The result was a series of reforms beginning in the mid-1970s that culminated in the Intelligence Authorization Act of 1991, which set forth the current statutory regime of regulation.

The main requirements of the US covert action statute are that the president must make a written finding in support of a covert action and must notify the Congressional intelligence committees before the action begins. The finding must reflect the president’s determination that “such an action is necessary to support

identifiable foreign policy objectives of the United States and is important to the national security of the United States". The President "may not authorize any action that would violate the Constitution or any statute of the United States".⁵ While notification may occur after a programme has been initiated, informal practice generally has been that it will occur within 48 hours. The statute provides:

If the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States, the finding may be reported to the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President [this is known as the "Gang of Eight"].

If the president elects to notify only the Gang of Eight, the intelligence committees of the House and Senate must be informed of this decision.

The provision that prohibits authorization of covert action in violation of the US Constitution or any US statute has been construed by the Executive Branch to permit the president to authorize covert action in violation of any US international law obligations that have not been incorporated into US law. Most notably, this would include the customary international law prohibition on intervention into the sovereign functions of another state.

The notification obligation of the president applies to covert action programmes, which may consist of several individual operations. The president must inform Congress of each programme, but is not required to provide notification prior to each separate operation. In addition, the president must notify Congress of any significant change in a previously approved covert action programme.⁶ Notification for these purposes generally takes the form of a Memorandum of Notification (MON). One expert on covert action suggests the MON requirement is important because a presidential finding may be in broad language. Thus, "where and how the president, his policymakers, and his lawyers define these threshold terms can be critical in determining what measure of internal and then external review [that] specific initiatives or operational proposals receive, if any" (Baker 2010). The statute imposes additional requirements on relevant agencies to keep congressional intelligence committees fully informed of covert action activities, "including significant failures" (Baker 2010).

The requirement of a written Presidential finding has resulted in the creation of procedures within the Executive branch for review and approval of covert action. Typically, the president sends the CIA a request for a covert action finding. That agency engages in an extensive analysis, which includes consultation with its station chiefs in all countries that may be affected by a programme. Review occurs at several levels of the agency, eventually resulting in a proposed finding that is sent to the CIA Director. One report suggests that there is some contact between the CIA and Congress even in advance of the submission of a proposed presidential finding:

According to a CIA officer with paramilitary experience, once the CIA begins to plan a covert action and define the terms of the finding, they begin to “socialize” the idea with the [House and Senate Intelligence Committee] chairmen. This opens up a dialogue with Congress, albeit limited in its scope, which affords an opportunity to address any initial questions that arise.

(Rudd 2015, 10)

When the director transmits the finding to the White House, it goes to an inter-agency working group for covert action that involves representatives from the State Department, the Defense Department, the Joint Chiefs of Staff, Office of Management and Budget and the Justice Department. After review by this group, it goes to the National Security Council, which submits to the president a recommendation, including all dissents, on each proposed covert action. Once the NSC presents a proposed finding to the president for his or her approval, the president notifies the Congressional intelligence committees. A separate document describes policy objectives, the plan of action, an assessment of the risks involved and a description of the resources that will be required.

The exclusion of traditional military operations from the statutory definition of covert action means that any covert military activities are not subject to the procedures set forth in the statute. There are, however, regulatory provisions that resemble those in the statute for specific types of military operations. The Secretary of Defense is required to notify the Congressional Armed Services committees no less than 48 hours before initiation of a “sensitive military operation”, which is defined as a lethal or capture operation against a specific person or persons outside certain conflict theatres. This requirement serves to furnish Congress with timely information about unacknowledged SOF operations. In addition, the Secretary of Defense must notify the Armed Services Committees no less than 15 days before using funds authorized for payment to foreign and local groups and must file an annual report summarizing SOF counter-terrorism operations assisted by groups receiving these funds.

Any “clandestine” military cyber operation that is covert must be authorized by the president or the Secretary of Defense.⁷ This requirement is similar to the requirement of a presidential finding under the covert action statute, although it is unclear the extent to which it involves consultation with multiple agencies as occurs with a covert action finding. The Secretary of Defense must notify the Armed Services Committees within 48 hours of any cyber operations outside theatres of hostilities. Legislation also exempts from the covert action statute military information operations “short of hostilities and in areas outside of areas of active hostilities”. The Secretary of Defense must report to the Armed Services Committees any “significant” such operations conducted by the Department in the preceding quarter.⁸

United Kingdom

Rory Cormac suggests that there may be at least two mechanisms in the UK for executive oversight of covert action. One is the Foreign Office, which by statute

must approve any such operation (Cormac 2018, 13). The other is the National Security Council (NSC) described earlier. Cormac notes that:

[t]here is some suggestion that the NSC is now the primary forum for covert action tasking and scrutiny. This may be because it brings together the heads of the agencies and the military with the PM and key cabinet members like the Foreign and Defence Secretaries on a weekly basis. The NSC and Foreign Office processes may work together or could be used interchangeably depending on operational needs.

With respect to oversight by Parliament, the 1994 Intelligence Services Act created the first parliamentary oversight mechanism, the Intelligence and Security Committee (ISC). The Act described the Committee's mandate as "to examine the expenditure, administration, and policy" of MI5, MI6 and GCHQ. The Committee was granted access to classified material. There were concerns, however, that it was insufficiently independent because, although comprised of members of Parliament, it was not a parliamentary committee but a statutory committee appointed by and reporting to the Prime Minister.

The Justice and Security Act of 2013 and the resulting Memorandum of Understanding Agreed Between the Prime Minister and the Intelligence and Security Committee of Parliament substantially changed the structure, authority and mandate of the ISC (Intelligence and Security Committee of Parliament 2014, 11). Members are now nominated by the Prime Minister and appointed by a vote of their relevant House of Parliament (Intelligence and Security Committee of Parliament 2014, 11). The ISC now has its own staff – the ISC Secretariat – although members are seconded from the Cabinet Office. The ISC reports its findings to the Prime Minister, who then reports them to Parliament with redactions of sensitive information. Only the Secretary of State may withhold information from the ISC, on the ground that "it is sensitive and should not be disclosed to the ISC in the interests of national security". Information can be withheld from other parliamentary committees if the Secretary of State thinks "it proper not to do so" and is "not limited to national security" grounds (Dawson 2020, 8). Notwithstanding this, the Prime Minister retains significant control over the process, as reflected, for instance, in delays in releasing ISC reports and in reconstituting the committee after an election.

The ISC's oversight authority was extended beyond the three major intelligence agencies to include the intelligence and security work of a number of other offices, including the Chief of Defence Intelligence (DI) and offensive cyber activities in the Ministry of Defence; the Joint Intelligence Organisation, National Security Secretariat and Assessments Staff in the Cabinet Office; and the Office for Security and Counter-Terrorism (OSCT) in the Home Office (Intelligence and Security Committee of Parliament 2014, 12).

The Committee's role with respect to covert action is entirely retrospective – that is, it has no role in oversight of operations before or while they were taking place. This reflects the preference of the ISC Chair, Malcolm Rifkind, at the time

that the committee was created. “There is no benefit, and a lot of risk”, Rifkind said, “in having been briefed in advance of a secret operation unless you can influence whether it goes ahead. Otherwise, you have responsibility without power, which is even worse than power without responsibility” (Rifkind 2016, 428).

In contrast to the US, one organization integral to covert action that remains free of parliamentary oversight is UK Special Forces (UKSF). The ISC is the only committee that has members cleared to review classified material, but it has no mandate to provide oversight of UKSF. The Defence and Foreign Affairs Committees that oversee the organizations to which UKSF are assigned have no security clearance. A member of the Foreign Affairs Select Committee raised this issue in November 2017, asking if the MoD would “undertake a review of access to information on Special Forces by Parliament to enable effective scrutiny”, and he was told, “Given the sensitivity of their activities, oversight of Special Forces is exercised through the Prime Minister and Defence Ministers. We have no plans to change the current arrangements”. The year before, the Defence Ministry representative refused to answer any of an MP’s questions related to the UK Special Forces, repeating seven times to seven separate questions, “I cannot comment on specific questions about personnel, equipment, discussions or activities in relation to these units” (Walpole and Karlshøj-Pedersen 2018, 4–6).

Comparative analysis

As the preceding discussion makes clear, there are not only some similarities but also some important differences in how the US and UK seek to ensure accountability for covert action. This section focuses on the main differences and their potential significance.

Definition of covert action and designation of lead agency

The US defines covert action in a statute that establishes requirements for engaging in such operations. That definition excludes some activities that may be conducted covertly, such as military activities. This results in different procedures and oversight mechanisms for activities formally defined as covert action and military covert operations that are not. Both require some form of notification of Congress, although military information operations need only be reported quarterly. Statutory covert action requires a presidential finding, while military covert action does not, although the Secretary of Defense presumably has a prominent role in the latter.

The designation of the CIA as primarily responsible for statutory covert action means that Congressional Intelligence committees exercise oversight over the CIA, while Armed Services committees do so over military covert operations. The US thus effectively has a parallel system of covert action accountability for CIA and military operations. Other agencies have interests in such operations and have opportunities to weigh in, most notably for CIA operations. It is clear, however, which agency has primary responsibility in each system.

By contrast, various UK agencies have definitions of covert action, but there is no statutory definition. Nor is any entity designated as the lead agency for such operations. The philosophy, perhaps shaped also by resource constraints, is that any given agency may have an interest in a particular operation and may have assets that are especially suitable for it. Covert action thus involves “[m]ultiple actors, often with diverging visions and goals”, which “require greater coordination” (Cormac, Goodman, and Holman 2016, 17). This creates the potential for counterproductive competition among agencies, although in practice MI6 generally takes the lead, with GCHQ also sometimes doing so. The NSC has the potential to coordinate operations, but it has broad responsibilities and less experience with covert action than its US counterpart.

This decentralized approach also may produce gaps in Parliamentary oversight. Unlike the US, there is no committee charged with covert action oversight. The ISC oversees the intelligence agencies, but since covert action is a means of executing foreign policy, the Foreign Affairs Committee (FAC) arguably has an interest in overseeing it. Oversight of covert action formally comes within the ISC remit, but until recently the committee had no authority to review operations in advance. With limited exceptions, it tends to focus on broad policy and strategic issues. In addition, since covert action may involve the military, the House of Commons Defence Committee (HCDC) could be involved. Because the line between covert action and intelligence can be indistinct, however, neither FAC nor HCDC are entirely natural oversight forums for covert action. Furthermore, the ISC is the sole committee whose members may view classified information, which as a practical matter prevents FAC and HCDC from conducting effective oversight.

Notification of the legislature

A significant difference between the US and UK covert action process is that the former requires advance notification of Congress while the latter does not. Parliament therefore is limited to retrospective review of operations. This reflects the historical preference of ISC leadership, which believes that advance notice would result in the committee sharing responsibility for operations without any authority to influence them.

Based on the US experience, it is not clear whether this concern is necessarily warranted. Congress has no statutory authority to approve or disapprove of any covert action, but it does have the potential to exercise influence (Cumming 2010, 5). The preparation of a finding by the CIA involves informal consultation with Congress, and formal notification historically has provided an opportunity for Congress to express its views on the practical, legal and political risks of proposed operations. Senator John Warner, who served on the Senate Intelligence committee, has written,

Congressional oversight has uncovered instances when covert actions were not properly reviewed or assessed within the executive branch. It has also

contributed to the reconsideration of activities or the particular details of their execution. On occasion, it has blocked some and terminated others.

(Warner 1989, 107)

The ISC thus may be forgoing an informal opportunity to shape covert action by declining to seek advance notification.

Oversight of special operations forces

Another major difference between the US and UK is that the former provides for Congressional oversight of SOF while the latter does not. US military covert action generally will be carried out by SOF. Military covert action is not subject to the requirements of the covert action statute, but the requirement that the Department of Defense notify the Armed Services committees of various kinetic, cyber and information operations provides a mechanism for oversight of military covert action in general and SOF in particular. By contrast, the UK has no statute authorizing SOF and declines to comment on their operations or existence. ISC members have security clearances, but that committee oversees the intelligence agencies. The HCDC may informally oversee SOF, but its members do not have access to classified information. The Ministry of Defence presumably engages in oversight, but of course is formally a member of the executive branch.

Washington and Westminster systems

Oversight of covert action by the legislature in the US and UK is of course affected by the differences in those countries' systems of government. The US sharply differentiates between the executive and Congress, with members of Congress prohibited from serving simultaneously in the executive branch. By contrast, the executive is a component of Parliament in the UK. The authority of the executive to govern in the UK is based on its dominance of Parliament, with the Cabinet composed mainly of leading members of the House of Commons. Thus, the chair of the UK ISC has been from the same party as the Prime Minister in all but four of the 25 years that committee has been in existence. By contrast, over that same period the chair of the House and Senate intelligence committees has been from the same party as the president only 32% and 50% of the time. More generally, since 1945 the House has been controlled by the opposing party 68% of the time and the Senate 50% of the time.

The timing of elections in the two systems also differs. The US has elections every two years for every House member and one-third of Senate members. Parliament may not exceed five years between elections, and the timing of those elections is usually determined by the Government, with 30 days' notice between announcement and the day of election (Peterson 2005). The work of the ISC may not carry over from one Parliament to the next and it and other committees must

be re-established after elections. After general elections, the ISC has been one of the last committees reconstituted.

[I]n the three years from 2015 to the end of 2017, Britain was without a legislative intelligence oversight body for almost 12 months. There were four terrorist attacks in the UK in the period in which the committee was in desuetude in 2017.

The situation has been described as “deeply unsatisfactory” (Defty 2019, 9).

Because US congressional elections occur at a regular interval, the outgoing Congress continues to sit during most of the period between election day and the swearing in of the new Congress. Committee assignments for the new Congress are decided during this time, which provides for continuity of oversight.

The lesser role of legislative oversight in providing accountability for covert action in the UK is reflected in the fact that although recent reforms to the ISC increased its authority to request information from the executive, the executive can refuse to provide such information with few repercussions. An example was a recent ISC inquiry into the decision-making behind drone strikes in Syria that resulted in the deaths of three UK citizens. The ISC announced that it planned to investigate the intelligence basis for the strikes. The Prime Minister responded that the strike was part of ongoing operations and therefore was beyond the scope of the Committee’s remit. He noted, however, the significant public interest in assessing the threat that one of the victims posed and asked the Committee to conduct an investigation confined to this question (Intelligence and Security Committee of Parliament 2017, 2).

The ISC conducted oral interviews and received the written intelligence assessments and reports that formed the basis for the threat determination. It requested information on targeting procedures, collateral damage estimates and other matters that were used in the decision-making. The executive refused on the ground that these were outside the scope of the investigation. ISC disagreed with that assessment and noted in its report that the unavailability of this information hindered its ability to provide a full review of the operation.

Finally, oversight of covert action by the US and UK also reflects cultural differences. The UK is more comfortable with secrecy by the executive and with unwritten policy and procedures, perhaps reflecting more trust in the government than exists in the US. The extensive formal regulatory provisions that govern covert action in the US reflected a tradition of greater distrust and emerged because of congressional hearings that revealed considerable questionable covert operations undertaken by the CIA from the end of World War II until the early 1970s.

Executive branch process

To the extent that there are limits on the ability of Congress or Parliament to oversee covert action, robust internal executive branch deliberation can further accountability by ensuring that decisions are informed by multiple perspectives that take into account a wide range of considerations. Crucial to this process is reason-giving, the

requirement that individuals be able to justify their positions to others. This requirement is especially important in settings in which many reasons cannot be publicly articulated, such as in the national security setting. In these situations, what Ashley Deeks calls secret reason-giving “improves the overall quality and effectiveness of government decision-making and operations, constrains the decision-maker, and strengthens the decision-maker’s legitimacy” (Deeks 2020, 616).

The requirement of a Presidential finding under the US covert action statute appears to foster this process within the executive branch. Extensive review of a proposed finding occurs within the CIA, sometimes involving informal consultation with Congress. The proposal is then sent to a working group comprised of members of several agencies, after which it is reviewed by the NSC before submission to the President. By the time a finding reaches the President, it has been reviewed by multiple individuals and organizations with varying expertise, perspectives and interests.

In the UK, “there needs to be particular emphasis on robust internal deliberation within the executive, since the onus of ensuring meaningful covert action oversight rests almost entirely” on this mechanism (Djabatey 2018). It is possible that the process is as comparably as wide-ranging as in the US, but there is no public information about it. The Foreign Office historically has been required to authorize covert action and may serve to coordinate consideration of proposed operations. Its influence at least in theory has meant that British covert action is tied to foreign policy and has given British covert action a generally cautious character (Djabatey 2018). On the other hand, the NSC now may have assumed the primary coordinating role, since it brings together the heads of the agencies and the military with the PM and key cabinet members on a weekly basis. Inter-agency consultation in the UK does not appear to be as formalized as it is in the US, but the NSC has the potential to foster this practice. In addition, interagency bodies that allegedly engage in forms of covert action exist, such as the RICU. The NSC and Foreign Office processes may work together, or could be used interchangeably depending on operational needs.

In any event, more transparency about the UK process could serve to enhance a sense of accountability for covert action. With respect to the US targeted killing programme, for instance, disclosure of the process for selecting targets, albeit as a result of litigation, provided the public with a greater understanding of the parties involved in the process, the criteria they apply and the evidence required at each step of the deliberations. Such disclosure also can provide at least general standards by which the public can assess the programme. Something comparable for UK covert action could both provide reassurance of rigorous deliberation and encourage officials to engage in it.

Conclusion

US covert action is explicitly authorized and regulated by publicly available standards, in contrast with the UK’s reluctance to formalize or disclose the process for conducting such activity. This likely reflects much greater reliance by the US

on covert action than the UK, the sharper separation of powers in the US system, and greater resources that allow the US to differentiate among intelligence, covert action and unacknowledged military operations. While the US system does not automatically ensure full accountability for covert action, it does at least provide some public standards against which it can be evaluated.

Other factors that contribute to the differences between the two systems may be the UK's history of greater reliance on and confidence in elites and a preference to avoid clear lines of demarcation in order to preserve freedom of action. Nonetheless, there is growing public demand for government transparency and for accountability even for secret operations. With a weaker system of legislative oversight than in the US, the UK may need to disclose more information about executive branch decision-making on covert action to meet this demand.

Notes

- 1 We are grateful for comments on a draft of this chapter by Rory Cormac.
- 2 National Security Act of 1947, Pub. L. No. 80–253, 80th Cong. 1st sess (1947).
- 3 National Security Act of 1947, Pub. L. No. 80–253, 80th Cong. 1st sess, § 102(d)(5) (1947).
- 4 50 USC § 3093(e).
- 5 50 USC § 3093(a).
- 6 50 USC § 3093(d).
- 7 Legislation uses the term “clandestine” to emphasize that such operations are not subject to the covert action statute, but the definition of clandestine includes unacknowledged operations.
- 8 As with military cyber operations, clandestine information operations include those that are unacknowledged.

References

- Andrew, Christopher. 2009. *The Defence of the Realm: The Authorized History of Mi5*. London; New York: Allen Lane.
- Baker, James E. 2010. “Covert Action: United States Law in Substance, Process, and Practice”. In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson. New York: Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780195375886.001.0001>.
- Cormac, Rory. 2014. “GCHQ’s Cyber Offensive: Online Covert Action”. *Ballots & Bullets School of Politics & International Relations, University of Nottingham*, February 13. <https://nottspolitics.org/2014/02/13/gchqs-cyber-offensive-online-covert-action/>.
- . 2018. *Disrupt and Deny: Spies, Special Forces, and the Secret Pursuit of British Foreign Policy*. New York; Oxford: Oxford University Press.
- Cormac, Rory, Michael S. Goodman, and Tom Holman. 2016. “A Modern-Day Requirement for Co-Ordinated Covert Action”. *The RUSI Journal* 161 (2): 14–21. <https://doi.org/10.1080/03071847.2016.1174478>.
- Cumming, Alfred. 2010. *Sensitive Covert Action Notifications: Oversight Options for Congress*. Washington, DC: Congressional Research Service. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a514137.pdf>.
- Daugherty, William. 2004. *Executive Secrets: Covert Action and the Presidency*. Lexington: University Press of Kentucky.

- Dawson, Joanna. 2020. *The Intelligence and Security Committee Briefing Paper No. 02178*. House of Commons Library. <https://commonslibrary.parliament.uk/research-briefings/sn02178/>.
- Deeks, Ashley S. 2020. "Secret Reason-Giving". *The Yale Law Journal* 129 (3): 612–89.
- Defty, Andrew. 2019. "Coming in from the Cold: Bringing the Intelligence and Security Committee into Parliament". *Intelligence and National Security* 34 (1): 22–37. <https://doi.org/10.1080/02684527.2018.1513441>.
- Devanny, Joe, and Josh Harris. 2014. *The National Security Council National Security at the Centre of Government*. Institute for Government. www.instituteforgovernment.org.uk/publications/national-security-council.
- Directorate of Special Forces. n.d. "UK Special Forces". Accessed December 1, 2020. www.gov.uk/government/groups/directorate-of-special-forces.
- Djabatey, Edwin. 2018. "On the Difficulties of Examining British Oversight of Covert Action (Unpublished Manuscript)".
- Gill, Peter. 2007. "Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'War on Terror'". *Intelligence and National Security* 22 (1): 14–37. <https://doi.org/10.1080/02684520701200756>.
- Harper, Lauren. 2015. "First Complete Look at the CIA's National Clandestine Service Org Chart". *Unredacted: The National Security Archive Blog* (blog). October, 27. <https://unredacted.com/2015/10/27/first-complete-look-at-the-cias-national-clandestine-service-org-chart/>.
- Homeland Security Digital Library. 1952. "National Security Agency Established". *Homeland Security Digital Library*. www.hsdl.org/c/tl/national-security-agency-established/.
- Intelligence and Security Committee of Parliament. 2014. *Annual Report 2013–2014*. London: HMSO. http://isc.independent.gov.uk/files/2013-2014_ISC_AR.pdf.
- . 2017. *UK Lethal Drone Strikes in Syria*. London: HMSO. http://isc.independent.gov.uk/files/20170426_UK_Lethal_Drone_Strikes_in_Syria_Report.pdf.
- . 2020. *Russia*. London: HMSO. <https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl>.
- Joint Forces Command. n.d. "About Us". Accessed December 1, 2020. www.gov.uk/government/organisations/joint-forces-command/about.
- Lester, Genevieve. 2015. *When Should State Secrets Stay Secret?: Accountability, Democratic Governance, and Intelligence*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9781107337015>.
- Peterson, Eric R. 2005. *Parliament and Congress: A Brief Comparison of the British House of Commons and the U.S. House of Representatives*. Washington, DC: Congressional Research Service. <https://fas.org/sgp/crs/misc/RL32206.pdf>.
- Rifkind, Sir Malcolm. 2016. *Power and Pragmatism: The Memoirs of Malcolm Rifkind*. 1st edition. London: Biteback Publishing.
- Rudd, Joshua. 2015. "Enhancing Congressional Oversight of DOD Clandestine Activities: A Case Study of SOF CT Paramilitary Operations". United States Army War College. <https://duke.app.box.com/s/p6quvogzdsupnkon3rlx87rrejs1xt8x>.
- Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. 1975. *Alleged Assassination Plots Involving Foreign Leaders*. Washington, DC: US Government Printing Office. www.intelligence.senate.gov/sites/default/files/94465.pdf.
- . 1976. *Intelligence Activities and the Rights of Americans Book II*. Washington, DC: US Government Printing Office. www.intelligence.senate.gov/sites/default/files/94755_II.pdf.

- Snider, L. Britt. 2008. *The Agency and the Hill: CIA's Relationship with Congress, 1946–2004*. Washington, DC: Center for the Study of Intelligence.
- Walpole, Liam, and Megan Karlshøj-Pedersen. 2018. *Britain's Shadow Army: Policy Options for External Oversight of UK Special Forces*. London: Oxford Research Group Remote Warfare Programme. www.oxfordresearchgroup.org.uk/Handlers/Download.ashx?IDMF=9bdb8bdd-2502-478f-9468-ac75af830d37.
- Warner, John W. 1989. "Covert Action and Congressional Oversight". *Harvard International Review* 11 (3): 106–9.
- Weiner, Tim. 2008. *Legacy of Ashes: The History of the CIA*. Illustrated edition. New York: Anchor.

Part VI

Future directions



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

15 GEOINT and the post-secret world

Who guards the guards?

Robert Cardillo

We are fast approaching the time in which technology will enable a continuous sensing of all of the world's activity – 24 hours a day, seven days a week, 365 days a year. Such holistic collection will facilitate a detailed model of the planet and all that is happening on it. 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, such a world will demand a rethinking of privacy itself, 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 this chapter. While a definitive answer will not be delineated, I will present the key questions which will guide our thinking.

“Quis custodiet ipsos custodes?” literally means “Who will guard the guards themselves?” For our purposes, a variant of that translation will be more constructive: “Who watches the watchers?” In the past, the watchers were governments – for good and for bad – and the original driver for remote sensing technologies was national security. When the Iron Curtain was drawn across Europe, the US Government and its allies needed to access the denied territory of the Soviet Union in order to identify the magnitude of the military threat. Wrapped in layers and layers of secrecy, such access was first provided by the U-2 aircraft's intelligence, surveillance and reconnaissance mission (Lockheed Martin n.d.).

Over the next five years, the U2's innovation provided President Eisenhower with *unprecedented insight into denied territory and enhanced understanding of a critical threat* and over 100 flights collecting thousands of images. However on May 1, 1960, a Soviet SA-2 surface-to-air missile shot down a U2 aircraft, not only removing our ability to surveil our adversaries but also revealing our tactics, techniques and procedures (History 2018). We were blind and that blindness created doubt, uncertainty and risk.

That blindness lasted a little more than 100 days; on August 18, 1960, the then-top secret CORONA satellite programme took its first image from space, a grainy picture of a strategic Soviet airfield. The United States again had access to denied

territory, providing insight and an ultimate advantage over our adversaries. In 1995, Vice President Gore stated the CORONA satellites,

recorded much more than the landscape of the Cold War. In the process of acquiring this priceless data, we recorded for future generations the environmental history of the Earth at least a decade before any country on this Earth launched any Earth resource satellites.

(CIA 2015)

In order to collect such critical imagery intelligence, the creators of the CORONA satellite had to overcome many obstacles:

- determine a way to expose film via a shutter and lens system travelling at 23,500 mph
- solve for the necessary speed of the film feed system
- contain the exposed film
- eject the capsule of film
- send the capsule of film back through the atmosphere
- deploy a parachute at altitude
- modify an Air Force transport with a trapeze to catch the capsule as it floated down over the Pacific

All to say, it took innovative science and enormous investment amidst extraordinary secrecy to create the ability to document activity on earth from space.

Over the course of the next 50 years, there was a halting and gradual shift of that capability from the government to the commercial sector. This shift has recently accelerated, resulting in a sharp increase in commercial capabilities in space. Beyond the visible images captured in the electro-optical spectrum, there are now commercial radar satellites as well as those that capture radio frequencies and infrared.

With this rapid and steep commercial growth, some argue that we are entering into an era of geospatial “singularity”. This scenario

coined the GEOINT Singularity, is a future where real-time Earth observations with analytics are available globally to the average citizen on the ground providing a tremendous wealth of information, insight, and intelligence.

(Koller 2019)

Dr Josef Koller, a global security and space science programme expert, believes, “technology trends are accelerating and there are indications that a sixth wave of innovation is coming”. Dr Koller reminds us of the five initial economic cycles defined as the industrial revolution; the age of steam and railways; the age of steel and electricity; the age of oil, cars and mass production and the age of information and communication (Koller 2019).

Each wave lasted from 40 to 60 years and consisted of alternating periods between high sector growth and periods of slow growth. The sixth cycle is

postulated by some as an increase in resource efficiency. A new wave would be heralded by massive changes in the market, societal institutions and technology that all reinforce each other, centered around connected intelligence with new devices, new applications, new business models and new services. Space-based commercial remote sensing that create massive datasets, joined by [AI] for analysis and product development will be just one aspect of the innovation wave.

(Koller 2019)

With this increase in innovation and technological advances, the potential for transparency escalates exponentially, an attribute I find pertinent to our success as a liberal democracy in this technological age.

One of the many benefits of embracing satellite imagery and artificial intelligence (AI) into our daily life is the ability to predict natural disasters. Since 2000, spaceborne satellites and sensors have helped experts “quantify geophysical phenomena associated with the movements of the earth’s surface (earthquakes, mass movements), water (floods, tsunamis, storms), and fire (wildfires)” (Gillespie et al. 2007). This technology plays an important role in assessing disasters before and after they occur (Gillespie et al. 2007). Specialists are turning to “geodetic methods – the math-based study of changes in the Earth’s shape – that use satellites and other instruments to complement data gathered by seismometers” to better predict the earth’s “movements and landslides” (Joshi 2019; Lewis 2019). A University of Iowa student demonstrated this by processing:

radar imagery, or interferograms, from a 6.9 magnitude quake that struck Indonesia in August 2018. She then used this imagery to produce a model of the earthquake and where it was located. The [United States Geological Survey] used this model directly to update its predictions of ground shaking and earthquake impact that were incorporated into its disaster-response systems.

(Lewis 2019)

These efforts directly improved earthquake estimates and solidified the importance of satellite imagery in predicting future natural disasters (Lewis 2019).

Furthermore, during Hurricane Harvey, The National Aeronautics and Space Administration (NASA) collaborated with the mapping and data visualization team at Development Seed to track Harvey’s rainfall, cloud heights and cloud top temperatures (Joshi 2019; Dempsey 2017). This technology allowed experts to track the hurricane’s progress every hour, as opposed to every six hours, which was the standard tracking capability (Joshi 2019).

AI is also being used to protect and improve the environment in the form of monitoring endangered species, tracking diseases and optimizing crops. For example, WildTrack uses a “computer vision solution called Footprint Identification Technology to monitor endangered species non-invasively. The tool analyses images of footprints of cheetahs, rhinos, and other endangered species to identify them, track them, and determine what threatens them” (DeNisco Rayome 2019). AI can “also track mosquito populations to anticipate or prevent the spread of

disease, as well as weather changes, to warn populations about upcoming storms” (DeNisco Rayome 2019).

Epidemiology, the study of disease propagation, has long relied on maps, starting with John Snow’s iconic maps of the London cholera outbreak in 1854. These maps may have been the beginning of geographic analysis as we know it – overlaying seemingly disparate elements on a map to reveal previously unseen patterns.

(OECD 2020)

Thanks to Geospatial technologies like AI, the spread of COVID-19 is being mapped in real time.

Before the world was even aware of the threat posed by the coronavirus (COVID-19), artificial intelligence (AI) systems had detected the outbreak of an unknown type of pneumonia in the People’s Republic of China (hereafter “China”). As the outbreak has now become a global pandemic, AI tools and technologies can be employed to support efforts of policy makers, the medical community, and society at large to manage every stage of the crisis and its aftermath: detection, prevention, response, recovery and to accelerate research.

(OECD 2020)

AI is a contributing factor as governments attempt to limit contagion. Countries are using AI methods to surveil their population and conduct contact tracing, among other things.

A number of countries are using population surveillance to monitor COVID-19 cases (for example, in Korea algorithms use geolocation data, surveillance-camera footage and credit card records to trace coronavirus patients). China assigns a risk level (colour code – red, yellow or green) to each person indicating contagion risk using cell phone software. While machine learning models use travel, payment, and communications data to predict the location of the next outbreak and inform border checks, search engines and social media are also helping to track the disease in real-time.

(OECD 2020)

Even before the COVID-19 outbreak, governments were adopting closed-circuit television cameras combined with AI in cities across the globe. Some cities may even utilize private companies to gather publicly available photographs and data from the internet (Goldenfein 2020). One service in particular, Clearview AI, is “like a reverse image search for faces” (Goldenfein 2020). As the global social networks expand, the raw material for such an application grows every day:

You take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared. The system –

whose backbone is a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites – goes far beyond anything ever constructed by the United States government or Silicon Valley giants.

(Hill 2020)

With this increase in imagery and data collection, we will be able to holistically cross-connect data streams from human activity to physical reality; ultimately answering the questions, “Where are the people?” “Why are the people there?” and “Where are they going to be tomorrow?” Having the ability to answer these questions could contribute to the prevention of mass shootings, police brutality or maintaining peace during protests or daily life. For instance, law enforcement officers, including local police in Florida, the Federal Bureau of Investigation (FBI) and the Department of Homeland Security, have used Clearview AI to assist with cases involving shoplifting, identity theft, credit card fraud, murder and child sexual exploitation cases (Hill 2020).

However, the collection of one’s daily actions, movements or publicly available information could be used with malice. If mishandled, employers, government leaders or adversaries (personal or political/non state actors) could use this information as leverage against those with opposing viewpoints. In this instance, we risk being manipulated for another person’s gain. Due to this fear, it is likely most Americans would feel their freedoms were violated if Congress attempted to mandate that every adult carry a tracking device to reveal their location 24 hours a day (Thompson and Warzel 2019a). Yet, in the decade since Apple created its App Store and General Motors created OnStar, the majority of Americans have, application by application, consented to such a system run by private companies, even though the corporations that control their data are far less accountable than the government would be (Thompson and Warzel 2019a). In an exposé on the topic, *The New York Times* states:

Americans have grown eerily accustomed to being tracked throughout their digital lives. But it’s far from their fault. It’s a result of a system in which data surveillance practices are hidden from consumers and in which much of the collection of information is done without the full knowledge of the device holders.

(Thompson and Warzel 2019b)

Many Americans simply risk embarrassment or inconvenience should their location data be exposed, but for victims of abuse, the risks are substantial as this information could be used by their abuser for further attacks (Thompson and Warzel 2019a). *The New York Times* also reminded their readers that not all people want their locational data shared:

Who can say what practices or relationships any given individual might want to keep private, to withhold from friends, family, employers or the

government? We found hundreds of pings in mosques and churches, abortion clinics, queer spaces and other sensitive areas.

(Thompson and Warzel 2019a)

With the innovations surrounding AI and geospatial technologies, the concept of privacy has evolved. Should our liberal democracy maintain transparency in regards to this technology, the concept of privacy will continue to morph, for good or for bad. For example, in May 2019, the city of San Francisco became the first city in the United States to ban the use of facial recognition software by police and other city agencies (Fowler and Breedlove 2019). While this technology could provide assistance in fighting crime, it could also be used for evil or unjust reasons. For example, if a child was kidnapped from a city park prior to this ban, San Francisco would be able to use a combination of CCTVs and facial recognition software to identify the kidnapper, track his or her location, retrieve the missing child and return them to his or her parents. A city employee, however, could misuse the technology at his or her disposal to track a former spouse during a divorce settlement. Perhaps this employee's former spouse is claiming to be unable to afford child support or alimony, claims to be eating at food shelters and struggling to make ends meet. However, with CCTVs and facial recognition, the city employee is able to prove that the former spouse is frequenting lavish stores and five star restaurants. In this instance, the technology that could be used for good becomes an abuse of power and a tool to invade someone's privacy. Furthermore, "facial recognition algorithms have long been criticized for poor performance in identifying non-white faces" (Hatmaker 2020). This issue contributes to San Francisco's decision to ban such technology: "[t]he propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits" (Fowler and Breedlove 2019).

If not properly regulated with transparency, this technology could also be used to threaten our national security. For example, in the same exposé referenced previously, the *New York Times* used locational data to track one of president Trump's secret service agents, and by association, likely president Trump himself (Thompson and Warzel 2019b). The potential this information could have against our national security is obviously immense and there's little stopping an adversary from utilizing this information to our detriment. For instance, according to former National Security Agency director General Michael Hayden, "the U.S. government 'kill[s] people based on metadata'". If this is a practice we take part in, it could also be adapted by adversaries through readily available, public information.

As the expansion and growth of such surveillance is inevitable and incessant, we must calculate a means to deal with such a reality. If approached with caution, this will benefit our society exponentially. In his 1998 book, *The Transparent Society*, David Brin shares similar sentiments:

This is a tale of two cities. Cities of the near future, say ten or twenty years from now. Barring something unforeseen, you are apt to be living in one these two places. Your only choice is which one.

Consider city number one. In this place, all the myriad cameras report their urban scenes straight to Police Central, where security officers use sophisticated image processors to scan for infractions against public order – or perhaps an established way of thought. Citizens walk the streets aware that any word or deed may be noted by agents of some mysterious bureau.

At first sight, things seem quite similar in city number two. Again, ubiquitous cameras perch on every vantage point. Only here we soon find a crucial difference. These devices do not report to the secret police. Rather, each and every citizen of this metropolis can use his or her wristwatch television to call up images from any camera in town.

In city number two, such micro-cameras are banned from some indoor places . . . but not from police headquarters! There any citizen may tune in on bookings, arraignments, and especially the camera control room itself, sure that the agents on duty look out for violent crime, and only crime.

Both futures may seem undesirable. But can there be any doubt which city we'd rather live in, if these two make up our only choice?

(Brin 1999)

Brin's challenging question to choose from extremes is useful in the grey area that is real life. But given the relentless nature of commercial surveillance, Brin gives us a reference point from which to anchor the necessary details of our policy debate. The abundance of publicly available information is changing the definition of "private". In an article for the Brookings Institute, Cameron Kerry states:

To most people, 'personal information' means information like social security numbers, account numbers, and other information that is unique to them. U.S. privacy laws reflect this conception by aiming at 'personally identifiable information,' but data scientists have repeatedly demonstrated that this focus can be too narrow. The aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them. The result is that today, a widening range of data has the potential to be personal information, i.e. to identify us uniquely.

(Kerry 2018)

The European Union agrees with this sentiment: Brought to fruition in May 2018, the General Data Protection Regulation (GDPR) significantly altered the privacy laws throughout the European Union. The GDPR is focused largely on protecting personal data, to include "racial or ethnic origin, political opinions, religious beliefs, membership of trade unions, genetic and biometric data, health information and data around a person's sex life or orientation" (Burgess 2020). At the core of the GDPR legislation, there are seven principles that "don't act as hard rules, but instead as an overarching framework that is designed to layout the broad purposes

of GDPR” (Burgess 2020). The seven principles are: “lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability” (Burgess 2020). However, certain provisions could override the GDPR legislation, including national security, defence and public security (European Parliament and Council of European Union 2016).

Currently, US privacy laws focus on threats against individual’s rights, but those protections are anachronistic in the face of AI, geospatial technologies and mobile technologies, which not only use group data but also are dependent on it. We must determine who controls our data, who can access it, why it can be accessed and with what oversight. Finally, we need to firmly establish what role – if any – the derived data would play in our legal framework. We ultimately need to answer the question, “How might our society adapt, innovate and evolve to harness the power of geospatial data and technology while mitigating its ethical challenges”?

As we seek to address that question, we must remember these are uncharted waters and uninformed, impetuous actions could have deleterious effects. It is essential this unprecedented situation be addressed with deliberate and well thought out actions, as well as the flexibility and ability to modify rules and regulations as we better understand the ramifications and consequences of our initial decisions. Currently, the most applicable legal notion along these lines may be the Fourth Amendment Equilibrium Adjustment, which:

posits that the Supreme Court adjusts the scope of protection in response to new facts in order to restore the status quo level of protection. When changing technology or social practice expands government power, the Supreme Court tightens Fourth Amendment protection; when it threatens government power, the Supreme Court loosens constitutional protection.

(Kerr 2011)

While this is a far cry from what liberal democracies must create in order to adequately protect individuals’ privacy outside the court of law, the premise may serve as an appropriate baseline and reminder for a fluid, constantly changing, law. I would observe that until we can agree on data privacy norms, it will be hard to create lasting rules around transparency. Suffice it to say, the stakes are enormous. In fact, one could see this discussion and debate as existential – at least as it pertains to human freedoms.

Just as search engines like Google led the way for indexing and categorizing the knowledge deposited by humans into the online world for mankind’s benefit, a globally persistent sensing architecture could lead the way to finding information, intelligence and understanding of the physical world in real time to benefit all life on earth. Like others, I have used the analogy of the rising tide of data that can overwhelm us by bringing us more data and less information, ultimately reducing our shared awareness. That tide is cresting in a way that puts us now on the curling edge of the wave. Computer vision, machine-learning and AI offer the chance for

us to propel into a world of radical transparency. Each advancement in technology will build upon and interface with their predecessors. This accumulation is essential from a commercial utility perspective. And it will redound to the public sphere if and when such transparency is misused – especially by the government.

Our transparent society is here to stay, no matter how hard one tries to eliminate their digital presence. There is no putting this technological genie back in the bottle. I submit that transparency favours justice – and that evil lurks in the dark. If you think of this transparency as light – as I do – it shines both ways. I believe transparency is good for liberal, democratic societies. As Supreme Court Justice Louis Brandeis observed, “Sunlight is said to be the best of disinfectants” (Brandeis 1914, chap. 5).

I further believe the bedrock of civil discourse is trust; not so we agree on every issue, rather so we appreciate the other perspective and empathize with differing views. Properly thought through, an era of radical transparency can lead to a more humane world. However, achieving such a world means striking a balance between access and control, between openness and privacy, between good and evil.

Thus, we should be considering our country’s core strengths – entrepreneurial spirit, risk capital, market competition and respect for the individual and their rights – as we rethink what the notion of privacy should mean today. If we anticipate many of the ways that the abundance of data might be misused, we can establish rules, regulations and governing authorities to encourage the best uses while thwarting bad actors. After all, as we’ve learned during the ongoing COVID-19 pandemic, modifying prior constructs of privacy has enabled countries to conduct holistic contact tracing, limiting the spread of a deadly disease. If approached with thought and caution, this technology has the potential to make transparency a force for good and change the world for the better.

References

- Brandeis, Louis D. 1914. *Other People’s Money and How the Bankers Use It*. New York: Frederick A. Stokes Company.
- Brin, David. 1999. *The Transparent Society: Will Technology Force Us to Choose between Privacy And Freedom?* 1st edition. Reading, MA: Basic Books.
- Burgess, Matt. 2020. “What Is GDPR? The Summary Guide to GDPR Compliance in the UK”. *Wired UK*, March 24. www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.
- CIA. 2015. “CORONA: Declassified – Central Intelligence Agency”. CIA.Gov. 2015. Accessed December 16, 2020. <https://web.archive.org/web/20201101124231/www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/corona-declassified.html>.
- Dempsey, Caitlin. 2017. “Tracking Hurricane Harvey with Satellites”. *Geography Realm* (blog). August 25. www.geographyrealm.com/tracking-hurricane-harvey-satellites/.
- DeNisco Rayome, Alison. 2019. “How AI Could Save the Environment”. *TechRepublic* (blog). April 19. www.techrepublic.com/article/how-ai-could-save-the-environment/.
- European Parliament and Council of European Union. 2016. “Art. 23 GDPR-Restrictions”. Accessed February 26, 2018. <https://gdpr-info.eu/art-23-gdpr/>.

- Fowler, Patrick, and Haley Breedlove. 2019. "Facing the Issue: San Francisco Bans City Use of Facial Recognition Technology". *JD Supra* (blog). July 15. www.jdsupra.com/legalnews/facing-the-issue-san-francisco-bans-35144/.
- Gillespie, Thomas W., Jasmine Chu, Elizabeth Frankenberg, and Duncan Thomas. 2007. "Assessment and Prediction of Natural Hazards from Satellite Imagery". *Progress in Physical Geography* 31 (5): 459–70. <https://doi.org/10.1177/0309133307083296>.
- Goldenfein, Jake. 2020. "Australian Police Are Using the Clearview AI Facial Recognition System with No Accountability". *The Conversation*, March 4. <http://theconversation.com/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667>.
- Hatmaker, Taylor. 2020. "AI Researchers Condemn Predictive Crime Software, Citing Racial Bias and Flawed Methods | TechCrunch". *TechCrunch* (blog). June 24. <https://techcrunch.com/2020/06/23/ai-crime-prediction-open-letter-springer/>.
- Hill, Kashmir. 2020. "The Secretive Company That Might End Privacy as We Know It". *The New York Times*, January 18, sec. Technology. www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
- History. 2018. "U-2 Spy Incident". *History* (blog). August 21. www.history.com/topics/cold-war/u2-spy-incident.
- Joshi, Naveen. 2019. "How AI Can and Will Predict Disasters". *Forbes*, March 15. www.forbes.com/sites/cognitiveworld/2019/03/15/how-ai-can-and-will-predict-disasters/.
- Kerr, Orin S. 2011. "An Equilibrium-Adjustment Theory of the Fourth Amendment". *Harvard Law Review*, December 20. <https://harvardlawreview.org/2011/12/an-equilibrium-adjustment-theory-of-the-fourth-amendment/>.
- Kerry. 2018. "Why Protecting Privacy Is a Losing Game Today – and How to Change the Game". *Brookings* (blog). July 12. www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.
- Koller, Josef S. 2019. "The Future of Ubiquitous, Realtime Intelligence: A GEOINT Singularity". In *35th Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America*. www.spacesymposium.org/wp-content/uploads/2019/09/Paper-Koller-Josef-A-Future-of-Ubiquitous-Real-Time-Intelligence.pdf.
- Lewis, Richard. 2019. "Satellite Observations Improve Earthquake Monitoring, Response". *ScienceDaily* (blog). June 14. www.sciencedaily.com/releases/2019/06/190614125848.htm.
- Lockheed Martin. n.d. "U-2 Dragon Lady". Lockheed Martin. Accessed December 16, 2020. www.lockheedmartin.com/en-us/products/u2-dragon-lady.html.
- OECD. 2020. "Using Artificial Intelligence to Help Combat COVID-19". OECD.org. April 23. www.oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-ae4c5c21/.
- Thompson, Stuart A., and Charlie Warzel. 2019a. "Twelve Million Phones, One Dataset, Zero Privacy". *The New York Times*, December 19. www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.
- . 2019b. "How to Track President Trump". *The New York Times*, December 20. www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html.

16 Evolving chemical, biological, radiological and nuclear (CBRN) terrorism

Intelligence community response and ethical challenges

Patrick F. Walsh

Introduction

This chapter has three objectives. First it assesses briefly contemporary and emerging chemical, biological, radiological and nuclear (CBRN) threats from non-state actors. Secondly, it identifies capability challenges across “Five Eyes” intelligence communities (ICs) in managing CBRN non-state actor threats and how these can be addressed. Thirdly, noting the threat posed by CBRN terrorism and “Five Eyes” ICs capabilities to prevent, disrupt or mitigate them, the chapter outlines key ethical challenges for ICs in managing such threats. The chapter is divided into three sections: *contemporary and emerging non-state actor CBRN threats, intelligence capability gaps and challenges, and ethical challenges.*

Contemporary and emerging non-state actor CBRN threats

Defining CBRN

The term “CBRN” includes a range of threats from the weaponization of chemical, biological, radiological and nuclear agents by state and non-state actors. “CBRN” is a departure from the traditional nomenclature – “Weapons of Mass Destruction” (WMDs), “with all its Cold War connotations of massive effect and mutual deterrence” (Cornish 2007, 2). As discussed shortly, not all CBRN threats present an existential threat to humanity or even massive casualties – of the kind depicted during the Cold War; where the former Soviet Union or the United States might have deployed tactical or strategic WMDs (particularly nuclear weapons).

A critical point of difference between “WMD” and “CBRN” weapons is the former’s principal objective of significant and predictable devastation. In order to achieve this objective, WMD weapons have to be reliable, safely deployable and able to result in major destruction of localities and in the deaths of hundreds of thousands in order to deter an adversary. Throughout the Cold War to the present, only a few threat actors have developed large-scale WMD programmes that could result in significant and reliable widespread destruction of an enemy.

In contrast, while some non-state actors have demonstrated an interest and even an intent to use WMD-related technologies, up to this point none has demonstrated the capability to weaponize chemical, biological, radiological or nuclear agents akin to a truly devastating military standard that state actors have achieved with their WMD programs. Additionally, non-state actors such as terrorists, who show an interest in WMD technologies, are likely to use a different strategic calculus for their deployment than military grade state actor programmes. For terrorists, widespread destruction and accurate delivery may be less important than reaping a propaganda dividend from damage of property or causing the deaths of several hundred (rather than thousands) of deaths. A rudimentary CBRN agent therefore offers another suite of weapons that some non-state actors may choose to use. Their deployment may not kill thousands of victims, but nonetheless could conceivably result in a large number of casualties as well as having profound psychological, social and economic effect on the target countries. In short, terminology (WMD vs. CBRN) matters to how ICs understand threats and plan capability responses against them.

Non-state actor CBRN threat assessment

Chemical weapons and terrorism

While the 1997 Chemical Weapons Convention (CWC) has provided normative constraint on most state signatories in abandoning their use, production and storage of military grade CWs, it has been less helpful in containing terrorist's use of such weapons. The CWC was not crafted with counter-terrorism in mind.¹ It has focused on the large-scale military production of chemical agents – not smaller amounts that terrorist groups would likely use. Within the current CWC verification regime it is also impossible to guarantee whether a few kilograms of toxic chemicals would be detected before they were used by a terrorist group. Additionally, a failure by all CWC signatory states to implement strictly all of its articles means it is easier potentially for terrorists to acquire a chemical weapon capability.

While the design and manufacture of advanced CWs will likely remain a technological challenge to many non-state actors, the intent by some to use them remains. Reliable data remains sketchy, though the Monterey WMD terrorism database reports for the period 1988–2004, 207 of the 316 CBRN incidents recorded involved CW (Ivanova and Sandler 2006, 423–48). These incidents, however, mostly involved the use of conventional explosives mixed with openly available chemicals to make them more deadly – or are failed attempts to weaponize chemical agents (Ivanova and Sandler 2006, 423–48).

It's clear that Al-Qaeda and its franchises have shown interest in the deployment of CWs and other WMDs. In 1998, bin Laden said that to acquire and use WMDs was his Islamic duty (Mowatt-Larssen 2010). Abu Musab al Zarqawi, the leader of Al-Qaeda in Iraq, planned to utilize his network to carry out multiple ricin and cyanide attacks in the London Underground from 2002 to 2003, though they were thwarted by the Metropolitan Police Service (Rathore 2016, 5).

Additionally, other Al-Qaeda franchises in Iraq (e.g. Ansar al-Islam) had begun to experiment with chemical and toxic weapons and declare their intent to obtain CW (Ackerman and Jacome 2018, 29; Pita 2007, 480–511).

The only attack, however, that involved a standard CW agent – the Tokyo Sarin gas attacks by Aum Shrinikyo in 1995 – showed how difficult it is to mount an effective CW attack – even for an organization with high levels of expertise and sufficient funding (Danzig et al. 2012; Kaplan and Marshall 1996; Cornish 2007; Tucker, Miller, and Lynn-Jones 2000). Shinrikyo’s attempts to synthesize Sarin cost as much as \$30 million, involved 80 scientists and took a year or more to achieve (Cornish 2007, 6).

While there remain technical barriers for most terrorist groups in building a conventional military grade CW, access to ready-made weapons could occur through theft or via state sponsorship. Likely sources are stockpiles in fragile and unstable states such as Syria, Iraq, Libya and North Korea. International retributions, however, including threats of regime change or economic sanctions may discourage states providing CWs to terrorists. Nonetheless, the instability of such regimes, including corrupt officials who have access to weapons, may facilitate access within these states. For example, recent reports from Iraqi officials (citing intelligence reports) suggested that the Islamic State (IS) during 2014 gained access to weapons stockpiles of the Syrian and former Iraqi regimes (Berger 2015, 423–48).

What of Islamic State (IS) use of CW? As IS grew in power (2014 to July 2017) the terrorist group reportedly used chlorine and sulphur mustard gas in Iraq and Syria several times. The number of actual attacks is still debateable, but researchers put them in the range of 37 to 76 times (Binder, Quigley, and Tinsley 2018, 27; Rathore 2016, 7; Strack 2017, 19–24). In 2014, IS was able to seize, purchase or craft military hardware that could be used in a chemical weapon programme in parts of Syria and Iraq. During the Caliphate’s physical expansion in Syria, IS forces deployed chlorine, sulphur mustard, phosphine and other toxic industrial chemicals such as vinyl-trichlorosilane, for tactical purposes – the first chemical warfare agents introduced onto the battlefield since the Iran–Iraq War. However, the mode of delivery of IS CW attacks seems to have been not in the same vein as classical WMD weaponry, instead involving the insertion of chemical substances into shells and firing them rather than the deployment of any sophisticated weaponry system (Elvey 2015).

With the final destruction of the Caliphate in 2019, the threat from IS including its capability to deploy CWs or other “WMD like weapons” has declined. Nonetheless, IS recruiters and sympathizers continue to message an interest in developing a CBRN capability. Given IS did occupy areas of Iraq where CWs were stored and actually deployed (however crudely) one cannot discount fully a scenario where an IS lone actor could smuggle some CW material into the West and/or launch a rudimentary attack by accessing one or more poorly secured precursor chemicals or facilities where agents are stored (Ackerman and Jacome 2018, 30).

Recent developments in dual-use chemistry and related technology mentioned earlier (e.g. the production of toxic industrial chemicals and advanced chemical

weapons) might also be attractive to some terrorist groups to weaponize in the future. The relatively weak international regulation and safety mechanisms around their manufacture, storage and transport in some nations remain a vulnerability.

Biological weapons and terrorism

In recent years, the debate around biological weapons (BW) and non-proliferation has increasingly focused on non-state actors and terrorist groups in particular. CBRN researcher Seth Carus assessed that there were “at least 25 ‘distinct sub-national actors’ who were known to have ‘shown concerted interest’ in acquiring BW, with at least eight of them known to have been successful” (Carus cited in NDU 2003, 5). The experiments of Aum Shrinikyo with Anthrax and Ebola, the religious cult the Rajneeshees that poisoned salad bars with *Salmonella typhimurium* in 1984, as well as the 2001 Anthrax attacks allegedly by United States Army Medical Research Institute of Infectious Diseases (USAMRIID) microbiologist Bruce Ivins are well documented examples (Carus 2000, 115–37; Rosenau 2001; Walsh 2018).²

After 9/11, Al-Qaeda had demonstrated an interest in developing BW agents. Following the 2001 coalition forces’ invasion of Afghanistan, US soldiers found technical documents and equipment in a biological weapons laboratory under construction near Kandahar (Walsh 2018, 29–31; Tenet 2007, 278–9). The capture, interrogation or death of most key Al-Qaeda operatives associated with its fledgling bio-weapons programme constrained further efforts by the group to continue down this pathway.

Since the ouster of Al-Qaeda from Afghanistan the evidence has remained mixed on whether other Al-Qaeda affiliated groups have developed technical expertise in BWs – though the interest to do so seems to be clearer (Walsh 2018, 30; Koblentz 2009, 223–4). More recently there is also some evidence that IS has had ambitions to develop BWs when a laptop was seized in 2014 from one of the group’s hideouts in Syria. The laptop, owned by a Tunisian, who had studied chemistry and physics at universities in Tunisia, revealed thousands of files pertaining to producing biological weaponry (Doornbos and Moussa 2014). Other reporting, though of questionable credibility, suggests IS had plans to recruit scientists in Iraq and the West to develop BWs (Elvey 2015; Doornbos and Moussa 2014).

The “Five Eyes” countries’ understanding of state and non-state actor BW proliferation has not been robust over the last 50 year period (SSCI 2004; Flood 2004; Butler 2004). The reasons why assessment of bio-threats and risks was not optimal relates to a number of complex capability issues. Some of these issues are discussed in the following section, but space is limited and the reader seeking detailed understanding of capability issues can go to Walsh (2018). Suffice it to say, a lack of understanding by “Five Eyes” ICs has had real policy implications since 9/11 about scoping bio-threats and risks and how to manage them. The faulty intelligence assessment on WMD provided prior to US-led coalition invasion of Iraq in 2003 is the most well-known example. While debates continue within IC and policy circles on what factors might drive contemporary and

emerging bio-threats and risks – they have coalesced around two broad threat/risk typologies: *stolen biological agents and dual use research and synthetic biology*. I will focus on the latter as this area is currently of greatest concern by ICs and the scientific community.³

Dual use research and synthetic biology

Dual use research relates to research of dangerous biological agents that might be weaponized, and the publication of same, which potentially could be disseminated to threat actors for use (Walsh 2018, 41). It remains an open debate on whether criminals and terrorists will exploit biotechnology and synthetic biology research developed for legitimate purposes (e.g. health care, energy and food supply) for harm or profit. Assessments of threat and risk diverge mainly around two analytical frameworks: technological (determinism) and socio-technological. The technological determinists argue that the upsurge in biotechnological advancements will make the access, use and exploitation of relevant knowledge and skills easier and cheaper for those with malevolent intentions (Chyba 2006; Carlson 2003; Petro and Carus 2005). Some of the consequences of the industrialization of biology add weight to their arguments about easier access and use of biotechnology. For example, the entire human genome sequenced by 2013 took a team of scientists 13 years and \$500 million to identify 20,500 genes. Today, the human genome can be sequenced in a day using bench top equipment costing around \$1000 (Walsh 2018, 44).

In contrast, the socio-technologists do not discount that criminals, and terrorists may exploit advances in synthetic biology and technology – yet argue access to knowledge and skills do not necessarily translate into threat actors adeptly exploiting these in order to produce a bio-weapon. They argue that other socio-technical variables will impact on choices made to exploit and weaponize biology (Vogel 2008; 2013). Both intellectual perspectives have something to offer “Five Eyes” ICs in improving their assessments of emerging bio-threats and risks.

What types of specific bio-threats are evolving? Assessing intention and capability to misuse dual use biological research remains difficult because the science is moving rapidly – making it difficult to get a “fix” on where vulnerabilities for malevolent exploitation are located. Such difficulties are amplified given the challenges all ICs confront when adapting to technologically enabled threats more broadly (e.g. cyber).

Leaving aside the assessment difficulties, I have argued elsewhere that there are at least three areas where “Five Eyes” countries can start developing better knowledge of bio-threats and risks. These are: *bio-unabombers*, *identity theft and biopiracy*. In regard to bio-unabombers, biotechnology is big business particularly in the United States (Walsh 2016, 341–67; 2018, 41–51).⁴ Given the acceleration in biotechnology and synthetic biological sciences – probability alone suggests that there will be more individuals (some mentally unstable) with a range of grievances (e.g. personal, psychological, political and religious) working in the biological sciences and some may escalate these to acts of violence. Disgruntled

insiders (scientists), who can make a synthetic organism and obtain natural organisms under lock and key in highly regulated high containment labs, are uniquely placed under the guise of a bigger legitimate scientific project to become bio-unabombers (Walsh 2018, 41–51).

Secondly, “identity” – long a facilitator of crime and terrorism in other contexts – is also likely to be a developing concern. The increase in DNA holdings in various government departments and the private sector provide greater opportunities to steal or manipulate DNA (Walsh 2018, 41–51). Thirdly, bio-piracy could become a greater bio-threat and risk in “Five Eyes” countries. Recent developments in drugs, vaccines and medicines can be manipulated via newer gene editing techniques like CRISPR, Finger Nuclease and Talen (see in the following).

Radiological weapons and terrorism

In contrast to BWs, where terrorist’s production of them could be constrained by insufficient skills and knowledge, the wider global availability of radioactive material has long formed the basis for arguments that such groups would more likely weaponize them instead. Different isotopes are used in large quantities in various civilian applications (e.g. radium or caesium isotopes used in cancer treatments). The dual use nature, common use globally, and in some locations insufficient security and monitoring arrangements related to storage, provide terrorist groups with easy access to dangerous radioactive substances that can be weaponized with little technical expertise or value added from them prior to use. Radioactive material may also be obtained from the civilian nuclear fuel cycle, for example by harvesting it from widely used mixed oxide fuel (MOX), which is a relatively simple technical procedure (Balatsky and Severe 2019, 357–87). While detection of radiation is not uncommon in ports, it is likely that terrorist groups would procure the material locally from sources mentioned earlier. Accessing radioactive materials could be easier than developing CWs or BWs – but they are nonetheless hazardous to handle and transport.

Assessments diverge on the lethality and damage caused by a radiological attack. The impact would depend on a number of variables, including the force of the explosion, the type of radioactive material used, the particle size of the dispersed material, weather conditions and countermeasures (Rosoff and Winterfeldt 2007; Cirincione and Wilson 2015). However, many analysts assess that the number of casualties would be relatively low and probably not reach three figures (Rosoff and Winterfeldt 2007; Cirincione and Wilson 2015). Nonetheless, damage to property and the disruption of people’s lives and economic activity could be significant if the bomb was released in a crowded downtown financial area or a critical infrastructure zone such as a port.

While it isn’t trivial to produce a dirty bomb with optimal particle size and dispersion pattern to maximize casualties, it is considerably simpler than constructing a nuclear device, as no fission or fusion reactions have to be triggered.⁵ Nonetheless, terrorist groups would still need to have some knowledge about the physical form of the radiation source and what the optimal amount and types of

explosives would be required to ensure a wide dispersal of radiation (Ackerman and Jacome 2018, 26).

In spite of the potential viability of attack scenarios just mentioned, radiological attacks are not common. This might be because they don't have the same kind of immediate kinetic lethality caused by simpler conventional explosives. Similarly, like other CBRN tactics they also carry significant operational risks of substantial retaliation by the country that falls victim to such an attack.

In 2015, media reporting by the Associated Press suggested that IS was interested in using a dirty bomb and may have tried to acquire radiological material from gangs with Russian connections (Butler 2015). It is unclear however, if IS successfully purchased it or if it was weaponized or used in any attacks.

Nuclear weapons and terrorism

Reports vary on whether non-state actors have either attempted or intend to acquire nuclear weapons (Mueller 2019, 5; McIntosh and Storey 2018, 289–300; Allison 2018). Further assessment of the validity of terrorist's intent and capability to develop nuclear weapons is therefore critical. From the intent perspective, Al-Qaeda leadership showed interest in developing nuclear capability – with Bin Laden quoted in an interview that the acquisition of a nuclear weapon (and other WMDs) is a “religious duty” of Muslims (van de Velde 2010, 682–99). However, despite Al-Qaeda's desire to use CBRN against enemies, the threat never materialized (Rathore 2016, 5), particularly after sustained counter-terrorism action either destroyed or degraded its bases in Afghanistan after 2001. According to experts at NATO's WMD Non-Proliferation Centre, IS has already acquired the knowledge and in some cases human expertise to use CBRN material (Boyle 2015). But it's unclear the extent to which any IS members developed a viable nuclear bomb during or after the Caliphate years.

Several terrorist groups have “metastasized” from Al-Qaeda and IS, and the pressing question is what intent and capability will even more radicalized and potentially catastrophic terrorists have to develop nuclear weapons? Such groups may calculate that acquiring and using them is worth the effort. Unlike the development or acquisition of chemical, biological and even radiological weapons, building a nuclear bomb remains extremely difficult for non-state actors. Producing fissile material from raw products would require a focused and extended process in either the enrichment of uranium or the chemical separation of plutonium – that will likely be too complex, costly and detectable for most currently known terrorist organizations to realistically undertake. Instead of conventional nuclear weapons, it is possible that some terrorist groups could build an improvised nuclear device, if they were able to obtain enough weapons-grade uranium or plutonium (Cornish 2007, vii).

Another commonly cited scenario is terrorist groups could either steal or be given nuclear weapons by vulnerable state actors such as Pakistan or countries of the former Soviet Union. The theft of nuclear weapons is feasible from countries where political and security risks reduce confidence in the safe storage of these

weapons by their governments. But it is a risky gamble for these states and their officials as it would invite instant retaliation from “Five Eyes” states (Weiss 2015, 75–87; Clarke 2013, 98–114).

In terms of emerging threat trajectories, as discussed shortly, there are other security concerns around the emergence of an “internet of nuclear things” and the digital nature of additive manufacturing, which might provide some non-state actors with new means to subvert nodes in nuclear supply chains at which proliferation activities have traditionally been detected (Hoffman and Volpe 2018, 102–13; Kroenig and Volpe 2015; Fey 2017; Bajema and DiEuliis 2017; Shaw 2017; Hvistendahl 2016; Kelly 2017).

Intelligence capability gaps and challenges

Detection of emerging threats

The IC’s ability to assess emerging CBRN *state-based threats* can be difficult enough given states can engage in well-organized deceptive strategies and claim suspicious activities are part of legitimate research, development and commercial activity. It is even more difficult for ICs to assess the emerging CBRN threat posed by terrorists. Terrorist “CBRN programmes” are not scaled up like their state-based counterparts. They typically do not consist of large research and industrial enterprises nor involve many people or the regular movement of CBRN-related goods and services. Being in most cases the opposite of state-based CBRN programmes reduces even further the likelihood of detection and disruption. Compounding the detection challenge of non-state actor CBRN threats is that analysis of them has often relied on sub-optimal empirical theorizing. Analytical extrapolations have tended to rely only on a handful of prominent cases to understand how threats will evolve (Binder and Ackerman 2019, 1).

Several authors have discussed how to improve CBRN terror threat detection (Tucker, Miller, and Lynn-Jones 2000; Caves and Carus 2014; Maurer 2009; Koblentz 2009), but such efforts remain difficult due to very few CBRN attacks by terrorists. A key barrier to better threat detection has also been the different classifiers scholars have used to record CBRN terrorism. In recent years, the University of Maryland’s Profiles of Incidents Involving CBRN and Non-state Actors (POICN) Database has recorded more than 517 CBRN terrorism-related events from 1990 to the present and offer potentially a more accurate way to classify such attacks (Binder and Ackerman 2019, 1).

In addition to classification issues, there remains a lack of certainty and consensus from within ICs and scholars about future CBRN attack vectors. As noted earlier, with the collapse of the Caliphate in March 2019, for example, it is even less clear what number of IS and affiliated groups have retained/acquired skills/knowledge convertible to potential CBRN attacks in the Middle East or by foreign fighters returning to home countries.

Improving threat detection on the intent, skills and knowledge of CBRN by lone actors/groups also includes greater collection effort against individuals

who provide financial and logistical support to terrorist groups for such attacks. Such individuals/groups are points of vulnerabilities for any planned attack that ICs may be able to detect and disrupt early; though increasingly encrypted communications and the use of dark web sites by terrorists can make tracking their finances and logistics difficult. More focused collection efforts, including those of vulnerabilities in dual use technologies – will hopefully result in the accumulation of empirical evidence useful to informing better CBRN terrorist threat and risk assessment models used by ICs (Ackerman and Jacome 2018, 16; Zhang and Gronvall 2020; Walsh 2018, 79–83, 121–43; Habegger 2010, 49–58; Gentry and Gordon 2019, 215–34).

It is likely also that a deeper understanding of psychological factors to acquire, produce and use CBRN weapons through earlier psychological profiles of individuals and group members would be useful. In particular, ICs need to understand the behaviour of “insiders” working in economic sectors that produce CBRN-related material vulnerable to their exploitation (Bunn and Sagan 2016). Threat actors could also be “outsiders” who can access material from insiders by purchasing it or by using blackmail or other threatening forceful behaviour.

Another dimension to improving threat detection relates to organizational and governance issues in “Five Eyes” ICs. These issues concern how ICs are structured, coordinated and led to manage the evolving non-state actor CBRN threat environment. Are organizational and internal leadership fit for purpose in managing CBRN terrorist threats into the future? And what agencies across “Five Eyes” countries are best suited to own the CBRN threat problem into the future? In the United States with a total of 17 intelligence agencies, there is an ongoing need for IC leaders, particularly the DNI, to review IC wide counter CBRN arrangement to ensure de-conflicted intelligence collection and analysis (Mauroni 2019, 2). The key governance issue for ICs in the foreseeable future will be how to fuse increasing volumes of CBRN-related information to develop better situational awareness. Another enduring governance dimension is how the IC leadership can more effectively bring in external technical expertise as well as ensuring that the analytical workforce also sustains an optimal level of expertise in CBRN issues. ICs also need to develop greater outreach to relevant dual use CBRN-related industries (Walsh 2021).

Threat detection and technology

Across the entire CBRN spectrum there is an increasing suite of dual-use technology available – making it easier and more affordable for terrorist groups to access and potentially weaponize. As noted earlier, assessing the significance of technology to future CBRN uptake by terrorists is fraught with inaccuracies. Care is warranted in avoiding overly technologically deterministic assessments given most terrorists are not operating at the cutting edge of science. Nonetheless, ICs need to investigate how quickly such technology can morph into commercial-off-the-shelf applications that could boost terrorist capabilities (Ackerman and Jacome 2018, 32). As new technologies become available for sale online, they

can be purchased and quickly delivered around the globe – effectively resulting in what Ackerman and Jacome refer to as “the ‘democratization’ of the means of mass destruction” (Ackerman and Jacome 2018, 32). Additionally, any assessments of technological developments need to consider that the rate of change and length of time between major breakthroughs is continually decreasing (Ackerman and Jacome 2018, 32).

Space does not allow an exhaustive assessment of all CBRN related dual use technology. Instead in the next section I briefly list three dual use technology areas: *3D printing/additive manufacturing*, *CRISPR* and *drones*, which may be exploited by terrorist groups.

3D printing/additive manufacturing

The rapid growth in 3D printing/additive manufacturing for legitimate science and technology sectors (e.g. medicine) also opens up opportunities for their illicit use by terrorists for CBRN weapons. The ability of a terrorist network to procure for example 3D printed nuclear components or their files is one example. Additive manufacturing provides avenues for cheaper, faster and stealthier methods for acquiring dual use sensitive information and technology where deception is more difficult to detect by ICs (Rid 2011; Anderson 2016; Albright, Brannan, and Stricker 2010).

There are a number of potential scenarios where terrorist groups could exploit current difficulties in the detection and movement of additive manufactured products and files. For example, 3D printing files of nuclear equipment could be shared with a terrorist group via a third party – thereby avoiding any export control detection (Fey 2017, 1–44).

CRISPR

Gene editing tools like CRISPR, which allow accurate genetic modifications achieved by the use of small strands of RNA to guide proteins (e.g. CAS protein) to a specific site in an organism’s DNA, holds much promise for a range of medical treatments and other legitimate uses in bio-sciences. As noted earlier, the US IC has already expressed concerns that this technology could be weaponized by terrorists (Clapper 2016). But further work is required by ICs on what ways terrorist groups could exploit CRISPR.

Drone swarms

Conventional drones are already being exploited by some terrorist groups (Gibbons-Neff 2017; Warrick 2017; Sims 2018). Rapid development of smaller drone swarms, however, could also be used in a coordinated delivery of CBRN attacks in the battlespace or a metropolitan environment (Kallenborn and Bleek 2018). Again, further collection and analysis is required on how this technology can be exploited by threat actors.

Threat disruption

Despite the potential for some terrorist groups to exploit CBRN-related dual use technology for attacks, ICs are progressing their understanding of technology, knowledge and skills, which can enhance their capabilities for CBRN detection and disruption. For example, developments in two multi-disciplinary fields (cyber and forensics) will likely continue to play an important role in CBRN terrorism threat disruption. We have seen how, for example, in the 2010 stuxnet attack on an Iranian uranium enrichment plant and other facilities, which introduced IC malware, can disrupt progression of CBRN terrorist capabilities (Mugavero et al. 2018, 52). In addition to investment by “Five Eyes” partners in offensive cyber intelligence capabilities (Vavra 2019), developments in forensic science are also useful in detecting and disrupting CBRN attacks. Limited space does not allow an exploration of the various forensic applications currently being developed. Some are sceptical of the role of forensics thus far in, for example, the unreliable detection rates of bio-agents in programmes such as the US Biowatch program (Walsh 2018, 182). But research efforts suggest that forensics will remain critical in the development of early sensor systems for countering CBRN terrorism (Zöller and Genzel 2018; Shea and Lister 2003; Walsh 2018; Kouzes et al. 2008, 383–400).

Ethical challenges

The key ethical challenge arising from CBRN terrorism relates to the moral duty “Five Eye” ICs have to protect both the lives of citizens and non-citizens from attacks. The ICs bear only some of the moral and institutional responsibility to protect society. Other state instruments (military, health, foreign ministries and dual use industries) also have a collective moral responsibility to protect society from CBRN terrorism (Miller 2006, 176–93). But in this chapter, the focus is on the IC’s role.

In this last section, I outline how IC collection against potential CBRN terror attacks presents additional hitherto not well-understood ethical and policy dilemmas that require further assessment. Fulfilling a moral duty by the state to preserve life is contingent on ICs having situational awareness about the intent and capability of terrorists to launch CBRN attacks. This in turn, as noted earlier, relies on “Five Eyes” ICs improving the accuracy of CBRN threat detection capabilities that can more reliably direct where intelligence collection, analytic and operational resources are best allocated to prevent and disrupt attacks. Improving threat and risk assessment capabilities will require as noted earlier continued institutional improvements across ICs. In particular, improvements are required in governance arrangements within ICs and a greater focus on analytical expertise and performance. Additionally and perhaps even more importantly, ICs need to develop strategies for sustained and systematic engagement with experts outside the community, who will be better placed to advise how various CBRN technologies could be exploited by terrorists. ICs are engaging more with outside experts on CBRN technology issues, but they will also need to develop their own

knowledge and skills about CBRN terrorist threat actors' intentions and capabilities through covert collection and rigorous analysis.

Given the grave psychological and physical consequences of even a small CBRN-enabled terrorist attack in Sydney, Washington DC or London, ICs need to conceptualize and operationalize a more expanded pro-active intelligence collection approach to this threat type. We have already witnessed in the period after 9/11 the growth in counter-terrorism policy and legislative powers that have lowered the threshold and expanded the kinds of collection that ICs are able to do on those suspected of being involved in terrorism offences (Cogan 2004; Walsh 2016, 51–74; Walsh and Miller 2016). For all ICs, these creeping powers — while undoubtedly in many cases helping in the earlier identification of a group/individual planning conventional terrorist attacks — have also sharpened debates in liberal democracies about the impact of collection on individuals' privacy and broader human rights. This includes the liberty for individuals, who might in some circumstances be subjected to preventative detention or control orders if suspected but not yet charged of being involved in terrorism as seen in the Australian context. While collection against known terrorists should align with principles of necessity, proportionality and discrimination, many of the enhanced proactive collection powers ICs now have at their disposal may be targeted (accidentally or by intent) at innocent citizens and thus potentially result in a violation of privacy and other human rights. Determining the extent of surveillance required in a counter-terrorism case will be decided by a range of contextual factors that will be different depending on the individuals involved (e.g. citizens, non-citizens, reasonable suspicion, foreign vs. domestic actors and immediacy of threat).

The ongoing debates about the impact of growing aggressive and permissive approaches to intelligence collection are also relevant to collection efforts against CBRN terrorism. However, given the discussion earlier of terrorists' potential exploitation of dual use technology, it is possible that ethical dilemmas posed by collecting against CBRN terrorism may grow beyond those seen in conventional terrorism. As noted earlier, a growing suite of knowledge, skills and technologies in the chemistry, biology, radiology and nuclear fields is providing significant advancements to fulfil legitimate human needs such as medicine and energy.

However, as seen acutely in the biological sciences and biotechnology sector, dual use technology can be exploited by bad actors for malevolent ends. The ability by ICs to gain more accurate evidence-based threat assessments is therefore dependent on collecting a great deal more information about the skills and knowledge of people working in a range of public and private organizations across the diverse chemical, biological, radiological and nuclear sectors. Space limitations do not allow a comprehensive analysis of all the ethical dilemmas arising from an expanded collection across all CBRN-related industries. But considering briefly the biological and biotechnology sector, it's clear that ICs would potentially be interested in information from a range of different experts working across a diverse number of contexts such as private biotech companies, universities, public research institutes, hospitals, graduate students, military personnel, lab biosafety officials, biology suppliers, forensic scientists and scientific publishers. Detection

of CBRN-enabled terrorist threats will remain difficult for all the reasons discussed earlier, particularly if plans and activities are hidden in legitimate dual use research. Hence the prevention and disruption of such threats will likely rely on more invasive collection from the experts and contexts just mentioned – at least for the case of biologically enabled attacks. What could more invasive collection in the biological sciences environment mean?

Firstly, it would go beyond the standard security clearance testing that all scientists must undergo if they wish to work with biological select agents. These are mandated legislatively, and people working with dangerous pathogens accept these checks as a condition of employment despite them being intrusive. Nonetheless, other more invasive collection strategies could be targeted against either suspects personally; the environment where they work; or a setting in which there may be some security concerns. Invasive collection might include enhanced CCTV surveillance in a facility under investigation, IC or police questioning of persons and other co-workers, more regular security checks, examination of hard copy and digital files and equipment, security vetting of research results and publications and accessing medical/mental health records.

While some IC agencies across “the Five Eyes” have developed trusting and productive relationships with important stakeholders in the biology and biotechnology sector such as the FBI’s research community outreach initiatives, these efforts are by no means uniform across either the US IC or other “Five Eyes” countries. Therefore, in addition to developing better collection and analytical capabilities to assess and disrupt CBRN terrorist threats, ICs need to consider the ethical consequences that may arise from additional invasive intelligence collection in dual use technology and research contexts. The actual ethical risks arising from collection across CBRN dual use research and technology sectors cannot be generalized and will rely on a range of variables including but not limited to *collection methods* (e.g. meta data, social media, mental health history records), *threat evolution* (reports of “suspicious activity” vs. direct evidence of conspiracy to commit terrorism), *contexts* (e.g. military, espionage, criminal, terrorism) and the *nature of the target* (physical location, history and provenance of all relevant information).

While more work is now being done to examine the ethical dimensions of dual use research and technology in the broader sense, particularly in synthetic biology (National Academies of Sciences, Engineering, and Medicine et al. 2017; Miller and Selgelid 2007; Miller 2018), it’s clear that an important next step must be a deeper ethical and policy analysis of how *intelligence collection* across the CBRN dual use spectrum impacts on the privacy and human rights of those working in these sectors. Such an endeavour would not only help to address the public’s concerns over the powers and legitimacy of ICs, but also help to improve the efficacy of actual collection approaches under taken.

Conclusion

This chapter has surveyed the emerging CBRN terrorist threat space. There are a number of assessment uncertainties for ICs, but it is likely given resource

constraints that any CBRN programmes will be smaller scale than conventional state-based WMD programmes. Likewise the impact of such attacks, though disruptive and psychologically profound, will not result in mass casualty levels associated with WMD programmes.

“Five Eyes” ICs are nonetheless gaining a greater understanding of threat and risk trajectories for CBRN terrorism. However, ICs need to develop sustained collection and analysis against potential attack vectors and more nuanced understanding of the psychological, social and technical drivers influencing terrorist’s interest and capability in CBRN dual use technologies. The IC’s ability to assess threat, risk and then prevent/disrupt CBRN terrorist attacks will increasingly rely on effective external and internal governance that can better integrate relevant and limited collection and analytical assets. Finally, given the diversity of the dual use technology and research sector, and in order to more effectively prevent and disrupt CBRN terrorism, it is likely that IC surveillance will need to expand further into these sectors. This will raise additional policy and ethical dilemmas for ICs and citizens of liberal democratic states which at this point are not well understood.

Notes

- 1 Though now the Organisation for the Prevention of Chemical Weapons (OPCW) has recently developed additional security and legal support initiatives to help CWC member-states manage chemical terrorism.
- 2 Since the FBI officially closed the investigation in 2010 several biologists and chemists disagree on whether the Bureau got the right perpetrator based on the presence of silicon and tin coating on the anthrax spores. In the opinion of some experts this suggests a greater complexity of manufacturing beyond the scope of what Ivins could do in his lab. Additionally, earlier in the investigation another army research scientist Steven Hatfield was targeted, but later exonerated, with the DOJ paying a \$4.6 million legal settlement to the scientist.
- 3 For a more detailed discussion of non-state actors and stolen biological agents, see Walsh (2018, 37–41).
- 4 In the US, easily over 2 million people are employed with over 73,000 businesses working across range of biosciences (medicine, agriculture, pharmaceuticals, research (Biotechnology Innovation Organization, 2014).
- 5 A dirty bomb, otherwise known as a radiological dispersal device (RDD), combines conventional explosives, like dynamite, with radiological material. The regular explosive helps in dispersing the radioactive material.

References

- Ackerman, Gary, and Michelle Jacome. 2018. “WMD Terrorism: The Once and Future Threat”. *PRISM* 7 (3): 22–37.
- Albright, David, Paul Brannan, and Andrea S. Stricker. 2010. “Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan”. *The Washington Quarterly* 33 (2): 85–106. <https://doi.org/10.1080/01636601003673857>.
- Allison, Graham. 2018. “Nuclear Terrorism: Did We Beat the Odds or Change Them?” *PRISM | National Defense University* 7 (3): 2–21.

- Anderson, David. 2016. *Report of the Bulk Powers Review*. London: HMSO.
- Bajema, Natasha, and Diane DiEuliis. 2017. *Peril and Promise: Emerging Technologies and WMD*. Washington, DC: National Defense University. Report for 12–13 October 2016 Emergence and Convergence Workshop.
- Balatsky, Galya I., and William R Severe. 2019. “Illicit Trafficking of Radioactive and Nuclear Materials”. In *Nuclear Safeguards, Security, and Nonproliferation*, edited by James E. Doyle, 2nd edition, 357–87. Boston: Butterworth-Heinemann. <https://doi.org/10.1016/B978-0-12-803271-8.00012-6>.
- Berger, Sarah. 2015. “What Is ISIS’ Chemical Weapons Stockpile? Islamic State Group Has Recruited Experts from across the World to Build Terror Arsenal”. *International Business Times*, November 19.
- Binder, Markus K., and Gary A. Ackerman. 2019. “Pick Your POICN: Introducing the Profiles of Incidents Involving CBRN and Non-State Actors (POICN) Database”. *Studies in Conflict & Terrorism* 0 (0): 1–25. <https://doi.org/10.1080/1057610X.2019.1577541>.
- Binder, Markus K., Jillian M. Quigley, and Herbert F. Tinsley. 2018. “Islamic State Chemical Weapons: A Case Contained By Its Context?” *CTC Sentinel* 11 (3): 27–32.
- Biotechnology Innovation Organization. 2014. “Battelle/BIO State Bioscience Jobs, Investments and Innovation 2014”. www.bio.org/articles/battellebio-state-bioscience-jobs-investments-and-innovation-2014.
- Boyle, Darren. 2015. “ISIS Scientists Set to Wage Chemical and Biological War on West”. Mail Online. December 6. www.dailymail.co.uk/news/article-3347671/ISIS-army-scientists-set-wage-chemical-biological-war-West-Experts-warn-weapons-mass-destruction-carried-undetected-Europe-Union.html.
- Bunn, Matthew, and Scott D. Sagan, eds. 2016. *Insider Threats*. 1st edition. Ithaca; London: Cornell University Press.
- Butler, Desmond. 2015. “Nuclear Black Market Seeks IS Extremists”. *AP NEWS*, October 7. <https://apnews.com/article/9f77a17c001f4cf3baeb28990b0d92eb>.
- Butler, Robin. 2004. *Review of Intelligence on Weapons of Mass Destruction Report of a Committee of Privy Counsellors*. London: The Stationary Office. <https://fas.org/irp/world/uk/butler071404.pdf>.
- Carlson, Robert. 2003. “The Pace and Proliferation of Biological Technologies”. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 1 (3): 203–14. <https://doi.org/10.1089/153871303769201851>.
- Carus, Seth. 2000. “The Rajneeshees”. In *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, edited by Jonathan B. Tucker, Steven E. Miller, and Sean M. Lynn-Jones, Illustrated edition. Cambridge, MA: MIT Press.
- Caves, John, and Seth Carus. 2014. *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*. Washington, DC: Center for the Study of Weapons of Mass Destruction.
- Chyba, Christopher F. 2006. “Biotechnology and the Challenge to Arms Control”. *Arms Control Today*, October 2006.
- Cirincione, Joe, and Geoff Wilson. 2015. “Why I Fear the Dirty Bomb and You Should Too”. *War on the Rocks*, November 10. <https://warontherocks.com/2015/11/why-i-fear-the-dirty-bomb-and-you-should-too/>.
- Clapper, James R. 2016. “Statement for the Record Worldwide Threat Assessment of the US Intelligence Community”. www.odni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.
- Clarke, Michael. 2013. “Pakistan and Nuclear Terrorism: How Real Is the Threat?” *Comparative Strategy* 32 (2): 98–114. <https://doi.org/10.1080/01495933.2013.773700>.

- Cogan, Charles. 2004. "Hunters Not Gatherers: Intelligence in the Twenty-First Century". *Intelligence and National Security* 19 (2): 304–21. <https://doi.org/10.1080/0268452042000302010>.
- Cornish, Paul. 2007. *The CBRN System: Assessing the Threat of Terrorist Use of Chemical, Biological, Radiological and Nuclear Weapons in the United Kingdom*. London: Chatham House (The Royal Institute of International Affairs). www.chathamhouse.org/sites/default/files/public/Research/International%20Security/cbrn0207.pdf.
- Danzig, Richard, Marc Sageman, Terrance Leighton, Lloyd Hough, Hidemi Yuki, Rui Kotani, and Zachary M. Hosford. 2012. *Aum Shinrikyo: Insights into How Terrorists Develop Biological and Chemical Weapons*. Washington, DC: Center for a New American Security. www.jstor.org/stable/resrep06323.
- Doombos, Harald, and Jenan Moussa. 2014. "Found: The Islamic State's Terror Laptop of Doom". *Foreign Policy* (blog). August 28. <https://foreignpolicy.com/2014/08/28/found-the-islamic-states-terror-laptop-of-doom/>.
- Elvey, Suz. 2015. "Timebomb: The Biological Weapons AND the Islamists Who Will Arm Them Are ALREADY Here". *Express*, December 6. www.express.co.uk/news/uk/624620/Warning-ISIS-Daesh-chemical-weapons-attack-West.
- Fey, Marco. 2017. *3D Printing and International Security: Risks and Challenges of an Emerging Technology*. Frankfurt: Peace Research Institute Frankfurt.
- Flood, Philip. 2004. *Report of the Inquiry into Australian Intelligence Agencies*. Canberra: AGPS.
- Genry, John A., and Joseph S. Gordon. 2019. *Strategic Warning Intelligence: History, Challenges, and Prospects*. 1st edition. Washington, DC: Georgetown University Press.
- Gibbons-Neff, Thomas. 2017. "ISIS Drones Are Attacking U.S. Troops and Disrupting Airstrikes in Raqqa, Officials Say". *Washington Post*, June 6. www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-drones-are-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say/.
- Habegger, Beat. 2010. "Strategic Foresight in Public Policy: Reviewing the Experiences of the UK, Singapore, and the Netherlands". *Futures* 42 (1): 49–58. <https://doi.org/10.1016/j.futures.2009.08.002>.
- Hoffman, Wyatt, and Tristan A. Volpe. 2018. "Internet of Nuclear Things: Managing the Proliferation Risks of 3-D Printing Technology". *Bulletin of the Atomic Scientists* 74 (2): 102–13. <https://doi.org/10.1080/00963402.2018.1436811>.
- Hvistendahl, Mara. 2016. "3D Printers Vulnerable to Spying". *Science* 352 (6282): 132–3. <https://doi.org/10.1126/science.352.6282.132>.
- Ivanova, Kate, and Todd Sandler. 2006. "CBRN Incidents: Political Regimes, Perpetrators, and Targets". *Terrorism and Political Violence* 18 (3): 423–48. <https://doi.org/10.1080/09546550600752014>.
- Kallenborn, Zachary, and Philipp C. Bleek. 2018. "Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons". *The Nonproliferation Review* 25 (5–6): 523–43. <https://doi.org/10.1080/10736700.2018.1546902>.
- Kaplan, David K., and Andrew Marshall. 1996. *The Cult at the End of the World: Incredible Story of Aum*. 1st edition. London: Crown.
- Kelly, Robert E. 2017. *Is Three-Dimensional (3-D) Printing a Nuclear Proliferation Tool?* Stockholm: SIPRI.
- Koblentz, Gregory D. 2009. *Living Weapons: Biological Warfare and International Security*. 1st edition. New York: Cornell University Press.
- Kouzes, Richard T., Edward R. Siciliano, James H. Ely, Paul E. Keller, and Ronald J. McConn. 2008. "Passive Neutron Detection for Interdiction of Nuclear Material at

- Borders". *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 584 (2): 383–400. <https://doi.org/10.1016/j.nima.2007.10.026>.
- Kroenig, Matthew, and Tristan Volpe. 2015. "3-D Printing the Bomb? The Nuclear Non-proliferation Challenge". *The Washington Quarterly* 38 (3): 7–19. <https://doi.org/10.1080/0163660X.2015.1099022>.
- Maurer, Stephen M., ed. 2009. *WMD Terrorism: Science and Policy Choices*. Cambridge, MA: The MIT Press.
- Mauroni, Albert. 2019. "The Rise and Fall of Counterproliferation Policy". *The Nonproliferation Review* 26 (1–2): 1–15. <https://doi.org/10.1080/10736700.2019.1593691>.
- McIntosh, Christopher, and Ian Storey. 2018. "Between Acquisition and Use: Assessing the Likelihood of Nuclear Terrorism". *International Studies Quarterly* 62 (2): 289–300. <https://doi.org/10.1093/isq/sqx087>.
- Miller, Seumas. 2006. "Collective Moral Responsibility: An Individualist Account". *Midwest Studies in Philosophy* 30 (1): 176–93. <https://doi.org/10.1111/j.1475-4975.2006.00134.x>.
- . 2018. *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Springer Briefs in Ethics. Springer International Publishing. <https://doi.org/10.1007/978-3-319-92606-3>.
- Miller, Seumas, and Michael J. Selgelid. 2007. "Ethical and Philosophical Consideration of the Dual-Use Dilemma in the Biological Sciences". *Science and Engineering Ethics* 13 (4): 523–80. <https://doi.org/10.1007/s11948-007-9043-4>.
- Mowatt-Larssen, Rolf. 2010. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" *Belfer Center for Science and International Affairs* (blog). January 2010. www.belfercenter.org/publication/al-qaeda-weapons-mass-destruction-threat-hype-or-reality.
- Mueller, John. 2019. "Nuclear Weapons Don't Matter". January 29. www.foreignaffairs.com/articles/2018-10-15/nuclear-weapons-dont-matter.
- Mugavero, Roberto, Stanislav Abaimov, Federico Benolli, and Valentina Sabato. 2018. "Cyber Security Vulnerability Management in CBRN Industrial Control Systems (ICS)". *International Journal of Information Systems for Crisis Response and Management* 10 (April): 49–78. <https://doi.org/10.4018/IJISCRAM.2018040103>.
- National Academies of Sciences, Engineering, and Medicine, Policy and Global Affairs, Committee on Science, Technology, and Law, and Committee on Dual Use Research of Concern: Options for Future Management. 2017. *Dual Use Research of Concern in the Life Sciences: Current Issues and Controversies*. Washington, DC: National Academies Press (US). www.ncbi.nlm.nih.gov/books/NBK458491/.
- National Defense University. 2003. "Toward a National Biodefense Strategy: Challenges and Opportunities, April 2003". Center for Counterproliferation Research, National Defense University, Washington, DC. <https://web.archive.org/web/20130221101014/www.ndu.edu/centercounter/CCR%202003.pdf>.
- Petro, James B., and Seth Carus. 2005. "Biological Threat Characterization Research: A Critical Component of National Biodefense". *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 3 (4): 295–308. <https://doi.org/10.1089/bsp.2005.3.295>.
- Pita, René. 2007. "Assessing Al-Qaeda's Chemical Threat". *International Journal of Intelligence and CounterIntelligence* 20 (3): 480–511. <https://doi.org/10.1080/08850600701249824>.
- Rathore, Shahzeb Ali. 2016. "Is the Threat of ISIS Using CBRN Real?" *Counter Terrorist Trends and Analyses* 8 (2): 4–10.

- Rid, Thomas. 2011. "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35 (1): 5–32.
- Rosenau, William. 2001. "Aum Shinrikyo's Biological Weapons Program: Why Did It Fail?" *Studies in Conflict & Terrorism* 24 (4): 289–301. <https://doi.org/10.1080/10576100120887>.
- Rosoff, Heather, and Detlof Von Winterfeldt. 2007. "A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach". *Risk Analysis* 27 (3): 533–46. <https://doi.org/10.1111/j.1539-6924.2007.00908.x>.
- Shaw, Robert. 2017. "3D Printing: Bringing Missile Production to a Neighborhood Near You | NTI". *NTI* (blog). February 22. www.nti.org/analysis/articles/3dprinting-bringing-missile-production-neighborhood-near-you/.
- Shea, Dana A., and Sarah A. Lister. 2003. *The BioWatch Program: Detection of Bioterrorism*. Washington, DC: Congressional Research Service.
- Sims, Alyssa. 2018. "The Rising Drone Threat from Terrorists". *Georgetown Journal of International Affairs* 19 (November): 97–107. <https://doi.org/10.1353/gia.2018.0012>.
- SSCI. 2004. *Report on the US Intelligence Community's Pre War Intelligence Assessments on Iraq*. Washington, DC: US Government Printing Office.
- Strack, Columb. 2017. "The Evolution of Islamic State's Chemical Weapons". *CTC Sentinel* 10 (9): 19–24.
- Tenet, George. 2007. *At the Center of the Storm*. 1st edition. New York: HarperCollins.
- Tucker, Jonathan B., Steven E. Miller, and Sean M. Lynn-Jones. 2000. *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*. Cambridge, MA: MIT Press.
- van de Velde, James R. 2010. "The Impossible Challenge of Deterring 'Nuclear Terrorism' by Al Qaeda". *Studies in Conflict & Terrorism* 33 (8): 682–99. <https://doi.org/10.1080/1057610X.2010.494155>.
- Vavra, Shanon. 2019. "'This Isn't IAD 2.0': NSA's New Cybersecurity Directorate Plots Its Mission". *Cyberscoop* (blog). July 25. www.cyberscoop.com/nsa-cybersecurity-directorate-neal-ziring-dave-frederick/.
- Vogel, Kathleen M. 2008. "Biodefense". In *Biosecurity Interventions Global Health and Security in Question: Global Health and Security in Practice*, edited by Andrew Lakoff and Stephen Collier, 1st edition, 227–55. New York: Columbia University Press.
- . 2013. "Necessary Interventions: Expertise and Experiments in Bioweapons Intelligence Assessments". *Science, Technology and Innovation Studies* 9 (2): 61–88.
- Walsh, Patrick F. 2016. "Managing Emerging Health Security Threats since 9/11: The Role of Intelligence". *International Journal of Intelligence and CounterIntelligence* 29 (2): 341–67. <https://doi.org/10.1080/08850607.2016.1121048>.
- . 2018. *Intelligence, Biosecurity and Bioterrorism. Intelligence, Biosecurity and Bioterrorism*. London: Palgrave Macmillan. <https://doi.org/10.1057/978-1-137-51700-5>.
- . 2021. *Intelligence Leadership and Governance*. Abingdon: Routledge.
- Walsh, Patrick F., and Seumas Miller. 2016. "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden". *Intelligence and National Security* 31 (3): 345–68. <https://doi.org/10.1080/02684527.2014.998436>.
- Warrick, Joby. 2017. "Use of Weaponized Drones by ISIS Spurs Terrorism Fears". *Washington Post*, February 21, sec. National Security. www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.
- Weiss, Leonard. 2015. "On Fear and Nuclear Terrorism". *Bulletin of the Atomic Scientists* 71 (2): 75–87. <https://doi.org/10.1177/0096340215571909>.

- Zhang, Lisa, and Gigi Kwik Gronvall. 2020. "Red Teaming the Biological Sciences for Deliberate Threats". *Terrorism and Political Violence* 32 (6): 1225–44. <https://doi.org/10.1080/09546553.2018.1457527>.
- Zöller, Lothar, and Gelimer H. Genzel. 2018. "The Role of Bioforensics in Medical Bio-Reconnaissance". In *Defence against Bioterrorism*, edited by Vladan Radosavljevic, Ines Banjari, and Goran Belojevic, 177–87. NATO Science for Peace and Security Series A: Chemistry and Biology. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-024-1263-5_13.

17 Reflections on the future of intelligence

Gregory F. Treverton

Introduction

This chapter reflects on my experiences in government, in both policy and intelligence positions, drawing especially on my recent tenure as Chair of the US National Intelligence Council (NIC).¹ It 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.

That would have been my list of challenges had Donald Trump not been elected president. Yet here, too, as in almost every aspect of US policy, the Trump administration scrambled the deck, injecting enormous uncertainty. Its malfeasance raised three additional challenges: reinvigorating a demoralized workforce; reorienting domestic intelligence, and last, and most worrisome, dealing with a world in which truth is personal or subjective, and, indeed, the very idea of truth is under attack. Thus, this chapter begins with the challenges as I might have portrayed them in more normal times, then concludes with reflections on my puzzlement about how lasting and how momentous the distinctly non-normal times of the Trump administration will prove to be.

Balancing strategic and tactical

An enduring challenge for the Intelligence Community is balancing the urgent need for actionable tactical intelligence with the need for too often-neglected strategic intelligence. The hand wringing about the primacy of urgent tactical intelligence over strategic has characterized all my years as a student, consumer and sometimes practitioner of intelligence. This issue is made all the worse by the shapelessness of the current world, which means that every crisis must be approached afresh on its own terms. This is especially heightened by the nation's hypersensitivity to the threat of terrorism, which poses a minimal threat to the United States homeland but is hardly perceived that way by the public – or so characterized by politicians (Malley and Finer 2018).

DOI: 10.4324/9781003164197-24

From my perch at the NIC, this acute sensitivity to terrorism was doubly deforming of our work. When we looked at Nigeria, there was not much Nigeria: it was Boko Haram. Instead of focusing on the complexities facing Nigeria, Africa's largest economy and highest population, we solely focused on a terrorist group in Nigeria's north. And even when we looked at Boko Haram, there was not much Boko Haram: it was all deciphering networks and targeting bad guys. We all wondered and worried, where do these people come from, and why are they doing what they're doing? Although we did what we could at the NIC trying to understand root causes and motivations, we were only scratching the surface of Boko Haram, let alone Nigeria.

In 2016, the NIC produced about 700 pieces of paper. More than half of those were memoranda that were set in motion by the deliberations of the two main policymaking bodies in the administration – the Principals Committee, comprised of the relevant cabinet secretaries, or, more often, the Deputies Committee, comprised of their deputies or number threes. These memoranda were produced in response to “taskings” by the National Security Advisor, one of her deputies, or another senior National Security Council official, and were used as the focal point for assessing options and teeing up decisions. Not all those papers were purely tactical. Some were the “what ifs?” of the sort that should be the warp and woof of intelligence-policy relations: “if we do x, how will Putin respond?” Because we were at all the policy meetings, we knew what was going on. Yet as Chair of the NIC, my task, every day, was to find the time and capacity not only to answer the questions policy officials asked but also to answer the more strategic ones they weren't asking.²

The perils of focusing on the tactical at the expense of the strategic run through many episodes of American foreign policymaking

A prominent example is the decision to arm Islamic mujahideen resistance during the Soviet Invasion of Afghanistan. Although America's decision ultimately led to the Soviet Union's eventual retreat from Afghanistan, it also empowered radical Islamic elements, some of which later became the Taliban, which in the end overthrew the government of Afghanistan, and perhaps most importantly harboured Osama bin Laden. To be sure, it would have been hard at the time to raise cautions about putting pressure on Moscow based on analysis of second-order, and thus iffy, effects.

Likewise, the decision to remove Saddam Hussein was a tactical success but a strategic disaster. It did remove from power a brutal dictator, but the second-order effects created a power vacuum filled by Iran, opened space for the rise of ISIL and intensified the Cold War between Saudi Arabia and an empowered Iran. Nowhere is this failure clearer than five years after the invasion. While visiting Iraq, Iranian President Mahmoud Ahmadinejad was greeted with an elaborate state visit, while a mere two weeks later, Vice President Cheney had to be flown under secrecy (Maloney 2008). America's later decision to leave Iraq left a power

vacuum that enabled the Islamic State to rapidly expand. In short, although tactical intelligence is essential in planning an action, it needs to be viewed in light of more strategic intelligence, intelligence that seeks to parse longer term implications and second-order effects of an action.

Building – and adjusting – “stories” in a shapeless world

The shapelessness of the world both confounds and demands strategic analysis. In providing strategic analysis, I have come to think that intelligence is ultimately about telling stories and most intelligence – or warning – failures derive from holding onto stories that events have outmoded. This challenge is akin to the strategic/tactical challenge facing intelligence and one that bears more directly on warning. A story from another realm, medicine, drives the point home. The medical community had a “story” about the Ebola virus: because death was quick, contagion was unlikely and so the disease would flare up and die out in remote regions. The story was right until it wasn’t: the story had been overtaken by better transit from rural to urban areas. This outdated story led to cases in the United States and to widespread, if not entirely founded, fear of an Ebola pandemic (World Health Organization 2015).

If intelligence is storytelling, many of our current stories are suspiciously long in the tooth. In policy terms, for instance, we have been telling ourselves the same story about North Korea for a generation. With just the right combination of carrots and sticks – primarily the latter – and with China as a real partner, we can induce North Korea to forswear nuclear weapons. Meanwhile, North Korea has gone from an incipient nuclear power to a real one. Intelligence cannot prove and thus cannot say the truth: North Korea is a nuclear power and almost certainly will remain one; that is all the regime has.³ But at the very least, challenging the prevailing story would be a start.

For other critical issues, like the Middle East, we have no real story beyond demonizing terrorists and Iran. To be sure, the task is hard. Throughout my tenure at the NIC, I looked for strategic insights and found precious few because the issues are complicated, and the causal arrows tangled. The best story I found came from our Australian intelligence colleagues. They divided the conflicts into three and a half factions – the ISIL-led Sunni extremists; the Saudi-led Sunni autocrats; the Iran-led Shias and the missing half, the Muslim Brotherhood-led Sunni moderates, recognizing that the term “moderate” is relative at best. But the difficulty of the task is no justification for not trying it. Without a story, we can all too easily blunder into major campaigns against minor threats or worse yet, create those threats.

In the past, America has shown its ability to alter an existing story to great effect. Perhaps most famously, the US decision to recognize the communist China at the expense of Taiwan and treat the country as a counterweight to the Soviet Union was a great success. This partnership fractured the communist world and helped further isolate the Soviet Union. When Nixon and Kissinger decided to covertly meet with Mao, they did this without warning the State Department or

US allies (notably Japan and Taiwan), fearing pushback. Yet once the new story was set, it paved the way for what seemed impossible a few years before – better Sino – American relations (Hutchings and Treverton 2018). Likewise, America’s decision to partner with its old enemy, communist Vietnam, against an ascendant China, shows that reshaping stories can strengthen American policy (Albert 2019).

Transparency and “big data”

These are two sides of the same coin. The same ubiquity of information that produces so much for intelligence agencies to assess also makes it impossible for intelligence operatives to remain secret for long. This, alas, guarantees that there will be more leaks of methods, if not more leakers, like Edward Snowden. Perhaps the vision of the future should be more akin to Silicon Valley, where secrets are kept but not for long and where the premium is on collaboration even if today’s partner may be tomorrow’s competitor.

At the NIC, I was only an observer to intelligence *operations*, but I had the sense that, with respect to clandestine operations, the United States was like the roadrunners in the old cartoons: when they ran off the cliff they didn’t start to fall until they looked down. Given biometrics, facial recognition and ubiquitous cameras, US spy tradecraft has run off the cliff; it just hadn’t looked down yet. Surely, operating under official cover without the knowledge of the host government will become all but impossible. Before I left the RAND Corporation, a retired former CIA station chief joined us. The CIA asked him to do a mission in the country where he had been chief. He said he was happy to do it but only under true name. He knew that any effort to operate under cover would be blown and – to say the least – complicate his future private visits to that country.

But that data will be a godsend for intelligence. Indeed, the analytic challenge is greater for intelligence than for private businesses. Businesses care mostly about learning my preferences and predicting where I will be tomorrow so they can besiege me with personalized ads. By contrast, intelligence is trying to sort out a messy world full of noise and misinformation. Yet Artificial Intelligence (AI) is a natural fit for many intelligence tasks. The Open Source Enterprise, for instance, seeks to read every newspaper in the world, in every language, and monitor every television news broadcast, seeking nuggets of new information or insight (Tucker 2020). AI is a natural fit for it. So, too, it is a natural fit for the National Security Agency (NSA), which uses it not just to sort through the massive amount of signals intelligence it collects, looking for anomalies and potential threats, but also for compliance. NSA does lots of “queries” – that’s NSA-speak for getting access to signals intelligence data on an individual – which requires the paperwork of an audit to decide whether that data can be reported. AI won’t replace human oversight, but it can be used to predict the audit results with pretty high confidence.

At the NIC, I started an experiment with the National Intelligence Officer (NIO) for Africa. Its premise was that while there isn’t a huge amount of intelligence gathered on Africa, there is a lot of data out there. Thus, the goal was an existence theorem: if the NIC, with 100 analysts, could make use of data, then any

place in the Intelligence Community could. Not surprisingly, we found that social media and other available data were pretty good at predicting famine and disease. The next step was to cull “tips” from the data: where should analysts look and what connections should they probe that they hadn’t considered.

The NIC also inherited a nifty bit of crowdsourcing that had been developed by the Intelligence Advanced Research Projects Activity (IARPA), intelligence’s counterpart to DARPA. There were two prediction markets: one classified and comprised of intelligence professionals, and the other unclassified and open. The unclassified one was the creation of Philip Tetlock and it had made two important discoveries. Just as some people are better athletes than others, so too, some people are better predictors. His open market came to feature “super-forecasters”.⁴ Even better, a small amount of training improves prediction. Unsurprisingly, the burden of that training is helping people keep an open mind just a few seconds longer.

I used the internal market as a kind of “red cell” – that is, a person or group charged with being contrarian. Here, I looked for places where the prediction market was contrarian: if the experts thought development x was y percent likely but the market was betting $2y$, what was going on? I didn’t care about the numbers; it was the conversation that mattered.⁵ And I hoped to move the market from fairly short-run predictions, which could be settled soon, to longer, more strategic questions. For them, I hoped we might create way-stations on which to bet and, in the process, perhaps do better at constructing what intelligence calls “indicators”.

Breaking the cycle

It has been often said that the canonical intelligence cycle, from requirements through collection to analysis and dissemination, is often short-circuited. That is true enough – no matter how much intelligence agencies dislike it, policy officials will hanker for the next “raw” spy report or intercept. But as a paradigm the cycle is increasingly unhelpful. In this as in many other ways, what worked tolerably well in the Cold War is dysfunctional now. Then, with one overarching and secretive foe, it made a certain sense to ask, in a linear way, what we needed to know and how we might collect it. Even then analysis had a certain industrial quality about it: a friend who was an NSA Soviet analyst recalls starting the day with a large stack of “her take”, the overnight SIGINT collection relevant to her account.

Moreover, the intelligence cycle simply does not operate as it is described. For instance, it is not guidance from policymakers that sets information requirements, but rather the need to fill gaps in intelligence. Furthermore, the information collectors do not wait for clear requirements before beginning to collect intelligence. If they were to do so, they would not have the intelligence collected when it is needed by policymakers and risk being surprised by sudden events (Hulnick 2006).

Before I returned to the NIC, I had become a fan of “activity-based intelligence”, or ABI.⁶ It was developed in the war zones in Afghanistan and Iraq primarily to unravel terrorist networks and identify bad guys. Identifying Osama bin

Laden's driver was one of its successes. ABI amassed information from many sources around particular locations and then used correlations to develop "patterns of life" that would distinguish potential terrorists from ordinary pious Muslims at prayer. For me, its side benefit was creatively disrupting the canonical cycle. It was "sequence neutral": we might find the answer before we framed the question. Think how often in life that occurs; you don't know you were puzzled about something until you find the answer. And in a world of ubiquitous information, ABI doesn't prize secret sources: if information is useful, it's good; if not, it's not. Finally, perhaps advancing age has made me sceptical of the causation that infuses the canonical cycle. I feel more comfortable with correlation: sure, many of the correlations will be spurious but some will be provocative.

Finding new ways to add value

The traditional model of relations between intelligence and policy, one that is not quite fair to blame entirely on Sherman Kent, is stand-offish lest intelligence be "politicized" by too close an association with policy (Kent 2015). It can be characterized, in caricature, as intelligence throwing elegant analyses over the transom to policy – though no young person these days would have any idea what a "transom" is. Intelligence will be producing those elegant products for as far as the eye can see, but much of the Intelligence Community's stock-in-trade is now available openly as technology continues to evolve. For instance, 30 years ago access to satellite imagery and GPS were only available to US government agencies. Yet today, anyone with a cell phone can access this data and often for free from Google. Although agencies like the National Geospatial-Intelligence Agency (NGA) still have access to imagery with better resolution, the gap of capabilities is only closing.

While these developments might be seen as making much of the Intelligence Community obsolete, they present a great opportunity. The widespread availability of open-source intelligence can be used to complement intelligence, providing a clearer understanding of complex issues. In 2014, for instance, a junior Defense Intelligence Agency (DIA) analyst, browsing Russian social media, was able to determine who shot down Malaysia Airlines Flight 17 (Barnes 2014). As another DIA colleague put it: "Selfies are our best friend".

As in other contexts, the language we use is revealing. Traditionally, intelligence officers thought of their policy counterparts as "customers", which connotes an arms-length, transactional relationship, one in which intelligence provides discrete "products". In my first stint at the NIC, I had one "aha" moment, realizing that while we thought we produced National Intelligence Estimates (NIEs), in fact, our product was National Intelligence Officers (NIOs) – people, not paper. They were in a position to have those elevator conversations with policy counterparts, to give advice informally and not have to be too careful about what was "intelligence" and what was "policy". Similarly, in a study I did of the use of the President's Daily Brief (PDB) by the three administrations before Obama, all of the senior officials who spoke to the issue liked the Brief, but they liked the briefer

better. The briefer offered a way to ask for more, or to take the conversation in a direction especially useful to the policy official (Treverton 2013a).

All possible terms have their negatives, but I think of the recipients of intelligence as “clients”, and liken the intelligence-policy connection to that between me and my financial advisor, a client-service relationship, not a business-customer one: he or she knows things I don’t, but the reverse is also true and it is a relationship between equals. I expect the advisor to ask lots of questions and to get better and better at understanding my interests. He or she is bound by professional code neither to sugar coat the truth nor exaggerate confidence levels. And, in the end, if I don’t feel he or she is adding value, I will go elsewhere.

Intelligence as an argument for policy

This, too, is hardly new. In the past times of divided government, Congress was tempted to, in effect, turn intelligence issues into policy choices by mandating that if intelligence caught Iran exporting x , then y sanctions would be automatic. To be sure, the practice was more than uncomfortable for intelligence, for it meant asking intelligence to put a gun to the heads of its policy counterparts in an administration! More recently, in days of intense partisanship, administrations have been tempted to use intelligence to argue for their policy choices. So it was in the run-up to the 2003 invasion of Iraq. The intelligence assessment that Iraq had weapons of mass destruction made it difficult for Democrats in Congress to oppose the invasion and provided policy cover for supporting it. So, future administrations will be tempted to turn intelligence findings into policy choices: imagine if the Intelligence Community had found what it did not find before the Trump administration scuttled the deal – evidence that Iran was persistently cheating on its obligations under the nuclear deal.

Ironically, when intelligence is used as an argument for policy, it can hamper policy decisions if framed incorrectly. Nowhere is this more evident than in decision to release the key judgements of the classified 2007 National Intelligence Estimate on Iran’s Nuclear Intentions and Capabilities. This estimate stated with high confidence that Iran had its nuclear weapons programme. What it meant by “programme”, as a footnote explained, was weapons design and covert enrichment of weapons-grade uranium. It had not stopped the enrichment of uranium – ostensibly for civil purposes – and the report also noted that Iran was keeping open the option to develop nuclear weapons. Yet when this report was released, the key, albeit false, takeaway was simply that Iran had halted its entire nuclear programme. After this report was released, international momentum for increased sanctions on Iran all but evaporated and the outcome was regarded as a great win in Iran (Treverton 2013b).

Moreover, the obvious desire for policymakers to cherry-pick intelligence that supports their policy is a grave issue. In the lead-up to the Iraq War, most analysis concluded that an Iraq with weapons of mass destruction (WMD) did not present a direct or immediate threat to the United States. Although there was widespread belief that Iraq possessed WMD, there was little concrete evidence

proving so. Despite this, the prevailing mind-set, including of those like me who opposed the war, was that Iraq *must* possess WMD, though not nuclear weapons. In that climate, it was difficult for any analysts to make the argument that Iraq had no WMD of any kind, and too easy for policymakers to accept information supporting their beliefs, including from discredited sources like Curve Ball (Heazle 2010).

New competitors, new colleagues

Intelligence has always worried about the competition. A generation ago, the competition was CNN: was intelligence always to be scooped by CNN? (I always thought that concern was misplaced: better to get it right than get it wrong, first). Now, though, the list of sophisticated private organizations doing “intelligence” is a long one, from Eurasia Group through Bloomberg and Oxford Analytica to Stratford.

The Russian intervention in the 2016 US elections came as a surprise, but it should not have. There was warning but from an unfamiliar quarter. A group of analysts outside government was tracking the online dimensions of the jihadists and the Syrian civil war when they came upon interesting anomalies as early as 2014. When experts criticized the Assad regime online, they were immediately attacked by armies of trolls on Facebook and Twitter. Unrolling the network of the trolls revealed they were a new version of “honeypots”, presenting themselves as attractive young women eager to discuss issues with Americans, especially those involved in national security. The analysts made the connection to Russia but found it impossible, that early, to get anyone in the American government to pay attention, given the crises competing for both policy and intelligence attention (Weisburd, Watts, and Berger 2016).

The cyber arena is also a striking example of the change. In the traditional process, if a major hack occurred, it would fall to the Intelligence Community to attribute it to the perpetrator. Afterwards, policy would decide on a response, name and shame, seek indictments or whatever. Now, however, that tidy process is disrupted, for while intelligence is doing attribution, so too are a host of private companies. And they will not be shy about identifying the perpetrator, never mind what the government might prefer. In the short run, this seems competition; in the long run, I hope it will become creative collaboration.

One of the Intelligence Community’s greatest challenges is ensuring it remains useful to policy makers, when they show a marked interest in other sources.

Dealing with the Trump train wreck, especially truth as malleable

So much for the future of intelligence in normal times. Like many Americans, I thought the pressure of governing would compel Mr. Trump to behave like a more usual president, despite the deep distrust in the bureaucracy of the Intelligence Community he had expressed during the campaign. But he did not; he was more prone to turn to Fox News than the Intelligence Community for advice.

The most visible damage, one which the new Director of National Intelligence (DNI), Avril Haines, emphasized in her confirmation hearings, was to the morale of the workforce, especially that of the Office of the DNI.⁷ It is one thing to suffer the privations of money and lifestyle to serve as an intelligence officer if you feel your work is valuable and recognized as such. Who would do it, though, if your work was dissed and you were at risk of being thrown under the bus for any deviation from the party line in a blatantly politicized ODNI? The three-letter agencies, CIA and its kin, were mostly, though not entirely, shielded from the political manipulations, so the damage is less there. For the ODNI, the simple fact of working for a president who values intelligence and a director who doesn't dismiss or twist it should restore morale fairly quickly. The longer term cost in the coin of those who left or shunned intelligence service is harder to reckon.

The January 6, 2021 riots at the Capitol underscored the need to reshape domestic intelligence, a need reflected in the president's charge to the director later in the month to produce a thorough assessment of domestic terrorism. White supremacist groups were responsible for 41 or 61 terrorist incidents in the first eight months of 2020.⁸ Yet the nation's sprawling counterterrorism apparatus, while adapting, remains preoccupied with Islamic terrorism, not to mention the former president's continual conjurings, virtually all baseless, of "antifa terrorism" on the left.

More broadly, domestic intelligence continues to be something of a stepchild in the US Intelligence Community, which is dominated by agencies, like CIA and NSA, whose mandate and mindset are limited to "foreign" intelligence. The raggedy connections among the "domestic" agencies, especially FBI and DHS, and between them and state and local law enforcement were, sadly, all too apparent on January 6.

The last challenge is existential, for intelligence now faces a world not just of "false" facts and presidential tweets of bald disinformation, and the prospect that "truth" will be widely regarded as personal, or political, or partisan, but also one in which the very concept of truth – that empirical realities can validate or invalidate spoken statements – is under assault. One of the great paradoxes of our times is that all the wonderful technology created to connect people has ended up segmenting them into "echo chambers" in which they hear only what they want and learn only what they already thought.

In passing, while I came to admire the marble entrance hall at the CIA, I've always found the Biblical quotation from John – "ye shall know the truth, and the truth shall set you free" – odd, and oddly placed there. Intelligence, still more than other endeavours, has always known how elusive the truth can be. And our language, like "true enough", is mirrored in the distinction between intelligence and law enforcement: true enough for policy is a looser standard than true enough for a court of law. And in effect, and sometimes in intent, intelligence's truth is more likely to constrain policy than to "set it free".

So far, I see no better response for intelligence than to double down on trying to distinguish what is likely true from what is not. False facts, in principle, make real ones more valuable and their identification more pressing. Haines put

it well: “The greatest challenge . . . is building the trust and confidence necessary to protect the American people. To be effective, the DNI must never shy away from speaking truth to power – even, especially, when doing so may be inconvenient or difficult. To safeguard the integrity of our Intelligence Community, the DNI must insist that, when it comes to intelligence, there is simply no place for politics – ever.”⁹

The question is: will anyone listen? I fervently hope so.

Notes

- 1 I thank Stephen Chesterman for valuable research and comment in the final preparation of this article.
- 2 For an assessment of what it would take for the United States to both think and act more strategically, and for examples of when the country has, see Hutchings and Treverton (2018).
- 3 The only country to develop its own nuclear arsenal, and later denuclearize is South Africa in 1989. At that time the apartheid was coming to an end and South Africa was working on ending its pariah status in the International Community. There are no clear parallels between the democratizing South Africa and ever authoritarian North Korea (Friedman 2017).
- 4 For more on this topic see Tetlock and Gardner (2015).
- 5 On red-teaming, see Zenko (2015).
- 6 For a thorough introduction to ABI, see Biltgen and Ryan (2015).
- 7 The hearings, including her statement, are available at www.intelligence.senate.gov/hearings/open-hearing-nomination-avril-haines-be-director-national-intelligence.
- 8 CSIS Issue Brief, *The War Comes Home: The Evolution of Domestic Terrorism in the United States*, October 22, 2020, available at www.csis.org/analysis/war-comes-home-evolution-domestic-terrorism-united-states.
- 9 Haines, cited earlier.

References

- Albert, Eleanor. 2019. “The Evolution of U.S.-Vietnam Ties”. *Council on Foreign Relations*, March 20. www.cfr.org/backgrounder/evolution-us-vietnam-ties.
- Barnes, Julian E. 2014. “U.S. Military Plugs into Social Media for Intelligence Gathering”. *Wall Street Journal*, August 6, sec. US. <https://online.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557>.
- Biltgen, Patrick, and Stephen Ryan. 2015. *Activity-Based Intelligence: Principles and Applications*. Boston: Artech House.
- Friedman, Uri. 2017. “There Is No Precedent for What America Wants from North Korea”. *The Atlantic*, September 6, sec. Global. www.theatlantic.com/international/archive/2017/09/history-north-korea/538800/.
- Heazle, Michael. 2010. “Policy Lessons from Iraq on Managing Uncertainty in Intelligence Assessment: Why the Strategic/Tactical Distinction Matters”. *Intelligence and National Security* 25 (3): 290–308. <https://doi.org/10.1080/02684527.2010.489780>.
- Hulnick, Arthur S. 2006. “What’s Wrong with the Intelligence Cycle”. *Intelligence and National Security* 21 (6): 959–79. <https://doi.org/10.1080/02684520601046291>.
- Hutchings, Robert L., and Gergory F. Treverton. 2018. *Rebuilding Strategic Thinking*. Washington, DC: CSIS. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181018_RebuildingStrategicThinking_WEB_v2.pdf.

- Kent, Sherman. 2015. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press.
- Malley, Robert, and Jon Finer. 2018. "The Long Shadow of 9/11". December 7. www.foreignaffairs.com/articles/2018-06-14/long-shadow-911.
- Maloney, Suzanne. 2008. "How the Iraq War Has Empowered Iran". *Brookings* (blog). March 21. www.brookings.edu/opinions/how-the-iraq-war-has-empowered-iran/.
- Tetlock, Philip E., and Dan Gardner. 2015. *Superforecasting: The Art and Science of Prediction*. New York: Crown.
- Treverton, Gregory F. 2013a. *First Callers: The President's Daily Brief across Three Administrations*. Washington, DC: Center for the Study of Intelligence; Central Intelligence Agency. www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/csi-intelligence-and-policy-monographs/pdfs/first-callers.pdf.
- . 2013b. *Support to Policymakers: The 2007 NIE on Iran's Nuclear Intentions and Capabilities*. Washington, DC: Center for the Study of Intelligence; Central Intelligence Agency. www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/csi-intelligence-and-policy-monographs/pdfs/support-to-policymakers-2007-nie.pdf.
- Tucker, Patrick. 2020. "Spies Like AI: The Future of Artificial Intelligence for the US Intelligence Community". *Defense One* (blog). January 27. www.defenseone.com/technology/2020/01/spies-ai-future-artificial-intelligence-us-intelligence-community/162673/.
- Weisburd, Andrew, Clint Watts, and J. M. Berger. 2016. "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy". *War on the Rocks* (blog). November 6. <https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/>.
- World Health Organization. 2015. "Factors That Contributed to Undetected Spread". January 2015. Accessed December 17, 2020. www.who.int/news-room/spotlight/one-year-into-the-ebola-epidemic/factors-that-contributed-to-undetected-spread-of-the-ebola-virus-and-impeded-rapid-containment.
- Zenko, Micah. 2015. *Red Team: How to Succeed By Thinking Like the Enemy*. 1st edition. New York: Basic Books.

Index

- 3D printing/additive manufacturing 270
9/11 3, 10; Al-Qaeda in wake of 264; CIA
torture practices in wake of 175, 229;
future perpetrators of similar terror
attacks 180; growth in counter-terrorism
policy in wake of 272; perpetrators of
23; US congressional investigations in
wake of 220; US military response in
wake of 179, 181
9/11 Commission 227
1972 Olympic Games, Munich 79–80
- ABI *see* activity-based intelligence (ABI)
Abourezk, James 204, 207–8, 211
Abu Hassan 80
Abu Iyad 80
Abu Nidal 84n41
Ackerman, Gary 270
activity-based intelligence (ABI) 284–5
Acton (Lord) 172
Afghanistan 189, 284; 2001 Coalition
forces invasion of 264; activity-based
intelligence developed in 284; Al-Qaeda
bases 264, 267; New Zealand Defence
Force (NZDF) Operation Burnham
127–8; Soviet army occupation of 176,
179–80, 281
agent provocateurs 110
Ahmadinejad, Mahmoud 281
AI *see* artificial intelligence (AI)
al-Alaki, Anwar 177
Albania 71
Al-Islam, Ansar 263
Allende, Salvador 174, 202–8, 218
Al-Qaeda 23, 127; al Zarqawi as leader
of 262; bin Laden as leader of 179–80,
267; Federally Administered Tribal
Area, sheltering in 96; Taliban and 180;
weapons of mass destruction (WMDs),
use of 262–4, 267; *see also* bin Laden,
Osama
al Zarqawi, Abu Musab 262
Amin, Idi 119n2
Anderson, David 53, 141–4, 150, 153
Anderson, Jack 203
Angleton, James 69–70, 73–4
anonymity (online or digital) 43, 112
anonymization 33, 102
anonymous official testimony 206–8
anthrax 264, 274n2
Apple Computer App Store 255
Appropriations Committee (US) 212
armed conflict 40, 50, 131; Australian laws
regarding 133; cyber weapons used in
55; harms caused by and proportionate
response to 189–90; Law of 119; laws of
126–7; military responses to 188; moral
discussion related to 197; Rule 144 of
ICRC Customary IHL Study 131; UK
Parliament’s Joint Committee on Human
Rights 132
Armed Services Committee (US): House
204–6, 216, 239, 241, 243; Senate 203,
210–11, 216, 239, 241, 243
armed strategy 15
Arms Export Control Act 223
Arnold, Terence 128, 134
artificial intelligence (AI): algorithms 1–2;
classification tasks carried out by 42;
data category selection biases in 48–9,
56; data sets questioned by 50; facial
recognition 39, 256; geolocation data
used by 254; intelligence work and 283;
natural disaster, prediction of 253–4;
Open Source Enterprise 283; pandemic
rule compliance, used to check 159;
persons of interest selected by 56
Assad, Bashar al- 69

- assassinations and assassination attempts:
 Amin 119n2; CIA plots 172, 207,
 212, 217, 237; by drone 3, 177, 180,
 181; Khalaf 84n41; Lumumba 85n46;
 Salameh 84n41; *see also* Castro, Fidel
 attribution (online) 43, 152, 287
 Aum Shrinikyo 264
 Australia: Five Eyes 35, 124, 175; human
 rights law 131; intelligence sharing with
 133; Iraq war, position on 127; terrorism
 laws 272
 Australian Defence Force 136n23
 Australian intelligence 282
- Baker, Howard 211
 Baker, James 222
 Ball, George 182
 Barbary Pirates 169
 Barr, William (“Bill”) 172, 183n4
 Bay of Pigs 172, 179, 180
 BBC News 55
 Bellaby, Ross W. 157, 160–3
 Benghazi, Libya 220
 Berlin, Germany 85n48
 Berlin, Isaiah 17n13
 big data 102, 280; transparency and 283–4;
see also bulk data; data
 bin Laden, Osama (OBL): Afghanistan’s
 harbouring of 179, 281; death of
 234; identifying the driver for 284–5;
 intercepting communications of courier
 for 20; nuclear weapons, intent to
 acquire 267
 biological agents: dual-use research 265–6;
 stolen 265; synthetic 265–6
 biological weapons (BW): radiological
 weapons and 266; terrorism and 264–5
 biopiracy 265–6
 biotechnology 265, 272–3
 bio-unabombers 265, 266
 BioWatch program (US) 271
 Bissell, Richard 67, 78, 83n9, 85n46
 blackmail 2, 100, 103–4, 269; recruiting
 CIA agents using 67, 72–3, 75–7, 79, 81
 Black September 80
 Blair, Dennis 181
 Blum Richard H. 83n11
 Boko Haram 281
 Bok, Sissela 76
 Boland Amendments 223
 Brandeis, Louis (Justice) 172, 259
 Braun, Megan 189–91, 194–5
 Brennan, John 177, 180
 Brin, David 256–7
 Brunstetter, Daniel 189–91, 194–5
 bulk data, databases, and data sets 2, 27;
 access to 42–3, 47–50, 53; collection of
 24; interception 97; national security-
 based 32–4; privacy and 141–54;
see also data
 Bulk Powers review (UK) 141, 142, 144
 Bumpers, Dale 210
 Bundy, McGeorge 178
 Bunga parasite 178
 Bunge, Mario 40
 Bush Administration (US) 176, 220
 Bush George H.W. 226
 Bush, George W. 224
 BW *see* biological weapons (BW)
- CA *see* covert action (CA)
 Caliphate 263, 267, 268
 Cameron, David 237
 Canada: CSIS 154n3; Five Eyes 35, 124,
 175; no personal data collected by 163
 Carle, Glenn L. 68
 Carpenter, Daniel P. 202
 Carus, Seth 264
 Casey, William J. 173, 179
 Castro, Fidel 202; CIA plan to assassinate
 119n2, 177–8, 181
 CBRN (chemical, biological, radiological
 and nuclear) 1, 261–74; biological
 weapons 264–5; chemical weapons
 262–4, 267; detection of emerging
 threats 268–9; dual-use research
 and synthetic biology 265–6; ethical
 challenges 271–3; non-state actor threat
 assessment 262–4; threat detection
 269–70; threat disruption 271; nuclear
 weapons 267–8; radiological weapons
 266–7; *see also* weapons of mass
 destruction
 CCTV 256, 273
 Central Intelligence Agency (CIA) (US):
 agent recruitment 71–8; Bay of Pigs
 179; covert operations, organizational
 hierarchy and chain of command of
 234, 235, 238–9; false flag approaches
 81; illegal domestic activities of 217;
 illegal sale of arms to Iran 223; kinetic
 tasks undertaken by 21; paramilitary
 operations (PM ops) 8, 169, 85n48,
 176–7, 233, 234, 239; oversight of
 202–13; Pompeo’s views of 183; quasi-
 epistemic tasks undertaken by 21; SSCI
 report on detention and interrogation
 program 229; Stinger missiles provided

- by 180; *see also* assassinations and assassination attempts; Bissell, Richard; Brennan, John; Castro, Fidel; Church Commission; coercion; coups; Deutch, John; drone warfare; Olson, James; Popov, Pyotr; Rositzke, Harry; Wisner, Frank
- Central Intelligence Agency (CIA)
headquarters *see* Langley, Virginia
- CESSPIT (Crime, Espionage, Sabotage and Subversion perverting internet technology) 55
- Chatham House Rule 136n26
- chemical weapons (CW) 178, 262–4, 267; *see also* CBRN
- Chemical Weapons Convention (CWC) 262
- Cheney, Dick 172, 281
- Chile: CIA manipulation of election in 170, 174; coup of Allende government 202–7; US policy and 203–9
- Chile inquiry by US government 211
- China: CIA mind-control experiments in reaction to 74; cyber-espionage against 36; COVID-19 in 44, 45, 186, 254; cyber-theft by 37n15; economic espionage by 151; elderly, reverence for 115; foreign intelligence operations of 98; intelligence for defense against 24; Iraq, stance on 127; sleeper economic espionage cells utilized by 111; surveillance technologies of 159; Taiwan and 282–3; Tibet and 70; United States and 282–3
- Church Committee (US) 173, 181; covert operations, critique of 228; early US intelligence oversight and 216–17; as gold standard 229; legacy of 221, 223; post-Committee reforms 218–19
- Church, Frank 179, 206–7, 211, 217
- Churchill, Winston 230
- CIA *see* Central Intelligence Agency (CIA)
- citizen's arrest 193
- Clark, Kathleen 224
- Clearview AI 254–5
- Clifford, Clark 179
- Clinton, William J. "Bill" 226
- CMF *see* Combined Maritime Forces (CMF)
- coercion: blackmail 67, 72–3, 75–7, 79, 81; CIA agent recruitment and 71–9, 81–2; morality or immorality of 191; national security surveillance as 157; opportunistic 186–7; by the state 98, 104, 192; US citizens' rights against the use of 65
- coercive interrogation 28, 31, 33, 66
- coercive force 24, 27
- Cohen, William 222
- Colby William 84n29, 202, 204–8
- "cold cash to the rescue" 175
- Cold War 183; CIA activities during 174, 179; CORONA satellite during 252; economic espionage as byproduct of 150; foreign policy consensus during 202; intelligence activity during 23–4; intelligence oversight during 201; "Secret State" of 44; United States' leadership during 183; weapons of mass destruction during 261
- Cold War, Saudi Arabia and Iran 281
- collaboration, collaborators: culpable 104; Nazi 85n44; recruiting 80
- collateral damage 177, 194, 244
- collateral harm 41, 49–50, 96
- collateral intelligence collection 93–6, 103, 105
- collateral intrusion 47
- Collingridge dilemma 109, 112
- Combined Maritime Forces (CMF) 125
- communism and communists: anti-communists 80; CIA propagation of anti-communist material 175, 177
- communist China, US recognition of 282
- communist countries 148
- communist expansion, threat of 180, 202
- communist Vietnam 283
- computer worm 111, 113
- Congo 85n46
- Congressional oversight of US intelligence *see* United States
- consequentialism 15, 56, 196
- conspiracy stories 45
- conspiracy to commit terrorism 273
- Constitutional Convention 1787 (US) 172
- Copeland, Miles 71–3, 75
- Cormac, Rory 239–40
- Corn, Gary 186
- CORONA satellite program 251–2
- coronavirus 45, 50, 186, 254; *see also* COVID-19
- Council of Europe Convention on Human Rights 56
- counterespionage 78, 81, 156
- counterfeit currency 176
- counter-insurgency 101
- counterintelligence: CIA head of 69, 74; locating digital sleeper cells as

- task of 112; security and intelligence, differences among 110, 114
- counterintelligence agencies 72
- counter-terrorism 7, 24; bulk data collection contributing to 141–3, 147, 150, 153–4; post 9/11 83n23, 272; SOF 239; surveillance technologies used domestically against COVID-19 156, 158–9, 161; use of intelligence for 162
- coups: 1953 coup against Mossadegh in Iran 84n34, 174–5; 1954 coup in Iran 179, 180; 1954 coup in Guatemala 174–5; 1955 coup in Guatemala 179; 1957 coup attempt in Syria 84n34, 1973
- coups against Allende in Chile 203–6; Church Committee’s revelations of 217
- covert action (CA) 179; accountability for (UK) 232, 233, 235–6, 239–40, 241–6; accountability for (US) 172, 232–3, 234–5, 237–9, 241–6; critics of 180; decision-making to authorize (US) 171–2; democratic principles and 172–3; economic 176; espionage compared to 78–9; ethics of 169–83; intelligence oversight of (US) 216–18, 223, 228; kinetic 26; legal foundations (US) 169–73; merit and ethics of 180–3; moral objections to 65–6; paramilitary 176–7; political 175; social concerns regarding 79–80; US foreign policy, instrument of 169; *see also* Hughes-Ryan Amendment
- covert action in practice 174–7: process and principles of 177–80; as propaganda 174–5
- cover deception 186
- cover communication: artificial intelligence used to identify 56
- covert intelligence gathering: British Army against Northern Ireland 48
- covert operations: authoritarian states engaging in 36; by CIA 21; by United States 71, 204–8, 210–12; *see also* Nazi war criminals
- covert sources 77
- covert supervisors 74
- COVID-19: disinformation campaigns launched by 186, 192, 196; geospatial technologies used to map 254; privacy and 259; surveillance and 1, 156–64; national security surveillance, first six months 157–60; technoethical challenges presented by 44–6
- Criminal Code Amendment (War Crimes) Act 2016 (Australia) 136n23
- criminal ransomware 43; *see also* ransomware
- CRISPR 266, 270
- critical infrastructure vulnerability 43
- Crumpton, Henry A. 83n10
- Cuba 71, 177–8, 202
- Cuban Missile Crisis 68
- Curve Ball source 287
- CW *see* chemical weapons (CW)
- cyberattack 43, 55, 111
- Cyber Command (CYBERCOM) (US) 234
- cyber conflict 112
- cyber criminals 40
- cyber-espionage 35–6
- cyber infiltration 113
- cyber-intelligence 107, 118–19, 277, 287; collection of 9; digital sleeper cells and 110–13, 116; ethics and risks of 114–18
- cyber operations, covert or clandestine 239
- cyber power, ethics of being 51–6, 57
- cyber sabotage 110
- cybersecurity 114, 117–19; UK 141, 152–3
- cyberspace 51–3; deterrence in 51–56; norms in 58n11; planning of (US) 234; *see also* Tallinn Manual
- cyber technology 1
- cyber threats 265; *see also* Five Eyes
- cyberwarfare 177
- cyber weapons 55
- data: actionable 158; algorithm 56; communication 48, 53, 141, 143; digital 41, 42; employment 147; financial 51; geolocation 254; health 156; illegal requests for 73; location 142, 256; metadata 26, 29–30, 97, 102, 147, 152; numerical 41; personal 43, 45–7, 50, 51, 57, 103, 257; potential misuses of 259; satellite 66; secret 77; stealing 77; *see also* big data; bulk data, databases, and data sets
- data breach 153
- data collection: bulk 24, 32–4, 48, 49; selective 22; by states 40
- data files and storage devices, hacking of 100
- data sabotage 43
- data subject 145–6
- Deeks, Ashley S. 245
- defectors 67, 70, 83n11
- Defence Attaché (UK) 151
- Defence Export Services Organization (DESO) (UK) 151
- Department of Defense (DoD) (US): drone attacks authorized by 177–8, 181

- Department of Homeland Security (DHS) (US) 255, 288
- Department of Justice (DoJ) (US) 177, 274
- deterrence by denial 54, 56
- deterrence by punishment 55
- deterrence in cyberspace 51–6
- Deutch, John 80
- Deuteronomy, Book of 196
- digital battlefield 44
- digital commerce 42
- digital disinformation 45
- digital information 39
- digital intelligence capabilities 46–7, 49, 51, 53, 55; defensive use of 57; Investigatory Powers Act (UK) 56
- digital sleeper cells 107–19; cyber intelligence and 110–13; ethics and risks associated with 114–18; intelligence ethics and 108–10
- digital technology 41
- digitization and internet, impact of 41–6
- Directorate of Operations (CIA)(US) 234, 235
- Director of National Intelligence (DNI) (US) 181, 218, 269, 288–9
- discrimination (judgement) 16, 41, 49–50; *in bello* criteria of 195; legitimate and illegitimate targets, applied to 12; principle of 9, 26–9, 33, 36, 113; proportionality and 7; truth-seeking and 21
- discrimination (prejudicial) 162
- disinformation: presidential tweets spreading 288; social media as spreader of 43, 44, 45
- disinformation campaigns 110, 180, 186
- DoD *see* Department of Defense (DoD) (US)
- DoJ *see* Department of Justice (DoJ) (US)
- Dover, Robert 151–2
- Drezner, Daniel W. 164
- drone assassinations: by United States 3, 132, 181; *see also* assassinations and assassination attempts
- drone attack 189; in Syria 244
- drone swarm 270–1
- drone warfare 7, 176–7, 180
- Ebola virus 264, 282
- “echo chambers” 288
- Edgar, Timothy H. 143
- Eisenhower, Dwight D. 251
- election interference *see* Central Intelligence Agency (CIA); coups; Russia
- Elliot, Nick 150
- entrapment: calculated 81; incremental 73; sexual 84n32
- epistemic character of truth-seeking activities 21, 23–5, 26–7, 29–31, 33, 36
- epistemic uncertainty 114, 117
- Epstein, Edward J. 74, 84n27
- espionage: covert action, compared to 78–9; digital 51; economic 150; ethics of 40, 52, 81–2; industrial 103; lack of international laws regulating 51; local laws against 148; principle of reciprocity and 34–6; security to prevent 110; sleeper cell 112; social concerns regarding 79–80; treason and 65–6; *see also* counter-espionage
- espionage agents, recruiting and handling of 63–82; deception and coercion in recruiting of 71–8; voluntary agents 67–71
- ethics, principles of 63, 65
- European Court of Human Rights (ECtHR) 131, 236
- extremism: right-wing 24; Sunni 282
- Falklands crisis 1982 108
- fake news 43, 110
- fakes 45
- false facts 288
- false flag...: recruiting 71, 72, 73, 77, 79, 81; tactics 2, 46
- falsehoods online 55
- false imprisonment 194
- false-positive communications 101, 102
- false reports 22
- Fascell, Dante 211
- FATA *see* Federally Administered Tribal Area (FATA)
- FBI *see* Federal Bureau of Investigation (FBI)
- Federal Bureau of Investigation (FBI) 254; al-Alaki, surveillance of 177; anthrax investigation 264, 274n2; Church Committee report on 217; Clearview AI, use of 255; criminal informants, use of 73; malware investigation by 113; organized crime, efforts to combat 66, 70; research community outreach initiatives 273
- Federally Administered Tribal Area (FATA) 96
- Felix, Christopher [McCargar, James] 78; *see also* McCargar, James
- first resort, intelligence activity as 25, 30, 51

- FISA *see* Foreign Intelligence Surveillance Act of 1978 (FISA)
 “fishing expedition” 49
 Five Eyes 35, 175; capability challenges across 261, 264–6, 268–9; CBRN threats and 271, 274; expansion of 124; intelligence community, relationship with 273; intention of 126
 Five Eyes Intelligence Oversight and Review Council (FIORC) 133
 Fleming, Jeremy 52–4
 Footprint Identification Technology 253
 Ford, Gerald 205, 207, 209, 212
 Ford motor company 115
 Foreign Affairs Committee (US) 211
 Foreign Intelligence Surveillance Act of 1978 (FISA) (US) 219; Amendment Acts 2008 219
 Foreign Intelligence Surveillance Court (US) 14
 foreign intelligence targets, rights of 89–105
 Foreign Relations Committee 211; subcommittee 206
 forward active dissuasion (FAD) 56
 Fourth Amendment Equilibrium Adjustment 258
 fourth industrial revolution 42
 Fourth Option 182; *see also* Third Option
 Fox News 287
 Frankena, William 63, 82n2
 Fraser, Donald M. 205
 Fulbright, J. William 172, 182, 204–6, 209–11
- G20 151
 Galliot, Jai 189
 Gates, Robert 188
 GCHQ *see* Government Communication Headquarters (GCHQ)
 General Data Protection Regulation (GDPR) (EU) 257–8
 General Motors 255
 Geneva Convention 1949 50
 geodetic methods 253
 GEOINT 24, 251–9
 GEOINT Singularity 252
 geolocation 41, 254
 globalization 44, 109
 global pandemic 161–2, 164, 254
 global positioning system (GPS) 159, 285
 Global Russia 187
 global terrorism 171
 Godfrey, E. Drexel Jr. 75, 84n33
 Godson, Roy 179
 Golden Rule 176
 Goldring, John (Sir) 54
 Golitsyn, Anatoliy 70
 Google 258, 285
 Government Communication Headquarters (GCHQ) (UK) 45–7, 54; bulk data collection by 147, 153; covert actions 235–7, 240, 247; establishment of 236; information trawls by 151; online covert action programme 233; oversight of 240; “Snowden revelations” and 132, 141; *see also* Fleming, Jeremy
 GPS *see* global positioning system
 Greece 179
 Guatemala: CIA asset in 223; CIA-engineered coups in 174–5, 179–80
- hackers 45–6
 Haines, Avril 288
 Halperin, Morton 179
 Hansson, Sven Ove 114, 116–18
 harm 7–15; anticipated 47; calculating 118; causing 189, 194; collateral 41, 49–50, 96; defending the innocent from 64; deliberate 196; indirect 188; moral principle to minimize 30; non-lethal 150; potential for 163; potential to actual, shift from 111; prevention of 57; principle of 33; privacy infringement as 33–4; probability of 114; risk of 195; subjectivity of 115; unintended 47; *see also* proportionality
 Harrington, Michael 204–5, 207–12
 Hayden, Carl 212
 Hayden, Michael (General) 256
 Hébert, F. Edward 211
 Helms, Richard 207
 Herman, Michael 15
 Hersh, Seymore 205–7, 217
 home-grown extremism 24; *see also* extremism
 homeland: American (US) 180, 280; digital 52
 Homeland Security *see* Department of Homeland Security (US)
 Hood, William 74, 84n31
 hospitals 89, 272; cyberattacks on 113, 177
 hospital ship 182
 House Armed Service Committee (US) *see* Armed Service Committee: House (US)
 House Armed Services Committee’s Special Subcommittee on Intelligence 204, 207

- House Foreign Affairs Committee 209; subcommittee 205; *see also* Senate Foreign Relations Committee (US)
- House–Senate Intelligence Committee (US) 227
- Hughes, Harold E. 208, 209, 211
- Hughes-Ryan Act 1974 170, 172–3, 182
- Hughes-Ryan Amendment 201–13, 218, 228
- human intelligence (HUMINT) 2, 66
- human rights 36; Chile’s abuses of 204; CIA abuses of 80; CIA violations of 85n49, 223; digital intelligence operations and 56; of foreign intelligence targets 89–105; intelligence data collection and 272, 273; security and 10; universal 56, 66; United States as (former) champion of 182–3; *see also* coercion
- Human Rights Act 1999 (UK) 51, 56
- human rights treaties 130–1, 144
- human subjects 74
- Hurricane Harvey 253
- ICC *see* International Criminal Court (ICC)
- ICRC Customary IHL Study 130–1
- identity theft 255, 265–6
- IFC *see* Information Fusion Center (IFC) (Singapore)
- Ignatius, David 84n34
- IHL *see* International Humanitarian Law (IHL)
- ILC *see* International Law Commission (ILC)
- image analysis intelligence (IMAGINT) 89, 98
- IMAGINT *see* image analysis intelligence
- IMSC *see* International Maritime Security Construct (IMSC)
- Information Fusion Center (IFC) (Singapore) 125–6; *see also* NATO Intelligence Fusion Centre (NIFC)
- intelligence: Bellaby’s six principles governing the practice of 160–1; criminal 24; as distinct from police work 8; as distinct from war 8; epistemic character of 21, 23–5, 26–7, 29–31, 33, 36; ethics of 160; just war tradition and 7–16; kinetic activities of 21–3, 25–6, 29–31, 33; military 24, 31; national security 21–6; Ormand’s six principles governing the practice of 160–1; as preemptive self-defense 11; proportionality in 11–12
- Intelligence and Security Committee (ISC) of Parliament (UK) 233–4, 240–4; *Report into Detainee Mistreatment and Rendition 2001–2010* 131
- intelligence capabilities: gaps and challenges 268–71
- intelligence oversight: “shock theory” of 216; *see also* covert action; Hughes-Ryan Amendment; United Kingdom; United States
- intelligence practice *see* technoethics
- Intelligence Services Act (ISA) (UK) 234, 236
- International Criminal Court (ICC) 133
- International Humanitarian Law (IHL) 130, 131, 136n18
- International Law Commission (ILC) 129
- International Maritime Security Construct (IMSC) 135n3
- Internet Weather Centre (NCSC) 153
- Inter-Services Intelligence Directorate (ISI) (Pakistan) 159
- Investigatory Powers Act 2016 (UK) 56, 57
- Iran 24, 98; 1953 coup 84n34, 175; CIA sale of arms to 223; Saudi Arabia and 281; Stuxnet attack against 111, 271
- Iran-*contra* affair 171–4, 176, 179–80; Congressional investigation of 220
- Iran-Iraq War 263
- Iraq 176, 181, 189; activity-based intelligence developed in 284; Al-Qaeda in 262–3; illegal arms sales to 236; US decision to leave 281–2; US invasion of 264
- Iraq War 2003 113, 126–7; faulty intelligence leading-up to 226, 264, 286–7
- IS *see* Islamic State (IS)
- ISC *see* Intelligence and Security Committee (ISC)
- ISI *see* Inter-Services Intelligence Directorate (ISI) (Pakistan)
- ISIL 281–2
- Islamic Revolutionary Guard Corps Quds Force 181
- Islamic State (IS; ISIS) 126, 263–8; in Syria 264
- Israel 24, 69, 72; COVID-10 surveillance tracking response 158–9, 161; Olympic Games in Munich, athletes massacred at 79; Stuxnet developed by 111; *see also* Mossad
- Israeli Security Agency (Shin Bet) 158

- Italy 175, 179
 Ivano-Frankivsk power network (Ukraine) 107, 111
 Ivins, Bruce 264
- Jackson, Henry “Scoop” 211
 Jacobs, Arthur 73
 Jacobson, Roberta 182
 Jacome, Michelle 270
 Japan 124, 180, 283
 Jefferson, Thomas 169
 Johnson, Loch 212, 216, 222, 225
 Johnson, William 72
 Joint Chiefs of Staff 239
 Joint Committee on Human Rights (UK) 132
 Joint Forces Command (UK) 237
 Joint Intelligence and Security Division (NIFC) (UK) 125
 Joint Intelligence Organisation (UK) 240
 joint moral rights of citizens 24
 Joint Committee on Human Rights (UK Parliament) 132
 Joint Special Operations Command (JSOC) (US) 234, 235
 Jonsson, Oscar 186, 192
jus ad bellum 9, 24, 25, 40, 187, 189–90; intelligence equivalent of 54; just war tradition and 187; Iraq War according to 126
jus ad intelligentiam 40, 107
jus ad vim 186–92
jus in bello 9, 25, 40, 55, 190, 193, 195–6
jus in intelligentia 39, 41, 44, 51, 109
jus post bellum 25
 just authority 13–15
 “just cause” 12, 13, 17, 160, 190
 “just exception tradition” 193
 Justice and Security Act 2013 (UK) 240
 Justice Department (US) *see* Department of Justice (DoJ) (US)
 just intelligence: foundation for theory of 89–90; intelligence gathering tactics of 96–105; principles 8, 12–16
 “just war doctrine” 7
 Just War Theory 25
 Just War thinking 54, 57
 just war tradition: contemporary warfare and 193–4; cyberspace and 112–13; intelligence and 7–16, 109; post-Westphalian 99; potential political abuse of 192
- Kant, Immanuel 40, 178
 Kennedy, Edward 204, 206, 211
 Kennedy Administration 178
 Kennedy, John F. 68
 Kent, Sherman 285
 Kerr, Orin S. 258
 Kerry, Cameron 257
 KGB 67–72; Italian Communist Party supported by 175; poisoning of Skripal by 149
 kill list: Department of Justice (US) 177
 kinetic actions of intelligence of 21–3, 25–6, 29–31, 33; agent provocateurs and sabotage 110; retaliation 112
 kinetic attack 55, 190
 kinetic force 189; lethal 267
 kinetic military response 113; morality of 25; *see also* military activity
 King, Angus 180
 Kisevalter, George 83n14
 Kissinger, Henry 169, 172, 183, 205–8; Mao, covert meeting with 282
 Kmiec, Douglas 183n4
 Koller, Josef S. 252–3
- ladder of escalation 11
 Langan, John 82n4
 Langley, Virginia 175, 177, 179–80
 Laos 179–80
 last resort 12, 15, 25, 30; covert action capability as 179; intelligence as 160–1, 163; secret intelligence as 160; war as 190–1, 194
 Law of Armed Conflict 119
 Le Carré, John 70, 149–50
 legitimate authority 7, 12, 160, 163; principle of 8, 13–14
 legitimate national interests 35, 47, 173
 legitimate targets 9, 16, 49, 50, 94, 113
 Leuprecht, Christian 112, 119
 Lewis, Richard 253
 Libya 189; 2011 intervention in 126; Benghazi 220; chemical weapons stockpiles in 263; sanctions in 135n1
 Lindsay, Franklin 85n48
 Lockerbie, Scotland 80
 Lumumba, Patrice 85n46, 119n2
 Lupton, Danielle 192
- Madison, James 171, 172
 Maghreb, the 176
 Malaysia Airlines Flight 17, 2014 downing of 285
 Mangold, Tom 69
 Mansfield, Mike 211
 Mao (Chairman) 282
 Marchetti, Victor 84n43

- Marshall Plan (US) 180, 182
 mass destruction *see* weapons of mass destruction (WMDs)
 Matrix Churchill scandal 236
 Maxwell, Nick J. 163
 Mazzetti, Mark 83n23
 McCargar, James 69, 70, 73, 78, 79
 McCubbins, Matthew D. 220–1
 Melman, Yossi 84n42
 Memorandum of Notification (MON) 238
 Memorandum of Understanding Agreed Between the Prime Minister and the Intelligence and Security Committee of Parliament 240
 “mere” threat 111
 MI5 23, 150, 235–6, 240
 MI6 42, 144, 150–1, 175, 233, 235–7, 240
 militants 93, 101
 military action 31; *see also* paramilitary
 military activity 23, 24, 25, 36, 234;
 kinetic 26, 29, 30
 military agent 99
 military intelligence 24, 124
 military necessity: principle of 25, 30–2
 Mill, John Stuart 47
 Ministry of Defence (UK) 113, 236–7, 240
 “mole” 74; Soviet 71
 Mondale, Walter 181, 211
 moral culpability 31
 moral good 89, 171, 172
 moral principles *see* discrimination;
 necessity; proportionality; reciprocity
 moral rights of citizens 24
 Morgan, Thomas 204–5, 208–10
 Morkevicius, Valerie 192
 Morris, Robert Tappan 113
 Mossad 24, 85
 Mossadegh 84
 Mulligan, Thomas 82n8
 Muslim Brotherhood 282
- Nasser (President) 85n45
 National Cyber Security Centre (NCSC) (UK) 45, 153
 National Defense Authorization Act (NDAA) (US) 219
 National Geospatial-Intelligence Agency (NGA) 285
 National Health Service (NHS) (UK) 45, 153
 National Intelligence Council (NIC) (US) 280–4
 National Intelligence Estimate on Iran’s Nuclear Intentions and Capabilities 2007 (US) 286
- National Security Act 1947 (US) 234
 National Security Advisor (NSA) (UK) 237
 National Security Advisor (US) 223
 National Security Agency (NSA) (US):
 bulk collection of data by 146;
 Church Committee’s report on 217;
 establishment of 234; normative frameworks of 24; “queries” done by 283; “Snowden revelations” and 132, 141; violation of privacy laws by 13, 141; *see also* Snowden, Edward
 National Security Agency (NSA) server (computer) 102
 National Security Council (NSC) (UK) 237, 240, 242
 National Security Council (NSC) (US) 173, 178, 182, 223–4, 239, 245
 national security intelligence: normative frameworks of 24; three levels of 23: violation of privacy laws by 13
 National Security Secretariat (UK) 240
 NATO Intelligence Fusion Centre (NIFC) 125; *see also* North Atlantic Treaty Organization (NATO)
 NATO WMD Non-Proliferation Centre 267
 Nazi war criminals 72, 80
 necessity 50–1; principle of 25, 29–32; *see also* military necessity
 Nedzi, Lucien 204–5, 208, 211
 New Zealand: Five Eyes 35, 124, 175
 New Zealand Defence Force (NZDF):
 Afghanistan, Operation Burnham 127–8
 NHSX 45
 NIC *see* National Intelligence Council (NIC) (US)
 Nicaragua 176, 182; Contras 223
 NIFC *see* NATO Intelligence Fusion Centre (NIFC)
 Nigeria 281
 Nixon Administration 203–7
 Nixon, Richard 170, 172; Ford’s pardon of 212; resignation of 205
 Noriega, Manuel 78
 North Atlantic Treaty Organization (NATO) 51, 130, 133–4; 1999 intervention in Serbia 126; allies 55
 Northern Ireland conflict of 1970s and 1980s 48
 North Korea 24, 36, 113; chemical weapons stockpiles in 263; disinformation by 180; nuclear power 282

- North Red Zone CIA operations 178–9
 NotPetya computer virus 51, 111
 NSA *see* National Security Advisor (NSA) (UK)
 NSA *see* National Security Agency (NSA) (US)
 NSC *see* National Security Council (NSC) (UK)
 NSC *see* National Security Council (NSC) (US)
 nuclear weapons: terrorism and 267–8
 Nye, Joseph 54
- Obama Administration 55, 176;
 partisan breakdown under 226; SSCI
 redacted report on CIA detention and
 interrogation program 229
 OBL *see* bin Laden, Osama
 O'Donnell, Justin 85n46
 Office for Security and Counter-Terrorism
 (OSCT) 240
 Office of Management and Budget (US)
 239
 Office of the Director of National
 Intelligence (ODNI) (US) 288
 Olson, James 70, 72–5, 84n32
 Olympic Games, Munich 79–80
 Omand, David 15, 53, 108, 157, 160–3
omne majus continent in se minus 40
 Organisation for the Prevention of
 Chemical Weapons (OPCW) 274n1
 Osama bin Laden *see* bin Laden, Osama
 (OBL)
- Pakistan 177; CIA drones deployed
 in 177; Inter-Service Intelligence
 directorate 159, 161; nuclear scenarios
 involving 267; secret surveillance
 system 159, 161
 Palestinian Liberation Organization (PLO)
 79–80
 PanAm jet bombing 1988 80
 Panama 78; *see also* Noriega, Manuel
 paramilitary operations (PM ops) 8, 169;
 Bay of Pigs 179; CIA 85n48, 176–7,
 233, 234, 239; British Loyalist 58n9;
 MI6 233
 pariah status: South Africa 289n3
 Penkovsky, Oleg 67–8, 83n14
 Philby, Kim 71, 148, 150
 Phillips, David 71, 83n16
 phishing attacks 111
 Pinochet, Augusto 203, 204
 piracy 98; *see also* bio-piracy
- PLO *see* Palestinian Liberation
 Organization (PLO)
 POICN *see* Profiles of Incidents Involving
 CBRN and Non-state Actors (POICN)
 Database
 Poland 71
 Pompeo, Mike 183
 Popov, Pyotr 67–9, 83n14
 Portugal 179
 Prados, John 70, 84n34, 85n46
 pre-emptive nuclear strike 67
 pre-emptive self-defense 11
 presidential plausible deniability 201–2
 President's Daily Brief (PDB) (US) 285
 principle of discrimination *see*
 discrimination
 principle of just intelligence *see* just
 intelligence
 principle of legitimate authority *see*
 legitimate authority
 principle of military necessity *see* military
 necessity
 principle of necessity *see* necessity
 principle of reciprocity *see* reciprocity
 principle of restraint *see* restraint
 principles: legal 25, 37n9, 40; moral 25,
 37n9
 privacy 141, 259; autonomy and 7, 32;
 bulk collection of data and 142–7; civil
 liberties and 156; NSA (US) violations
 of 13; security and/or 1, 9–11, 164;
 surveillance as violation of 26–7, 31–6;
 technoethics of intelligence and debates
 over 45, 46; temporary forfeiture of 93
 privacy law: European 144; US 257–8
 privacy rights 29, 99–100, 103; digital age
 and 132
 Profiles of Incidents Involving CBRN and
 Non-state Actors (POICN) Database 268
 proportionality: coercive manipulation and
 78; cyberintelligence and 107; definition
 and terms of 12, 41; discrimination and
 7; ethics of practice of intelligence and
 160–1, 163; *ius ad bellum* 190; *ius in
 bello* 195; *ius in intelligentsium* 118;
 just war and 15–16, 194; Investigatory
 Power Act (UK) and 56; national
 security and 21, 36; macro- 193;
 necessity and 25, 29, 47, 51; principle
 of 9, 32–3, 118; privacy rights and 144;
 professional norms and 90, 91, 92, 93;
 in war thinking 108–10
 proportionality conditions, lack of
 granularity in 118–19

- proportionality judgement 47–8
 proportionality of means 47–8
 proportionality question 161
 proportionality tests 47, 50
 proportional responses 11
 prospective agents 68, 72, 76–8, 148, 150
 prospective principle of reciprocity 34–6
 prospective threats 97
 psychological warfare 21
- Quantuminsert surveillance program 13
 Qassem Soleimani *see* Soleimani, Qassem
 Quinlan, Michael 108
- Radio Free Europe 175
 radiological weapons: terrorism and
 266–7; *see also* nuclear weapons
 Rajneeshees religious cult 264
 RAND Corporation 124, 283
 Ranelagh, John 70
 ransomware: criminal 43; WannaCry 153
 Raviv, Dan 84n42
 Reagan Administration 171, 174, 179, 223,
 226; *see also* Iran-contra affair
 reciprocal cost 103
 reciprocal response 95, 99
 reciprocal trust 79
 reciprocity 73, 107; perspective of 108;
 principle of 26, 34–6, 96; vicious cycle
 of 109; *see also* espionage; prospective
 principle of reciprocity; retrospective
 principle of reciprocity
 Research, Information and
 Communications Unit (RICU) (UK) 235
 reasonable prospect of success 41, 49, 50,
 161, 190
 restraint, principle of 57
 retrospection as oversight 17n17
 retrospective principle of reciprocity 34–6
 RICU *see* Research, Information and
 Communications Unit (RICU) (UK)
 Rid, Thomas 189, 192
 Rifkind, Malcolm 240–1
 “right” authority, intelligence activity
 context 41, 48–9, 57, 160
 right intention 7, 9, 41, 160, 193, 195
 right intention and integrity of motive
 46–7
 rights, forfeiting or waiving 92–6; *see also*
 human rights; privacy rights
 right to appeal 14
 RNA 270
 Rositzke, Harry 68–9, 78–80, 85n44
 Ross, David 82
- Royal Air Force 237
 Royal Institute of International Affairs 134
 Royal Navy 125, 236–7
 Rudd, Joshua 239
 Rumsfeld, Donald 113
 Russell, Richard 211
 Russia 24; CIA anti-communist
 propaganda in 175; coronavirus
 disinformation pushed by 45;
 coronavirus lockdown in 159;
 disinformation pushed by 180, 186;
 intelligence operations in Ukraine 112;
 Iraq, position on 127; Islamic State
 and 267; Kim Philby as spy for 148;
 meddling in US elections 174, 177, 220,
 226, 229, 287; right to engage in foreign
 intelligence operations 98; war and
 weakening the West, views of 186–7,
 189; *see also* defectors; KGB
 “Russian way of war” 192
 Ryan, Leo 211
- sabotage: conventional 178; cyber 110;
 data 43; digital sleeper cells and 111–14,
 116; sub-war activity of 189
 Sagar, Rahul 14, 17n17
 Saltonstall, Leverett 201
 Sarin gas 263
 Saudi Arabia: airstrikes in Yemen 126;
 arms sales to 152; Iran and 281; Sunni
 autocrats 282
 Schwartz, Thomas 220–1
 Secret Intelligence Service (SIS) (UK) 42,
 147, 150, 237
 Senate investigation of CIA 203–12
 Senate Armed Services Committee (US) *see*
 Armed Service Committee (US); Senate
 Foreign Relations Committee (US)
 Senate Foreign Relations Committee (US)
 182, 204, 206–8
 Senate Select Committee on Intelligence
 (SSCI) (US) 242–3; Bush
 Administration, investigation of 220;
 CIA and other covert operations subject
 to review by 170–3; CIA detention and
 interrogation program, investigation
 of 229; CIA in Guatemala, hearing
 regarding 222; drone strikes reporting
 to and cleared by, proposed system 177;
 establishment of 218; foreign policy
 debated before 182; term limits on
 members 224
 security, idea of 9–11; *see also*
 cybersecurity; privacy; proportionality;
 reciprocity

- Shared Awareness and De-confliction (SHADE) conference (CMF) 125
- Shrinikyo *see* Aum Shrinikyo
- SIGINT *see* signals intelligence (SIGINT)
- signals intelligence (SIGINT) 89, 96, 98, 284
- Silva, Desmond de (Sir) 58n9
- Simpson, Christopher 80, 84n43, 85n45
- SIS *see* Secret Intelligence Service (SIS)
- Skipal, Sergei 149
- smartphones 42, 156, 159
- Smith, Joseph 67, 72
- Snowden, Edward 283
- Snowden disclosures 1, 47, 53, 132, 141, 143; post-Snowden 53, 147
- Snow, John 254
- Soleimani, Qassem 181
- Somalia 176
- South Africa 289n3
- South Asia 150
- South Korea 44, 113, 124, 159
- South Vietnam 179
- Special Activities Center (SAC) (CIA) (US) 234, 235
- Special Operations Group (SOG) (CIA) (US) 176, 234, 235
- Special Forces (UK) 236–7
- Stennis, John 210–11
- Stone, Howard 84n34
- Stuxnet virus 111, 271
- sub-war activities 187, 189
- Sunni extremists 282
- sunset clauses 163–4
- surveillance capitalism 43
- synthetics *see* biological agents
- Syria 69, 189; 1957 unsuccessful coup attempt 84; chemical weapon (CW) stockpiles in 263; civil war 287; drone strikes in 244; Islamic state hideout in 264
- Taiwan 282, 283
- Taliban 179–81, 281
- Tallinn Manual 51; version 2.0 119
- technoethics 39–57; Bunge's outline of 40; contemporary intelligence and 46–51; deterrence in cyberspace 51–56; digitization and internet, impact of 41–6
- Tempora surveillance program 13
- terrorism: biological weapons and 264–5; chemical weapons and 262–4, 267; detection of emerging threats 268–9; dual-use research and synthetic biology and 265–6; non-state actor threat assessment 262–4; nuclear weapons and 267–8; radiological weapons and 266–7; threat detection 269–70; threat disruption 271
- Tetlock, Philip 284
- Third Option in American foreign policy 169–83
- threat disruption 271
- Tibet 70–1, 83n18
- treason 76, 154; espionage and 65–6, 68
- Treverton, Gregory F. 174
- Trojan Horse attack 111
- Truman Administration 170
- Truman Doctrine 180
- Truman, Harry 234
- Trump Administration 183, 226, 286; non-normalness of 280
- Trump, Donald J. 4, 256; autocracy, embracing of 172; demagoguery of 22; drone warfare under 176; Qassem Soleimani, assassination of 181; secret service agents 256; truth in the wake of 287–9
- trust: civil discourse and 259
- UKTMO 125–6
- unethical acts 109
- United Kingdom: bribery law in 151; Bulk Powers review 141–2; covert action, accountability for 233, 235–6, 239–40, 241–6; detaining someone against their will 193; domestic manufacture of weapons 142; economic espionage in 151; Five Eyes, establishment of 124; France and 150; human rights, concerns and reports regarding 131–2; intelligence recruitment efforts 142, 147; intelligence acting on behalf of economic wellbeing of 152; National Cyber Security Centre 153; NATO Intelligence Fusion Centre in 125; pandemic response 45; Philby's betrayal of 148; privacy violations by 143; *see also* Government Communication Headquarters (GCHQ); MI5; MI6; Snowden, Edward
- United Kingdom Maritime Trade Operations (UKMTO) 125
- United Nations (UN) 123, 134
- United Nations (UN) Declaration of Human Rights 119

- United Nations Security Council (UNSC)
 Resolution 123; Resolution 1441 127
- United States (US): biotechnology in 265; clandestine operations 283; Constitution 216; congressional oversight of intelligence activities 216–30; covert action, accountability for 232–3, 234–5, 237–9, 241–6; covert action by 169–83; COVID-19 response 158; disease tracking technology in 163; Ebola panic 282; economic espionage in 151; espionage on behalf of 67; Five Eyes, establishment of 124; human rights treaties 131; intelligence agencies in 269; intelligence oversight, development of 201–13; Iraq and 286; national security information in 14; reciprocity with 35; San Francisco banning of facial recognition technology 256; subjectivity of harm MIT thought experiment 115; terrorism threats, hypersensitivity to 280; Ukraine, support of 70; weapons of mass destruction deployed by 261; *see also* Armed Services Committee (US); Central Intelligence Agency (CIA); Bush Administration; China; Chile; Church Committee; Clinton, Bill; Department of Defense; Department of Justice; drone assassinations; Federal Bureau of Investigation (FBI); Five Eyes; House...; Iraq War; Obama Administration; National Security Agency (NSA); paramilitary operations; Palestinian Liberation Organization (PLO); Reagan Administration; Senate...; Stuxnet virus 111; Truman, Harry S.; Trump, Donald J.; Vietnam War
- United States capitol riots 288
- United States Army Medical Research Institute of Infectious Diseases (USAMRIID) 264
- United States Geological Survey 253
- Upstream surveillance program 13
- USAMRIID *see* United States Army Medical Research Institute of Infectious Diseases (USAMRIID)
- Vance, Cy 179
- Vietnam 163, 189, 283; South 179
- Vietnam War 172, 180, 202, 206
- Waldron, Jeremy 10
- Walzer, Michael 82n6, 189, 194
- WannaCry ransomware attack 51, 111, 113, 153
- war, social conditions of 192; *see also* drone warfare; just war; sub-war activities
- Warner, John 242–3
- Washington, D.C. 70, 175, 178; hypothetical terrorist attack in 272
- Washington, George 172
- Washington Post* 209
- Watergate scandal 172, 204–5, 212; post- 221
- weapons of mass destruction (WMDs): bin Laden’s view of 267; CBRN weapons, as distinct from 261–2; “classical” 263; state-based programmes 274; US invasion of Iraq led by faulty intelligence on 264, 286–7; *see also* terrorism
- Webster, William H. 181
- Whitlock, Craig 84n36
- Whittington, Keith E. 202
- Wicker, Tom 207
- WildTrack 253
- Wines, Michael 69
- wiretapping 177, 206–7, 218
- Wisner, Frank 68
- WMDs *see* weapons of mass destruction (WMDs)
- WMD Non-Proliferation Centre (NATO) 267
- Workshop on Intelligence Sharing in Multinational Military Operations (University of Nottingham) 135
- World War II 123, 148, 174, 244
- worm *see* computer worm
- Wyden, Ron 225
- Yemen 126, 176, 177
- Yoo, John 172
- Younger, Alex 42, 44
- Zedner, Lucia 9
- zero-day exploits 43



Taylor & Francis Group
an informa business



Taylor & Francis eBooks

www.taylorfrancis.com

A single destination for eBooks from Taylor & Francis with increased functionality and an improved user experience to meet the needs of our customers.

90,000+ eBooks of award-winning academic content in Humanities, Social Science, Science, Technology, Engineering, and Medical written by a global network of editors and authors.

TAYLOR & FRANCIS EBOOKS OFFERS:

A streamlined experience for our library customers

A single point of discovery for all of our eBook content

Improved search and discovery of content at both book and chapter level

REQUEST A FREE TRIAL
support@taylorfrancis.com

 **Routledge**
Taylor & Francis Group

 **CRC Press**
Taylor & Francis Group