INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2023.2287255

Routledge
Taylor & Francis Group

Big data, emerging technologies and the characteristics of 'good intelligence'

Miah Hammond-Errey

ABSTRACT

What constitutes good intelligence is best understood by practitioners but has not been explored through empirical analysis and in the context of a digital age. This paper presents the first research inside all the agencies that form the Australian National Intelligence Community exploring how they are impacted by big data. Intelligence is often opaque to outsiders, yet understanding the characteristics of good intelligence is important to societies that rely on intelligence agencies for national security. This paper reflects the previously unheard perspectives of members of the agencies that form the Australian National Intelligence Community – where there is a significant empirical gap. Semi-structured interviews with 47 participants explored the impact of big data on intelligence and decision-making in Australia. This paper finds that intelligence must meet the following characteristics, many established in historical literature, in order to be considered good intelligence; (i) timely, (ii) purposeful, (iii) actionable, (iv) accurate, (v) provides value-add for an intended audience, and, (vi) is unbiased. This article explores and unpacks each of these characteristics of good intelligence and finds they remain critical in a big data era.

ARTICLE HISTORY
Received 7 August 2022
Accepted 14 November 2023

What we know about good intelligence

Empirical research about intelligence agencies and their activities is notoriously sparse.[1] Even though intelligence activities are an enterprise funded by the nation state, with the express purpose of protecting national interests and keeping citizens safe, little is known about them. The scarcity of information is arguably necessary; however, the increasing role of intelligence in society requires greater understanding of the public value of intelligence agencies as well as ensuring their accountability in democracies. Intelligence agencies exist to provide strategic advantage, protect national interests and security and support national responses to threats and emergencies. Gill and Phythian argue that for too long, citizens have been excluded from knowledge of intelligence policies and practices.[2] Intelligence is essential to modern statecraft in times of war and peace as well as activities in the grey zone.[3] This vital role intelligence plays in statecraft deserves – and requires – better general comprehension.[4] Practitioners themselves are often clear about how to define intelligence and what good intelligence looks like, however it remains an empirical gap.

Empirical research to date on intelligence activities has been extremely limited and much of the existing knowledge about intelligence comes from the analysis of official government documentation or historical accounts, especially outside the United States.[5] As a result, contemporary perspectives of intelligence leaders and practitioners are limited in scope and often historical. 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'.[6] One exception from this paucity of

CONTACT Miah Hammond-Errey Miah.Hammond-Errey@sydney.edu.au

information is the development of a contemporary effective intelligence framework based on interviews and case study analysis within law enforcement and intelligence agencies in Five Eye countries.[7] Walsh presents a framework and offers analysis on effective and sustainable intelligence practice, but what good intelligence actually looks like is largely outside the scope of this work.[8]

Furthermore, there is no singularly adopted definition of intelligence.[9] As Lowenthal points out, every intelligence text begins with a discussion about what intelligence means and how the author intends to define the term.[10] This article adopts the modern definitions offered by Rolington and Omand below. Rolington defines intelligence as 'information [that] is gathered and analysed, sometimes secretly, and then used to understand a particular situation and act with advantage in it'.[11] In this article, the definition is narrowed to activity related to national security.[12] Omand's purpose of intelligence is that it 'helps to improve the quality of decision-making by reducing ignorance, including reducing the vulnerability of the decision-maker to uncertainty'.[13] The combination of these two definitions acknowledges the changing information environment, accounts for the impact of big data and open-source information on intelligence activity and provides insight to a general audience.

Whereas the definition of intelligence is often debated in academia, the characteristics of good intelligence and the purpose of intelligence have been articulated in the literature. Omand shows that 'good intelligence can help the policymaker reduce the risks involved in making decisions. It can reduce the vulnerability to uncertainty itself, making surprise less surprising and less potentially damaging'.[14] Omand describes the process to achieve this as responding to the questions the decisionmakers need answered and filling the gaps in knowledge needed to make rational decisions, and to do so in accordance with the timescales set by events.[15] Sue Gordon asserts that the fundamental premise of intelligence is 'knowing the truth, seeing beyond the horizon, and allowing our policymakers to act before events dictate'.[16] The primary goal is 'eliminating or reducing uncertainty for government decision-makers'[17], and its main purpose is to 'provide information to policymakers that may help illuminate their decision options'.[18] Whilst 'it is easy enough to state the core purpose of intelligence – providing information to policymakers – the challenge of actually gathering, assessing, and delivering useful insights to those who make decisions is an intricate matter'.[19]

Attempts to codify the elements of aspirational, good or effective intelligence have proliferated. Indeed, Kent's consideration of the characteristics of intelligence is one of the reasons he became known as the father of modern American intelligence.[20] Subsequently, scholars have explored the characteristics of good intelligence, highlighting a number of characteristics identified as essential for intelligence to be useful to policymakers; however, very few unpack their meaning, and none offer empirically backed analysis. Indeed, it seems clear that a single term or definition alone cannot fully encapsulate good intelligence. Rather, it must be a combination of components. Kent outlines that intelligence is what must be known to arm leaders with the necessary knowledge to make decisions on foreign policy.[21] Decision-makers 'need knowledge which is complete, which is accurate, which is delivered on time, and which is capable of serving as a basis for action'.[22] Johnson argues that good intelligence 'will be relevant, timely, accurate, complete, and unbiased. It must also be "actionable"– that is, specific enough to allow policy officials to act upon the information'.[23]

Accuracy is considered an indispensable component of intelligence,[24] but according to Lowenthal it is hard to define because a key part of intelligence work is about operating in uncertainty and trying to make sense of disparate pieces of information.[25] Evaluation of the accuracy of information and quality of judgments within the uncertain world of political, security, and military forecasting is complex,[26] but nevertheless, accurate intelligence is aspired to because, according to Haass, it significantly enhances the effectiveness of diplomatic and military undertakings.[27] Fingar argues that intelligence must be accurate and that it specifies clearly; what is and is not known about the issue, the quantity and quality of available information, what assumptions have been used to bridge intelligence gaps, what alternatives have been considered and how much confidence analysts have in the information and their judgements.[28] In contrast, Lowenthal asserts that accuracy is not a useful criterion for defining good intelligence due to the challenge of assessing accuracy in an intelligence context.[29]

Whilst the literature outlines what constitutes good intelligence broadly, these analyses fail to define what good intelligence looks like in practice and unpack their deeper meanings and contexts. Increasingly, scholars have considered the impact of big data, machine learning and emerging technologies on intelligence broadly.[30] The focus in this research – big data – is an amorphous concept used to refer to large, diverse, growing and changing datasets,[31] colloquially referred to as data that is too large to be manually processed,[32] or defined as 3Vs – volume, velocity and variety[33] – and 5Vs adding veracity (certainty and consistency in data) and value (insights into and from data).[34] It has also been described as a big data landscape, comprising data abundance, digital connectivity, and ubiquitous technology.[35] Big data is the foundation for the 'constellation of technologies'[36] that comprise artificial intelligence and many emerging technologies.[37]

Understanding the purpose of intelligence in a democracy and exploring what constitutes good intelligence, within the emerging technology context, is an important component of demonstrating public value and enabling democratic debate. This paper presents the first, comprehensive empirical analysis of what constitutes 'good intelligence' in Australia. Furthermore, it explores and reaffirms the role of good intelligence in national security decision-making in the context of emerging technologies. Many of these characteristics appear applicable to other democratic countries.

Data and method

This article is part of a larger research project that explores the impact of big data on intelligence production and national security decision-making in Australia. The project involved interviews with 47 senior and operational decision-makers as well as technologists working in Australia's national security and intelligence agencies, as well as a selection of independent subject matter experts. For the purposes of this research, Australia's national security agencies are the National Intelligence Community (NIC)[38] as well as the oversight body, the Office of the Inspector General for Intelligence Security (IGIS). The NIC agencies include a broad range of intelligence functions including security, foreign, domestic, criminal/law enforcement and defence. Each of these agencies participated in this research with between one and ten members interviewed per agency. Access was granted by request with specific anonymising and security measures taken to protect participants.

Interviews were semi-structured to cater for the different roles and responsibilities of interviewees, and their unique context within the NIC. Interviews were transcribed and coded in NVivo 12, where a thematic analysis was undertaken. A thematic analysis 'is used to classify and organise data according to key themes, concepts and emergent categories'[39] and is 'useful in capturing the complexities of meaning within a textual data set'.[40] Each transcript was initially examined, using line by line coding with a number of broad themes/categories emerging, and was subsequently re-examined and several sub-categories identified.[41] Themes were cross-referenced across interviewees from each agency and category and explored between members of the NIC. To provide anonymity to interviewees and their respective agencies, interviewees are referred to in this research as senior decision-maker (SDM), operational decision-maker (ODM) or independent subject matter experts (ISME).

This research was conducted within the context of a broader discussion about big data and emerging technologies. Participants were asked; what are the key characteristics of good intelligence and how are they impacted by big data? This paper reflects participant responses to this question, in the context of the broader research. Discussion about the characteristics of 'good' intelligence took place with 35 of the total 47 interviewees, as these participants had roles and responsibilities related to intelligence leadership, collection, analysis, decision-making or oversight rather than expertise in analytics or other technologies interviewed – the non-technologist participants. Some participants were or had been consumers or end-users of intelligence and this research reflects a range of perspectives. The researcher was a practitioner and acknowledges that while the terms 'good or effective' can be interpreted in a variety of ways academically, in a practitioner context the question was pragmatic and allowed latitude for participants to select the most salient ideas. As such, the interviewees responded with what they saw as both essential and aspirational characteristics of

intelligence activity. The participants shared their perspectives on essential components of intelligence production in pursuit of Australian security and often elaborated on what made intelligence effective in their environment, jurisdiction and field.

Findings: key components of 'good intelligence'

Whereas academically there is no consensus on the definition of intelligence,[42] this research demonstrates that Australian intelligence practitioners and leaders do have a clear definition of intelligence and an understanding of what good intelligence constitutes. It finds that big data and the emerging technologies it drives have current and future impacts on what constitutes good intelligence. The findings of this research highlight six key components of good intelligence; (i) timely, (ii) purposeful, (iii) actionable, (iv) accurate, (v) value-added, and (vi) unbiased, which have been previously published but not listed together in this way. This paper sets out these components, unpacking their meaning and prioritisation in the context of big data as seen by contemporary and currently serving intelligence practitioners and leaders. It is significant that this approach brings well-established practitioner frameworks into this field of study – especially given that it currently under-represented in the literature. Each of these components of good intelligence is discussed in this section.

Participants from agencies across the NIC have more common ground than differences when it comes to understandings and expectations of intelligence. This study shows that participants from within NIC agencies expressed shared understanding of an intelligence definition and a common framework for considering good intelligence. Notwithstanding the different missions, values and purposes of each of the NIC agencies and inevitable nuance within each, this research suggests there is in fact a common definition to intelligence – albeit broad enough to enable a range of intelligence activities.

Participants clearly articulated or alluded to a definition similar to Omand's, set out in the introduction,[43] and also added that the activity must be related to reducing some national security threat or harm to the Australian community. Participants in this study also used the term intelligence in a way similar to that suggested by Rolington, outlined in the introduction.[44] The combination of these definitions acknowledges the changing information environment, accounting for the impact of big data and open-source information on intelligence activity and provides insight to a general audience. One participant suggested that intelligence is often defined by the consumers in their agency, rather than practitioners. Another participant noted that nuanced definitions will exist that are specific to agencies, or even differ between different members of the same agency. Nevertheless, participants expressed similar notions of what constitutes good intelligence.

Participants expressed the view that this big data landscape has already irrevocably changed and continue to evolve the intelligence paradigm.[45] Six themes emerged from the data as the most important components of good intelligence. Repeatedly, interview participants began simply with a statement including three key words before elaborating; 'Timely, Accurate, Actionable. That's what good intelligence should be' (SDM) and 'I have an end user view, but; Timely, Accurate and Actionable' (SDM). Despite different agency missions, cultures, purposes and values, almost every participant mentioned timeliness, accuracy and the need to be actionable; considered a classic working definition. Value-add and purpose were mentioned by almost every participant but in some cases referred to differently by participants, depending on their role, agency or experience. Many alluded to the requirement to be unbiased, while a few – often those most engaged with policy-makers – discussed this at length.

Distinctions asserted in the literature suggest that there are profound differences between security, foreign and law enforcement intelligence; however, this research indicates that the key components of good intelligence are in fact areas of consensus between all participants – at least at a macro level. In the Australian intelligence community – including law enforcement and domestic functions – the key characteristics of good intelligence look very similar, if not the same. Participants from all agencies in the Australian National Intelligence Community (NIC) indicated intelligence must meet the following characteristics in order to be good intelligence; (i) timely, (ii) purposeful, (iii) actionable, (iv) accurate, (v) provides added value for an intended audience, and (vi) is unbiased, as show in the image below.

CHARACTERISTICS OF GOOD INTELLIGENCE

TIMELY
Able to be considered within decision-making cycle

'Intelligence has got to be made available in a way and in the time that it makes a difference to the person who makes a decision.'

PURPOSEFUL
The intent with which it is created

'Intelligence must have a purpose. It is not acquired for its own sake; the acquisition is determined by its intended use.'

ACTIONABLE
The ability to do something with it

'What can you do with it [intelligence]?... 'If there is no actionable intelligence you have got to ask yourself why are you producing it?'

ACCURATE
Exacting, correct, specific, precise

'The responsibility of leaders in intelligence agencies is to ensure that the presentation of their information to decision-makers is properly balanced in articulating what is definitively known, what is an opinion and what is not known.'

VALUE-ADDED
The value it added to decision-making

'Offers insight, makes something unknown known, makes the unseen visible or reveals something new.'

UNBIASED
Impartial, independent, apolitical

'Intelligence should be independent and impartial, which is really important for political decision makers to understand. It must be apolitical.'

Findings: key components of 'good intelligence' *timely*

Timeliness represents an essential and unanimously agreed on component of good intelligence. This research demonstrate that timeliness is perceived as foundational to good intelligence. Many participants said simply 'it's got to be timely' and this was pervasive throughout the research in all categories of SDM, ODM and ISME. When participants expressed that intelligence needs to be timely, they were largely talking about the fact that it needs to be delivered to a decision-maker within a time frame that enabled it to be included in their considerations. One SDM explained simply what many expressed; 'Intelligence has got to be made available in a way and in the time that it makes a difference to the person who makes a decision'. Timeliness in the intelligence community can be used as shorthand for understanding when a decision-maker needs information and ensuring that intelligence is delivered in a timeframe than enables those deliberations. Another SDM described how crucial it is that they received intelligence in a timely way; 'Twenty-twenty hindsight is a perfect thing, but in a decision-making place you can't wait for that. If I wait for all of the answers and knowledge before I need to make a decision, the time has passed'. In a similar vein, another participant clearly articulated why timeliness is a characteristic of intelligence needs to be met, perhaps before others can be considered; 'It's got to be timely so that it can be considered by the policy agencies. If it's not timely then they're not going to use it and it's not going to have impact'. (ODM). Another ODM suggested that timeliness is a minimum criterion; 'What needs to be learnt is how to be timely while meeting all the other characteristics of good intelligence'.

A few participants highlighted specifically how big data impacted the timeliness of intelligence production and delivery. SDM: 'Timeliness is crucial. The reasons agencies get involved in data analytics is about timeliness. The data volume has grown, the complexity has grown and people hide in plain sight in all the noise'. This quote reflects the view frequently expressed by participants that big data and the information age more broadly have sped up the information ecosystem and impacted intelligence activities. Furthermore, timeliness was an area some participants highlighted for potential improvements, as one SDM suggested: 'we can always improve in prioritising intelligence to user needs and in developing and providing it faster'. An ODM outlined why timeliness (of collection) is critical for their particular work; 'Timeliness. That also relates to data – the faster we get it and the nearer to the activity that was supposed to have happened, the better. So, there is no point getting, for instance, visa movements or border movements four years after they've happened'. Another ODM elaborated, indicating the important role data currency plays in timeliness;

> Timeliness. Currency - one of the big challenges of data is that it's out of date from the moment you collect it. This is one of the big challenges for us because we are still in a system where we take captures of data and then apply analytics over it. We really want to be in a place where we are applying analytics over the data in place so we can do that in real time or near real time.

Participants talked about data currency and the timeliness of information in a range of circumstances and a number specifically mentioned residual risk cases. Residual risk management refers to a situation where a person has been assessed to see if they pose a security threat, but do not – at the time of the assessment – meet the designated threshold. An ODM highlighted the significance of timeliness explaining how it affected their management;

> A simple example of that is when I was talking about our residual risk management, some of the work we do around that is a network analysis around people's communications so it is only as good as the information we have. When we closed the case, we knew what the person's telephone number was but three years down the track we need to make sure that the numbers we are checking – or the telephone selectors as we call them – are still the ones that that person is using.

Findings: key components of 'good intelligence' *purposeful*

Justice Hope, an eminent Australian QC who has conducted two intelligence reviews, observed; 'Intelligence is not collected in or to establish a library. Its collection is justified only by its use'.[46] The final intelligence advice or product that ends up being delivered by intelligence agencies is arrived at in myriad different ways, but the first step is always to establish the purpose of conducting the activity and the purpose the product or advice will be used for. This is defined in the literature as; the appearance or formulation of the problem,[47] defining an intelligence problem,[48] an intelligence question to be answered,[49] or intelligence 'requirements'.[50] These initial questions asked of intelligence 'are critical as they shape and frame the analytic endeavour and provide the basis for knowledge development'.[51] These characterisations highlight what is to be assessed and restrict the scope of the activity, based on its purpose.

Purpose emerged from the participant data as an essential component of intelligence, adding some nuance to what is already known. The participants viewed the purpose of undertaking activity (i.e., scoping the question, intel collection and analysis) as vital to understanding and specifying the requisite knowledge required. One participant articulated the views of most stating; 'Intelligence must have a *purpose*. It is not acquired for its own sake; the acquisition is determined by its intended use' (ISME). Another ISME responded to the question about key characteristics of good intelligence in the context of analytical tools, with purpose up front;

> Purpose. It's actually purpose. What is it you are there for and how are you answering that problem? So, there is no point to do intel for Jesus. SIGINT for Jesus is a well-known term, but all agencies actually do it. You go along and they brief you and you think this is really clever but what's the point, who is going to use that? So, you actually have to understand what is the purpose you are doing it for? Who is the customer that is going to use that information? The analysis can be really brilliant and the tools can be really fancy and do amazing things but actually if there is no outcome at the end of it what is the point?

The purpose of conducting intelligence activities and the ability to use, apply – or action – the intelligence they produce, are obviously inextricably linked. In this article, they have been separated to further explore the slight differences, improve understanding and contribute to the body of knowledge. All the participants in this study with a signals intelligence background talked about purpose by first mentioning the oft coined phrase in their field 'SIGINT for Jesus', which is shorthand for referring to intelligence activities and products with no customer or decision-maker.[52] One SDM provided more context into the term;

> It means 'is this signals intelligence made only for Jesus and read only by Jesus therefore having no impact on the material world?' So, when we look at things, there are a whole bunch of catchphrases you could use, but are you reinforcing or changing a government policy decision. So, can you provide government certainty about the fact that its policy position is accurate and having the impacts it wants to have? Or alternatively can you provide evidence to the government that its policy position is not getting the outcome they would want it to have based on the intelligence you get from another actor?

The infamous phrase is a useful idiom to understand the key component of purpose and the role it plays for decision-makers. An ISME provided the background;

> Allen Hawker, previous Secretary of [the Department of] Defence [circa 1999–2002], was visiting DSD [now ASD] at one stage when it was down in Melbourne and people were showing him some very clever work they were doing . . . He asked who were they doing it for and they couldn't answer and he said 'SIGINT for Jesus?' So that's a classic of great technical expertise, but the relationships were lacking – who was going to make any use of this?

Each of these statements unpacks a little more about purpose, the importance of customer relationships and reason for work being undertaken. As one participant noted, 'organisations exist for a purpose and the outcome of the intelligence needs to have a purpose' (SDM). Purpose was integral to the definition of all agency participants with a number of SDM's expounding what purpose means for them; 'A deep understanding of what it is that your customer is trying to achieve or the decision they are trying to make'. Another noted that 'good intelligence must be servicing a customer. That is,

'what is the intelligence question you are trying to answer?' (SDM). One participant noted that the purpose is related closely to the ability of the decision-maker in 'actioning' intelligence;

> There are lots of ways you could slice it. Whether it's about reducing uncertainty, or providing a decision-maker an advantage, there is lots of jargon out there but ultimately what it's about is helping our decision makers, be they the Prime Minister, the Chief of the Defence Force to the soldier in the field, make the right decision at the right time. (SDM)

Purpose is also a vital element of intelligence in Australia – as in most democracies – because the purpose for which something is collected is usually legislatively bound (either by definition or exclusion) and therefore has specific restrictions for how it is used, shared and retained. Many participants referenced the legislative framework that exists in Australia and its connection to purpose. One participant for example said; 'national security advice is what we do for our particular organisation. It is around threats to security. So, everything we do is about transforming data into producing that national security advice' (SDM). There is naturally some conceptual overlap between purpose and actionable. To help clarify the difference between action and purpose, a good way of thinking about it is that purposeful is the reason for conducting the intelligence activity – often linked to legislative responsibility – and actionable is the ability to achieve an outcome directly, or indirectly such as influencing a decision-maker's understanding of their environment.

Findings: key components of 'good intelligence' *actionable*

The requirement for intelligence to be actionable is a consistent theme in the literature; however, what actionable intelligence actually looks like is rarely explicitly described. Scholars, such as Johnson, say 'intelligence must be "actionable"'[53] describing the concept as being specific enough to allow policy officials to act on the information. Johnson asserts that vague intelligence reports are of limited value, but goes on to argue that a vague warning (if reliable) is better than no warning at all.[54] Gill and Phythian concur that intelligence is 'not just about the production of knowledge, but also includes "action"'.[55] In this study, participants were similarly united on the need for intelligence to be actionable, however they also organically drew out their meanings of the term and its implications, providing a deeper understanding of what actionable looks like in the minds of contemporary practitioners and leaders. One SDM asked; 'if it [intelligence] relates to something that is significant, the question is what can you do with it?' Another said, 'if there is no actionable intelligence you have got to ask yourself why are you producing it?' One SDM outlined what actionable meant in their context;

> Ultimately, intelligence is intended to influence and shape decision-making. So, if it doesn't do that, what is the point? That means it has a good understanding of the intelligence question and is presented to the decision-maker in a way that is understandable, can be acted upon and is answering, or even pre-empting, a question.

The idea that intelligence is provided to decision-makers for a purpose and in a time frame within which they could consider it, has been addressed in the first two characteristics of good intelligence outlined in this paper. What makes intelligence actionable was further considered by the participants as; the fact that it had an impact on deliberations and decision-making, achieved an outcome, and/or was delivered in a way that enabled a course of action. As one SDM stated;

> Our main focus is that it has impact. The key impact of intelligence is that we are supporting decision-makers. We are relevant, we are giving them the right intelligence in the right way at the right time in a way they receive it. I think at the end of the day, that is the most important thing by far.

Almost all participants suggested that intelligence that is not actionable – or did not inform decision-making – was considered a failure. One participant explained with a hypothetical example – noting intelligence agencies would always endeavour to communicate to our allies;

> As far as possible, it's got to be actionable. There is no point in saying to a government, look we've got information that the NZ PM will be shot tomorrow. If the Australian PM said (as they would do), 'have we told the New Zealanders', but were told 'oh no we can't tell them'. They'd ask 'why not?' and if they were told, we couldn't' because it'll reveal this source or whatever then it's totally and utterly useless intelligence. (ISME)

This was one of a large number of similar examples from participants which suggested that if intelligence was not 'actionable' or could not be used effectively by a decision-maker it was rendered meaningless. This study shows that being actionable is considered a critical component of good intelligence across all domains (security, law enforcement, foreign and domestic agencies) as well as by participants in agencies responsible for tactical, operational and strategic intelligence activities. Existing research indicates that certain agencies believe they are more oriented towards response (i.e., law enforcement)[56] and seeking intelligence to inform decisions enabling quick action rather than informing long-term thinking.[57] One SDM addressed this distinction directly; 'For a law enforcement agency it needs to be actionable. That is probably different to what intelligence agencies would look at. For us, it needs to be actionable'.

All participants in this study highlighted the requirement for intelligence to be actionable, within tactical, operational and strategic intelligence environments and across all domains (security, law enforcement, domestic and foreign intelligence). Participants raised the requirement for intelligence to be actionable – irrespective of their agency, role or intelligence focus. There was unanimity on the need for intelligence to be actionable for decision-makers; however, how that occurred was interpreted differently by participants, largely dependent on the kinds of agencies they had worked for and the types of intelligence work they had undertaken. One SDM summarised the views of many, although their focus was on defence; 'Is your intelligence actually leading to consequences in the real world; whether in policy development or policy implementation, or direct support to military interventions?'

Many participants discussed the different types of intelligence, in the form of products and advice, to be delivered to decision-makers but concurred that intelligence must be considered actionable. Participants agreed that the evaluation of current policy was considered 'actionable' – and one SDM initially talked about the requirement for intelligence to be actionable before summing up alternatives;

> Although it doesn't have to be actionable sometimes. Sometimes it is really useful to know that what you are doing is right. So, I have a policy position and we are implementing it like this and the intelligence suggests to me that that policy position is accurate and having the impact that I want it to have. So, you don't act on it at all– you carry on.

The focus on actionable intelligence is exacerbated by big data and as one US report put it; a 'reflection of the speed at which events can move in an era when mobile communications are the norm even in the most remote locations' noting that decision makers 'want their "current, actionable" intelligence not in days or hours, but in real time'.[58] A number of participants, especially those within law enforcement and domestic security agencies, highlighted the need for intelligence to use data and analytics to prioritise and best direct agency efforts, which were unable to comprehensively assess all potential security threats. One SDM explained how they saw it working for their agency, in a discussion where the intelligence process was occurring using big data technologies;

> Intelligence should be there in the first instance to be able to triage and prioritise because again there will always be greater demand than supply in our space … So, intel should inform the initial triaging, prioritisation and decision making in relation to how we are going to go about investigating that matter. What is known? What is the likely threat being posed? That informs, hopefully, the national security investigative plan that follows. So, intel should be helping to drive the decision making.

Findings: key components of 'good intelligence' *accurate*

The view of the vast majority of participants in this research included accuracy as a critical component to their definition of good intelligence. Emerging from the data was the idea that accuracy can refer to a range of things and participants talked about; clearly communicating what is known and not known, the reliability of specific pieces of information and their sources as well as the requirement for judgements and assessment to accurately reflect the information and be unbiased.

Specifying clearly what is and is not known is key to accuracy in the intelligence context, as is clearly articulating the quantity and quality of available information.[59] This is both difficult and critical because 'intelligence is about dealing with fundamentally uncertain information with certainty'.[60] Intelligence work is often described as an imperfect jigsaw puzzle that practitioners try to piece together,[61] however there are many problems with this perspective not least that it assumes a both a goal or end state and one single truth – a completed puzzle.[62] A thorough and insightful assessment of puzzles in intelligence analysis can be seen in Agrell and Treverton, but suffice to say, there is an inherent tension between intelligence assessment and accuracy.[63] Intelligence analysis is ultimately an assessment of the unknown and uncertain. As one SDM put it; 'It is called intelligence for a reason. It's not knowledge, it is an imperfect view of the world. It's always going to be an imperfect view of the world and this idea that the more data you collect that you'll end up with a perfect view of the world. It doesn't work that way'. This comment echoes what many participants noted and implies why understanding and articulating what is and is not known is vital.

Fingar asserts the need to elucidate; 'what assumptions have been used to bridge intelligence gaps, what alternatives have been considered and how much confidence analysts have in the information and their judgements'.[64] Participants also discussed this, especially in a big data context, and many concluded that accuracy – and particularly the need for clearly delineating the known and unknown – has a newfound significance in this environment. As one ISME claimed;

> It's an issue more real today than what it was fifty years ago. Intelligence agencies today collect more information … So, they have got more information. Even with that, intelligence rarely provides you with a 100% picture. I think the responsibility of leaders in intelligence agencies is to ensure that the presentation of their information to decision-makers is properly balanced in articulating what is definitively known, what is an opinion and what is not known.

An SDM outlined that 'intelligence needs to be accurately described … it is clearly explained in terms of sourcing and source credibility and the intelligence gaps are clearly articulated'. Another explained the necessity in their context [domestic security]; 'As you know, we never have everything you want to make that assessment … My job is really thinking about assessments, and you are making a call based on the intelligence. You are acknowledging what you do and don't know … This is the intelligence we have and so this is what we think is the most likely scenario or assessment' (SDM). Another participant described the need for specificity, expressed by many; 'Good intelligence and assessment should be able to communicate with some nuance about the complexity of a situation … and you should be able to articulate that' (ODM).

Many participants prioritised veracity and verifiability of information sources as well as their reliability as part of accuracy. 'It needs to be founded on good information, whether that's obtained covertly or through open source. It's got to be good information, reliable of high fidelity' noted an SDM. Another SDM advised that intelligence needs to be 'clearly sourced. The source needs to be reliable and it needs to be timely', while one SDM participant suggested 'veracity, or at least an attempt to understand the veracity, so being aware of biases and accounting for them. A variety of sources'. Participants described the need for communication about the sources relied on in intelligence products, as the information collected for intelligence purposes was often unable to be verified. Another SDM offered a perspective on verification and why it matters for decisions – particularly in law enforcement;

> The key [to good intelligence] is [that it is] verifiable … Every bit of information sits on a probability scale from 5 percent through to verifiable. Well, it's not intelligence when it gets to 100 percent, it's just evidence. So, everything along that whole spectrum. And the key to good intelligence is recognising where the information sits on that probability spectrum because that's important because if you're going to make tactical and strategic decisions based on that you want it you want to be closer to the probability of one than you want to be to probability of zero.

The ability to confirm how reliable data is and its veracity was seen as more pertinent in the big data era, but a number of participants organically raised that this had in fact become more difficult as a result of big data, especially the use of misinformation and disinformation. The evolving information environment was seen by participants as altering the veracity and truthfulness of information. One SDM argued; 'It is the validity of the data. Particularly in this increasing world of misinformation, there is nothing stopping people from using sophisticated machine learning systems to put out highly classified information that is wrong. We are going to be increasingly challenged in that space.' A component of sourcing is about reliability and consistency. One ODM articulates the similarities in traditional intelligence domains and larger data sets; 'Then you have reliability of intelligence. It's not totally dissimilar to intelligence from our HUMINT collection, we always assessed that in terms of reliability and credibility. That comes from the source of the information and then whether or not the actual information is plausible. The same applies to data sets; who is it obtained from? Can you rely on it, is it accurate? We need to get it in time, and we need to keep it up to date'. One ODM discussed the impact of consistency of data sources – and the absence of data – when using big data analytics for intelligence;

> Having people fill in the date of birth field exactly the same way and having agreed standards for phone numbers, for example. The consistency of data but also the consistency of what is provided. So that we know that every time we get this kind of material it should have this piece of information attached to it. They've been things that certainly we've seen as important …

This ODM went on to explain a critical point in understanding the absence of data and changes in data collection, which have significant ramifications for machine learning technologies, where implications and inferences can be, and often are drawn, by data absence. The ODM noted that understanding data sets was critical to accuracy;

> A clear understanding of what the absence of data means. Why are things not filled in and what does vacant data mean in a data set. Sometimes the transfer of data can see dates missing from a range – so you can make an assessment but if the activity you're looking for happened on that date the absence of data doesn't mean the activity didn't occur. So actually, having that understanding of what is in the data set but also importantly what is absent from the data set is really key to having good bulk data.

Findings: key components of 'good intelligence' *value-added*

Omand, Bartlett and Miller argue that 'the "success" of intelligence is not the information or even secrets that it collects, but the value it adds to decision-making'.[65] In order for intelligence agencies to be considered of true value to government, they must produce and disseminate intelligence that has impact for government.[66] Wesley describes the requirement for the intelligence community to have genuine impact as 'delivering information that can inform government actions with transformative effect, at the right time, and to the right place'.[67] This study provides empirical data confirming these perspectives and reaffirms the role of adding value in national security decision-making. The requirement for intelligence to add value for the decision-maker is extensively discussed within the intelligence community and referenced in academic literature although rarely unpacked in detail.[68] Participants in this study discussed the term 'value-add' in different ways, suggesting it is a subjective notion that

evolves with experience and practice. Participants also elaborated on the process of adding value, however this extends beyond the scope of this article and is an area worthy of future research.

All participants talked about intelligence needing to provide value to the decision-maker, however what 'value add' looks like depends on the environment and purpose of intelligence activities or products. What value represents was described in a number of different ways by participants; that it offers insight – or is 'insightful'–, is relevant, makes something unknown known, makes the unseen visible or reveals something new. One ODM suggested that it must offer something valuable and is not just about 'describing the data and not about summarising data'. As one SDM said; 'it should be able to shed a light on something that without that thought, or effort wouldn't be seen'. Another SDM argued that 'there is a contextual piece to intelligence, especially in the early stages of a threat. If nothing else, that value add is that it can give you a context within which you start to understand the nature of the problem'. An ODM argued that it needs to 'quantify the threat' for a decision-maker, while an ISME elaborated that 'intelligence should be relevant to the policy issues that are at hand'. An SDM outlined what value-added intelligence looks like from their perspective;

> It is obtaining information that is either available or not deliberately available and making that information available to the right person at the right time. If you unpick that a little bit, who is the right person. Well it starts from our national leaders, our politicians down to our intelligence community and policy community itself. It's gotta be valued, it's gotta be valuable. It has got to have validation – it has to be validated with its own sense of integrity to what it is. It has got to be made available in a way and in the time that it makes a difference to the person who makes a decision.

Gookins outlines how this happens; 'the intelligence analyst turns information into intelligence by connecting data to issues of national security, thereby giving it value'.[69] Sometimes this process of adding value is referred to as the *so what* factor. In a big data context, Symon and Tarapore offer that the 'so what' is the 'need to provide the necessary context or value-added interpretation of the data analytics – which requires not only subject matter expertise but also sensitivity to customer requirements'.[70] Indeed, contemporary intelligence theory argues that intelligence activities should provide an answer to the fundamental intelligence question, or '*so what*'.[71] Whilst the process of adding value is too large to be comprehensively considered within this article, it is undoubtedly worthy of further study and participants unanimously agreed it was fundamental to good intelligence. One SDM suggested; 'it is just information until analysed. The value-add by good intelligence officers is what provides good intelligence', while an ISME stated; 'It has to add value. If it's not of any use to anyone what's the point? This is perhaps most relevant to the modern world in which we live, it has to add value. In the sense that it's information that's not available somewhere else'. One SDM further elaborated, 'I used to hate getting intelligence reports that told me something I read in the Economist'.

Wesley argues that demands for instant advice and analysis mean that intelligence organisations must constantly examine how they are communicating against the requirements of end users.[72] Wesley makes the point that intelligence product does not have, among ministers, an audience for whom reading it is compulsory, and that to the extent that there is an audience, it is notoriously time and attention poor.[73] This was reflected in participants comments. One SDM noted that 'no one wants to read a 50-page brochure quite frankly. No one has time for that so it has to be relevant. It has to be succinct and to the point'. Another SDM noted that there is 'no point investing in huge data stores and analytical techniques if the intelligence we produce at the end of the day is not useful to anyone or it's not delivered in a way that policy and decision-makers need it to be'.

Participants were clearly cognisant of the need to consider the decision-maker and what value they are providing. As one SDM noted 'you need to understand how your intelligence feeds the national security mission, how you can help value-add to those decisions'. Another SDM highlighted the links between actionable and value-added intelligence;

> We are very conscious that there is a significant role for us in assisting either policy-makers or the people who take action, such as police knocking on the door, to I guess operationalise in all senses of the word, the intelligence we are giving and we need to add value to the information to help that decision be made.

While some characteristics appear uniform across sectors in the intelligence community, value-added intelligence depends on the context and expertise of the intelligence practitioner, the needs of the decision-maker and the environment within which it is delivered. One SDM highlighted the growing challenge of policymakers with diverse experience and the impact big data and artificial intelligence might have on the relationship between intelligence producers and consumers or decision-makers;

> The people that use intelligence are not especially good at driving the intelligence machine to match users priorities. The intelligence machine is not especially good at communicating how it can meet decision-makers priorities. I think that the end users of machine intelligence are going to experience a similar challenge. I don't know that the end user will be good at asking the machine the right questions either. The intelligence producer–user divide will be exacerbated by machines. (SDM)

Findings: key components of 'good intelligence' *unbiased*

Unbiased intelligence is high on the list of desirable intelligence qualities – the highest of all, according to Johnson, where the goal is to keep information free of political spin.[74] Despite this strong assertion, very few scholars provide insight into or detail on what constitutes bias and unbiased or objective intelligence. Whilst the discussion about individual cognitive bias affecting analysis is extensively considered, the requirement for intelligence products and advice to be unbiased and free from influence is mentioned frequently but discussed in depth rarely in the intelligence literature.[75] Objectivity is, as British expert Michael Herman argues, an 'elusive ideal'[76] and as an input to national policy-making is a world standard of good governance. Lefebvre argues that despite the challenges, objectivity 'remains important if intelligence analysts are to produce estimates that are as unbiased and free of logical fallacies as possible'.[77] Analysts (or anyone else) cannot ever really be 'objective' in the strictest sense of that word for everything we know 'comes from interpretation which is subjectively different for every human being – it depends on our experience, state of mind, motivations, all mostly accessed unconsciously'.[78]

What policymakers 'can demand of analysts is that they are independent, impartial and politically neutral, and honest'.[79] Whilst not a universally discussed issue in this study, a number of participants indicated that being unbiased was an important characteristic of good intelligence products and advice and particularly to the practice of intelligence. One ODM spoke of the requirement for intelligence to be; 'an objective analysis of whatever the subject is, so it's not, it shouldn't be biased, it shouldn't be presenting just one view and it should just be clear and succinct in relation to whatever the issue is'. One ISME noted that, 'intelligence should be independent and impartial, which is really important for political decision makers to understand. It must be apolitical'. Participants described unbiased in a variety of ways. Some articulated it as objective, while others saw a need to explore how to mitigate cognitive bias as much as possible. As one ODM described; 'I think objective might be a better term than unbiased because we all have biases and it's impossible to move away from them. The best we can do is acknowledge our biases and try our best to be objective'. A number of participants, especially ODMs, indicated that one of the steps to delivering good intelligence was becoming conscious of bias (your own and within your data).

Participants extensively discussed biases of big data. According to participants, assessment of a source must take into account the source's bias and any bias built in to data sources needs to be acknowledged, including collection bias and implications for machine learning. Participants suggested that 'objectivity' is a primary challenge of big data, machine learning and artificial intelligence. As one participant highlighted;

> I think you have just got to proceed with a profound understanding of the inherent limitations. Just because it is a machine is making the decision doesn't mean it is going to be free of bias. You have got to think about your data sets . . . You can't do good data science on poorly curated data. You have got to make sure you understand the data you have got, that you understand its provenance, its strengths and weaknesses from a bias perspective, from a quality perspective. (SDM)

The notion that intelligence should be unbiased was pervasive throughout the research, however described in different ways particularly by participants who had experience interacting with policy-makers. According to participants, the need for intelligence to be unbiased was often interwoven with other requirements such as the need to be accurate and persuasive as highlighted in this SDM comment;

> I think good intelligence is characterised by argumentation rather than assertion. Sometimes there is a tendency, particularly in strategic intelligence agencies, that with the demand to be succinct they become pieces of assertion rather than reasoned argument which should convince the reader that the judgements reached are well founded. So, I think that element of argumentation.

Touching on bias and the perception of remaining unbiased but still having influence, one SDM offered a view that they acknowledged as unconventional;

> It's [intelligence] got to be politically astute, so we sort of expect intelligence now to be aligned with the policy and agency mission, so there's an awareness that the relationship between policy and intelligence is closer than it's ever been before. Before, it was seen as a threat and the analysts would be very proud that they were independent, but I think today intelligence, like anything, has a context, so as long as it's not impacting on the analytical integrity of the product you need the policy to set the context because in that way it's framed for the decision-maker . . . If intelligence is all about influence and your message is at odds with the other factors of influence you have less chance of influencing, so what you have to do is align to have that influence.

Discussion and conclusion

This paper provides new data to support the key characteristics of good intelligence, finding that 'good intelligence' must be; (i) timely, (ii) purposeful, (iii) actionable, (iv) accurate, (v) provide added value for an intended audience, and (vi) unbiased. The big data landscape has cemented the significance of these characteristics; however, it has in many ways transformed the environment or context of intelligence production and how in practice these characteristics are achieved. The paper unpacked how contemporary intelligence leaders and practitioners in Australia think about and how they prioritise the characteristics of good intelligence in an emerging technology context.

Timeliness, or timely intelligence – able to be considered within decision-making cycle – remains of extant importance. The big data landscape – comprised of data abundance, digital connectivity, and ubiquitous technology – has shortened parts of the decision-making cycle and as a result expectations have increased about the speed of intelligence production. Purpose – the intent for which it is created – remains at the core of intelligence, although some suggest in practice it is more important and more difficult in an environment of data abundance. The challenge too of purpose is more complex within legislative frameworks not yet keeping pace with the evolution of digital technologies. Actionable intelligence – the ability to do something with it – is, like timeliness, significantly impacted by the speed of digital transformation and contemporary communications environments. Additionally, the requirement for actionable intelligence – which is used by decision-makers, often publicly – has increased existing tensions between transparency and secrecy.[80] Further research into best-practice actionable intelligence – and provision to decision makers – would provide insight for scholars and practitioners, informing practice and training. Additionally, research examining the impact of declassification on intelligence activities and capabilities would be welcome.

Accurate intelligence – that is exact, correct, specific and precise – is critical, and according to this study its delivery requires good leadership. The impacts of mis and disinformation were raised as

a crucial challenge of big data and emerging technologies and one which requires deeper consideration. Value-added intelligence – the requirement to add value to decision-making – has increased significantly given the myriad information sources available to contemporary decision-makers. Value-add is a practitioner mantra but often the area of least consensus, based on a variety of different users. Understanding what different groups of decision-makers (be they operational or policy) require and can reasonably expect out of intelligence – and the national intelligence apparatus – in a big data landscape is an area of utmost importance. Additionally, understanding the shifts in how new stakeholders, from academia to industry to citizens themselves, use and can access intelligence is rising in importance.[81]

Unbiased – impartial, independent and apolitical – intelligence continues to be of critical importance to intelligence as a process, practice and profession. Ensuring political users of intelligence uphold systems and oversight is necessary to maintaining unbiased intelligence capabilities. Of course, many of the key characteristics of good intelligence; the requirement to be timely, purposeful, actionable, accurate, value-added and unbiased, are inextricably linked. For something to be actionable, it must also be timely and purposeful. The key characteristics of good intelligence are interwoven and inexplicably linked. Additionally, according to participants, good intelligence takes good leadership as well as lots of practice and experience. The contemporary processes and practices of producing good intelligence in a digital era is emerging as a field of research[82] but remains an area for future study, especially in relationship to leadership and innovation.

A clear understanding of what constitutes good intelligence and how it is achieved is critical for consumers of intelligence – and for the general public to appreciate the value of the intelligence community and demystify this critical part of our national security apparatus. This is particularly important when intelligence itself is unable to be shared to protect national security. Given the dearth of literature – and indeed public commentary – on 'how the community works, its contributions, or of its importance to policy and decision-makers across government',[83] most aspects of the NIC operations are opaque and research into these are necessary. Despite being a three-billion-dollar 10,000-person-strong enterprise in Australia, the intelligence community and the work it does is not particularly well understood.[84] This broader research project, and these characteristics specifically, offer the start of a meaningful, working definition of good intelligence for the Australian NIC and contributes to a broader public discussion. As the Office of National Intelligence leads the transition of the Australian Intelligence Community to NIC, developing common ground, a cohesive intelligence community and centralised training is essential for Australian national security. More research is needed to support this work and some specific areas in particular that arise from this study include; research within the community about the possible differences between agencies, research into the impact of intelligence and how it affects national security decision-making, and, the impact of big data, artificial intelligence and machine learning on national security agencies.

Given their historically different origins, much has been made of the differences between the intelligence produced by different agencies, such as security, foreign and law enforcement, in different intelligence disciplines, such as collection or assessment, and for the kind of decisions the intelligence is intended to improve; tactical, operational and strategic intelligence. However, this study finds that despite these many ways of categorising intelligence activity, there is in fact consensus on what constitutes 'good intelligence', with the most variation seen in participant assessments of value-add. Throughout this research, there was near unanimity that the essential characteristics of good intelligence are that it is timely, purposeful, actionable, accurate, value-added and unbiased. This view was consistent across all domains; security, law enforcement, defence and foreign intelligence and types of intelligence; tactical, operational and strategic. Participants in this research, representing senior and operational decision-makers in the Australian NIC agencies, indicated that despite strong academic views about the differences; there are in fact many areas of consensus among practitioners.

The characteristics of good intelligence – that it is timely, purposeful, actionable, accurate, value-added and unbiased are likely applicable to other nations – especially within the Five Eye alliance as

the comprising nations share many similarities. Further research is needed in different jurisdictions to see if the view of 'good intelligence' is replicated across nations and findings can be generalised more broadly, as well as how new and emerging technologies can improve intelligence in practice. Alignment of the understanding and practice of intelligence is important among allies as cooperation and the expectations of intelligence and information exchanges increase. The process of intelligence analysis was outside the scope of this article but is nonetheless a worthy topic of future research. Participants also raised the process of new ways to add value through the intelligence cycle. Additionally, how intelligence is prioritised by Australian intelligence practitioners, leaders and policy makers – especially when supported by algorithms – remains an area ripe for future research. More research into the process of adding value in intelligence is needed, both to guide current and future practitioners and decision-makers as well as illuminate aspects of intelligence activities to the public, whom the intelligence community ultimately serves.

Notes

1. Andrew, *The Secret World*; Hughes, Jackson and Scott, *Exploring Intelligence Archives*; Van Puyvelde, 'Qualitative Research Interviews', 6–7; and Zegart, *Spies, Lies, And Algorithms*.
2. Gill and Phythian, 'Intelligence'.
3. Lundy et al., 'The Ethics of Applied Intelligence'; DeGennaro, 'The Gray Zone'.
4. Lundy et al., 'The Ethics of Applied Intelligence'.
5. Andrew, *The Secret World*; Hughes, Jackson and Scott, *Exploring Intelligence Archives*; Van Puyvelde, 'Qualitative Research Interviews'; and Zegart, *Spies, Lies, And Algorithms*.
6. Symon, 'ASIS Director-General Launches New Book', 4.
7. Walsh, 'Building Better Intelligence Frameworks'; Walsh, *Intelligence and Intelligence Analysis*. Five Eyes is a term used to describe the national security intelligence sharing arrangements of Australia, Canada, New Zealand, the United Kingdom, and United States of America.
8. Walsh, *Intelligence and Intelligence Analysis*.
9. Coyne and Bell, 'Strategic Intelligence', 25; Gill, 'Theories of Intelligence', 213–4; Kahn, 'An Historical Theory'; Rolington, *Strategic Intelligence*, 17–8; Scott and Jackson, 'The Study of Intelligence'; and Wheaton and Beerbower, 'Towards a New Definition'.
10. Lowenthal, *Intelligence*, 1–9.
11. Rolington, *Strategic Intelligence*, 17.
12. Omand, *Securing the state*. National Security is defined broadly. Omand sets out three propositions underpinning the modern approach to national security; collective psychological safety, citizen centric view of threats and hazards as well as informed decision-making, adopted in this article.
13. Omand, 'Reflections on Intelligence Analysts', 2.
14. Ibid., 9.
15. Ibid.
16. Hayden Center for Intelligence, Policy, and International Security, 'Conversation with Sue Gordon', 24.
17. Clapper, "Luncheon Remarks", 3.
18. Johnson, "National Security Intelligence", 6.
19. Johnson, "National Security Intelligence", 6.
20. George, "Fixing the Problem".
21. Kent, *Strategic Intelligence*.
22. Ibid., 5.
23. Johnson, "National Security Intelligence", 5.
24. Ibid.
25. Lowenthal, *Intelligence*.
26. Wastell, "Cognitive Predispositions", 451.
27. Haass, *Making Intelligence Smarter*.
28. Fingar, *Reducing Uncertainty*, 4.
29. Lowenthal, *Intelligence*, 158–9.
30. There are an increasing number of articles exploring the impact of technologies, from machine learning to AI on intelligence. These are excellent contributions; however the inclusion of these works would take the discussion away from good intelligence characteristics – the focus of this article.
31. Bennett Moses and Chan, "Using Big Data"; Chan and Bennett Moses, 'Making Sense'; Chan and Bennett Moses, 'Is Big Data Challenging'; and Malomo and Sena",Data Intelligence".
32. Hammond-Errey, *Big Data*.

33. Kitchin, *The Data Revolution*, 68; Laney",3D Data Management".
34. Akhgar et al., *Application of Big Data*; van der Sloot, Broeders & Schrijvers, *Exploring the Boundaries*.
35. Hammond-Errey, *Big Data*; Hammond-Errey, *Secrecy, Sovereignty and Sharing*.
36. Bell, "The Character", 175.
37. Hammond-Errey, *Secrecy, Sovereignty and Sharing*.
38. Office of National Intelligence, 'The National Intelligence Community'. In Australia, there are ten agencies that form the Australian Government's intelligence enterprise, working to collect, analyse and disseminate intelligence information and advice in accordance with Australia's interests and national security priorities.

    The agencies that form the NIC are: the Office of National Intelligence (ONI), the Australian Signals Directorate (ASD), the Australian Geospatial-Intelligence Organisation (AGO), the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO), Defence Intelligence Organisation (DIO), the Australian Criminal Intelligence Commission (ACIC) and the intelligence functions of the Australian Federal Police (AFP), Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Department of Home Affairs.
39. Ritchie and Lewis, *Qualitative Research Practice*, 220.
40. Guest, MacQueen and Namey, *Applied Thematic Analysis*, 10.
41. Charmaz, *Constructing Grounded Theory*.
42. Lowenthal, *Intelligence*; Wheaton and Beerbower, 'Towards a New Definition'.
43. Omand, 'Reflections on Intelligence Analysts', 2.
44. Rolington, *Strategic Intelligence*, 17.
45. Ibid.
46. Hope, *Royal Commission on Intelligence and Security*, quoted in Richardson, *Comprehensive Review*, 155.
47. Kent, *Strategic Intelligence*, 157–8.
48. Agrell and Treverton, *National Intelligence and Science*, 35.
49. Vandepeer",Question-Asking".
50. Lowenthal, *Intelligence*, 58–62.
51. Vandepeer, 'Intelligence and Knowledge Development', 785.
52. For a full discussion see Hammond-Errey, 'Big Data, Emerging Technologies and Intelligence. National Security Disrupted', 86.
53. Johnson, "National Security Intelligence", 21.
54. Ibid., 22.
55. Gill and Phythian, 'What Is Intelligence Studies?', 7.
56. Treverton, 'Terrorism, Intelligence and Law'.
57. Hammond-Errey and Ray, 'A New Methodology'.
58. INSA Rebalance Task Force, *Expectations of Intelligence*, 6.
59. Fingar, *Reducing Uncertainty*, 4.
60. CBS News, 'Former top DNI official'. Sue Gordon at the six-minute, thirty-seconds mark.
61. Vandepeer, *Applied Thinking*, 46.
62. Ibid., 46; Heuer, *Psychology of Intelligence Analysis*, 62.
63. Agrell and Treverton, *National Intelligence and Science*, 32–9.
64. Fingar, *Reducing Uncertainty*, 5.
65. Omand, Bartlett and Miller",Introducing Social Media Intelligence", 807.
66. Symon, 'ASIS Director-General Launches New Book'.
67. Wesley, 'Intelligence Dissemination', 111.
68. Johnson, 'National Security Intelligence'; Walsh",Building Better Intelligence Frameworks"; and Wesley, 'Intelligence Dissemination'.
69. Gookins, 'The Role of Intelligence', 66.
70. Symon and Tarapore, "Defense Intelligence Analysis", 8.
71. Coyne, Neal and Bell, 'Reframing Intelligence'.
72. Wesley, "Intelligence Dissemination".
73. Ibid.
74. Johnson, "National Security Intelligence".
75. Agrell and Treverton, *National Intelligence and Science*, 43–8; Heuer, *Psychology of Intelligence Analysis*.
76. Herman, "11 September: Legitimizing Intelligence?", 229.
77. Lefebvre, "A Look at Intelligence", 243.
78. Omand",Reflections on Intelligence Analysts", 6–7.
79. Ibid., 6–7.
80. Hammond-Errey, *Secrecy, Sovereignty and Sharing*.
81. Hammond-Errey, *Secrecy, Sovereignty and Sharing*; Sue Gordon in Hammond-Errey, 'Intelligence, AI and AUKUS'.
82. See Hershkovitz, *Future of National Intelligence*.
83. Symon, 'ASIS Director-General', 4.
84. Richardson, *Comprehensive Review*, 100.

Acknowledgements

This work was supported by a Data 2 Decisions CRC National Security Big Data PhD Scholarship and a Deakin University Postgraduate Research Scholarship. I am very grateful to those who contributed to – and vastly improved – prior versions of this article. Thank you, Chad, Clinton, Kate, Meredith and Mish. Thank you to the anonymous reviewers for your suggestions. Image design by Susan Beale.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Miah Hammond-Errey's work explores the intersections of emerging technologies and security. She hosts the Technology & Security podcast, where she is joined monthly by global experts to talk technology, security and leadership. Dr Miah Hammond-Errey is the Director of the Emerging Technology Program at the United States Studies Centre at the University of Sydney.

ORCID

Miah Hammond-Errey http://orcid.org/0000-0002-9239-6019

Bibliography

Akhgar, B., G. B. Saathoff, H. R. Arabnia, R. Hill, A. Staniforth, and P. Saskia Bayerl. *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*. Amsterdam: Elsevier, 2015.

Andrew, C. *The Secret World: A History of Intelligence*. New Haven: Yale University Press, 2018.

Bell, G. "The Character of Future Indo-Pacific Land Forces." *Australian Army Journal* 14, no. 3 (2018): 171–184. https://researchcentre.army.gov.au/sites/default/files/AAJ%20Vol%20XIV%20No%203%20-%20Army%20in%20Motion%202018%20%28CALFS18%29%20optimized_0.pdf.

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

Chan, J., and L. Bennett Moses. "Is Big Data Challenging Criminology?" *Theoretical Criminology* 20, no. 1 (2016): 21–39. doi:10.1177/1362480615586614.

Chan, J., and L. Bennett Moses. "Making Sense of Big Data for Security." *The British Journal of Criminology* 57, no. 2 (2017): 299–319. doi:10.1093/bjc/azw059.

Charmaz, K. *Constructing Grounded Theory*. 2nd ed. Los Angeles: SAGE Publications, 2014.

Clapper, J. R. *"Luncheon Remarks, Association of Former Intelligence Officers*." In The Intelligence, AFIO Newsletter, McLean, VA (October 3, 1995).

Coyne, J. W., and P. Bell. "Strategic Intelligence in Law Enforcement: A Review." *Journal of Policing, Intelligence and Counter Terrorism* 6, no. 1 (2011): 23–39. doi:10.1080/18335330.2011.553179.

Coyne, J., S. Neal, and P. Bell. "Reframing Intelligence: Challenging the Cold War Intelligence Doctrine in the Information Age." *International Journal of Business and Commerce* 3, no. 5 (2014): 53–68. https://www.ijbcnet.com/3-5/IJBC-14-3510.pdf.

DeGennaro, P. "The Gray Zone and Intelligence Preparation of the Battle Space." *Small Wars Journal*, August 17, 2016. https://smallwarsjournal.com/jrnl/art/the-gray-zone-and-intelligence-preparation-of-the-battle-space.

Fingar, T. *Reducing Uncertainty: Intelligence Analysis and National Security*. Redwood City: Stanford University Press, 2011.

George, R. Z. "Fixing the Problem of Analytical Mind-Sets: Alternative Analysis." *International Journal of Intelligence & CounterIntelligence* 17, no. 3 (2004): 385–404. doi:10.1080/08850600490446727.

Gill, P. "Theories of Intelligence: Where are We, Where Should We Go and How Might We Proceed?" In *Intelligence Theory*, edited by P. Gill, S. Marrin, and M. Phythian, 222–240. New York: Routledge, 2009.

Gill, P., and M. Phythian. "Intelligence for a More Secure World?" In *Intelligence in an Insecure World*, edited by Peter Gill and Mark Phythian, 172–180. 1st ed. Cambridge, UK: Polity Press, 2006.

Gill, P., and M. Phythian. "What Is Intelligence Studies?" *The International Journal of Intelligence, Security, and Public Affairs* 18, no. 1 (2016): 5–19. doi:10.1080/23800992.2016.1150679.

Gookins, A. J. "The Role of Intelligence in Policy Making." *SAIS Review of International Affairs* 28, no. 1 (2008): 65–73. doi:10.1353/sais.2008.0025.

Greg, G., K. M. MacQueen, and E. E. Namey. *Applied Thematic Analysis*. Los Angeles: SAGE Publications, 2011.
Haass, R. N. *Making Intelligence Smarter*. New York: Council on Foreign Relations Press, 1996.
Hammond-Errey, M. "Intelligence, AI and AUKUS with Former US Principal Deputy Director of National Intelligence Susan Gordon." *Technology and Security (TS)*. Podcast. May 24, 2023. 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
Hammond-Errey, M. *Big Data and National Security: A Guide for Australian Policymakers*. Sydney: Lowy Institute, 2022. https://www.lowyinstitute.org/publications/big-data-national-security-guide-australian-policymakers.
Hammond-Errey, M. *Secrecy, Sovereignty and Sharing: How Data and Emerging Technologies are Transforming Intelligence*. Sydney: United States Studies Centre at the University of Sydney, 2023. https://www.ussc.edu.au/analysis/secrecy-sovereignty-and-sharing-how-data-and-emerging-technologies-are-transforming-intelligence.
Hammond-Errey, M. *Big Data, Emerging Technologies and Intelligence National Security Disrupted*. United Kingdom: Routledge, 2024.
Hammond-Errey, M., and K. Ray. "A New Methodology for Strategic Assessment of Transnational Threats." *Police Practice & Research* 22, no. 1 (2021): 40–56. doi:10.1080/15614263.2019.1699411.
Hayden Center for Intelligence. Policy, and International Security. "A Conversation with Sue Gordon Principal Deputy Director of National Intelligence." *Hayden Center for Intelligence, Policy, and International Security*, September 7, 2017. https://www.youtube.com/watch?v=Khrzs8Jc9V0
Herman, M. "11 September: Legitimizing Intelligence?" *International Relations* 16, no. 2 (2002): 227–241. doi:10.1177/0047117802016002004.
Hershkovitz, S. *The Future of National Intelligence: How Emerging Technologies Reshape Intelligence Communities*. Lanham: Rowman & Littlefield, 2022.
Heuer, R. J. *Psychology of Intelligence Analysis*. Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 1999.
Hughes, R., G. P. Jackson, and L. Scott. *Exploring Intelligence Archives: Enquiries into the Secret State*. London: Routledge, 2008.
INSA Rebalance Task Force. *Expectations of Intelligence in the Information Age*, 1–16. 2012.
Johnson, L. K. "National Security Intelligence." Chap. 1 *In The Oxford Handbook of National Security Intelligence*, edited by Loch Johnson, 3–32. New York: Oxford University Press, 2010.
Kahn, D. "An Historical Theory of Intelligence." In *Intelligence Theory*, edited by P. Gill, S. Marrin, and M. Phythian, 4–15. New York: Routledge, 2009.
Kent, S. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press, 1966.
Kitchin, R. *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. London: Sage, 2014.
Laney, D. "3D Data Management: Controlling Data Volume, Velocity and Variety." *META Group* 949 (2001): 1–4.
Lefebvre, S. "A Look at Intelligence Analysis." *International Journal of Intelligence & CounterIntelligence* 17, no. 2 (2004): 231–264. doi:10.1080/08850600490274908.
Lowenthal, M. M. *Intelligence: From Secrets to Policy*. 5th ed. Los Angeles: SAGE/CQ Press, 2012.
Lundy, L., A. O'Brien, C. Solis, A. Sowers, and J. Turner. "The Ethics of Applied Intelligence in Modern Conflict." *International Journal of Intelligence & CounterIntelligence* 32, no. 3 (2019): 587–599. doi:10.1080/08850607.2019.1607693.
Malomo, F., and V. Sena. "Data Intelligence for Local Government? Assessing the Benefits and Barriers to Use of Big Data in the Public Sector: Data Intelligence for Local Government." *Policy & Internet* 9, no. 1 (2017): 7–27. doi:10.1002/poi3.141.
Moses Lyria, B., and J. Chan. "Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools." *The University of New South Wales Law Journal* 37, no. 2 (2014): 643–678. https://ssrn.com/abstract=2513564.
Office of National Intelligence. "The National Intelligence Community." *Office of National Intelligence* (2017). https://www.oni.gov.au/national-intelligence-community
Omand, D. *Securing the State*. New York: Columbia University Press, 2010.
Omand, D. "Reflections on Intelligence Analysts and Policymakers." *International Journal of Intelligence & CounterIntelligence* 33, no. 3 (2020): 471–482. doi:10.1080/08850607.2020.1754679.
Omand, D., J. Bartlett, and C. Miller. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence & National Security* 27, no. 6 (2012): 801–823. doi:10.1080/02684527.2012.716965.
Richardson, D. *Comprehensive Review of the Legal Framework of the National Intelligence Community*. Vol. 1. Canberra: Commonwealth of Australia, 2020.
Ritchie, J., and J. Lewis. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. London: Sage Publications, 2003.
Rolington, A. *Strategic Intelligence for the 21st Century: The Mosaic Method*. Oxford: Oxford University Press, 2013.
Scott, L., and P. Jackson. "The Study of Intelligence in Theory and Practice." *Intelligence & National Security* 19, no. 2 (2004): 139–169. doi:10.1080/0268452042000302930.
Symon, P. *ASIS Director-General Launches New Book - 'Intelligence and the Function of Government'*. Australian National University, 2018. Transcript https://sdsc.bellschool.anu.edu.au/news-events/stories/6028/asis-director-general-launches-new-book-intelligence-and-function

Symon, P. B., and A. Tarapore. "Defense Intelligence Analysis in the Age of Big Data." *Joint Force Quarterly* 79 (2015): 4–11.
Treverton, G. F. "Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons." *Intelligence & National Security* 18, no. 4 (2003): 121–140. doi:10.1080/02684520310001688899.
Vandepeer, C. *Applied Thinking for Intelligence Analysis: A Guide for Practitioners*. Canberra: Air Power Development Centre, Department of Defence, 2014.
Vandepeer, C. "Question-Asking in Intelligence Analysis: Competitive Advantage or Lost Opportunity?" *ASPJ Africa & Francophonie* 7, no. 4 (2016): 24–43.
Vandepeer, C. "Intelligence and Knowledge Development: What are the Questions Intelligence Analysts Ask?" *Intelligence & National Security* 33, no. 6 (2018): 785–803. doi:10.1080/02684527.2018.1454029.
van der Sloot, D. B. Bart, and E. Schrijversedited byExploring the Boundaries of Big Data.*The Hague: Netherlands Scientific Council for Government Policy*2016https://www.ivir.nl/publicaties/download/1764.pdf
Van Puyvelde, D. "Qualitative Research Interviews and the Study of National Security Intelligence." *International Studies Perspectives* 19, no. 4 (2018): 375–391. doi:10.1093/isp/eky001.
Walsh, P. F. *Intelligence and Intelligence Analysis*. New York: Routledge, 2011.
Walsh, P. F. "Building Better Intelligence Frameworks Through Effective Governance." *International Journal of Intelligence & CounterIntelligence* 28, no. 1 (2015): 123–142. doi:10.1080/08850607.2014.924816.
Wastell, C. A. "Cognitive Predispositions and Intelligence Analyst Reasoning." *International Journal of Intelligence & CounterIntelligence* 23, no. 3 (2010): 449–460. doi:10.1080/08850601003772802.
Wesley, M. "Intelligence Dissemination." In *Chap. 5 in* Intelligence and the Function of Government, edited by D. Baldino and R. Crawley, 109–126. Melbourne: Melbourne University Publishing, 2018.
Wheaton, K. J., and M. T. Beerbower. "Towards a New Definition of Intelligence." *Stanford Law & Policy Review* 17, no. 2 (2006): 319–330.
Wilhelm, A., and G. F. Treverton. *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*. New York: Oxford University Press, 2015.
Zegart, A. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton: Princeton University Press, 2022.