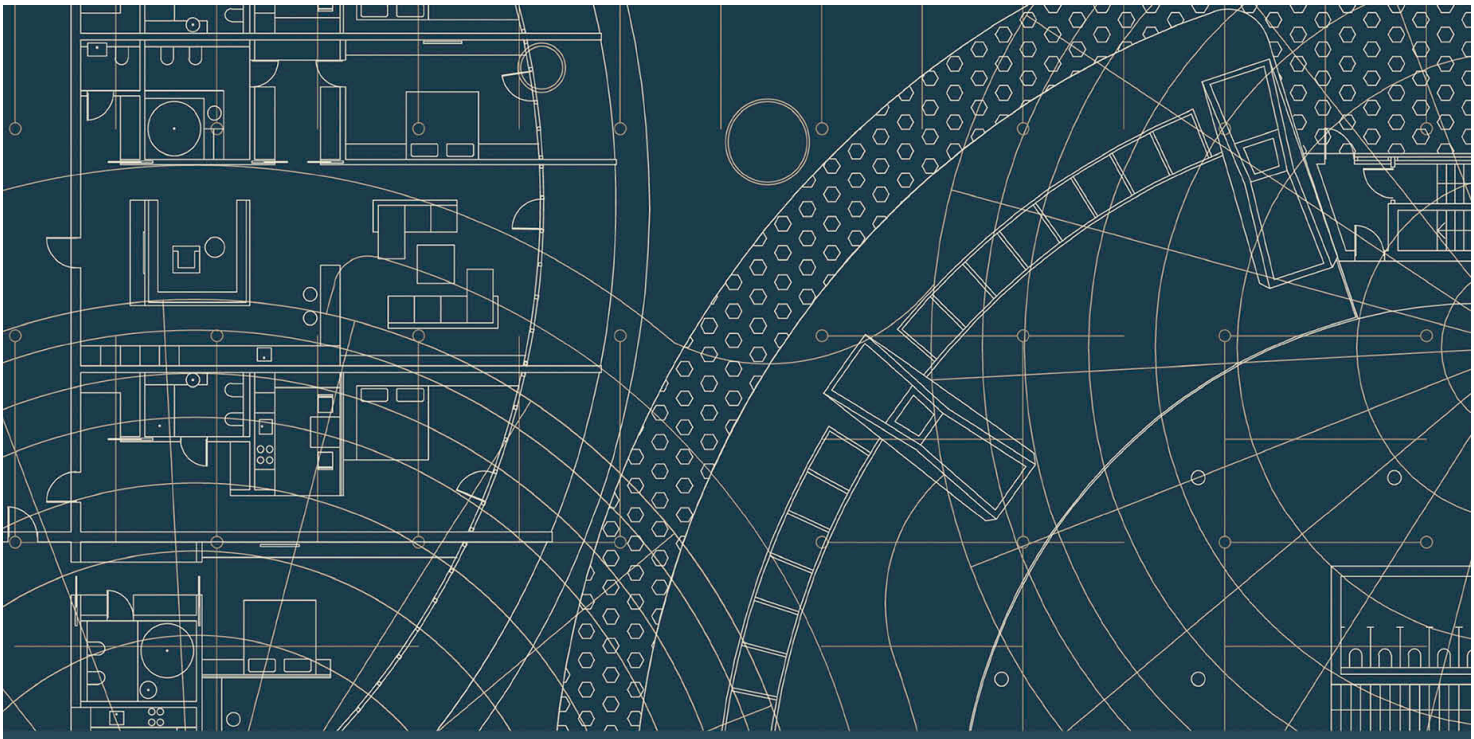

Studies in Intelligence

BIG DATA, EMERGING TECHNOLOGIES AND INTELLIGENCE

NATIONAL SECURITY DISRUPTED

Miah Hammond-Errey

"Drawing on substantial and exclusive access to the Australian Intelligence Community, this book provides a timely, detailed, and thorough analysis of the many ways in which big data is transforming intelligence and broader society. Dr Miah Hammond-Errey brings intelligence studies into the digital era with this original contribution to the scholarly field on intelligence and national security."

Kira Vrist Rønn, *Associate Professor, University of Southern Denmark*

"With this book, Dr Hammond-Errey has produced a path-breaking empirical analysis of how Big Data is transforming intelligence and the challenges to which this transformation gives rise. Based on interviews with around 50 people working in and around the Australian National Intelligence Community, this book offers an invaluable guide to understanding the impact of the Big Data landscape on intelligence practice in liberal democracies and how this affects the intelligence-state-citizen relationship. It is essential reading for students of intelligence and for all those working in the field of intelligence, including its oversight."

Mark Phythian, *University of Leicester, UK*

"This book is a timely account of the way big data and emerging technology have been disrupting intelligence and society. Dr Hammond-Errey develops an innovative framework of the landscape of big data that raises important questions about legitimacy and public trust in democratic institutions, the changing role of intelligence analysts, and the tendency to subject surveillance capabilities to greater democratic accountability."

Christian Leuprecht, *Royal Military College of Canada and Queen's University, Canada*


Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Big Data, Emerging Technologies and Intelligence

This book sets out the big data landscape, comprising data abundance, digital connectivity and ubiquitous technology, and shows how the big data landscape and the emerging technologies it fuels are impacting national security.

This book illustrates that big data is transforming intelligence production as well as changing the national security environment broadly, including what is considered a part of national security as well as the relationships agencies have with the public. The book highlights the impact of big data on intelligence production and national security from the perspective of Australian national security leaders and practitioners, and the research is based on empirical data collection, with insights from nearly 50 participants from within Australia's National Intelligence Community. It argues that big data is transforming intelligence and national security and shows that the impacts of big data on the knowledge, activities and organisation of intelligence agencies is challenging some foundational intelligence principles, including the distinction between foreign and domestic intelligence collection. Furthermore, the book argues that big data has created emerging threats to national security; for example, it enables invasive targeting and surveillance, drives information warfare as well as social and political interference, and challenges the existing models of harm assessment used in national security. The book maps broad areas of change for intelligence agencies in the national security context and what they mean for intelligence communities, and explores how intelligence agencies look out to the rest of society, considering specific impacts relating to privacy, ethics and trust.

This book will be of much interest to students of intelligence studies, technology studies, national security and International Relations.

Miah Hammond-Errey is the Director of the Emerging Technology Program at the United States Studies Centre at the University of Sydney. She has a PhD from Deakin University, Australia.

Studies in Intelligence

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

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 Brigt H. Vaage

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

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

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

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

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

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

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

Big Data, Emerging Technologies and Intelligence

National Security Disrupted

Miah Hammond-Errey

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

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

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

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

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

Library of Congress Cataloging-in-Publication Data
A catalog record has been requested for this book

ISBN: 978-1-032-48558-4 (hbk)
ISBN: 978-1-032-48559-1 (pbk)
ISBN: 978-1-003-38965-1 (ebk)

DOI: 10.4324/9781003389651

Typeset in Times New Roman
by Taylor & Francis Books

Contents

Illustrations

Figures

Tables

Acknowledgements

This book is an adaptation of my PhD thesis. Thank you to my primary supervisor Chad Whelan and secondary supervisor Diarmaid Harkin for all your support, guidance and friendship throughout both processes. Thank you, Tom Barrett, for your research and referencing assistance.

A huge thanks to colleagues, friends and family who have supported this research. I can't name many of you by name, however, am incredibly grateful for your support–you made this research possible. I can't thank you enough.

I'm grateful to the individuals and agencies who participated in this research. I feel honoured to be privileged with your insights, experiences and time. Thank you for sharing of these so willingly. Thank you to the agencies for entrusting me with this research. This research draws on a variety of perspectives from within the NIC. I have tried to reflect these (sometimes contradictory!) views and common discourse faithfully. However, this book contains only a small part of the discussions and is not a comprehensive reflection of all the topics and issues covered.

The research was supported by a National Security Big Data Scholarship from D2D CRC and a University Postgraduate Research Scholarship from Deakin University. Additional support was also provided by D2DCRC in the form of an Applied Research and Collaboration Award (2017) and an Applied Research Grant (2019).

This book is a contribution towards greater understanding of national security and big data as well as the ways the big data landscape fuels emerging technologies. I'd like to continue this conversation with you. You can also find out more by listening to my podcast, *Technology and Security*.

List of Acronyms and Abbreviations

ACIC	Australian Criminal Intelligence Commission
AFP	Australian Federal Police
AGO	Australian Geospatial-Intelligence Organisation
AIC	Australian Intelligence Community
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ASD	Australian Signals Directorate
AUSTRAC	Australian Transaction Reports and Analysis Centre
HA	Department of Home Affairs
IGIS	Inspector-General of Intelligence and Security
DIO	Defence Intelligence Organisation
NIC	National Intelligence Community
SDM	Senior Decision-Maker
ONI	Office of National Intelligence
ODM	Operational Decision-Maker
TECH	Technologist
ISME	Independent Subject Matter Expert

Introduction

This book examines the impact of the technological phenomenon 'big data' on national security intelligence and decision-making. Data is all around us. Big data has become a prevalent feature in commercial enterprise (Cukier 2010; Manyika et al. 2011; Reinsel, Gantz & Rydning 2017; Yiu 2012) from shopping to socials, travel to transport and communications to finance. It is also increasingly used in national security (Landon-Murray 2016; Van Puyvelde, Coulthart & Hossain 2017). Big data and associated analytics are presented as offering significant potential for a safer and more secure nation (Akhgar et al. 2015; Manyika et al. 2011; Mayer-Schönberger & Cukier 2014) and are being adopted before their impacts are well understood. Despite the significant impacts of big data on intelligence activities, empirical research into its impacts is still in its infancy.

The 'information age' continues to provide an ever-expanding quantity and variety of information (Degaut 2015, p. 511) that underpins many of the data-driven technologies impacting national security. In 2014, it was forecast that by 2020 there will be as many bits in the digital universe as stars in the physical universe (International Data Corporation 2014), and in 2019 this was revised to forty times the number of bytes than stars in the observable universe (DOMO 2019). According to the International Data Corporation (International Data Corporation 2022), by 2026 there will be more than 220 Zettabytes (220 billion Terabytes) of data added annually to the global datasphere – the summation of data we create, capture or replicate. This will be almost three times the 83 Zettabytes produced in 2021 – growing at a rate of 21 per cent per year (International Data Corporation 2022). We are also more digitally connected than ever before. The increasing interconnectedness of our systems and our infrastructure – including our reliance on them – is transformative and unprecedented. In January 2023, more than 5.4 billion people out of the eight billion global population (68 per cent) were using a mobile device, with the majority being smartphones (Kemp 2023). Estimates of the number of devices connected to the internet vary widely; however, there is consensus (Evans 2011; Gartner 2017) that this number has overtaken the global population – Ericsson (2022) estimated the number of connected devices in 2022 to be 23.6 billion and predict that by 2028 that number will reach 45.8 billion.

DOI: 10.4324/9781003389651-1

Increasingly vast amounts of data are captured from and about humans, machines and the natural environment, challenging political and economic models (Mayer-Schönberger & Ramge 2018; Sadowski 2020; Schwab 2017; Zuboff 2019). The abundance of data made possible by improvements in data storage and computational capabilities, combined with digital connectedness and ubiquity of technology, drive the big data phenomenon. The speed of technological change has impacted how we store, interpret, analyse and communicate information in society (boyd & Crawford 2012; Kitchin 2014a).

Intelligence activities are funded by the nation-state, with the express purpose of protecting national interests and keeping citizens safe; however, information about intelligence agencies and their activities is notoriously sparse (Andrew 2018; Van Puyvelde 2018, pp. 380–381). Lundy et al. (2019, p. 587) argue that 'intelligence is essential to modern statecraft in times of war and peace… [and] its vital role deserves – and requires – better general comprehension'. Empirical research to date on intelligence activities, especially outside the United States, has been extremely limited (Hughes, Jackson & Scott 2008; Van Puyvelde 2018; Zegart 2022). There have been 'very few, if any, reflections on how the Australian intelligence community works, its contributions, or of its importance to policy and decision-makers across government' (Symon 2018). Whilst the scarcity of information is understandable, the growing role of intelligence in society presents a significant need for understanding of the public value of intelligence agencies and ensuring their accountability in liberal democracies. Gill and Phythian (2006) argue that citizens have been excluded from knowledge of intelligence policies and practices for too long.

The book shows that big data is transforming what intelligence is, how it is practised, and the relationships intelligence organisations have with society. This includes both the collection of information and secret intelligence as well as the analytical processes used to create intelligence products and advice to inform decision-making. The book details how big data is transforming aspects of intelligence production specifically and the national security environment more broadly. The book leverages semi-structured interviews with almost fifty senior and operational intelligence officers and decision-makers within the Australian National Intelligence Community (NIC).[1] The NIC represents a unique group of interview participants, and this research is the first to access them as a community. The focus of the research is from the perspective of Australian national security professionals; however, these perspectives are applicable and relevant internationally to all states that invest significantly in intelligence collection technologies.

The introductory chapter examines and defines the key concepts of the book, providing some background and context as well as offering insight into how this research contributes to our understanding. First, it looks at big data, followed by national security and intelligence. It is important to explain these terms here as they are often used in different ways. The inconsistent use of such concepts can lead to confusion and all three are essential to

understanding the impact of big data on intelligence and national security. Furthermore, the book argues that the advent of big data is shaping these concepts, including what we see as intelligence and expanding the notion of national security to include new social harms. The book shows how big data is shaping the activities, knowledge and organisation of intelligence functions that are intended to support policy makers in developing responses to these new harms and vulnerabilities.

Big Data, National Security, and Intelligence

Big Data

Big data is an amorphous concept that is used to refer to large, diverse, growing and changing datasets (Bennett Moses & Chan 2014; Chan & Bennett Moses 2016, 2017; Malomo & Sena 2016). Big data arose from technical advances in storage capacity, speed and price points of data collection and analysis as well as by the move towards understanding data as 'continuously collected, almost-infinitely networkable and highly flexible' (Metcalf, Keller & boyd 2016, p. 2). Prior to big data, databases were constrained and unable to simultaneously deal with the original 3Vs of big data – volume, velocity and variety (Kitchin 2014b, p. 68; Laney 2001). However, increased computational power, new database design and distributed storage enabled the collection and analysis of big data (Kitchin 2014b, p. 68). The unprecedented volume and size of data sets that cannot be manually processed precipitated analytical solutions to analyse data and derive insights, expanding the term big data from referring solely to the storage of data (Mayer-Schönberger & Cukier 2014).

The term has evolved from the original 3Vs to include value derived from understanding data sets as a whole and by drawing insights using new analytical techniques (boyd & Crawford 2012; Kitchin 2014a; Kitchin & Lauriault 2014). Kitchin (2014b) considers big data as fine-grained in resolution and uniquely indexical in identification; relational in nature, containing common fields that enable the conjoining of different data sets; and flexible, holding the traits of extensionality (new fields can be added easily) and scaleability (can be expanded in size rapidly). Importantly, big data 'is less about data that is big than it is about a capacity to search, aggregate and cross-reference large data sets' (boyd & Crawford 2012, p. 663). It is this ability to use the data for some type of decision or action that defines big data. As others have aptly put, 'big data are worthless in a vacuum. Its potential value is unlocked only when leveraged to drive decision-making' (Gandomi & Haider 2015, p. 140). The requirement to consider the veracity of data and value led to the expansion of the 3Vs definition of big data – volume, velocity and variety (Kitchin 2014b, p. 68; Laney 2001) – to a 5V definition that includes veracity (certainty and consistency in data) and value (insights into and from data) (Akhgar et al. 2015; van der Sloot, Broeders & Schrijvers 2016).

A range of terms are used, sometimes interchangeably, to describe analysis of big data. These include: big data analytics (Cloud Security Alliance 2013; Beer 2018; Minelli, Chambers & Dhiraj 2013; Power 2014; Pramanik et al. 2017; Shu 2016), advanced analytics (Babuta 2017; Chawda & Thakur 2016; Shahbazian 2016), big data computing (Chen, Mao & Liu 2014) and data mining (Pramanik et al. 2017). Additionally, the terms artificial intelligence, machine learning and algorithms are included in big data analytics for the purpose of this study. In the book, big data is viewed broadly and refers to all these components, including the technologies and analytics. Participants in this research highlighted three key features of big data for national security which, the book argues in Chapter 1, come together to form a big data landscape.

National Security

National security – and our conceptualisations of it – evolves over time as it is situationally, culturally and temporally contextual (Katzenstein 1996). National security is a commonly used concept in international relations and the analysis of policy decisions; however, its essential meaning is more widely disputed than agreed upon (Baldwin 1997; Dupont 1990; Liotta 2002). Maintaining national security is usually posited as the reason for the application of intelligence resources. In a foundational text, Arnold Wolfers characterised security as 'the absence of threats to acquired values and subjectively, the absence of fear that such values will be attacked' (Wolfers 1962, p. 485). Baldwin (1997, p. 13) subsequently refined 'the absence of threats' as 'a low probability of damage to acquired values'. Wolfers (1962, p. 150) notes that the demand for a policy of national security is primarily normative in character and security points to some degree of protection of values previously obtained: 'Security is a value, then, of which a nation can have more or less and which it can aspire to have in greater or lesser measure'. Wolfers' position has not gone unchallenged, as the field struggles to agree on 'how much security' is desirable.

Zedner (2003, p. 155) posits that 'security is both a state of being and a means to that end'. Whelan (2014, p. 310) explains that we can understand Zedner's (2009) conceptualisation of security as an 'objective state of being more or less "secure" and as a subjective condition based on how secure we "feel"'. Gyngell and Wesley (2007, p. 233) see security as a prudential value, conceived as a condition which must be maintained against others' potential to degrade it. Buzan, Waever and de Wilde (1998) highlight that nation-state security requires a referent object to make sense. The objective state of security continues to imply a 'referent object' and an existential threat to that object and the special nature of security threats justifies the use of extraordinary measures to handle them (Buzan, Waever & de Wilde 1998). Whelan (2014, p. 310) furthers this, noting the 'referent objects and range of potential threats have considerably broadened', including the special nature

of national security threats, among others. Thus, the political context of national security is an important dimension (Dupont 1990). Wolfers (1952, p. 500) highlights the challenges for those who bear the responsibility for choices and decisions, that is, national security decision-makers:

> Decision-makers are faced then, with the moral problem of choosing first the values that deserve protection … the guarantee it may offer to values like liberty, justice and peace … They must decide which level of security to make their target … finally they must choose the means and thus by scrupulous computation of values compare the sacrifices.

The book argues that big data has created new social harms which are – or need to be – considered by decision-makers as national security threats or vulnerabilities. In the book, national security is considered a state of trust on the part of the citizen that risks to everyday life, whether from threats with a human origin or impersonal hazards, are being adequately managed to the extent that there is confidence that normal life can continue (Omand 2010, p. 9). Omand (2010) sets out three propositions underpinning the modern approach to national security: psychological safety, citizen-centric view of threats and hazards, and informed decision-making. This last point is crucial in the use of big data: 'the key to good risk management, maintaining that delicate balance, is to have better informed decision-making by government and thus place greater weight on the work of the intelligence community' (Omand 2013, p. 21).[2] Symon & Tarapore (2015, p. 9) add that 'making sense of complex systems and phenomena – creating knowledge – is central to sound national security decision making.'

Understanding national security, what it broadly encompasses and how decisions are made to secure nations is critical to the way that big data impacts on it and in understanding how intelligence resources are focused. This research shows that participants see new technologies, like big data, as expanding notions of national security to include, for example, information warfare and aspects of how society functions online as infrastructure critical to national security. Participants perceive that big data impacts on how intelligence agencies can identify and respond to these increasing, diverse and diffuse national security threats.

Intelligence

Intelligence here is understood through a combination of definitions. Intelligence is 'information [that] is gathered and analysed, sometimes secretly, and then used to understand a particular situation and act with advantage in it' (Rolington 2013, p. 17). Intelligence is 'knowledge vital for national survival' (Kent 1966, p. vii). It is information that has been collected, processed and narrowed to meet the needs of policy and decision-makers in relation to

defence, foreign policy, national state affairs (such as diplomacy, trade and economics) and security (Lowenthal 2012).

Intelligence in practice can be thought of in three ways, sometimes simultaneously (Lowenthal 2012, p. 9), as knowledge, as an organisation and as either an activity (Kent 1966) or product (Lowenthal 2012). Kent's classic characterisation covers the 'the three separate and distinct things that intelligence devotees usually mean when they use the word': knowledge, the type of organisation that produces that knowledge and the activities pursued by that organisation (Scott & Jackson 2004, p. 141).

Omand (2020, p. 472) defines the purpose of intelligence to help 'improve the quality of decision-making by reducing ignorance, including reducing the vulnerability of the decision-maker to uncertainty'. Intelligence production is one of the primary mechanisms for framing information and analysis to inform national security decision-making (George & Bruce 2014; Kent 1966; Lowenthal 2012; Omand 2010). The purpose of the intelligence community is to assist policy makers with national security issues (Gookins 2008).

The relationship between intelligence, policy production and senior decision-makers is vital in the national security environment (Coyne 2014; Lowenthal 2012) as intelligence is intended to reduce uncertainty for decision-makers (Agrell 2012; Betts 2009; Davies, Gustafson & Rigden 2013; Dupont 2003; Fingar 2011; Kent 1966; Lowenthal 2012; Marrin 2009; Heuer & Pherson 2015; Spracher 2009). Without use by decision-makers – in order to achieve national security – intelligence would be redundant.

The combination of these definitions acknowledges the changing information environment, accounts for the impact of big data and open-source information on intelligence activity, while acknowledging the extant role of secret intelligence collection as well as decision-makers acting on the intelligence. Furthermore, as Omand (2020) highlights, it is significant that intelligence aims to reduce uncertainty and improve decision-making in matters of nation-state security.

The relationship between national security and intelligence is noted by Agrell and Treverton (2015, pp. 32–5): 'the essence of intelligence is hardly any longer the collection, analysis, and dissemination of secret information, but rather the management of uncertainty in areas critical for security goals for societies.' Additionally, the 'use of the term in circles outside of government – "commercial intelligence", for example – can dilute its meaning, rendering intelligence a synonym for information' (Richardson 2020a, p. 154). The term intelligence is also used extensively in different government domains, such as law enforcement, criminal, security, domestic, foreign and counterintelligence.

The book looks broadly across national security and intelligence activities undertaken within the context of the National Intelligence Community, rather than at a single academic discipline. It includes the intelligence apparatus, but also the policy and political decision-making component essential to national security. Big data, national security and intelligence are complex concepts with a variety of meanings. Nevertheless, they can be loosely

defined. The book argues that the relationship between intelligence producers and users of intelligence – those that make political calculations about national security – is critical and interconnected, especially in a big data era. Furthermore, the book demonstrates the need to take a holistic view of intelligence, defined by its purpose rather than field of application, and to include policy and decision-makers.

Australian National Intelligence Community

This section provides an overview of the Australian national security architecture and background to the Australian National Intelligence Community – including its composite agencies, oversight framework and legislative foundations for an international readership. It also outlines the methodology and analytical process of the research. It provides some context, especially for international readers, to engage with the perspectives that participants offered. Whilst this research is Australia specific, the themes surfaced here are expected to apply in many democratic countries.

Ten agencies make up the Government's intelligence enterprise – collectively known as the National Intelligence Community (NIC) – working to collect, analyse and disseminate intelligence information and advice in accordance with Australia's interests and national security priorities (ONI 2017). The NIC is a relatively new grouping of agencies, having expanded from the six agencies known as the Australian Intelligence Community (AIC): the Office of National Intelligence (ONI) – formerly the Office of National Assessments (ONA), the Australian Signals Directorate (ASD), the Australian Geospatial-Intelligence Organisation (AGO), the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO) and the Defence Intelligence Organisation (DIO). To these six have been added the Australian Criminal Intelligence Commission (ACIC) and the intelligence functions of the Australian Federal Police (AFP), the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Department of Home Affairs (Home Affairs).

This expansion followed the 2017 Independent Intelligence Review (IIR), which argued that the AIC's collective tasks were growing more difficult, given the increasing complexity of Australia's geostrategic environment, the rapid pace of technological change, and the broadening scope of security and intelligence challenges (Department of the Prime Minister and Cabinet 2017). The IIR found that, while individual agencies were performing very well, a higher level of collective performance could be achieved by strengthening integration across Australia's national intelligence enterprise (Department of the Prime Minister and Cabinet 2017). The IIR recommended expansion from the six agencies of the AIC to the current ten agencies, and the establishment of an Office of National Intelligence (ONI), incorporating the Office of National Assessments, to lead the community (Department of the Prime Minister and Cabinet 2017).

The creation of the NIC has been matched by a substantial growth in budgets for Australian intelligence agencies. AIC budgets quadrupled from 2000 and 2010 to reach AUD$1.07 billion (Richardson 2020a, p. 100). In the three years between 2018–19 and 2021–22 the combined publicly available budget of NIC agencies has grown by AUD$1.5 billion to AUD$7.1 billion, and staffing grew by 1,000 positions to 25,000 – noting this budget is for the agencies as a whole not just their intelligence functions.[3] The budget for the six AIC agencies alone (excluding the NIC additions) grew by AUD$400 million from 2018–19 to 2021–22, and 1,000 staff positions were added.[4] NIC agencies also share a joint capability fund, which NIC member agencies pay into and can apply for larger funding to improve overall NIC capability, supporting gaps in technological innovation, training and other workforce developments (Walsh 2021). Figure 0.1 shows the agencies and their primary functions within the NIC.

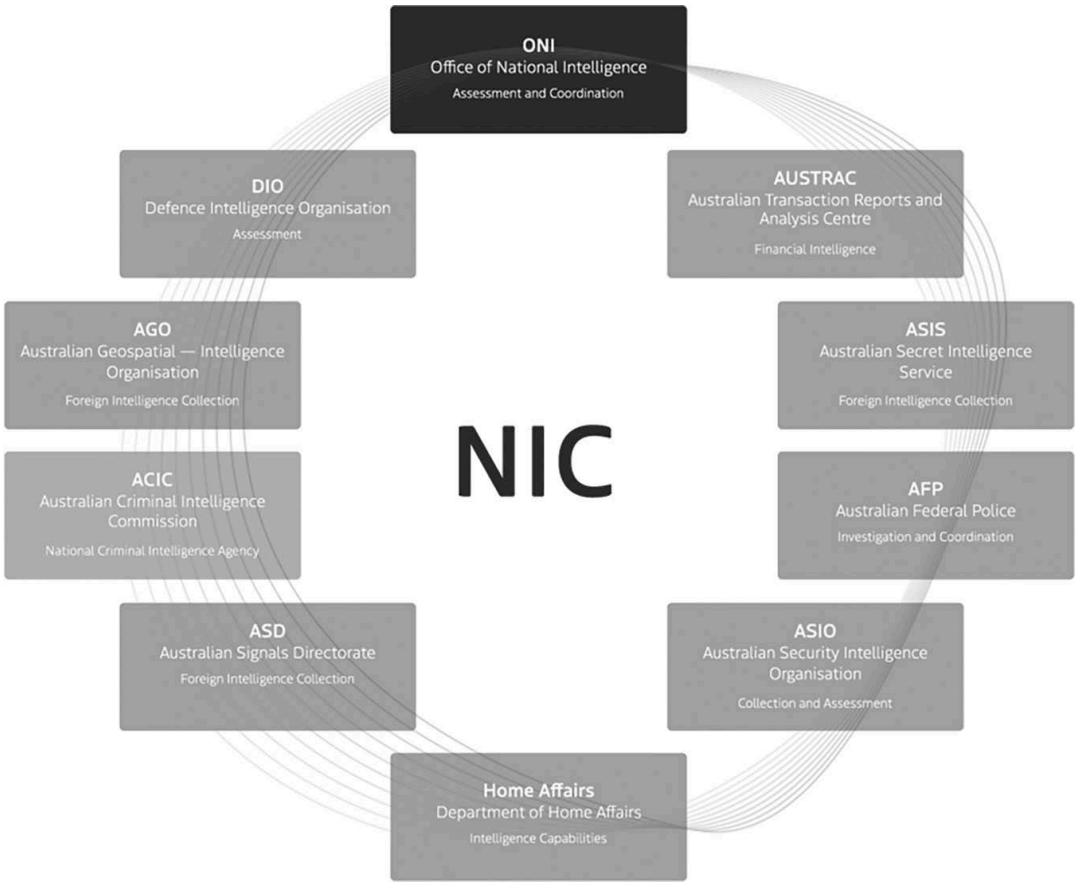

Figure 0.1 NIC Agencies (ONI 2017)

Intelligence Principles and Disciplines

In Australia, each NIC agency has a critical, distinct and enduring function (Department of the Prime Minister and Cabinet 2017). More detail about each of the agencies and their intelligence disciplines – as well as similar agencies in the United Kingdom and United States of America – are listed in Appendix A. How emerging technologies impact their activities is specific to the legal framework, mission, purpose, and technological maturity of each agency, as well as the kinds of intelligence work they do. Despite these different perspectives, they have a shared interest in improving their capability to collect, analyse and disseminate information.

Australia has made several deliberate, principled choices to manage the powers and activities of the NIC agencies (Richardson 2020a, p. 165). These principles have been considered over time and include, among others, the separations between security intelligence and law enforcement, and intelligence collection and assessment; and the distinctions between foreign and security intelligence, onshore and offshore operations, and Australians and non-Australians (Richardson 2020a, p. 165). These distinctions have been long discussed and, arguably, blurred – with some exceptions and assistance between functions – but ultimately upheld.

The three most significant distinctions in the context of emerging technologies are set out here. One of the most important distinctions concerns the jurisdiction in which intelligence collection or action takes place. Outside of exception by ministerial authorisation, the distinction between domestic and foreign intelligence collection is clear in the AIC agencies. This distinction is not as straightforward with the agencies added for the NIC, because a number have domestic *and* foreign missions, they are not intelligence collectors and their activities not jurisdictionally bound. The second distinction is how agencies are legislatively required to manage privacy. Three NIC agencies – Home Affairs, AFP and AUSTRAC – are bound to the Australian Privacy Principles of *The Privacy Act 1988*, which governs the way each agency collects, stores, uses and discloses personal information (Richardson 2020b, p. 22). The other seven agencies in the NIC are exempt from *The Privacy Act 1988* completely (Richardson 2020b, p. 22).

A third distinction is the ways information can be obtained and what it contains. Appendix B outlines the various disciplines, 'types' or means of intelligence collection (Lowenthal 2012). Collection can refer to collection agencies, or the activity of intelligence collection (Lowenthal 2012).[5] Outside of one agency – ASIO – intelligence gathering (collection) and intelligence assessment functions take place in separate AIC agencies to compartmentalise intelligence. For example, DIO relies on intelligence gathered by ASD and others to inform its assessments (Hope Royal Commission on Intelligence and Security 1974–77). However, the four NIC agencies do not fit into this collection and assessment framework. As agencies are not directly named in interview data, types of intelligence, in Appendix B, are an important way to understand the activities of the NIC agencies.

The Study

This research advances our understanding of the impacts of big data on intelligence agencies and national security in Australia. The principal aim of the book is to explore the impacts of big data for intelligence production and decision-making in national security. In doing so it sets out the impacts of big data for knowledge (the information and data needed for intelligence), intelligence activities and the organisation of intelligence communities. It demonstrates that big data has pronounced impacts on many aspects of national security, and our conception of what it includes, but is especially significant for the knowledge, activities and organisation of intelligence agencies.

The overall aim of the book is to map broad themes relating to transformations in intelligence agencies and the national security environment. First, it considers very broad impacts on the national security environment and the national security threats posed by big data. Second, it moves to examine more specific impacts for intelligence agencies and the production of intelligence. Third, it explores large themes present in society but with specific impacts for intelligence, including privacy, ethics and trust. A thread running through the book is the change that big data brings and its potential to transform the intelligence community and national security environment.

Interviews: Approach, Participant Selection and Considerations

For an emerging technology trend like big data, where research is limited, semi-structured interviews provide the most appropriate data collection method to access primary source data from national security agencies and personnel. They are ideal when little is known about a phenomenon (Gray 2009; Saunders, Lewis & Thornhill 2007; Whelan & Molnar 2018; Yin 2013) and act as a means of developing an understanding of social phenomena in their natural setting. They have been successfully applied to the national security, intelligence and policing fields where it can be difficult to access primary source data.[6]

Forty-seven participants from across all NIC agencies – as well as five independent subject matter experts – participated in semi-structured interviews. Interview questions followed semi-structured interview protocols, such as including a list of questions that were posed to all interviewees. All participants were asked to briefly outline their background and then answer a mixture of common questions, and additional questions that came up organically.[7]

Semi-structured interviews allow for a grounded theory approach which 'aims to make patterns visible and understandable' (Charmaz 2014, p. 89). Grounded theory begins with inductive data; it involves 'going back and forth between data and analysis, uses comparative methods and keeps you interacting and involved with your data and emerging analysis' (Charmaz

2014, p. 1). Through coding, the researcher *defines* what is happening in the data and begins to grapple with what it means — developing an emergent theory to explain the data (Charmaz 2014, p. 113).[8]

Interviewee selection used a purposive sampling design, meaning the primary focus was to obtain a rich set of data rather than a representative sample (De Vaus 2014). Participants were identified using snowball sampling, where the researcher accesses interviewees suggested by other interviewees and informal networks (Noy 2008). This process varied by agency. In some cases, agency heads were interviewed first, and after approval, additional participants were approached separately. In other cases, agency heads delegated the process to a suitable point of contact and suggested suitable interview participants. In other agencies, informal networks of the researcher, or the D2DCRC[9] were used. In practice, it essentially became an availability sample (De Vaus 2014) as subjects 'self-selected' or 'opted-in' to the research.

Interviews were conducted within all ten National Intelligence Community agencies as well as the oversight body, IGIS. The research involved 47 interviewees, comprising 40 individual interviews and two small groups (one of four and one of three), identifying as either independent subject matter experts (ISMEs) or within government agencies as senior decision-makers (SDMs), operational decision-makers (ODM) or technologists (TECH). The breakdown can be seen in Table 0.1.

Prior to all interviews, organisational consent was received, and the interviewees were provided with a plain language statement (PLS) and individual consent form to ensure involvement was voluntary. After the interviews, the audio was transcribed and provided to participants or agencies for their approval to ensure against the small possibility that classified or sensitive material may have been inadvertently disclosed. Minor amendments were

Table 0.1 Categories of Interviewees

Category	*Number of interviewees*
Senior decision-maker (SDM) Heads, deputy heads of agency and agency head delegates.[10]	20
Operational decision-maker (ODM) Typically, mid-management level employees responsible for leading operational decision-making and activities with small or large teams.[11]	10
Technologist (TECH) Those with a technology background.	12
Independent subject matter expert (ISME) Those with decades of experience in intelligence, national security fields and academia.[12]	5

made in many of the transcripts, predominantly to improve the overall flow of the text, clarify ambiguous points or remove specific references to organisational structure or proprietary technologies. These transcripts were then entered into QSR NVivo 12 for analysis.[13]

Ethics & limitations

This study received ethics approval from Deakin University's Faculty of Arts and Education Ethics Advisory Group and was assessed as 'negligible risk'.[14] As a researcher with experience in the field, it is possible this impacted the author's access to participants. It is possible that being perceived as an insider within the broader national security community contributed to this access. It certainly affected the author's approach to the research and their perspective. However, author's real or perceived 'insider' understanding and status enables them to articulate the impact of big data for intelligence agencies in a manner only possible with an emic understanding of a culture (Given 2008; Pike 2015).

This research does face limitations. First, due to the purposive sampling design, the views of participants are not necessarily representative of the NIC community. Second, their understanding of key questions and terms, such as 'big data', could vary. However, the interview process mitigated this by asking participants how they understood the term and then providing a clear definition spelling out which technologies were included. Finally, the findings of this research may also not be generalisable to other countries – although, the key themes it explores are both relevant and present in other democratic nations, and it is highly likely that aspects of this research will be relevant and transferrable to similar democracies.

Book Outline

The book shows that big data fuels emerging technologies and is transforming intelligence production specifically as well as changing the national security environment broadly, including what is considered a part of national security and the relationships intelligence agencies have with the Australian people. The book highlights some of the current and future transformational changes associated with big data in society writ large that have implications for the intelligence community.

Chapter 1 establishes the big data landscape and shows how it fuels emerging technologies. It shows that big data has created a new landscape comprising data abundance, digital connectivity and ubiquitous technology. This chapter argues that the features of big data need to be considered together as a landscape to fully understand the impacts on intelligence production and national security. In examining each of these features, this chapter shows how they individually and collectively as a landscape impact intelligence activity, operations and the community. It then shows how this

new big data landscape is concentrating information, computation and economic power and that this has the potential to challenge ideas of nation-state security.

Chapter 2 shows how big data challenges some of the longstanding and foundational principles and practices of intelligence. First, the changing practice of secrecy in intelligence work and activities. Second, the way the big data landscape impacts understandings of geographical jurisdiction, affecting the distinction of between operations that occur onshore and offshore, as well as what constitutes nationality in the context of data. Third, how emerging technologies are complicating intelligence as well as challenging the national security approach to innovation and the way in which intelligence agencies adopt technologies. Fourth, big data challenges fundamental principles of intelligence storage and compartmentalisation which agencies rely on to reduce security risks. This will be further challenged by new approaches to technology. Fifth, the big data landscape has created national decision-makers outside of government. Finally, it shows that the big data landscape has exponentially increased security vulnerabilities and directly challenges existing methods of assessing social harms and national security threats.

Chapter 3 outlines new social harms and national security threats created by the big data landscape. First, this chapter charts the impacts of the rapid growth in data and analytics and shows how it is making these capabilities accessible to new actors. It shows that big data 'democratises' intelligence capabilities, making intrusive digital surveillance, profiling, influence, monitoring, tracking and targeting capabilities available to a wider range of actors (state and non-state). Second, it shows how this is democratising surveillance and creating new vulnerabilities for privacy intrusion. Third, it highlights the capability for asymmetrical information dominance, enabling a strategic advantage. It explores how disinformation and misinformation are challenging intelligence. Fourth, it reveals how big data drives disinformation and misinformation. Finally, it examines how the big data landscape enables information warfare as well as social and political harm.

Chapter 4 examines the impact of the big data landscape on intelligence production. It outlines the impacts on the knowledge, activities and organisation of intelligence agencies. This chapter shows how big data is changing intelligence as knowledge, including changes to the kinds of knowledge used for intelligence and gaps in knowledge used for intelligence, requiring a stronger focus on the purpose of intelligence. This section demonstrates how big data is changing where the knowledge and data used for intelligence come from and how knowledge for intelligence is received, digested and understood. This chapter then demonstrates the impact of big data on intelligence as an activity, showing changes to the intelligence cycle broadly and specifically highlighting three areas that participants articulated as the most pressing or of the highest priority (collection and analysis as well as data sharing and communication of intelligence). Finally, it examines the impact

of big data on intelligence as an organisation, including digital transformation and a change to the traditional models of intelligence analysis.

Chapter 5 analyses the impacts of big data on data privacy. The big data landscape has and continues to radically transform privacy across society. First, it builds on the extensive literature evidencing that big data is changing privacy norms globally and the perception that in Australia there is a need to rethink the privacy principles underpinning privacy laws. It looks at the way in which big data has changed social conceptions of privacy and challenges the Australian legislative framework for privacy and why this is important for intelligence agencies. This chapter argues the impact of big data on privacy – and privacy regulation – in society at large has potential future implications for the intelligence community. Second, this chapter shows how privacy is temporal and the impact of 'anonymisation' and aggregation of data. Chiefly that an abundance of data and the capacity to identify, link and use data quickly have created the potential for privacy intrusion remote from the individual, in less visible ways and at any point in the future. The vastness of data collectors, sellers and users has led to complex and confusing privacy landscape. Lastly, this chapter shows that intelligence agencies are differently affected by shifts in privacy. However, this research suggests that currently the direct impacts of big data on privacy in intelligence agencies are limited and predominately dependent on an agency's role and legislative mandate, affecting some agencies more than others. Participants highlighted that the impact of big data on privacy is characterised by one significant distinction among the AIC collection agencies – that is, whether the agency has a foreign or domestic mandate. Big data is changing how some agencies collect, store and analyse data, particularly those subject to a legislative requirement to determine whether the data relates to an individual who is Australian.

Chapter 6 examines how the big data landscape impacts ethics in intelligence. It reveals how the big data landscape is changing established ethical boundaries of intelligence, including where big data will not improve intelligence activities. According to participants, there are aspects of intelligence where big data and automation will not ever be useful and other situations where more testing and refinement is needed before such systems are introduced. This chapter highlights ethical dilemmas of big data in intelligence that have not previously been studied. First, 'ethics at scale' – that some of the decisions around ethics are being automated and applied at scale in social contexts by private companies, which would represent a considerable ethical dilemma if applied to intelligence activities. Second, ethics in intelligence includes considering bias. This chapter indicates that intelligence practitioners should be aware of the difference between cognitive bias and data bias as well as the intelligence challenges of incomplete data sets and the bias of intelligence collection itself.

Chapter 7 shows how the big data landscape is changing public perception of trust, transparency, and the legitimacy of intelligence agency operations.

Interviewees reflect on their relationships with the public and how big data has and will impact that relationship. Emerging strongly from the data was a sense that trust is significant in the role of national security agencies in Australia. Participants indicated that they saw big data and the information ecosystem it enables as changing the relationships between intelligence agencies and the public. Furthermore, this chapter argues that big data impacts trust in the entire system of government and public service agencies as it is reliant on trust in the way data is collected and used across all government agencies, not just the national security sector. This chapter proposes that big data is changing the public's perceptions of the intelligence community around trust, transparency and the legitimacy of intelligence agency operations. It unpacks how participants understand trust and the key concepts of trust, legitimacy and the social contract, which each emerging from the interview data. This chapter shows that participants perceive that how trust is built and developed is impacted by big data, with participants suggesting intelligence agencies need to align big data use with agency values and purpose, transparency and public engagement.

The Conclusion reflects on the findings throughout the book and highlights some of the implications for policy and limitations of as well as areas for future research. The book reveals how the big data landscape is transforming what intelligence is, how it is practised, and the relationships intelligence organisations have with society and with each other. It shows that big data has impacts on many aspects of national security, including our conception of what it constitutes. The impact of big data is especially significant for the knowledge, activities and organisation of intelligence agencies. The book highlights specific impacts for intelligence agencies and the production of intelligence, and then examines how intelligence agencies interact with each other and look out to the rest of society. The book details how big data is impacting the relationship between intelligence agencies and citizens, specifically in the areas of privacy, ethics and trust.

Notes

1 The NIC is comprised of the original Australian Intelligence Community (AIC) agencies plus four new ones. The agencies in the AIC are the Office of National Intelligence, Australian Security Intelligence Organisation, Australian Secret Intelligence Service, Defence Intelligence Organisation, Australian Signals Directorate and Australian Geospatial-Intelligence Organisation. The Home Affairs Portfolio brings together Australia's national and transport security, criminal justice, emergency management, multicultural affairs, and immigration and border-related functions and agencies. Agencies within the Department of Home Affairs include the Australian Criminal Intelligence Commission (ACIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC). ACIC is included in the NIC in its entirety, whereas the other new agencies in Home Affairs (AUSTRAC and the Department of Home Affairs itself and the AFP) have only the intelligence functions of their organisations included.

2 While this is a UK-specific definition, a similar definition from the US defines national security as 'the ability of national institutions to prevent adversaries from

using force to harm Americans or their national interests and the confidence of Americans in this ability', from both the physical and psychological dimensions (Sarkesian, Williams & Cimbala 2008, p. 4).

3 Richardson 2020a, p. 267; ACIC 2022; AFP 2022; ASD 2022; ASIO 2022; AUSTRAC 2022; Department of the Prime Minister and Cabinet 2020; 2022; Department of Home Affairs 2019; 2022. Note: These the budget and staffing figures exclude ASIS, DIO and AGO, as their details are 'not for publication'.

4 Richardson 2020a, p. 267; ACIC 2022; AFP 2022; ASD 2022; ASIO 2022; AUSTRAC 2022; Department of the Prime Minister and Cabinet 2020; 2022; Department of Home Affairs 2019; 2022.

5 For a thorough outline of collection and collection disciplines see Lowenthal (2012, pp. 71–118).

6 Examples include examinations of data science use in the United States' Defense Intelligence Agency (Knopp et al. 2016), the UK police's use of data (Babuta 2017), and the impact of big data on the production of security in Australia (Chan & Bennett Moses 2017), which fell short of specifically exploring big data's impact on intelligence production. Additional studies in intelligence, analysis and national security also utilised qualitative interview methods (Chan & Bennett Moses 2017; Chen et al. 2017; Coyne 2014; Ratcliffe 2012; Treverton & Gabbard 2008; Walsh 2011; Whelan 2014).

7 Common questions included: (i) What is your understanding of big data? (ii) How does big data impact on your organisation? (iii) How would you describe the current and future challenges and opportunities of big data?

8 Coding was conducted line by line (Charmaz 2014, pp. 124–127), followed by focused coding to draw out larger concepts (Glaser & Strauss 1967, pp. 101–117). The final stage of the analysis involved the in-built search and frequency query functionality of QSR NVivo 12 to ensure no categories or data were missed.

9 Data 2 Decisions Cooperative Research Centre provided a scholarship to partially fund this research.

10 SDMs were SES2 and above in the Australian Public Service context.

11 ODMs were mainly EL1, EL2 and SES1 in the Australian Public Service context.

12 The five ISMEs were Stephen Merchant PSM, Dennis Richardson AC, Clive Lines, Ian McKenzie PSM and Dr Lesley Seebeck. In the data their comments are de-identified as ISME.

13 QSR NVivo is a software designed to help researchers to gain richer insights from qualitative and mixed-methods data. It stores and organises data as well as helping researchers to categorise, analyse and visualise their data.

14 This involved submitting a 'low risk' application form, the PLS and consent form as well as sample interview questions. The two ethical considerations of this study were ensuring participant anonymity, and the security of the interview data – as a result, all participants are anonymised, and the recordings and transcripts are only accessible to the author.

References

Agrell, W 2012, 'The next 100 years? Reflections on the future of intelligence', *Intelligence and National Security*, vol. 27, no. 1, pp. 118–132.

Agrell, W & Treverton, GF 2015, *National intelligence and science: beyond the great divide in analysis and policy*, Oxford University Press, Oxford.

Akhgar, B, Saathoff, GB, Arabnia, H, Hill, R, Staniforth, A & Bayerl, PS 2015, *Application of big data for national security: a practitioner's guide to emerging technologies*, Waltham Elsevier, Amsterdam.

Andrew, C 2018, *The secret world: a history of intelligence*, Penguin Books, London.
ACIC 2022, *Australian Criminal Intelligence Commission Annual Report 2021–22*, Commonwealth of Australia, Canberra.
AFP 2022, *Australian Federal Police Annual Report 2021–22*, Commonwealth of Australia, Canberra.
ASIO 2022, *Australian Security Intelligence Organisation Annual Report 2021–22*, Commonwealth of Australia, Canberra.
ASD 2022, *Australian Signals Directorate Annual Report 2021–22*, Commonwealth of Australia, Canberra.
AUSTRAC 2022, *AUSTRAC Annual Report 2021–22*, Commonwealth of Australia, Canberra.
Babuta, A 2017, *Big data and policing an assessment of law enforcement requirements, expectations and priorities*, RUSI Occasional Paper, RUSI, London.
Baldwin, DA 1997, 'The concept of security', *Review of International Studies*, vol. 23, no. 1, pp. 5–26.
Beer, D 2018, 'Envisioning the power of data analytics', *Information, Communication & Society*, vol. 21, no. 3, pp. 465–479.
Bennett Moses, L & Chan, J 2014, 'Using big data for legal and law enforcement decisions: testing the new tools', *University of New South Wales Law Journal*, vol. 37, no. 2, pp. 643–678.
Betts, R 2009, 'Analysis, war, and decision', in P Gill, S Marrin & M Phythian (eds), *Intelligence theory: key questions and debates*, Routledge, New York, pp. 87–111.
boyd, d & Crawford, K 2012, 'Critical questions for big data', *Information, Communication & Society*, vol. 15, no. 5, pp. 662–679.
Buzan, B, Waever, O & de Wilde, J 1998, *Security: a new framework for analysis*, Lynne Rienner, Boulder, CO.
Chan, J & Bennett Moses, L 2016, 'Is big data challenging criminology?', *Theoretical Criminology*, vol. 20, no. 1, pp. 21–39.
Chan, J & Bennet Moses, L 2017, 'Making Sense of Big Data for Security', *The British Journal of Criminology*, vol. 57, no. 2, pp. 299–319.
Charmaz, K 2014, *Constructing grounded theory*, Sage, London.
Chawda, RK & Thakur, DG 2016, 'Big data and advanced analytics tools' [conference presentation], *Symposium on Colossal Data Analysis and Networking*, Indore, India, 18–19 March.
Chen, D, Fraiberger, SP, Moakler, R & Provost, F 2017, 'Enhancing transparency and control when drawing data-driven inferences about individuals', *Big Data*, vol. 5, no. 3, pp. 197–212.
Chen, M, Mao, S & Liu, Y 2014, 'Big data: a survey', *Mobile Networks and Applications*, vol. 19, no. 2, pp. 171–209.
Cloud Security Alliance 2013, *Big data analytics for security intelligence*, Cloud Security Alliance, Seattle, WA.
Coyne, J 2014, 'Strategic intelligence in law enforcement: anticipating transnational organised crime', PhD thesis, Queensland University of Technology.
Cukier, K 2010, 'Data, data everywhere', *The Economist*, 27 February, accessed 2 December 2021, https://www.economist.com/special-report/2010/02/27/data-data-everywhere.
Davies, PHJ, Gustafson, K & Rigden, I 2013, 'The intelligence cycle is dead, long live the intelligence cycle: rethinking intelligence fundamentals for a new intelligence doctrine' in M Phythian (ed.), *Understanding the intelligence cycle*, Routledge, London, pp. 56–75.

De Vaus, DA 2014, *Surveys in social research*, 6th edn, Routledge, London.
Degaut, M 2015, 'Spies and policymakers: intelligence in the information age', *Intelligence and National Security*, vol. 31, no. 4, pp. 509–531.
Department of Home Affairs 2019, *Department of Home Affairs 2018–19*, Commonwealth of Australia, Canberra.
Department of Home Affairs 2022, *Department of Home Affairs 2021–22*, Commonwealth of Australia, Canberra.
Department of the Prime Minister and Cabinet 2017, *2017 Independent Intelligence Review*, Commonwealth of Australia, Canberra.
Department of the Prime Minister and Cabinet 2020, *Portfolio Additional Estimates Statements 2019–20*, Commonwealth of Australia, Canberra.
Department of the Prime Minister and Cabinet 2022, *Portfolio Budget Statements 2022–23: Budget Related Paper No. 1.11*, Commonwealth of Australia, Canberra.
DOMO 2019, *Data never sleeps 7.0*, DOMO, accessed 2 December 2021, https://www.domo.com/learn/infographic/data-never-sleeps-7.
Dupont, A 1990, *Australia and the concept of national security* (Working paper no. 206), Strategic and Defence Studies Centre, Australian National University, Canberra.
Dupont, A 2003, 'Intelligence for the twenty-first century', *Intelligence and National Security*, vol. 18, no. 4, pp. 15–39.
Ericsson 2022, 'Ericsson Mobility Visualizer' Ericcson, November, accessed 17 April 2023, https://www.ericsson.com/en/reports-and-papers/mobility-report/mobility-visualizer?f=1&ft=2&r=2,3,4,5,6,7,8,9&t=1,2,3,4,5,6,7&s=4&u=1&y=2022,2028&c=3.
Evans, D 2011, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco, San Jose, accessed 26 May 2023, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
Fingar, T 2011, *Reducing Uncertainty: Intelligence Analysis and National Security*, Stanford University Press, Redwood City.
Gandomi, A & Haider, M 2015, 'Beyond the hype: big data concepts, methods, and analytics', *International Journal of Information Management*, vol. 35, pp. 137–144.
Gartner 2017, 'Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016', *Gartner*, 7 February, viewed 25 May 2023, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.
George, RZ & Bruce, JB, eds., 2014, *Analyzing intelligence: national security practitioners' perspectives*, 2nd edn, Georgetown University Press, Washington, DC.
Gill, P & Phythian, M 2006, *Intelligence in an insecure world*, Wiley, Hoboken, NJ.
Given, L (ed.) 2008, *The Sage encyclopedia of qualitative research methods*, Sage, Thousand Oaks, CA.
Glaser, BG & Strauss, AL 1967, *The discovery of grounded theory: strategies for qualitative research*, Aldine, Chicago.
Gookins, AJ 2008, 'The role of intelligence in policy making', *SAIS Review*, vol. 28, no. 1, pp. 65–73.
Gray, DE 2009, *Doing research in the real world*, 3rd edn, Sage, Los Angeles.
Gyngell, A & Wesley, M 2007, *Making Australian foreign policy*, 2nd edn, Cambridge University Press, Cambridge.
Heuer, RJ & Pherson, R 2015, *Structured analytic techniques for intelligence analysis*, 2nd edn, CQ Press, Thousand Oaks, CA.
Hughes, RG, Jackson, P & Scott, L (eds) 2008, *Exploring intelligence archives: enquiries into the secret state*, Routledge, London.

International Data Corporation 2014, *The digital universe*, International Data Corporation, Needham, MA.

International Data Corporation 2022, *Worldwide IDC Global DataSphere Forecast, 2023–2027: It's a Distributed, Diverse, and Dynamic (3D) DataSphere*, International Data Corporation, Needham, MA.

Katzenstein, Peter J 1996, *The culture of national security: norms and identity in world politics*, edited by Peter J. Katzenstein. Columbia University Press, New York.

Kemp, S 2023, 'Digital 2023', *We are social*, 26 January, accessed 5 April 2023, https://wearesocial.com/au/blog/2023/01/the-changing-world-of-digital-in-2023-2/.

Kent, S 1966, *Strategic intelligence for American world policy*, Princeton University Press, Princeton, NJ.

Kitchin, R 2014a, 'Big data, new epistemologies and paradigm shifts', *Big Data & Society*, vol. 1, no. 1.

Kitchin, R 2014b, *The data revolution: big data, open data, data infrastructures & their consequences*, Sage, London.

Kitchin, R & Lauriault, TP 2014, 'Small data in the era of big data', *GeoJournal*, vol. 80, no. 4, pp. 463–475.

Knopp, BM, Beaghley, S, Frank, A, Orrie, R & Watson, M 2016, *Defining the roles, responsibilities, and functions for data science within the defense intelligence agency*, RAND Corporation, Santa Monica, CA.

Landon-Murray, M 2016, 'Big data and intelligence: applications, human capital, and education', *Journal of Strategic Security*, vol. 9, no. 2, pp. 94–123.

Laney, D 2001, '3D data management: controlling data volume velocity and variety', *META Delta*, 6 February.

Liotta, PH 2002, 'Boomerang effect: the convergence of national and human security', *Security Dialogue*, vol. 33, no. 4, pp. 473–488.

Lowenthal, MM 2012, *Intelligence: from secrets to policy*, 5th edn, Sage/CQ Press, Los Angeles, CA.

Lundy, L, O'Brien, A, Solis, C, Sowers, A & Turner, J 2019, 'The ethics of applied intelligence in modern conflict', *International Journal of Intelligence and Counter Intelligence*, vol. 32, no. 3, pp. 587–599.

Malomo, F & Sena, V 2016, 'Data intelligence for local government? Assessing the benefits and barriers to use of big data in the public sector', *Policy & Internet*, vol. 9, no. 1, p. 7–27.

Manyika, J, Chui, M, Brown, B, Bughin, J, Dobbs, R, Roxburgh, C & Byers, AH 2011, *Big data: the next frontier for innovation, competition, and productivity*, McKinsey Global Institute, New York.

Marrin, S 2009, 'Intelligence analysis and decision-making', in P Gill, S Marrin & M Phythian (eds), *Intelligence theory: key questions and debates*, Routledge, New York, pp. 131–150.

Mayer-Schönberger, V & Cukier, K 2014, *Big data: a revolution that will transform how we live, work, and think*, Mariner Books, Houghton Mifflin Harcourt, Boston, MA.

Mayer-Schönberger, V & Ramge, T 2018, *Reinventing capitalism in the age of big data*, John Murray Press, London.

Metcalf, J, Keller, EF & boyd, d 2016, *Perspectives on big data, ethics, and society*, Council for Big Data, Ethics, and Society.

Minelli, M, Chambers, M & Dhiraj, A 2013, *Big data, big analytics: emerging business intelligence and analytic trends for today's businesses*, Wiley CIO, Hoboken, NJ.

Noy, C 2008, 'Sampling knowledge: the hermeneutics of snowball sampling in qualitative research', *International Journal of Social Research Methodology*, vol. 11, no. 4, pp. 327–344.

Omand, D 2010, *Securing the state*, Columbia University Press, New York.

Omand, D 2013, 'Securing the state: national security and secret intelligence', *Prism: A Journal of the Center for Complex Operations*, vol. 4, no. 3, pp. 14–27.

Omand, D 2020, 'Reflections on intelligence analysts and policymakers', *International Journal of Intelligence and CounterIntelligence*, vol. 33, no. 3, pp. 471–482.

ONI 2017, *The national intelligence community*, accessed 7 July 2020, https://www.oni.gov.au/national-intelligence-community.

Pike, KL 2015, *Language in relation to a unified theory of the structure of human behavior*, De Gruyter Mouton, The Hague.

Power, DJ 2014, 'Using "big data" for analytics and decision support', *Journal of Decision Systems*, vol. 23, no. 2, pp. 222–228.

Pramanik, MI, Lau, RYK, Yue, WT, Ye, Y & Li, C 2017, 'Big data analytics for security and criminal investigations', *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 7, no. 4, art. e1208.

The Privacy Act 1988 (Cwlth), accessed 22 May 2023, https://www.legislation.gov.au/Details/C2022C00361.

Ratcliffe, J 2012, *Intelligence-led policing*, Taylor and Francis, Hoboken, NJ.

Reinsel, D, Gantz, J & Rydning, J 2017, *Data age 2025: the evolution of data to life-critical*, International Data Corporation, Needham, MA.

Richardson, D 2020a, *Comprehensive Review of the Legal Framework of the National Intelligence Community*, vol. 1, Commonwealth of Australia, Canberra.

Richardson, D 2020b, *Comprehensive Review of the Legal Framework of the National Intelligence Community*, vol. 4, Commonwealth of Australia, Canberra.

Rolington, A 2013, *Strategic intelligence for the 21st century: the mosaic method*, Oxford University Press, Oxford.

Royal Commission on Australia's Intelligence and Security Agencies (Hope Royal Commission on Intelligence and Security) 1974–77, *Royal Commission on Australia's Intelligence and Security Agencies*, Commonwealth of Australia, Canberra.

Sadowski, J 2020, *Too smart: how digital capitalism is extracting data, controlling our lives, and taking over the world*, MIT Press, Cambridge, MA.

Sarkesian, SC, Williams, JA & Cimbala, SJ 2008, *US National Security: Policymakers, Processes, and Politics*, Lynne Rienner Publishers.

Saunders, M, Lewis, P & Thornhill, A 2007, *Research methods for business students*, Financial Times/Prentice Hall, Harlow, UK.

Schwab, K 2017, *The fourth industrial revolution*, Penguin Books, London.

Scott, L & Jackson, P 2004, 'The study of intelligence in theory and practice', *Intelligence and National Security*, vol. 19, no. 2, pp. 139–169.

Shahbazian, E 2016, *Intelligence analysis: needs and solutions*, IOS Press, Amsterdam.

Shu, H 2016, 'Big data analytics: six techniques', *Geo-spatial Information Science*, vol. 19, no. 2, pp. 119–128.

Spracher, WC 2009, 'National security intelligence professional education: a map of U.S. civilian university programs and competencies', Doctor of Education thesis, George Washington University.

Symon, P 2018, *ASIS Director-General launches new book – 'Intelligence and the Function of Government'*, Australian National University, News and Events, 21

March, accessed 2 December 2021, https://bellschool.anu.edu.au/news-events/stories/6028/asis-director-general-launches-new-book-intelligence-and-function.

Symon, PB & Tarapore, A 2015, 'Defense intelligence analysis in the age of big data', *Joint Force Quarterly*, vol. 79, no. 4, pp. 4–11.

Treverton, GF & Gabbard, CB 2008, *Assessing the tradecraft of intelligence analysis*, Intelligence Policy Center, RAND National Security Research Division, Santa Monica, CA.

van der Sloot, B, Broeders, D & Schrijvers, E (eds) 2016, *Exploring the boundaries of big data*, Netherlands Scientific Council for Government Policy, The Hague.

Van Puyvelde, D 2018, 'Qualitative research interviews and the study of national security intelligence', *International Studies Perspectives*, vol. 19, no. 4, pp. 375–391.

Van Puyvelde, D, Coulthart, S & Hossain, MS 2017, 'Beyond the buzzword: big data and national security decision-making', *International Affairs*, vol. 93, no. 6, pp. 1397–1416.

Walsh, PF 2011, *Intelligence and intelligence analysis*, Routledge, London.

Walsh, PF 2021, 'Transforming the Australian intelligence community: mapping change, impact and challenges', *Intelligence and National Security*, vol. 36, no. 2, pp. 243–259.

Whelan, C 2014, 'Managing dynamic security networks: towards the strategic managing of cooperation, coordination and collaboration', *Security Journal*, vol. 1, no. 18, pp. 310–327.

Whelan, C & Molnar, A 2018, *Securing mega-events: networks, strategies and tensions*, Palgrave Macmillan UK, London.

Wolfers, A 1952, '"National security" as an ambiguous symbol', *The Academy of Political Science*, vol. 67, no. 4, pp. 481–502.

Wolfers, A 1962, *Discord and collaboration: essays on international politics*, Johns Hopkins Press, Baltimore, MD.

Yin, RK 2013, *Case study research: design and methods*, Sage, Thousand Oaks, CA.

Yiu, C 2012, *The big data opportunity: making government faster, smarter and more personal*, Policy Exchange, London.

Zedner, L 2003, 'The concept of security: an agenda for comparative analysis', *Legal Studies*, vol. 23, no. 1, pp. 153–175.

Zedner, L 2009, *Security*, Routledge, London.

Zegart, A 2022, *Spies, Lies, and Algorithms: The History and Future of American Intelligence*, Princeton University Press, Princeton.

Zuboff, S 2019, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, Profile Books, London.

1 Big Data Landscape Fuels Emerging Technologies

Big data has transformed the information environment we live in. The digital age is complex, challenging and transformative for intelligence agencies and intelligence communities globally. Big data, as well as the emerging technologies it fuels, such as artificial intelligence (AI), continue to change intelligence production and the national security environment. Big data 'is less about data that is big than it is about a capacity to search, aggregate and cross-reference large data sets' (boyd & Crawford 2012, p. 663). Whilst there are many definitions of big data, there are three foundational features relevant to national security: data abundance, digital connectivity and ubiquitous technology. Although seemingly obvious, data abundance, digital connectivity and ubiquitous technology need to be considered together – as the big data landscape – to fully understand the current type and speed of change in intelligence production and national security as well as potential effects of emerging technologies. The sheer abundance of data means that moments that were previously unrecorded are now captured, and it is possible to create comprehensive profiles about people, places and things from this data. Digital connectivity means this data can be collected and exchanged in real time. The ubiquity of technology shows how big data is core to many emerging technologies and has centralised information, computation and economic power.

The features of the big data landscape examined in this section – data abundance, digital connectivity, and ubiquitous technology – individually and collectively transform aspects of intelligence production and national security. Because little is known about intelligence activities and agencies (Andrew 2018, Van Puyvelde 2018, Zegart 2022) it is necessary to define each of these features of big data and to understand them as a landscape. This helps to capture the nuanced impacts of big data on intelligence activities, within individual agencies and in the intelligence community as a whole – as well as on national security broadly. It also provides a framework to engage with new technologies. This chapter shows how the features of the big data landscape individually and collectively impact intelligence activities, operations and intelligence communities. Further, the book shows this new big data landscape is centralising information and computation power, and that this has the potential to change concepts of nation-state security.

DOI: 10.4324/9781003389651-2

The Big Data Landscape

Big data is an amorphous and contested concept which refers to large, diverse, growing and changing datasets (Bennett Moses & Chan 2014; Chan & Bennett Moses 2016, 2017; Malomo & Sena 2016). Historical databases were constrained and unable to simultaneously deal with the original 3Vs – volume, velocity and variety (Kitchin 2014b, p. 68; Laney 2001) of big data. Increased computational power, new database design and distributed storage enabled collection and analysis of big data (Kitchin 2014b, p. 68). The 3V definition of big data (Kitchin 2014b, p. 68; Laney 2001) was expanded to a 5V definition that includes veracity (certainty and consistency in data) and value (insights into and from data) (Akhgar et al. 2015; van der Sloot, Broeders & Schrijvers 2016), which includes knowledge derived from understanding data sets as a whole and by drawing insights using new analytical techniques (boyd & Crawford 2012; Kitchin 2014a; Kitchin & Lauriault 2014)

It is the ability to combine and use large data sets for some type of decision or action that defines big data (boyd & Crawford 2012). As others have aptly put, 'big data are worthless in a vacuum. Its potential value is unlocked only when leveraged to drive decision-making' (Gandomi & Haider 2015, p. 140). Big data, as one of the building blocks of AI, is essential for continued success in the emerging technology market. Whilst the 3V and 5V definitions of big data are very useful ways of categorising big data for computer science, they do not accurately reflect the complete impact of big data on national security, or how it is being used, constraining understanding about its impact on intelligence.

This section shows that there are in fact three foundational features of big data for national security: data abundance, digital connectivity and ubiquitous technology,[1] and that these features combined have created a big data landscape. These three features emerged clearly in this study as foundational features through which to understand the impact of big data on intelligence and national security. This research offers empirical evidence to deepen understanding of these terms as well as to present them together as a landscape (see Figure 1.1). Data abundance, digital connectivity and ubiquitous technology can be observed in wider society. Whilst they do overlap and intersect, they are essential to understanding the impact of big data on intelligence and national security.

Data abundance is the vast and growing volume of data in society. It includes digitisation, datafication and the global datasphere – the summation of data created and shared (Reinsel, Gantz and Rydning 2018).[2] National security practitioners have published on data abundance (Corrigan 2019; Gordon 2017, 2019, 2020; Symon & Tarapore 2015), also calling it a digital revolution (Gerstell 2019) and the information age (Coyne, Neal & Bell 2014; Degaut 2015; Rovner 2013).

Digital connectivity is the ability to connect people, places and ideas through digital networks (BBC 2018). Pandya (2019) explores how connected

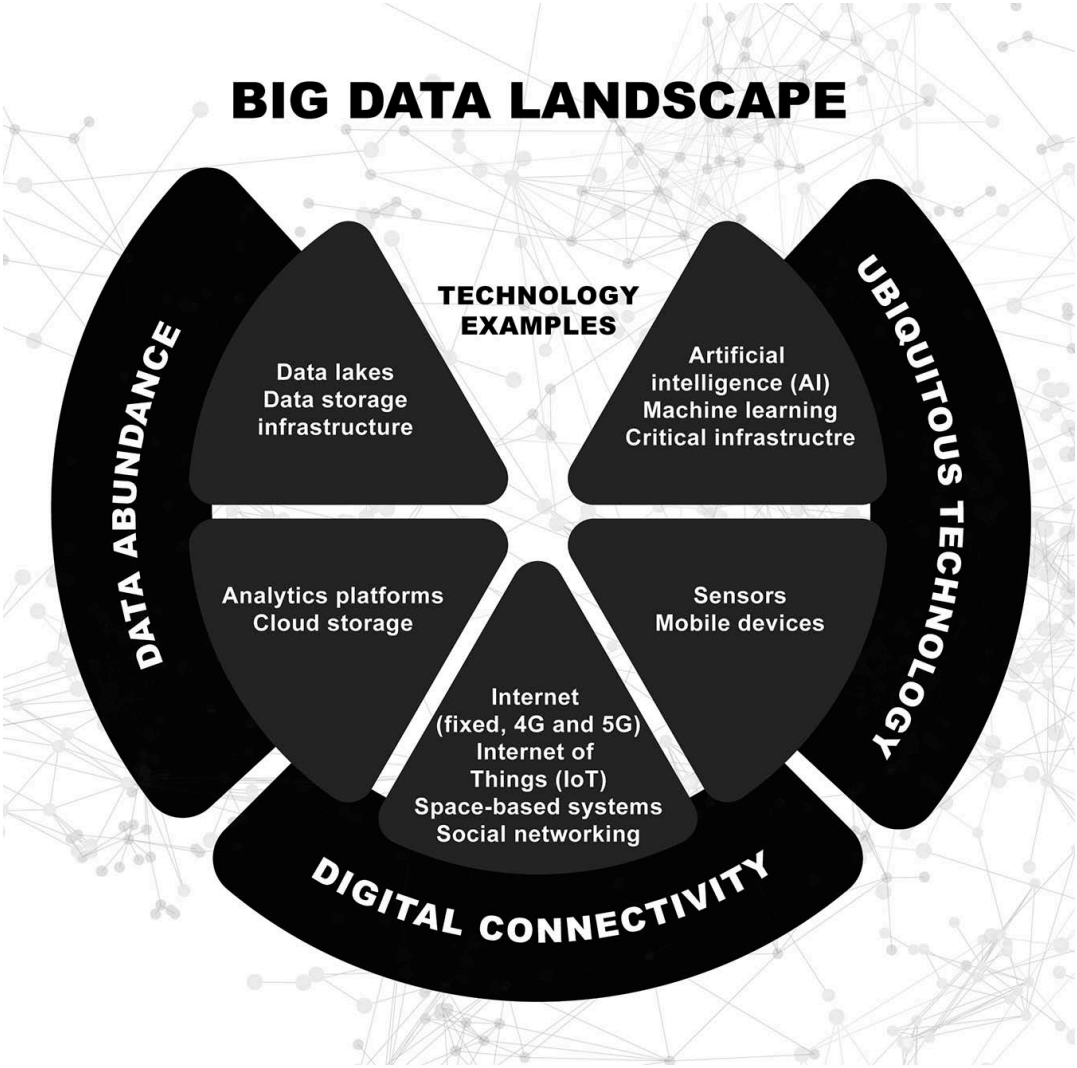

Figure 1.1 Features of the Big Data Landscape
Source: Designed by Susan Beale.

computers, networks and cyberspace have become an integral part of all digital processes across society. Bell (2018) connects the number of internet users and the notion of digital connectedness. Schwab (2017) suggests that digital connectivity includes billions of sensors and devices around the world connected to the internet. Additionally, digital connectivity includes the relationship between things and people made possible by connected technologies and various platforms (Schwab 2017), enabling hitherto unconnected agents to connect (Australian Government Productivity Commission 2016). Technology is a part of everyday life for all members of the community; we are living, working and communicating in a digitally connected world (ASIO 2018).

Ubiquitous technology is the pervasiveness of technology in our lives and the extent to which we interact with it, knowingly or unknowingly. Technology including phones, sensors and algorithms is now so ubiquitous that

living without it seems impossible as it is so deeply embedded in our lives (Unsworth 2016). Ubiquitous technology includes artificial intelligence and machine learning, whether visible or invisible.

These features combined have created a big data landscape, or 'infrastructural core', which forms the heart of the information ecosystem upon which many other apps and platforms are built and for which a handful of companies control the information services (van Dijck, Poell & de Waal 2018). As one of the building blocks of artificial intelligence, big data is essential for success in most emerging technology markets and understanding where it is created, used, and resides, and who it adds value for, is important. Data underpins the use of artificial intelligence in society and in intelligence. The big data landscape is critical because many emerging technologies rely on this framework. Automation, machine learning and artificial intelligence are possible due to data and the software, hardware and infrastructure systems supporting their growth. New technologies from generative pre-trained transformers (GPT) to quantum computing to biotechnologies are inextricably linked to the big data landscape. Without it our digital world would cease to operate seamlessly. The next part of this chapter outlines the features of the big data landscape in detail.

Data Abundance

The global evolution from data scarcity to data abundance (Gordon 2019, 2020) is a key area in which big data has affected intelligence. Information has gone from scarce to superabundant (Cukier 2010) and scholars and practitioners alike have considered the changing role of information in national security as: the 'information age' (Coyne, Neal & Bell 2014; Degaut 2015; Gordo 2017; Herman 2001; Tucker 2014), 'information explosion' (Press 2013), an 'infoglut' or data overload (Andrejevic 2013) and a 'digital revolution' (Gerstell 2019). Despite awareness of the volume of information, the implications of data abundance on intelligence activities and impacts on intelligence agencies and communities are only just beginning to emerge (Hershkovitz 2022; Zegart 2022) and have not been widely, or empirically, examined.

This research shows that the Australian National Intelligence Community (NIC), like most intelligence communities, is struggling to manage the abundance of digital data, including digitisation and datafication. The sheer volume and accessibility of information and variety of formats of digital information now available in society have unique implications for intelligence agencies. A theme evident from the participant interviews is that national security practitioners and agencies are still trying to adjust to digital transformation and the data abundance that big data has created. All participants described the abundance of data about individuals as a profound change for intelligence agencies because there is now a record of almost all human activities that can be identified to the individual level. This section demonstrates the impact of digitisation and datafication, then outlines ways in which data abundance is perceived to be transforming intelligence.

Digitisation

Digitisation is the process of turning analogue information into computer-readable formats (Mayer-Schönberger & Cukier 2014, p. 83). It is often combined with the creation of new information on digital platforms. Interview participants organically raised digital information and indicated that many of the impacts of digitisation for intelligence agencies are disruptive in ways that are consistent with the wider societal disruption. Almost all participants highlighted the transformative nature of digitisation and access to digital information, noting it is in fact a precursor to using and applying big data-enabled technologies for increasingly sophisticated analysis and interpretation. One participant highlighted that digitisation is disruptive and challenging for intelligence agencies because it requires technical capacity to manage data in a digitised format:

> It's a well understood realisation that everything is digital, but still it is disruptive, in many respects. You know, you can't really do what you might have otherwise done and get very far without the capability or capacity to deal with the digital environment. And that obviously means dealing with large volumes of data. I guess, then, it's starting to appreciate ways that you can actually go through that process of not just getting to data that you may need but also being able to analyse it in such a way that you can then determine what's of relevance and ultimately build knowledge. So, I guess that's a realisation that is obvious but can be quite complex in a lot of areas.
>
> (SDM)

Emerging from the participant interviews was a sense that aspects of data abundance, digitisation and digital information are still having disruptive impacts on intelligence agencies. Responding to a question about the biggest impact of big data on intelligence, one participant noted the seemingly self-evident: 'everything is being digitised, everything is readily available for a price or not even for a price … It is just inadvertently available' (SDM). The implications of digital information are now widely discussed and understood in society; however, their impacts on intelligence production have been largely unexplored and underappreciated. This study shows that, while these impacts are largely not unique to national security – hence they are touched on only briefly here – they are nonetheless significant for agencies and practitioners.

Datafication

Datafication – transformation of social action into online quantified data that enables real-time tracking and analysis – is not new (Mayer-Schönberger & Cukier 2014, pp. 73–97) but is increasingly sophisticated and nuanced (Mayer-Schönberger & Ramge 2018). The volume of data that is now recorded about the world and our individual activities within it is almost

inconceivably large and data collection is largely inescapable (McQueen 2018, p. 8). 'Internet companies have come to know much more about us and our personal habits and tastes than any intelligence agency ever could (or should)' (Omand & Phythian 2018, p. 145).

Comprehensive profiles about individuals can be created from commercially available data, which includes being able to aggregate data and identify individuals from data sets to a granular level – increasingly to a specific individual (Kitchin 2014b). Inferences are made about individuals, often without their knowledge, by the aggregation of data collected from seemingly mundane activities, including beliefs, values, preferences, psychological states, and intimate details. One of the paradoxes of big data is that, while it implies vast and impersonal data stores, data is often collected at such a granular level that it can be used to identify individuals (Richards & King 2013). Some data is individualised and some of it is collected in so-called 'anonymised' data sets, although almost all of it can be re-identified to small groups or individual level (Culnane, Rubinstein, & Teague 2016; El Emam et al. 2009; Rocher, Hendrickx, & de Montjoye 2019; Sweeney 2015; Sweeney, Abu, & Winn 2013; Office of the Director of National Intelligence 2022; Wondracek et al. 2010). Big data has exploded the scope of personal and personally identifiable information (Crawford & Schultz 2014; Australian Government 2017) and this has major implications for intelligence agencies.

Much of the existing research on data abundance in society has focused on companies monitoring, tracking and selling data about our social habits (Kitchin 2014b; Sadowski 2019; Zuboff 2019), due to their capacity in creating, storing and sharing this kind of behavioural data and in connecting individuals to each other, places and things. Commercial data sets are bought and sold by third-party data brokers, acquired by purchase from private companies and trawling public information generated by states, such as property records, voter and motor vehicle registrations, court records, and census data (Crain 2016). To provide a sense of perspective to the size of this market, just one of the thousands of data-aggregating companies that collect and sell personal data, Acxiom, processed more than 50 trillion data transactions in 2014 (Neef 2014). As one of the largest data brokers, they claim to have 2.5 billion addressable people across the globe, including one database that has 1,500 entries on all marketable American households (Acxiom 2018). Meanwhile another large broker, LexisNexis (2023) adds more than 1.2 million documents a day to their database. The Office of the Director of National Intelligence (2022, p. 4) noted LexisNexis had 84 billion records and Exactis held over 3.5 billion records that are updated monthly, and emphasised the 'large' and 'dynamic' nature of the commercially available information market.

The very fact that volumes of data about individuals exist and it is possible to build a comprehensive profile about people and things remotely – from data alone – is in fact a transformational shift for the intelligence community, as clearly explained by Omand and Phythian (2018, p. 145):

> It is thus now very hard to live without leaving a digital trace as the private sector can widely capture personal data through, for example, our debit and credit card purchases, loyalty cards, and airline and hotel bookings, as well as the records kept by the government through border controls, vehicle licensing, and passports. Intelligence agencies realized that by mining data and overlaying data sets, it would be possible to answer questions – for example, about the patterns of life, the identities, and the locations of suspects – that would have been infeasible using analogue (shoe leather) methods of detective investigation.

In this study, participants consistently stated that datafication and the volume of personally identifying information is transformative for intelligence. Participants described the capability that big data heralds; the current ability to access and link pieces information is unprecedented and has profound implications for intelligence activities, agencies and the community. One technologist explained the seemingly self-evident reality that our movements are constantly recorded but also that whoever owns or can access the data can build a comprehensive profile of individuals from this volume of data:

> [Historically] if there was a taxi journey that a surveillance team picked up you would see the start and the end of it and you might map the route if it was important. However, if there was nothing suspicious on the route you wouldn't bother mapping it, you're only interested in the start and end point. However now, you get this huge volume of noise … You know, your taxi app now records your phone number, your credit card, where you went from, to, via, when you booked it, your other trips and it's just phenomenal, all that detail.
>
> (TECH)

Almost all participants highlighted the volume of data about our movements that is captured, collected and stored, resulting in complete (or near-complete) data coverage of our lives. Datafication and the ability to derive insights from data affects agencies throughout every stage of the intelligence cycle;[3] it is evolving the way that national security agencies operate. A participant commented:

> We live in a digital age and everything is captured in a digital format or can be analysed in a digital format, hoovered up in a way that gives you the ability to be able to forensically drill in on patterns, on activities, on relationships, on everything that humans do.
>
> (SDM)

Another SDM elaborated that datafication has increased the significance of analytics for intelligence, including knowing what analytics and algorithms are required and what data you need:

> The fact that people's lives are so integrated with technology and that creates various data sets and the ability for us to potentially exploit those for good – not for evil, although of course the potential exists for that as well – is really a huge advantage for intelligence. Whether it is a big or a small data set, the amount of information you can develop about a person without ever being in contact with that person is different now to what it was twenty years ago when I started when we relied most heavily on human intelligence. Now, we can build up a profile of an individual to a fairly detailed level, provided we have the right data and the right analytics to run over it.

Data Abundance and Intelligence

The volume of personal or personally identifying information available and the degree of datafication means comprehensive profiles of individuals can be quickly and remotely created. Participants indicated this is true for individuals, interest groups, institutions, political groups and even nation-states by using shipping, procurement and other data to understand nation-state science and technology programs like nuclear or facial recognition capabilities. According to participants, the capability to create comprehensive profiles remains difficult to achieve in real time in practice for those who are not the original data collectors, including intelligence agencies. Participants described that this is because the data is collected and held in diffused and dispersed data sets for different purposes by a range of different entities and owners. Participants noted that, in some cases, it is possible to anchor personal information and biometrics to a person – especially where data sets are connected to confirmed government identity documents (such as passports and driver's licences) rather than from private data sets alone.

Many participants raised datafication and the sheer volume of personal information as an enabler in detection, monitoring and tracking. There are counter trends to this extensive data collection, with participants highlighting that some groups take action to avoid digital surveillance such as using encrypted communications and the dark web. A number of participants acknowledged that this detection, monitoring and tracking can include intelligence officers (whether they be Australian or foreign officials) but did not discuss this in further detail. One participant asked:

> If we can do it, who else can do it? Hostile intelligence services but also commercial entities. Just the amount of information they collect for marketing purposes or for advertising purposes. When we are operating operationally and using technology we are subject to all of that collect as well and it could compromise the operational activity we are doing. We are almost at a stage where in certain, potentially sensitive operations we are having to disengage from technology and fall back on old, traditional methods to try and eliminate the electronic footprint. The same way that

> the data provides an advantage for us, it could cause a disadvantage to us.
>
> (ODM)

Another ODM described some of the practical challenges in relation to terrorism offences, highlighting what it means to 'know' something in a big data environment:

> Once upon a time, someone may have done something with a knife [terrorist attack] and we may or may not have known about them. These days we know about them. Somewhere within our information holdings, or on the internet, we probably have an aggregate of data about this person. Which, if we could reverse engineer and collect with other data and analyse in the right way, might have shown indicators and all that sort of stuff. It's an interesting trade-off in terms of the opportunity that new data brings in terms of the analytic insights you can derive from it but also in terms of the new risks we have to understand and mitigate as part of our work.
>
> (ODM)

Participants articulated the notion that the volume of data coverage means that activity may be 'knowable', or 'predictable', with access to the right data in advance. How big data is changing what it means to know something, and the knowledge used for intelligence, is discussed in Chapter 4. For agencies with a domestic security function, the ability to identify potential offences in order to prevent major harm is clearly critical. Participants from agencies with a domestic security focus expressed that they felt that if information exists (for example about individuals, activities or beliefs) – or can be inferred – and agencies fail to obtain and consider that information, they would be unable to act decisively to prevent harm and would be failing in their mission.

The data collection for this research occurred over a time period including the Christchurch Mosque attacks in March 2019, with interviews occurring at the time of the attack. It is natural that interviewees referred to the intelligence challenges inherent in preventing domestic terrorist attacks in that time and context. Some intelligence agencies have access to information and indicators related to potential terrorist attacks already – while other participants communicated they are cognisant of potential access – and some participants described the challenges inherent for intelligence agencies in complete data collection about our lives existing in the world. Many participants also raised the challenges of accessing this kind of data, given the vast majority is in the private sector, as well as questioning their ability to do so in an ethical and proportionate manner.

Digital Connectivity

Digital connectivity is 'most visible in the myriad forms people employ to send, receive, broadcast, disseminate, and share information' (Murphy &

Kuehl 2015, p. 72), but includes a far more extensive, less visible network including billions of sensors in business, manufacturing, health care, retail, security, transportation and 'smart home' devices (Intel 2020). The proliferation of digital devices that are constantly connected is driven by technical advances in big data collection and analysis, storage capacity and transmission speeds. This is a trend towards 'continuously collected, almost-infinitely networkable, and highly flexible' data (Metcalf, Keller & boyd 2016, p. 2). The increased computational power, new database design and distributed storage capacity of big data (Kitchin 2014b, p. 68), alongside increased connection capabilities, have enabled the expansion of digital connectivity.

The number of devices connected to the internet has increased exponentially over the past 20 years although estimates for both current and projected connections vary greatly. Intel (2014) projected that by 2020 there would be 200 billion devices connected, meanwhile a McKinsey report (Dahlqvist et al. 2019) expected numbers to reach 43 billion by 2023 – far higher than Ericsson's (2022) more recent estimate of 26.3 billion in 2023, who predict that by 2028 that number will reach 45.8 billion. Regardless of which number you choose, all predict continued rapid growth, meaning connected technology is now increasingly a part of everyday life for Australians.

The fact that the number of digital devices in the world is growing and connectivity between devices is increasing seems obvious enough; however, the implications are just beginning to be explored in the context of national security. The book contributes empirical research on the implications of digital connectivity at scale for the intelligence community and supports the public discussion, emerging from largely US practitioners and researchers (Hershkovitz 2022; Zegart 2022). Participants in this study also raised that digital connectivity provides the potential for real-time situational awareness, such as the extensive antivirus networks that are deployed globally. Gerstell (2019, n.p.) points out that 'the larger antivirus vendors, with their sensors connected to their global corporate clients, already know more at any given moment about the state of networks around the world than does any government agency'. One participant offered insight into how that works in practice:

> If you think about the appliances that are deployed inside networks, they rely on big data and machine learning. So, if I get a Palo Alto box, attached to a smart firewall, it is getting pushed stuff from Palo Alto and their sensor network of hundreds of millions of devices that they correlate and push their smarts back into that box.
>
> (SDM)

Another participant, whose agency has a cyber-security function, suggested that there were opportunities yet to be taken up:

> If you're asking how big data impacts our data lives here, way less than it should. We should have big arrays of sensors out there, dropped in networks of other things, at end points, host-based type sensors that are generating just incredible amounts of data that we look to find oddness and we are not doing it at a scale that is sufficient for an economy such as this.
>
> (SDM)

Participants in this research organically raised digital connectivity as an aspect of big data with global transformational potential, including for the NIC. Every interview included some discussion about digital connectivity, although participants used a range of terms such as digitally connected, connectivity, networked and internet-enabled mobile devices to discuss the concept. Most participants were knowledgeable about the role of digital connectivity in providing real-time data. One ISME participant clearly articulated a frequently presented perspective:

> It is the internet and the hyper-connectivity of the internet that has created unbelievable volumes of data. This is the big data based on just the fact that everything's connected and it's generating lots of information constantly.

Another noted: 'we now carry a device around with us that enables us to communicate whenever we want to and it collects information about where we are all of the time' (TECH). Participants explained that digital connectivity has made the process of connecting pieces of personal information or personally identifying information much easier, for a wide variety of actors, because of metadata, the common denominator of an IP address, phone number or advertising identifier.

Participants universally discussed the combination of data abundance and digital connectivity as transformational for the NIC. 'Information generation, sharing, and consumption is unprecedented in its diversity, extent, fragmentation, and reach' (Mazarr et al. 2019, p. 13). Indeed, the very nature of constant digital connectivity is that it is global and omnipresent. As one participant put it:

> In the old days you could lift a telephone and talk to one person or there was the radio broadcast, but with the internet you can post and persist something globally … and of course, interact in real time globally. So, in fact, you could talk to a billion people and communicate two-way to a billion people in real time.
>
> (TECH)

Ubiquitous Technology

The exponential speed of growth and adoption of technology means that much is yet to be understood (Schwab 2017, p. 1). The ubiquity of technology and the type and speed of its growth has specific and significant

implications for the NIC. Many participants described instances where they felt the pace of technological change exceeded human ability (individually or as a community) to fully comprehend the complexity of systems, available and emerging technologies as well as challenges in evaluating technology and capability needs. One participant noted:

> Given the ubiquity of the technology, the cheapness of the technology and the level of transformation around the technology, my view is that its impact will be vastly more fundamental [to society and national security] than most people believe.
>
> (SDM)

Pandya (2019) outlines how connected computers, networks and cyberspace have become ubiquitous technologies, becoming an integral part of all digital processes across society. Many activities and processes are now controlled or go through cyberspace and this fundamentally changes the security landscape for humanity, creating unprecedented interconnectivity – and vulnerability (Pandya 2019). One participant articulated the complexity of technology ubiquity for understanding impacts:

> Broadly speaking I have to say it [big data] is going to impact on national security, intelligence agencies and the public sector in ways that people in it don't yet comprehend. Or probably can barely imagine – I include myself in that. If it doesn't then we are not doing our job properly.
>
> (TECH)

Another technologist participant explained that our understanding of technology is nascent:

> The purposes to which big data as a phenomenon and a thing can be put have nowhere near been fully explored. The positives to our collective mission – the security and safety of Australia – are yet to be fully understood but have all the potential in the world.
>
> (TECH)

The type and speed of adoption of transformative technologies is often considered in isolation from the maturity and sophistication of systems. Indeed, as they are 'so deeply embedded in our lives and have so much power in society that it is easy to forget many are barely older than teenagers' (Hammond-Errey 2022). This was clearly articulated by an NSA official and is representative of the views of the research participants:

> We all sense that we are on the cusp of unimaginable technological changes. Cell-phones and the internet seem of such manifest utility that

> we take them for granted, but that is only because they have become so central to our daily lives, not because they have been around forever … Google started in 1998. YouTube is only 14 years old, and the iPhone is merely 12 years old. The digital revolution thus far is distinguished by its ability to become ubiquitous in our daily personal and commercial lives in an astonishingly rapid time.
>
> (Gerstell 2019, n.p.)

Concentrated Data and Computational Capacity Shifts Economic and Geopolitical Power

Digital infrastructure is the backbone of our societies. The big data landscape has concentrated unprecedented information, computational and economic power within a small number of private companies, which is causing shifts in geopolitical power. This is transforming the relationships they have with nation-states and arguably challenging conceptions of national security. The technology sector has become increasingly dominated by a small number of companies, concentrating information flows, critical data sets and technical capabilities (Andrejevic 2013; Cohen 2017; Edward 2020; Moore 2016; van Dijck, Poell & de Waal 2018), including computing power essential for functioning democracies (Richmond 2019; Watts 2020). The dominance of these companies has handed them scale and influence akin to nation-states (Lehdonvirta 2022, p. 3).

The 'epicenter of the information ecosystem that dominates North American and European online space is owned and operated by five high-tech companies, Alphabet-Google, Facebook, Apple, Amazon, and Microsoft' (van Dijck, Poell & de Waal 2018, p. 6). These companies have monopolised aspects of the big data landscape of data abundance, digital connectivity and ubiquitous technology. These five companies are therefore able to control what van Dijck, Poell and de Waal (2018) call the node of global information services, in a way that participants in this study suggested was previously limited to telecommunications companies – assets that were historically government owned (Howell & Potgieter 2020). In an interview on the author's podcast series, *Technology and Security* (2023), Sue Gordon argued that there are number of companies who are 'the biggest non-state actors globally, and they do shape organisations, and they do shape activities.' One participant in this study outlined this view that was frequently expressed by participants:

> Yes. We're moving to an era where the nation-state is challenged by companies, or groups, or data providers essentially that own more data – like Amazon – who have far more knowledge and power over citizens than the government … That's a concern and something needs to be done about it, although perhaps we've missed that opportunity to take some of the power from those companies … But the essential services

> you can't opt out of … Once all your essential services run on that system you can't opt out.
>
> (ISME)

Immense volumes of data – and computational capacity – are what Alphabet-Google, Apple, Meta, Amazon and Microsoft all have in common (Mazarr et al. 2019; Neef 2014; Zuboff 2019), despite offering a variety of different services (Lotz 2018). They are described as 'data behemoths' (Zegart 2022) and the 'infrastructural core' (van Dijck, Poell & de Waal 2018) because they form the heart of an information ecosystem upon which other platforms and applications are built. Most internet users – government agencies included – are dependent on these companies at some level for their infrastructural information services (Cohen 2017; Moore 2016; van Dijck, Poell & de Waal 2018) including for computing power (Lehdonvirta 2023). Of significance is that not only do these companies have a concentration of data, they also largely own the most data storage centres and have advanced analytics and computational capabilities. China has a similar set of companies in AliBaba, Baidu, Tencent, Bytedance, and Meituan, whose reach through platforms like AliExpress (AliBaba's platform for cross-border audiences) and Bytedance's TikTok – having reached one billion monthly active users globally in September 2021 – has grown rapidly (Guoli & Li 2022; Kemp 2023, TikTok 2021).

According to participants in this study, contemporary power is in and through information and computing power which is centralised within companies that have monopolised the big data landscape of data abundance, digital connectivity and ubiquitous technology. The changing big data landscape has and will continue to alter national security by changing power in society:

> My view is that it [big data and AI] will become the new arms race … The balance of power is shifting away from the nation-state towards companies that hold the most power, Google, Facebook, AWS [Amazon Web Services] … They can start talking about how they could break up Facebook, but good luck with that.
>
> (SDM)

Participants described how concentrated data and computational capacity has contributed to practical changes for the intelligence community with an increase in decisions impacting national security being made in the private sector, explored in Chapter 2 of this book. Additionally, many participants described this shift as portending significant new social harms – and exacerbating existing ones – outlined in Chapter 3 as well as requiring changes to the existing methods of assessing national security harm and threat, outlined in Chapter 2.

Santesteban and Longpre (2020) demonstrate how data and the ability to analyse it endows substantial market power to only the largest online

platforms. Moreover, as noted in the UK Government's Independent Review of The Future of Compute (Ghahramani 2023), the compute these platforms rely on is geographically concentrated. Australia has reportedly 0.88% of the world's compute capacity as of November 2022, and the United Kingdom only 1.3% – while the top five countries (the United States, Japan, China, Finland, and Italy) have 79.1% (Top500 2022). Past efforts to change this balance, such as France's publicly funded sovereign cloud project that began in 2009, have been unsuccessful, with France's newly announced effort involving partnerships with large US companies (Lehdonvirta 2023). Participants in this study suggested that such dominance impacted the national security conception and challenged the status quo:

> The largescale data owners, Facebook, Google, Amazon, have challenged the nation-state for quite a while … It's not without reason that people like Elon Musk are concerned with the advent of AI that it's going to be the destruction of a number of nation-states.
>
> (TECH)

Companies that have monopolised data abundance, digital connectivity and ubiquitous technology control global information flows and services. Additionally, they have massive and unprecedented economic power (Lee 2021; Moore 2016; Fernandez et al. 2021; Santesteban & Longpre 2020). The top five American technology companies (Alphabet-Google, Apple, Meta, Amazon and Microsoft) had cumulative revenues of US$1.1 trillion in 2022, although their market capitalisation has dropped from a high of US$9.5 trillion in 2021 to US$7.7 trillion in April 2023 (Lee 2021; Wall Street Journal 2023a, 2023b, 2023c, 2023d, 2023e). Their combined market capitalisation in 2021 was more than six times the size of Australia's gross domestic product (US$1.55 trillion), while their revenues were almost twice the total revenue of the Australian governments (US$586 billion) in the same year (Australian Bureau of Statistics 2023; World Bank 2023). Participants spoke of the challenges they saw in this commercial power:

> I am pointing out is that an individual has more capacity in space now than nation-states. He [Elon Musk] has put up sixty satellites, the first of a couple of thousand, to provide global internet. A government could do that!
>
> (SDM)

The pandemic further accelerated digitalisation in society and contributed to widening power asymmetries between users, government and large technology companies (Véliz 2021). The value of goods that passed through Amazon in 2022 (US$514 billion) exceeded the gross domestic product (GDP) of many countries – it's 2021 revenue figure would place it in the top 30 countries for GDP (Amazon 2023, p. 23; World Bank 2023). Amazon's

fees for merchants in 2022 brought in more revenue (US$117 billion) than most states do through taxation (Lehdonvirta 2022, p. 3). Moreover, these companies have taken on key functions akin to the judicial systems of nation-states – eBay rules on more financial disputes (60 million) per year than any court outside of the United States hears on an annual basis (Lehdonvirta 2022, p. 3).

Speaking to the power and capabilities of companies that have concentrated data and computational capacity, participants raised the global nature of technology and highlighted challenges in mitigating threats and regulating activities.

> We can't regulate big data that's managed overseas. We can't manage something that someone from a covert area or someone from another country can come on and write something or do something that's going to influence our people. We can't regulate that. You can try but you really are running behind a very fast-moving train.
>
> (TECH)

Several participants highlighted that one of the key challenges of the big data landscape is regulating the global nature of data, information and computational power and that this complicates their ability to understand and manage national security threats:

> I suppose one of the big challenges with big data is that it operates globally and so our nation-states have a problem dealing with it … It's a bit like putting security on the internet. It's an afterthought. They're trying to put nation-state regulation on big data and the internet, and it is actually hard.
>
> (ISME)

Big data has transformed the information environment we live in. The type and speed of technological transformation in society has radical implications for intelligence communities globally. The first section of this chapter showed how the big data landscape of data abundance, digital connectivity and ubiquitous technology impact on intelligence and how these features have centralised power. Although seemingly obvious, data abundance, digital connectivity and ubiquitous technology form a landscape through which to unpack how big data impacts intelligence. Data abundance means there are now records of moments that were previously unrecorded and it is now possible to create profiles about people, places and things from this data. Digital connectivity means that this data is collected in real time, altering intelligence processes. The ubiquity of technology shows how big data is involved in many emerging technologies and has centralised information, computation and commercial power. The features of the big data landscape examined in this section – data abundance, digital connectivity, and ubiquitous

technology – show that it transforms aspects of intelligence production and national security.

Notes

1 I first heard this coalescence of terms used by former US intelligence practitioner and leader Sue Gordon. In subsequent communications, she confirmed that to the best of her knowledge this grouping was her own construction.
2 According to Reinsel, Gantz and Rydning (2018) there are three primary locations where digitisation is happening and where digital content is created: the core (traditional and cloud data centres), the edge (enterprise-hardened infrastructure like cell towers and branch offices), and the endpoints (PCs, smart phones and IoT devices). The summation of all this data, whether it is created, captured or replicated, is called the global datasphere, and it is experiencing tremendous growth. IDC predicts that the global datasphere will grow from 33 zettabytes (ZB) in 2018 to 175 ZB by 2025.
3 The term 'intelligence cycle' (Coyne 2014; Hulnick 2006; Lowenthal 2012; Marrin 2009, 2014) is shorthand for the process undertaken by intelligence agencies and is structured model of producing advice for decision-makers. It is also sometimes referred to generally as intelligence analysis (Lowenthal 2012; Odom 2008). The stages of the intelligence cycle vary (depending on jurisdiction, agency, task and even analyst) but generally include, in some form, direction, collection and collation, analysis, production, dissemination and evaluation (Agrell 2012; Betts 2009; Australian Criminal Intelligence Commission 2012; Davies, Gustafson & Rigden 2013; Davies 2004, 2010; Dupont 2003; Gill 2009; Hulnick 2006; Johnson 2005; Kahn 2009; Lahneman 2010; Lowenthal 2012; Marrin 2014, 2017; Ratcliffe 2012; Heuer & Pherson 2015; Rolington 2013; Thomas 1988; Treverton & Gabbard 2008; Vandepeer 2011).

References

Acxiom 2018, 'Acxiom Data Overview', *Acxiom*, September 2018, access 17 April 2023, https://www.acxiom.com/wp-content/uploads/2018/11/Acxiom_Data_Overview_2018_11.pdf.

Agrell, W 2012, 'The next 100 years? Reflections on the future of intelligence', *Intelligence and National Security*, vol. 27, no. 1, pp. 118–132.

Akhgar, B, Saathoff, GB, Arabnia, H., Hill, R., Staniforth, A. & Bayerl, P.S. 2015, *Application of big data for national security: a practitioner's guide to emerging technologies*, Waltham Elsevier, Amsterdam.

Amazon 2023, '2022 Amazon Annual Report', *Amazon.com Inc.*, 25 January, accessed 20 April 2023, https://ir.aboutamazon.com/annual-reports-proxies-and-shareholder-letters/default.aspx.

Andrejevic, M 2013, *Infoglut: how too much information is changing the way we think and know*, Routledge, New York.

Andrew, C 2018, *The secret world: a history of intelligence*, Penguin Books, London.

ASIO (Australian Security Intelligence Organisation) 2018, *Corporate plan 2018–2019*, Commonwealth of Australia, Canberra.

Australian Bureau of Statistics 2023, *Government Finance Statistics, Australia*, ABS, 28 February, accessed 6 April 2023, https://www.abs.gov.au/statistics/economy/government/government-finance-statistics-australia/latest-release.

Australian Criminal Intelligence Commission 2012, *Australian Criminal Intelligence Management Strategy 2012–15*, Commonwealth of Australia, Canberra.

Australian Government 2017, *What is personal information?*, Office of the Australian Information Commissioner, Canberra, Australia.

Australian Government Productivity Commission 2016, *Digital disruption: what do governments need to do?*, Australian Government Productivity Commission, Canberra.

Babuta, A 2017, *Big data and policing an assessment of law enforcement requirements, expectations and priorities*, RUSI Occasional Paper, RUSI, London.

BBC (British Broadcasting Corporation) 2018, *Bridging the world through digital connectivity*, BBC StoryWorks, accessed 2 December 2021, https://www.bbc.com/storyworks/specials/digital-connectivity/.

Beer, D 2018, 'Envisioning the power of data analytics', *Information, Communication & Society*, vol. 21, no. 3, pp. 465–479.

Bell, G 2018, 'The character of future Indo-Pacific land forces', *Australian Army Journal*, vol. 14, no. 3, pp. 171–184.

Bennett Moses, L & Chan, J 2014, 'Using big data for legal and law enforcement decisions: testing the new tools', *University of New South Wales Law Journal*, vol. 37, no. 2, pp. 643–678.

Betts, R 2009, 'Analysis, war, and decision', in P Gill, S Marrin & M Phythian (eds), *Intelligence theory: key questions and debates*, Routledge, New York, pp. 87–111.

boyd, d & Crawford, K 2012, 'Critical questions for big data', *Information, Communication & Society*, vol. 15, no. 5, pp. 662–679.

Chan, J & Bennett Moses, L 2016, 'Is big data challenging criminology?', *Theoretical Criminology*, vol. 20, no. 1, pp. 21–39.

Chan, J & Bennet Moses, L 2017, 'Making Sense of Big Data for Security', *The British Journal of Criminology*, vol. 57, no. 2, pp. 299–319.

Chawda, RK & Thakur, DG 2016, 'Big data and advanced analytics tools' [conference presentation], *Symposium on Colossal Data Analysis and Networking*, Indore, India, 18–19 March.

Chen, M, Mao, S & Liu, Y 2014, 'Big data: a survey', *Mobile Networks and Applications*, vol. 19, no. 2, pp. 171–209.

Cloud Security Alliance 2013, *Big data analytics for security intelligence*, Cloud Security Alliance, Seattle, WA.

Cohen, JE 2017, 'Law for the platform economy', *University of California, Davis Law Review* vol. 51, pp. 133–204.

Corrigan, J 2019, 'Spy agencies turn to AI to stay ahead of adversaries', *NextGov*, 27 June, accessed 2 December 2021, https://www.nextgov.com/emerging-tech/2019/06/spy-agencies-turn-ai-stay-ahead-adversaries/158081/.

Coyne, J 2014, 'Strategic intelligence in law enforcement: anticipating transnational organised crime', PhD thesis, Queensland University of Technology.

Coyne, J, Neal, S & Bell, P 2014, 'Reframing intelligence: challenging the cold war intelligence doctrine in the information age', *International Journal of Business and Commerce*, vol. 3, no. 5, pp. 53–68.

Crain, M 2016, 'The limits of transparency: data brokers and commodification', *New Media & Society*, vol. 20, no. 1, pp. 88–104.

Crawford, K & Schultz, J 2014, 'Big data and due process: toward a framework to redress predictive privacy harms', *Boston College Law Review*, vol. 55, no. 1, pp. 93–128.

Cukier, K 2010, 'Data, data everywhere', *The Economist*, 27 February, accessed 2 December 2021, https://www.economist.com/special-report/2010/02/27/data-data-everywhere.

Culnane, C, Rubinstein, B & Teague, V 2016, 'Crime and Privacy in Open Data: Testing the strength of methods used for protecting privacy in open data shouldn't be a crime', *Pursuit*, accessed 17 April 2023, https://pursuit.unimelb.edu.au/articles/crime-and-privacy-in-open-data.

Dahlqvist, F, Patel, M, Rajko, A & Shulman, J 2019, 'Growing opportunities in the Internet of Things', *McKinsey & Company*, 22 July, accessed 17 April 2023, https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things.

Davies, PHJ 2004, 'Intelligence culture and intelligence failure in Britain and the United States', *Cambridge Review of International Affairs*, vol. 17, no. 3, pp. 495–520.

Davies, PHJ 2010, 'Intelligence and the machinery of government: conceptualizing the intelligence community', *Public Policy and Administration*, vol. 25, no. 1, pp. 29–46.

Davies, PHJ, Gustafson, K & Rigden, I 2013, 'The intelligence cycle is dead, long live the intelligence cycle: rethinking intelligence fundamentals for a new intelligence doctrine' in M Phythian (ed.), *Understanding the intelligence cycle*, Routledge, London, pp. 56–75.

Degaut, M 2015, 'Spies and policymakers: intelligence in the information age', *Intelligence and National Security*, vol. 31, no. 4, pp. 509–531.

Dupont, A 2003, 'Intelligence for the twenty-first century', *Intelligence and National Security*, vol. 18, no. 4, pp. 15–39.

Edward, W 2020, 'The Uberisation of work: the challenge of regulating platform capitalism. A commentary', *International Review of Applied Economics*, vol. 34, no. 4, pp. 512–521.

El Emam, K, Dankar, FK, Vaillancourt, R, Roffey, T & Lysyk, M 2009, 'Evaluating the risk of re-identification of patients from hospital prescription records', *Canadian Journal of Hospital Pharmacy*, vol. 62, no. 4, pp. 307–319.

Ericsson 2022, 'Ericsson Mobility Visualizer' *Ericcson*, November, accessed 17 April 2023, https://www.ericsson.com/en/reports-and-papers/mobility-report/mobility-visualizer?f=1&ft=2&r=2,3,4,5,6,7,8,9&t=1,2,3,4,5,6,7&s=4&u=1&y=2022,2028&c=3.

Fernandez, R, Klinge, TJ, Hendrikse, R & Adriaans, I 2021, 'How big tech is becoming the government', *Tribune*, 5 February, accessed 22 March 2022, https://tribunemag.co.uk/2021/02/how-big-tech-became-the-government.

Gandomi, A & Haider, M 2015, 'Beyond the hype: big data concepts, methods, and analytics', *International Journal of Information Management*, vol. 35, pp. 137–144.

Gerstell, GS 2019, 'I work for N.S.A. We cannot afford to lose the digital revolution', *New York Times*, 10 September, accessed 20 March 2023, https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html.

Ghahramani, Z 2023, 'Independent Review of The Future of Compute: Final report and recommendations', *Department for Science, Innovation & Technology*, United Kingdom.

Gill, P 2009, 'Theories of intelligence', in P Gill, S Marrin & M Phythian (eds), *Intelligence theory: Key questions and debates*, Routledge, New York, pp. 208–226.

Gordo, B 2017, '"Big data" in the information age', *City & Community*, vol. 16, no. 1, pp. 16–19.

Gordon, S 2017, *A conversation with Sue Gordon Principal Deputy Director of National Intelligence*, Walter E. Washington Convention Center, Washington, D.C., 7 September.

Gordon, S 2019, *Sue Gordon and Michael Morrell in conversation*, CBS, Intelligence Matters Podcast, https://www.cbsnews.com/news/former-top-dni-official-sue-gordon-discusses-circumstances-of-her-departure-from-odni-transcript/.

Gordon, S 2020, 'Former top DNI official Sue Gordon discusses circumstances of her departure from ODNI', *CBS News*, 14 February, https://www.cbsnews.com/news/former-top-dni-official-sue-gordon-discusses-circumstances-of-her-departure-from-odni-transcript/.

Guoli, C & Li, J 2022, *Seeing the Unseen: Behind Chinese Tech Giants' Global Venturing*, Wiley, Newark,

Hammond-Errey, M 2022, 'You're being watched: How Big Data is changing our lives', *The Sydney Morning Herald*, 2 February, accessed 20 May 2023, https://www.smh.com.au/national/you-re-being-watched-how-big-data-is-changing-our-lives-20220201-p59st0.html.

Herman, M 2001, *Intelligence services in the information age: theory and practice*, Frank Cass, London.

Hershkovitz, S 2022, *The future of national intelligence: how emerging technologies reshape intelligence communities*, Rowman & Littlefield, Lanham.

Heuer, RJ & Pherson, R 2015, *Structured analytic techniques for intelligence analysis*, 2nd edn, CQ Press, Thousand Oaks, CA.

Howell, BE & Potgieter, PH 2020, 'Politics, policy and fixed-line telecommunications provision: Insights from Australia', *Telecommunications Policy*, vol. 44, no. 7, pp. 1–19.

Hulnick, AS 2006, 'What's wrong with the intelligence cycle', *Intelligence and National Security*, vol. 21, no. 6, pp. 959–979.

Intel 2020, 'A guide to the Internet of Things', *Intel*, accessed 29 June 2020, https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

Intel 2014, 'Intel® Gateway Solutions for the Internet of Things', *Intel*, accessed 19 April 2023, https://www.intel.com.tw/content/dam/www/public/us/en/documents/product-briefs/sb-intel-gateway-iot.pdf.

Johnson, R 2005, *Analytic culture in the US intelligence community: an ethonographic study*, Center for the Study of Intelligence, CIA, Washington, DC.

Kahn, D 2009, 'An historical theory of intelligence', in P Gill, S Marrin & M Phythian (eds), *Intelligence theory: key questions and debates*, Routledge, New York, pp. 4–15.

Kemp, S 2023, 'Digital 2023', *We are social*, 26 January, accessed 5 April 2023, https://wearesocial.com/au/blog/2023/01/the-changing-world-of-digital-in-2023-2/.

Kitchin, R 2014a, 'Big data, new epistemologies and paradigm shifts', *Big Data & Society*, vol. 1, no. 1.

Kitchin, R 2014b, *The data revolution: big data, open data, data infrastructures & their consequences*, Sage, London.

Kitchin, R & Lauriault, TP 2014, 'Small data in the era of big data', *GeoJournal*, vol. 80, no. 4, pp. 463–475.

Lahneman, WJ 2010, 'The need for a new intelligence paradigm', *International Journal of Intelligence and CounterIntelligence*, vol. 23, no. 2, pp. 201–225.

Laney, D 2001, '3D data management: controlling data volume velocity and variety', *META Delta*, 6 February.

Lee, J 2021, 'Big data for liberal democracy', *The Australian*, 5 March, accessed 12 March 2022, https://www.theaustralian.com.au/inquirer/big-data-for-liberal-democracy/news-story/10ed6d4d8b01677955fc468d3751a4b7.

Lehdonvirta, V 2022, *Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control*, MIT Press, Cambridge, MA.

Lehdonvirta, V 2023, 'Behind AI, a massive infrastructure is changing geopolitics', *Oxford Internet Institute*, 17 March, access 10 April 2023, https://www.oii.ox.ac.uk/news-events/news/behind-ai-a-massive-infrastructure-is-changing-geopolitics/.

LexisNexis 2023, 'About', *LexisNexis*, accessed 17 April 2023, https://www.lexisnexis.com/en-us/about-us/about-us.page.

Lotz, A 2018, '"Big tech" isn't one big monopoly – it's 5 companies all in different businesses', *The Conversation*, 24 March.

Lowenthal, MM 2012, *Intelligence: from secrets to policy*, 5th edn, Sage/CQ Press, Los Angeles, CA.

Malomo, F & Sena, V 2016, 'Data intelligence for local government? Assessing the benefits and barriers to use of big data in the public sector', *Policy & Internet*, vol. 9, no. 1, p. 7–27.

Marrin, S 2009, 'Intelligence analysis and decision-making', in P Gill, S Marrin & M Phythian (eds), *Intelligence theory: key questions and debates*, Routledge, New York, pp. 131–150.

Marrin, S 2014, 'Improving intelligence studies as an academic discipline', *Intelligence and National Security*, vol. 31, no. 2, pp. 266–279.

Marrin, S 2017, 'Understanding and improving intelligence analysis by learning from other disciplines', *Intelligence and National Security*, vol. 32, no. 5, pp. 539–547.

Mayer-Schönberger, V & Cukier, K 2014, *Big data: a revolution that will transform how we live, work, and think*, Mariner Books, Houghton Mifflin Harcourt, Boston, MA.

Mayer-Schönberger, V & Ramge, T 2018, *Reinventing capitalism in the age of big data*, John Murray Press, London.

Mazarr, MJ, Bauer, RM, Casey, A, Heintz, S & Matthews, LJ 2019, *The emerging risk of virtual societal warfare: social manipulation in a changing information environment*, RAND Corporation, Santa Monica, CA.

McQueen, M 2018, *How to prepare now for what's next: a guide to thriving in an age of disruption*, Wiley, Milton, Qld.

Metcalf, J, Keller, EF & boyd, d 2016, *Perspectives on big data, ethics, and society*, Council for Big Data, Ethics, and Society, https://bdes.datasociety.net/council-output/perspectives-on-big-data-ethics-and-society/.

Minelli, M, Chambers, M & Dhiraj, A 2013, *Big data, big analytics: emerging business intelligence and analytic trends for today's businesses*, Wiley CIO, Hoboken, NJ.

Moore, M 2016, *Tech giants and civic power*, King's College London Policy Institute, London.

Murphy, D & Kuehl, D 2015, 'The case for a national information strategy', *Military Review*, September-October, pp. 70–83.

Neef, D 2014, *Digital exhaust: what everyone should know about big data, digitization and digitally driven innovation*, Dale Neef, Upper Saddle River, NJ.

Odom, WE 2008, 'Intelligence analysis', *Intelligence and National Security*, vol. 23, no. 3, pp. 316–332.

Office of the Director of National Intelligence 2022, *Senior Advisory Group Panel on Commercially Available Information*, Office of the Director of National Intelligence, Washington, DC.

Omand, D & Phythian, M 2018, *Principled spying: the ethics of secret intelligence*, Oxford University Press, Oxford.

Pandya, J 2019, 'The dual-use dilemma of artificial intelligence', *Forbes*, 28 January, accessed 20 March 2023, https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/?sh=5854d6306cf0.

Power, DJ 2014, 'Using "big data" for analytics and decision support', *Journal of Decision Systems*, vol. 23, no. 2, pp. 222–228.

Pramanik, MI, Lau, RYK, Yue, WT, Ye, Y & Li, C 2017, 'Big data analytics for security and criminal investigations', *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 7, no. 4, art. e1208.

Press, G 2013, 'A very short history of big data', *Forbes*, 9 May, accessed 2 December 2021, https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/?sh=51c7904065a1.

Ratcliffe, J 2012, *Intelligence-led policing*, Taylor and Francis, Hoboken, NJ.

Reinsel, D, Gantz, J & Rydning, J 2018, *The digitization of the world from edge to core* (IDC White Paper), IDC, Needham, MA.

Richards, NM & King, JH 2013, 'Three paradoxes of big data', *Stanford Law Review Online*, vol. 41, no. 3, pp. 41–46.

Richmond, B 2019, *A day in the life of data*, Consumer Policy Research Centre, Melbourne.

Rocher, L, Hendrickx, JM & de Montjoye, YA 2019, 'Estimating the success of re-identifications in incomplete datasets using generative models', *Nature Communications*, vol. 10, no. 1, art. 3069.

Rolington, A 2013, *Strategic intelligence for the 21st century: the mosaic method*, Oxford University Press, Oxford.

Rovner, J 2013, 'Intelligence in the Twitter age', *International Journal of Intelligence and CounterIntelligence*, vol. 26, no. 2, pp. 260–271.

Sadowski, J 2019, 'When data is capital: datafication, accumulation, and extraction', *Big Data & Society*, vol. 6, no. 1.

Santesteban, C & Longpre, S 2020, 'How big data confers market power to big tech: leveraging the perspective of data science', *Antitrust Bulletin*, vol. 65, no. 3, pp. 459–485.

Schwab, K 2017, *The fourth industrial revolution*, Penguin Books, London.

Shahbazian, E 2016, *Intelligence analysis: needs and solutions*, IOS Press, Amsterdam.

Shu, H 2016, 'Big data analytics: six techniques', *Geo-spatial Information Science*, vol. 19, no. 2, pp. 119–128.

Sweeney, L 2015, 'Only You, Your Doctor, and Many Others May Know', *Technology Science*, 28 September, accessed 17 April 2023, https://techscience.org/a/2015092903/.

Sweeney, L, Abu, A, & Winn, J 2013, 'Identifying Participants in the Personal Genome Project by Name', *Data Privacy Lab*, White Paper, Harvard University.

Symon, PB & Tarapore, A 2015, 'Defense intelligence analysis in the age of big data', *Joint Force Quarterly*, vol. 79, no. 4, pp. 4–11.

Technology and Security 2023, *Audio podcast*, United States Studies Centre, 24 May, https://www.ussc.edu.au/analysis/technology-and-security-ts-podcast-intelligence-ai-and-aukus-with-former-us-principal-deputy-director-of-national-intelligence-susan-gordon.

Thomas, ST 1988, 'Assessing current intelligence studies', *International Journal of Intelligence and CounterIntelligence*, vol. 2, no. 2, pp. 217–244.

TikTok 2021, 'Thanks a billion!', *TikTok News*, 28 September, accessed 10 May 2023, https://newsroom.tiktok.com/en-us/1-billion-people-on-tiktok.

Top500 2022, 'Development over Time', *Top500*, 1 November, accessed 20 April 2023, https://www.top500.org/statistics/overtime/.

Treverton, GF & Gabbard, CB 2008, *Assessing the tradecraft of intelligence analysis*, Intelligence Policy Center, RAND National Security Research Division, Santa Monica, CA.

Tucker, D 2014, *The end of intelligence: espionage and state power in the information age*, Stanford University Press, Stanford, CA.

Unsworth, K 2016, 'The social contract and big data', *Journal of Information Ethics*, vol. 25, pp. 83–97.

van der Sloot, B, Broeders, D & Schrijvers, E (eds) 2016, *Exploring the boundaries of big data*, Netherlands Scientific Council for Government Policy, The Hague.

van Dijck, J, Poell, T & de Waal, M 2018, *The platform society: public values in a connective world*, Oxford University Press, New York.

Van Puyvelde, D 2018, 'Qualitative research interviews and the study of national security intelligence', *International Studies Perspectives*, vol. 19, no. 4, pp. 375–391.

Vandepeer, C 2011, 'Rethinking threat: intelligence analysis, intentions, capabilities, and the challenge of non-state actors', PhD thesis, University of Adelaide.

Véliz, C 2021, 'Privacy and digital ethics after the pandemic', *Nature Electronics*, vol. 4, no. 1, pp. 10–11.

Wall Street Journal 2023a, 'Alphabet Inc. Cl C', *Wall Street Journal*, 6 April, accessed 6 April 2023, https://www.wsj.com/market-data/quotes/GOOG.

Wall Street Journal 2023b, 'Microsoft Corp.', *Wall Street Journal*, 6 April, accessed 6 April 2023, https://www.wsj.com/market-data/quotes/MSFT.

Wall Street Journal 2023c, 'Apple Inc.', *Wall Street Journal*, 6 April, accessed 6 April 2023, https://www.wsj.com/market-data/quotes/AAPL.

Wall Street Journal 2023d, 'Meta Platforms Inc.', *Wall Street Journal*, 6 April, accessed 6 April 2023, https://www.wsj.com/market-data/quotes/META.

Wall Street Journal 2023e, 'Amazon.com Inc.', *Wall Street Journal*, 6 April, accessed 6 April 2023, https://www.wsj.com/market-data/quotes/amzn.

Watts, T 2020, *Democracy and the authoritarian challenge*, Lowy Institute, Canberra, https://myaccount.lowyinstitute.org/events/2020-npc-tim-watts.

Wondracek, G, Holz, T, Kirda, E, & Kruegel, C 2010, 'A Practical Attack to De-anonymize Social Network Users', in 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp. 223–238.

World Bank 2023, 'GDP (current US$)', *The World Bank*, accessed 12 April 2023, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

Zegart, A 2022, *Spies, Lies, and Algorithms: The History and Future of American Intelligence*, Princeton University Press, Princeton.

Zuboff, S 2019, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, Profile Books, London.