National Security Journal

http://nationalsecurityjournal.nz

Published by:
Centre for Defence
and Security Studies,
Massey University

ISSN: 2703-1926 (print) *ISSN: 2703-1934 (online)*

The Other Side of the Hill - Endeavouring to Define Intelligence in the 21st Century: A Perspective.

Author: John Battersby

To cite this article: Battersby, J. (2024). The Other Side of the Hill - Endeavouring to Define Intelligence in the 21st Century: A Perspective. *National Security Journal*. Published 25 September 2024. doi: 10.36878/nsj20240925.01

To link to this article: https: doi.org/10.36878/nsj20240925.01

View CrossRef data: http://search.crossref.org/?q=10.36878%2Fnsj20240925.01

Journal Article published 25 September 2024 in National Security Journal.

THE OTHER SIDE OF THE HILL - ENDEAVOURING TO DEFINE INTELLIGENCE IN THE 21ST CENTURY: A PERSPECTIVE

John Battersby[1]

This paper discusses not a definition but defining characteristics of intelligence, those it has inherited from the Cold War, and those which new conditions are forcing it to adapt to. Intelligence cannot be reduced to a simple sentence-length definition. Intelligence is iterative – its nature varies depending on the context in which it is produced. Its unconventional methods combined with its exclusivity of method and content makes intelligence information different from other sorts. These essential characteristics allow us to understand the relationship between different *intelligence's* and between them and related concepts of 'intelligence-adjacency' as well as good old fashioned, but ever reliable, basic 'research'. Intelligence has a wide ambit; it is not a discipline in itself, but something combining varying methods of information gathering and analysis to create ephemeral knowledge of genuine, but ephemeral, value - within the varying contexts in which it is used.

Key words: Intelligence, Intelligence-adjacency, Open-source intelligence, Decision-making, Research.

Introduction

> All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know from what you do; that's what I call 'guessing what was on the other side of the hill'.[1]
>
> Arthur Wellesley, Duke of Wellington

1 Dr John Battersby is a Senior Fellow at the Centre for Defence and Security Studies, Massey University (Wellington Campus).

The impetus for this paper comes from several years teaching 'intelligence professionals' some of whom are (or previously were) in traditional intelligence agencies but include many more from other intelligence-active agencies, where intelligence is not the latter's core function. A number are military, a pursuit in which intelligence has a much more ingrained and understood role in attaining operational objectives. Many are from law enforcement or regulatory agencies, most obviously NZ Police – for which the difference between collecting data, collecting intelligence and collecting evidence can be something of a greyscale. Finally, there is a seasoning of younger students intellectually interested, curious about, or critical of, intelligence agencies and their role in the state – or, just as often, wanting to join them. Overall, they reflect a membership of a morphed and morphing intelligence environment in New Zealand, and elsewhere, in the 21st century.

Working with this grouping, it has become increasingly apparent firstly that collective memory of the Cold War is rapidly fading – many current practitioners of intelligence did not experience it, nor have any recollection of the peculiar all-embracing security orientation of intelligence agencies during it. The intelligence game of the shadows, of covert agents and their handlers, of monopolies of secret and stolen information, is something many know only by movie and television depictions of that time. Professor Christopher Andrew notes the historical amnesia of 21st century intelligence agencies, [2] and former US Assistant Director of Central Intelligence Mark Lowenthal observes the lack of lessons learned by intelligence practitioners from recent experience due to the constant press of new demands.[3] Intelligence is indeed ephemeral; but intelligence has a history, and history is classroom.

Secondly, the rapid expansion of information technology has, as historian Calder Walton notes, inverted the nature of intelligence from primarily covert-collection-dominant, to a world in which almost everything is in the open.[4] So much so, in fact, that the intelligence process has in cases morphed to harvesting massive amounts of information floating in media or cyber space, sieving and threshing it, to isolate the bits and pieces that may be useful for analysis. The 'google-analyst' is now a reality, for better or for worse. An irony observed by historian Rhys Ball, is that this open-source intelligence (OSINT) is then converted into closed and secret knowledge – 'top secret' stuff derived from everyday fare.[5] This is an important element of intelligence now.

Outside of defined security intelligence agencies New Zealand government organisations conducting such analysis are not covered by the Intelligence and Security Act 2017, and their outputs are disclosable under the *Official Information Act 1982*. This leaves something of a quandary. How can intelligence be intelligence when potentially anyone can know about it?

This paper will therefore discuss the characteristics of intelligence, those it has inherited from the Cold War, and those which new conditions are forcing it to adapt to. It will be argued here that critical elements of intelligence are its unconventional method, and the exclusivity of both method and resulting information; its importance, value and restricted access makes intelligence information different from all other sorts. But intelligence is ephemeral; its value erodes as the need for it does, or as its shroud of secrecy is broken. These essential characteristics allow us to better understand what 'intelligence' is, what intelligence professionals do, as well as the relationship between 'intelligence' and concepts of 'intelligence-adjacency' and good old fashioned, but ever reliable, basic 'research'.

'Guessings' about the Future

Many authors have posited definitions of 'intelligence' attempting to succinctly define the notion. Their definitions vary, and always seem to lack one thing or another, never quite grasping the entirety of the intelligence pursuit. Thus, it is opted here to discuss instead, not definition, but defining characteristics of intelligence, in a quest to grasp as much of the phenomenon as possible. 'Intelligence' is often asserted to comprise the exploitation of information sources, the collection of timely and accurate information, the interrogation, corroboration and analysis of that information into a form - an intelligence product, estimate or report - which provides a decision-maker with the best information-based assessment for possible and likely future situations that may occur.

Sir David Omand, former Director of the British Government Communications Headquarters (GCHQ), describes the purpose of intelligence as improving "the quality of decision-making by reducing ignorance."[6] Arthur Wellesley, the Duke of Wellington, summarised it succinctly as "the endeavour to find out what you don't know, from what you do."[7] Interestingly, he did not actually mention the word 'intelligence' in the quote cited above, suggesting the difficulty of defining and distinguishing intelligence from the activities to which it is most often related. Wellington used the word 'guessing', a poor word selection given he had just implied a process designed to analyse rather than guess, to project possibilities about what was not known based on a logical extension of what was.

A further caveat is required to Wellington's statement – his 'guessing' should have been 'guessings'. It is a common misperception that intelligence can or should predict what the future *will be*. Omand asserts 'prediction' is a key use of intelligence and the result of most intelligence activity.[8] But this is easier said than done. Lowenthal observes that intelligence "is supposed to be about the future" but notes immediately "how difficult it is to achieve this future vision with any clarity."[9] Looking back and seeing a single

lineal historical sequence and too often assuming its obvious inevitability (as post-event inquiries and the media often do) is not the same as attempting to imagine certainty among a fog of future possibilities. Former CIA Counter Terrorism Centre Deputy Director Paul Pillar, observes that intelligence simply cannot predict the future when much of it depends on decisions that others have not yet made.[10] When spontaneous events involving the random decisions and actions of thousands of people suddenly occur, (as arguably it did outside New Zealand's Parliament in February 2022) they are often triggered by small unplanned or lesser incidents.[11] These are often not predictable phenomena, especially when the people making these small decisions haven't yet made them, or are unaware they are even going to. While the predictive aspect of intelligence is important (why else would we attempt it?), it has significant limitations in this regard. Intelligence prediction, therefore, is oriented toward scoping the parameters of what could logically happen next based on what already has. It is not gazing into a crystal ball and magically declaring exactly what will. This is less remarkable than the expectations many have of intelligence, and assumptions about 'intelligence failure' often fail to comprehend this.

Having determined a range of potential future possibilities, intelligence analysts will generally offer a degree of likelihood that any given possibility may eventuate. In 2011 US intelligence analysts put the probability that Osama bin Laden was inside a high-walled compound in Islamabad at 40-60%.[12] This was done by a rigorous process of interrogating each piece of information, weighing its reliability, and testing the logical nexus that connected each piece together. It is based on a set of tested assumptions which allow for a conclusion about how likely an event is considered to be.[13] Having defined possibilities, analysts will attempt to narrow the scope, using what they know, to attempt to get a closer and clearer picture of which possibility seems most likely.[14] Even done conscientiously, this process harnesses a mathematical concept of 'probability' to completely non-mathematical phenomena – a distinctly ill-fitting exercise. Professor Lawrence Freedman refers to "the dangerous allure of numbers" – the flawed assumption that information expressed numerically conveys greater weight than what is written in words.[15] What analysts are attempting here is an appeal to keep options open, possibilities being weighed against each other as to which may be the potential outcome – using numbers, assumed to convey relative probability better. As it happened, Osama bin Laden was in the Islamabad compound, but until US special forces located him there on 2 May 2011 there was no certainty he was. The CIA didn't tell President Barrack Obama what to do, it simply gave him the best possible information about what was over the hill in Islamabad. Obama could then make his decision about whether, or not, to go over it.

Intelligence can be about now!

Not all intelligence is about the future. Intelligence can be concerned with finding out what an adversary (or target) is doing right now. Knowledge of what an adversary or competitor is doing is important only partly because of their ultimate intention. Related to this is the common assertion made by many authors/practitioners that 'intelligence' is information with *value added* by analysis, and 'intelligence' is not actually 'intelligence' until it has been 'evaluated and analysed'. Former British Army Intelligence Officer Colonel John Hughes-Wilson is adamant: "Intelligence is nothing more or less than information that has been systematically and professionally processed and analysed."[16] Professor Mark Pythian explains the theory of the Intelligence Cycle. "Information is not intelligence…." To be transformed into intelligence, "raw information must pass through the **processing** and **analysis** stages [bold in the original]."[17] Omand explores the question infusing a magical quality - "By what alchemy is raw information to be transmuted into intelligence?"[18] Thus a distinction is drawn between 'information', or 'raw' uncooked material which is not yet of use, and 'intelligence' which has its value discovered, inserted or added by the truly transformational process of intelligence analysis.

But these authors are looking down on intelligence, some from the experience of the pinnacle of large intelligence organisations. Intelligence happens at the bottom too; it can be about what is happening now, and it can be rough and ready with no value 'added'. Solomon Island coast watcher Jacob Vouza escaped Japanese captivity at Guadalcanal in 1942 warning US forces of a pending Japanese attack – providing clear, raw, unanalysed information which allowed US marines time to react and defeat the assault at Tenaru on 21 August 1942.[19] This is intelligence used in a manner which does not point to a range of possibilities and allowed no time for corroboration or analysis. The information revealed to US forces what the Japanese were in the process of doing, allowing the former to anticipate and react to what would most likely happen next. While this may be a distinction of scale and immediacy, nevertheless information by itself can indeed be intelligence, and it can be about what is already happening. A critical element of intelligence is not necessarily its level of 'processing' therefore, but the value that information has at the point it is discovered. It is not valued for its own sake, it must be of value to someone.[20] Such value is however, ephemeral – conferring an advantage at a moment in time. If Vouza had arrived after the Japanese attack, his information would not have been of any use to anyone.

Woodrow Kuhns asserts that "intelligence is really little more than useful knowledge", but it is far more than simply that and the 'value' of information has other implications.[21] During successive America's Cup yachting regattas there have been frequent allegations by various competitors against each other of covert surveillance and infor-

mation gathering. None of this was to establish a range of possible future outcomes – it was all firmly oriented to establish inside knowledge of an adversary's boat design to understand how they would race. Obtaining knowledge of this enables the collectors to adjust their own approach to counteract their opponent. A New Zealand yachting journalist noted "[t]his is nothing new to an event where innovations have been at the core of success and working out what your opponents are doing is as important as your own programme."[22] In July 2024 Canadian women's football coaches were sent home from the Paris Olympic Games for spying on their New Zealand adversaries using drones.[23] Intelligence can mean "insider' information gained by deception, deceit and skullduggery across a wide range of domains.

A large measure of Soviet espionage in the Cold War was actually aimed at Research and Development (R&D) information in the West, serving less the analysis of future outcomes, and more to steal the technology the Soviets could not afford to research themselves. KGB officer Vladimir Vetrov handed over to the West "the names of all the KGB's 250 officers working on 'Line X', the smuggling of technology in embassies across the world."[24] Walton observes that Soviet technical espionage was so prolific, the West was practically arming both sides of the Cold War.[25] The aviation technology information supplied by Soviet engineer and American spy Adolf Tolkachev to the United States between 1979 and 1985 again, did not lead to future predictions of Soviet intentions, but revealed the inner workings of Soviet aviation and weapons design, enabling subsequent US designs to counteract them.[26] Israel stole much of its nuclear technology and even its initial stocks of weapons grade Uranium, from the United States – their own ally.[27] The People's Republic of China (PRC) has been involved in the covert theft of commercial and R&D information from the US routinely for decades and continues to do so.[28] The latest Chinese military aircraft bear a striking resemblance to modern Western aircraft designs – because the latter stole the technology they built them with through persistent (and likely ongoing) espionage.[29]

Intelligence therefore is not confined to the analysis of possibilities dwelling in the future, it is also about obtaining knowledge of what adversaries, enemies, competitors, partners *and friends* are doing, or what they may have that would be an advantage for us to know about. Thus emerges a fluidity and ambiguity surrounding the term 'intelligence,' as information of value, processed or unprocessed, about future possibilities, current realities, and technological no-how or intellectual property that someone has, that someone else wants! It also focuses the spotlight on the routine illegality involved in intelligence collection by nations' secret services. Intelligence can be obtained by theft, inciting treason by bribery or blackmail, hacking into 'secure' systems or bugging private conversations from enemies and friends alike.

Regardless of whether 'intelligence' is about now or the future, its value has traditionally been in it comprising at least something that an adversary (an enemy or rival), a counterpart (a friend or possible partner) or target (criminal or terrorist) would rather the

collector not have. This information is "special or different."[30] It is private, privileged, confers an advantage to the bearer, is deemed sensitive, or secret, is often covertly (even illegally) obtained, and is a dimension that traditionally distinguishes 'intelligence' from other methods of information assessment. Edward Snowden's revelations in 2013 that the US National Security Agency (NSA) was recording and collecting phone conversations of European leaders exposed the need for secrecy for such efforts to function – once publicly known they became a scandal.[31] Similarly the covert bugging of Timorese government offices by the Australian Secret Intelligence Service (ASIS) in 2004 conveyed a significant financial advantage to Australia in subsequent oil and gas negotiations between the two countries. The advantage was blown by subsequent revelations of ASIS's involvement, and the Australian/Timor-Leste oil and gas deal had to be renegotiated.[32] Intelligence, and the means of obtaining it, are therefore necessarily kept secret to an insider group. Intelligence, and the fact that it is possessed, cannot be general knowledge.

A note of caution, however. Hughes-Wilson observes the falsehood of intelligence officers believing information that is harder to discover necessarily being more reliable, and Omand notes the 'intoxication' effect on the reader of a document marked "TOP SECRET" conferring an unjustified reliability to it.[33] This "TOP SECRET" marker merely prohibits the circulation of information, it does not elevate its credibility.

Despite all the upbeat descriptions of intelligence serving to inform a decision-maker of what is over the next hill, no decision-maker actually has a right to know what the future will hold and can have no expectation that anyone will be able to provide that information. The CIA may have conferred a probability that Osama bin Laden was in Islamabad in 2011, but for years previously they were unable to find him. The Australians may have planted listening devices in the Timorese Prime Minister's office – but there was no guarantee he would necessarily say anything useful. Therefore, 'intelligence', as the Duke of Wellington put it, is an *endeavour* to find out what the future may comprise of, or about what enemies or friends may be thinking, not a guarantee that such an endeavour will succeed, or that it will do so in time to be useful. Former Director-General of the NZSIS, Rebecca Kitteridge described the challenge for all intelligence agencies in 2021 as "accessing and analysing the right information at the right time…. joining the crucial dots – but we have to find the right dots in the first place."[34]

Intelligence is not only an endeavour, but often a *contested endeavour*. While an array of intelligence officers, scouts, patrols, spies and analysts may be deployed to discover an adversary's (or friend's) intention – there is a wall of obstacles in the way of them accomplishing their objective. The keepers of secrets will stamp them "TOP SECRET" to deliberately restrict access to the information that the spies of an adversary will want to get their hands on. Criminals will conceal their activities to a realm of those suspicious of law enforcement agencies, those circumventing regulatory requirements will keep their deeds as low-key as possible and major firms will attempt to protect commercially

sensitive information that carries risk or advantage. Would-be intelligence gatherers must overcome these obstacles; many have – Ana Montes[35] and the Myers's[36] successfully spied for the Cubans for decades. Oleg Gordivesky spied for the UK for several years, escaping just before being caught. Adolf Tolkachev was not so fortunate. Others failed entirely – every German intelligence agent sent to Britain during World War II was captured![37]

Intelligence and the new Intelligence Environment

Prompted by the 21st century's revolution in cyber based information and social media there has been a rapid proliferation of intelligence units across a span of bureaucratic government services, outside the domain of traditional security intelligence. On any given day employment websites list vacancies for intelligence analysts across a span of private business, banks, local bodies, and government agencies. The vast bulk of these newer intelligence groups do not seek to collect information by the recruitment of sources, or through the use of covert espionage or surveillance in their work. They operate lawfully with information harvested from either data collected during their normal business or from openly available cyber sources or social media. Intelligence people call this Open-Source Intelligence (OSINT). Bellingcat, the well-known investigative and fact-checking journalism-based group, call it 'open-source research'.[38] The difference is Bellingcat wants to share the fact-verified outputs they produce; OSINTers generally want to conceal theirs!

Traditionally, political and military intelligence was largely defined by covertly obtained information analysed for its insights, and added to what was more openly obvious. OSINT or open-source research, is more attuned to coping with a vast bulk of available information there for the taking, with what is useful being sieved out for analysis. That bulk comprises information legally accessible on networks or voluntarily made available by ordinary people, inadvertently exposing their search behaviour or posting their normal exploits, document, video and photo files online. This was described by a former CIA Deputy Director as 'electronic exhaust' - the electronic emissions we leave behind in the cyber atmosphere every time we use our devices on the internet.[39] We are unaware, or unconcerned that private and state intelligence collectors, commercial enterprises, and cyber-savvy criminals, using human and algorithmic code can harvest our information, and the metadata that travels with it, to exploit this material for a range of purposes. Walton observes that "the new globalised information environment has inverted the nature of intelligence" meaning the vast bulk of collection is now in the open.[40]

Preceding the cyber revolution was the evolution of globalised 24-hour mass media, which had journalists openly reporting from developing crises in real time, meaning intelligence analysts – even if they had collectors on the ground – could be receiving information at the same time as everybody else. Moreover, the media spotlight being

public, and public reactions usually being emotional, political decision-makers were responding less to a given crisis itself, and more to the emotional reaction of the general public to it. Social media has enormously amplified this effect. The role of intelligence in public service units is at risk of being skewed from solving the problem of what could happen next, to serving the need of chief executives to make press releases about what they are going to say next.

Open sources are not new and are a foundational element of more traditional intelligence. Wellington's need to know what was on the other side of the hill always involved 'open sources', with critical geographical information, and the absence or presence of the enemy, requiring only the effort of looking for it.[41] Globalised media and cyber space presents an infinite number of virtual hills to peer over and extends that ability to cyber users across the globe. The intelligence collectors of the 21st century now patrol a communications-and-cyber 'no man's land' or create algorithms to do so. The sheer volume of data, and the capacity to separate what is genuinely useful from a mass of surrounding and irrelevant white noise, remain major challenges for OSINT.[42] Intelligence agencies of the 21st century at risk of information overload have turned to Artificial Intelligence (AI) to sift through their collected data.

A further dimension of the cyber revolution is cyber warfare – the deliberate use of online hackers, thieves and saboteurs – most notably recently by Russia against the Ukraine - has meant intelligence detectors of enemy, adversarial, or competitive activity now exist well beyond the state.[43] Looking over the next hill has become an exercise in guarding the commercial computer and satellite systems upon which almost everything we do now relies. In a remarkable failure of human foresight, we have neglected contingencies for what we will do when (not if) these systems are irreversibly compromised or destroyed. Albert Einstein's prediction of World War 4 being a sticks and stones affair, can be amended – it will also be fought cyber blind and in the dark.

Analysing datasets of collected information from normal business processes to identify recent or historic trends can be useful, and done well, extremely so. But by itself, this is research, not an intelligence-specific exercise. The application of analytical techniques commonly used by intelligence agencies to derive value beyond the open information collected, and to use it in an attempt to visualise what is not known, or what could happen next, is more like intelligence. The term 'intelligent-adjacent' was coined by the New Zealand Ministry of Business, Innovation and Employment's (MBIE) Future Strategy Team (FST) during the COVID pandemic to refer to their use of intelligence methodologies "to provide strategic advice products, rather than traditional intelligence outputs."[44] The results of the FST's work conducting "indepth research and predictive analysis" toward strategy formulation utilised open and available data and did nothing covertly. This was innovative work, and the concept of 'intelligence-adjacency' provides a definitional alternative encompassing evolved changes in the intelligence domain. The notions of intelligence-led policing (ILP), or intelligence-informed or enabled practice,

where recent patterns, trends or crime hotspots are mapped to base current resource and deployment decisions could be more aligned with intelligence-adjacency, or arguably good old fashioned data analysis, than intelligence. Chief protagonist Jerry Radcliffe defines ILP as "a business model" and "management philosophy" based on data analysis informing police decision and deployment.[45] It could be more appropriately called Data-Led Policing. In any event, its effectiveness has been questioned globally, and recent research suggests the implementation of ILP in New Zealand has not been as successful as initial promise suggested it could be.[46]

Intelligence and Evidence

Law enforcement agencies have a longer intelligence experience than most public sector agencies with their use of more traditional intelligence functions dating back into the nineteenth century, well before most modern intelligence agencies existed.[47] Even in New Zealand, Police intelligence functions developed decades before the NZSIS was established in 1956. Globally, twentieth century demands to counter terrorism, sedition and organised crime blurred the distinction between police collection of information as evidence for prosecution, and the collection of information to gain insight (or intelligence) on what illegal activities were in the offing. In the twenty-first century, police intelligence functions are still primarily oriented toward supporting the gathering of evidence for the apprehension and prosecution of criminals, or to inform the deployment of police resources to fulfil their key function - the maintenance of order.[48] Police routinely use undercover officers to infiltrate targeted groups or surveillance teams to monitor their activity. These are tradecraft practices they share with intelligence agencies. But the results for police are still the apprehension of suspects committing offences and the presentation of evidence in court, which is different from the priorities of intelligence agencies to maintain a flow of critical information. Police will find what is over the hill and arrest it, bringing offenders to account after the fact. Intelligence agencies will leave the hill behind them without concern.

Police intelligence (and other public agency) assessments are generally disclosable - in most democratic settings the Accused has the right to see all the evidence brought against them including how it was obtained. This leads to what would be normally regarded as sensitive collection and analytical tradecraft, as well as the raw information itself, being made available not only to the target, but generally in an open Court setting. Australia's Joint Counter Terrorism Teams (JCTTs) established in 2002 brought information collected by the Australian Security Intelligence Organisation (ASIO) within a prosecution context. [49] The United Kingdom's approach is similar, allowing a centralised coordinated information sharing process to occur for the prosecution of terrorist offences. But judgements on this process remain outcome based – measured by plots disrupted or convictions obtained. The fundamental problem remains, how information obtained by a range of generally non-disclosable means, relates to legally

admissible and openly explained evidence. If information and its origins, as well as its method of collection are all publicly disclosed and subject to judicial review – it cannot be intelligence. Intelligence cannot be 'intelligence' if everyone knows about it. This is why the more common assertions of 'transparency' in intelligence struggle to convince – are they not a contradiction in terms?

Private Sector intelligence

Outside the public sector a range of private organisations have adopted the use of the term 'intelligence' to refer to the information-based content they provide. A number of these are commercial enterprises operated by former security intelligence operators, who use their skills to harvest and analyse information to provide outputs that are commercially useful. With the development of AI, the perception of crime rising and declining trust in police responses, private operators are now providing commercially tailored fit-for-purpose intelligence-informed security solutions for businesses and larger public/private spaces. Even within national security environments private-tech is becoming a major (perhaps even dominant) partner in cyber intelligence environments.[50] Moreover, while they must act lawfully, surveillance and information-sharing processes by private sector firms are less fettered by legal requirements imposed on police and government intelligence agencies. Private sector intelligence is a real and growing phenomenon and is generally not subject to any oversight or regulation, a situation emulating the genesis of most state intelligence agencies. Intelligence is an organic phenomenon, it will evolve to conditions and it will find a way to stay secret.

As a largely unregulated industry there are those in the private intelligence realm who care little who they work for, or what lengths they need to go, as long as the 'intelligence' they provide is what the client wants and pays handsomely for.[51] Less sinister, are those who regard the way a product is 'packaged' as more important than its actual content. Thus, a range of consultants provide market, business and product 'intelligence', travel agents provide 'travel intelligence', even NGO's occasionally use the term 'intelligence' to describe aspects of their information-based activities. This is not actually 'intelligence' and it does not reflect any evolution of the intelligence environment but are likely old practices of data collection and correlation re-labelled with the more alluring image 'intelligence' conjures up.

After all that… what is 'intelligence' in 21st century?

Intelligence is the attempt to learn what we do not know, by collating and analysing what we do know (and what else we can find out), augmenting it with what others do not want us to know, or are careless in securing, and using it to create insight to aid the decision about what to do next. This process may happen very quickly with little or no analysis, or it may involve more intense analysis. Modern communications, mass me-

dia and social media developments have evolved to create a mass of open-source information, which by analysis can be sifted to add to what we know and which – while it is all 'open' information – can be interrogated to provide insights into private worlds. The product of this, as Ball has observed, is the transformation of open-source information into a closed or classified intelligence format. To divine secret and valuable meaning out of something apparently without any, is a true utility of an intelligence analyst. However, 'intelligence' cannot be 'intelligence' simply by virtue of the term's use as a marketable label, and 'intelligence' cannot be 'intelligence' if everybody knows about it. Secrecy or security in some form, to know something others do not, and to maintain the secret, remains an essential element of intelligence.

Intelligence is privileged information; it confers an advantage to the possessor and a disadvantage to their adversary. Intelligence is not "mere data" or data crunching.[52] Intelligence is dynamic – it's the definite article, as well as an on-going process. It is not a permanent state of information. If intelligence ages, becomes irrelevant or is found to be inaccurate, then it ceases to be intelligence.

Decision-makers at any level have no right to expect that their intelligence staff will warn them of every eventuality, or that they will not be surprised by a turn of events entirely unanticipated by anyone.[53] Nor may the media appoint themselves to judgement, declaring unanticipated events - which frankly no one saw coming - as intelligence failures. Intelligence analysts simply cannot predict what numbers will be drawn out of a weekly lottery draw and they have no more ability than anyone else to predict with certainty what will happen an hour, a day, a week, or a year from now. But they can define the parameters of what might.

Modern intelligence analysis borrows heavily from academic writing and critical thinking, using analytical techniques adopted from business and marketing practices. Similarly, intelligence collection operations themselves have always run to the limits of lawfulness and not unusually gone beyond them, engaging in activities similar to those of researchers, police, military special forces or indeed, of criminals and criminal organisations. As such, intelligence is not a discipline entire in itself, but a vocation adopting the components of many others in an effort to exploit information gathering opportunities and harness the most effective ways to secure and apply that information (or the value derived from it). Intelligence is information obtained by any method deemed practical and necessary, and despite attempts to impose codes of ethics and transparency – genuine intelligence may always contain an element, in greater or lesser measure, of deceit.

Intelligence is not general knowledge, public knowledge or the product of transparent academic ethically compliant and methodologically sound analysis. It is not market research or crunching data – although it may include parts of all these things. Intelligence is research done unconventionally, collected however and wherever necessity

demands unaffected by legal rules of admissibility. Intelligence that becomes evidence in Court is no longer intelligence – and perhaps it never was. Ethics and transparency have entered into narratives about intelligence in more recent times, but these likely depend on the degree of insecurity that prevails. A country like New Zealand, perceiving itself thousands of miles from an existential risk, may indeed demand lawful and ethical methods of intelligence collection and analysis; Israel facing constant clear and present threats, will do whatever it has to do (and even then, may be found wanting as the events of 7 October 2023 demonstrated). Public service intelligence emulates to greater or lesser degrees, aspects of the intelligence process of collection, collation, analysis and dissemination, but likely falls short in many instances of what has been discussed here as traditional intelligence. The term *intelligence-adjacent* has been coined to cover the application of intelligence processes in more policy or practical problem-solving contexts. The term 'research' has been around for eons; it describes the collection, collation and analysis of openly available data. Done well, it is every bit as useful, but it more often serves to publicly inform and advance collective understanding, than privately or secretly confer an advantage to a few.[54]

Finally, intelligence is an *endeavour* to see what may be over the next hill. Intelligence will only on very rare occasions correctly and accurately foretell a coming event. Most of the time intelligence will seriously *endeavour* to find out what its targets will equally seriously strive to keep hidden. From this intelligence analysts will *endeavour* to project the limits of possibilities about the future, or about an adversary's or competitor's private actions or intentions. They will weigh probabilities about which of the possibilities may emerge from among a range of 'maybes'. Intelligence groups should tell a decision-maker what needs to be prepared for, not what will happen for sure, nor what to do about it. Intelligence practitioners run the risk of 'crying wolf' far more often than the wolves are there; and ultimately decision-makers have to make-up their own minds about the future risks and outcomes of a current decision.

Intelligence then is the sum of many components, of parts of things, with caveats; an aspirational attempt to know about now, or about the future, something that cannot be known for sure. Intelligence is reconnaissance in space and time, and now in cyber-space as well, contemplating every hill, real or virtual, in an endeavour to anticipate what is on the other side of it. Who knows what will be found there, or whether everything that is there will be found. Once it is known for sure what is on the other side of the hill, the need for intelligence about it vanishes. Intelligence is ephemeral by its very nature, its producers will not dally, they will move onto the next hill and, as Andrew and Lowenthal have noted, they will seldom look back.

1 Memorandum by Mr Croker, 4 September 1852, *Croker Papers: The Correspondence and Diaries of the Late Right Honourable John Wilson Croker, Secretary to the Admiralty from 1809 to 1830*, Vol.3, Louis J Jennings ed., Cambridge University Press, (Cambridge, 2012) p.275.

2 Christopher Andrew, *The Secret World: A History of Intelligence*, Penguin (London, 2019), p.1.

3 Mark M. Lowenthal, *The Future of Intelligence*, Polity (Cambridge, 2018), p.63.

4 Walton, p.508.

5 Personal communication, 7 June 2024; this was a discussion signaling Rhys's article anticipated for this volume.

6 David Omand, *Securing the State*, Oxford University Press (Oxford, 2010), p.22.

7 *Croker Papers,* p.275.

8 Omand, pp.25-26.

9 Lowenthal, pp.1-2.

10 Paul R. Pillar, *Intelligence and U.S. Foreign Policy, Iraq, 9/11 and Misguided Reform*, Columbia University Press (New York, 2014,), p.7.

11 See Dan Wildy, Intelligence and Public Trust, *International Journal of Contemporary Intelligence Issues*, 1:2 (2024), p.12.

12 Keith Cozine, Teaching the Intelligence Process: The Killing of Bin Laden as a Case Study, *Journal of Strategic Security,* 6, No.3 Suppl. (2013), p.86.

13 Joab Rosenberg, The Interpretation of Probability in Intelligence Estimation and Strategic Assessment, *Intelligence and National Security*, 23:2 (2008), p.142.

14 See Dahl, pp.54-56., as US intelligence seeks to narrow down the range of possible locations of the Japanese Fleet prior to the Battle of Midway.

15 Lawrence Freedman, *The Future of War: A History*, Allen Lane (London, 2017), p.114.

16 Colonel John Hughes-Wilson, *Military Intelligence Blunders*, Revised Edition, John Blake Publishing, (London, 2023), p.27.

17 Mark Phythian, Introduction: Beyond the Intelligence Cycle?, in *Understanding the Intelligence Cycle*, Mark Phythian, ed., Routledge (Abingdon, 2013), p.3.

18 Sir David Omand, "The future of intelligence: What are the threats, the challenges and the opportunities, in *The Future of Intelligence Challenges in the 21st Century*, Isabelle Duyvesteyn, Ben De Jon & Joop Reijn, eds., Routledge, (2014), p.14.

19 Al Hemingway, Jacob Vouza's Defiant Stand During the Guadalcanal Campaign, *Warfare history Network*, n.d., https://warfarehistorynetwork.com/jacob-vouzas-defiant-stand-during-the-guadalcanal-campaign/

20 Zhivan Alach, "The Emperor is Still Naked: How Intelligence-Led Policing has Repackaged Common Sense as Transcendental Truth," *The Police Journal: Theory, Practice and Principles,* 84:1 (2011), p.79.

21 Woodrow J. Kuhns, "Intelligence Failures: Forecasting and the Lessons of Epistemology," in *Paradoxes of Strategic Intelligence: essays in honor of Michael I. Handel*, Betts & Mahnken, Eds, Routledge (London, 2003), p.77.

22 Duncan Johnstone, 'Americas Cup: Team NZ latest victims in long history of spy scandals,' 30 June 2020, Stuff.co.nz; https://www.stuff.co.nz/sport/opinion/121982280/americas-cup-team-nz-latest-victims-in-long-history-of-spy-scandals.

23 "Canada deducted points and coach banned over drone," BBC News, 28 July 2024, https://www.bbc.com/sport/olympics/articles/ckdg0gqk4kqo

24 Catherine Belton, *Putin's People: How the KGB Took Back Russia and Then Took on the West*, William Collins (London, 2020), pp.28-29. Walton gives this number as 200, with another 100 being cultivated, see Walton, p.364.

25 Walton, p.364.

26 David E. Hoffman, *The Billion Dollar Spy: A True Story of Cold War Espionage and Betrayal*, Icon Books (London, 2017).

27 Jefferson Morley, *The Ghost: the secret life of CIA spymaster James Jesus Angleton,* Scribe (Brunswick & London, 2017), p.177.

28 See Mara Hvistendahl, *The Scientist and the Spy: A True Story of China, The FBI and Industrial Espionage*, Riverhead (New York, 2020).

29 David E. Sanger (with Mary K. Brooks), *New Cold Wars: China's Rise, Russia's Invasion and America's Struggle to Defend the West*, Scribe (Melbourne, London, Minneapolis, 2024), p.23.

30 Ruth Delaforce, Public and Private Intelligence: Historical and Contemporary Perspectives, *Salus Journal*, 1:2 (2013), p.21.

31 "Edward Snowden: Leaks that exposed US spy programme," BBC News, 17 January 2014, https://www.bbc.com/news/world-us-canada-23123964

32 Tiffanie Turnbull, "Bernard Collaery: The spy case that ignited an Australian secrecy row," BBC News, 14 July 2022, https://www.bbc.com/news/world-australia-61836078

33 John Hughes-Wilson, *On Intelligence: The History of Espionage and the Secret World*, Constable (London, 2016), p.345; Omand, p.47.

34 NZSIS Director-General opening statement to Intelligence and Security Committee, 24 March 2021, https://www.nzsis.govt.nz/news/nzsis-director-general-opening-statement-to-intelligence-and-security-committee-24-03-2021?url=news%2Fnzsis-director-general-opening-statement-to-intelligence-and-security-committee-24-03-2021%2F

35 Ana Montes: Former top spy says she will live in Puerto Rico, BBC News, 10 January 2023, https://www.bbc.com/news/world-us-canada-64213901

36 Toby Harnden, Spying for Fidel: The Inside Story of Kendall and Gwen Myers, *Washingtonian*, 5 October 2009, https://www.washingtonian.com/2009/10/05/spying-for-fidel-the-inside-story-of-kendall-and-gwen-myers/

37 See Ben Macintyre, *Double Cross: The True Story of The D-Day Spies*, Bloomsbury (London, 2016).

38 See https://www.bellingcat.com/

39 Omand, p.33. The term is attributed to former CIA Deputy Director Carmen Medina.

40 Walton, p.508.

41 Omand, p.31. underplays the role of open sources, regarding them as traditionally serving as a cross-check for covertly obtained information, but much tactical military intelligence has been open – although often requiring risk and effort to get it.

42 Omand, p.32.

43 Sanger, pp.3-15.

44 Harriet Kay, Paul Keymer, Sarah Mackey & Shae Vickers, Fusing Intelligence and Strategy Capabilities: The MIQ Experience, *National Security Journal*, 5:2 (2023), doi 10.36878/nsj20230402.01

45 Jerry H. Radcliffe, *Intelligence-Led Policing*, 2nd Ed., Routledge (New York, London, 2016), p.4.

46 Alach, p.88; Angus Lindsay, Trevor Bradley & Simon Mackenzie, "Organisational barriers to institutional change: The case of intelligence in New Zealand policing," *The Howard Journal of Crime and Justice,* 61 (2022), pp.407-426, https://onlinelibrary.wiley.com/doi/full/10.1111/hojo.12486

47 See Smith, p.43. Smith argues only the FBI was a genuine HUMINT collector in the US prior to WWII.

48 Omand, p.52 discusses Canada's formation of the Canadian Security Intelligence Service (CSIS) in 1984 removing the intelligence function from the Royal Canadian Mounted Police (RCMP). A similar separation had occurred in New Zealand in 1956 removing security intelligence from New Zealand Police's Special Branch, conferring it to the newly formed New Zealand Security Intelligence Service (NZSIS). To underscore the point, however, both RCMP and NZP continue to have intelligence units.

49 Sam Mullins, Counter-terrorism in Australia: practitioner perspectives, *Journal of Policing, Intelligence and Counter Terrorism*, 11:1 (2016), p.99.

50 Sanger, pp.10-15.

51 See Barry Meier, *Spooked: The Secret Rise of Private Spies,* Sceptre (London, 2021).

52 Warner, p.17.

53 Omand, p.48.

54 Damien Rogers & Shaun Mawdsley, Reconfiguring the Relationship Between Intelligence Professionals and the Public: A First Step Towards Democratising New Zealand's National Security?, *National Security Journal*, 3:3 (2021), p.4., *10.36878/nsj20210929.02*