New Zealand
Institute of Intelligence Professionals

Intelligence Practitioner's

HANDBOOK

www.nziip.org.nz

Foreword

In 2008, when the New Zealand Institute of Intelligence Professionals was founded, one of the aspirations of the Institute was to assist in setting national standards for the profession. This booklet delivers on that aspiration, providing a foundational reference for intelligence practitioners nationally.

The Intelligence Practitioners Handbook is not prescriptive, nor directive. Instead, it offers a high-level guide which provides a basis to develop a shared understanding of our profession, including its ethical and tradecraft fundamentals. In other words, the Handbook provides a framework on which other, more detailed and specific intelligence practice can be built.

In terms of practical use, the Handbook is designed to serve as a generic guide, or kaiārahi, for practitioners. It is something that can be taken anywhere, to any employment context, and remain relevant. It provides a firm point of reference – a cardinal direction if you will – to aid practitioners in what is a dynamic career field, defined by uncertainty and ambiguity.

The Handbook also recognises the unique characteristics of intelligence in Aotearoa New Zealand, which is best reflected in the ethical framework established in the handbook. The Handbook has been built with the intention of blending mātauranga Māori and principally Western conceptions of intelligence practice in a manner appropriate to a New Zealand context.

Finally, while the Handbook is designed to capture and reflect the enduring nature of our profession, it is also a living document – intended to be updated in line with changes that occur in our professional context.

My thanks to all of those that assisted in the creation of the Handbook. You have made an important contribution to setting the standards of our profession in this legacy document. Without your breadth of experience and expertise drawn from the enforcement, security, and regulatory intelligence sectors, we would never have been able to complete this vital work. Thank you also to Paul Prouse from Astro Intelligence for his critical role in bringing together the profession's collective wisdom into a single document.

Dan Wildy

CHAIR

NEW ZEALAND INSTITUTE OF INTELLIGENCE PROFESSIONALS

Contents

Reading Notes

This handbook is written for intelligence analysts looking to improve their tradecraft and understanding of their role in the wider intelligence system. While it contains broader information, it is written for the perspective of an analyst. Additional handbooks for the equally important roles of intelligence collectors and intelligence leaders will look at similar topics contained here but from their perspective, emphasising their contribution to the effective functioning of the intelligence system in support of decision makers.

The best explanations and advice from multiple references and doctrinal publications have been used in these pages, along with hard won experience in the application of theory to practice. No single country, organisation, or agency has been used as an authoritative overarching source.

All information contained within is from unclassified sources and this publication remains unclassified.

Version 1.0, August 2023.

Intelligence Principles

1. **Decision-driven.** The output of intelligence is to provide an understanding of external factors that directly support organisational decisions about the commitment of people, time, and resources. The objective is to give decision makers at the appropriate level the relevant understanding to make informed and timely choices, with consideration for the context and potential consequences of their actions.
2. **Objective.** Due to the impact intelligence has on organisational decisions, the conduct of intelligence collection, analysis, and communication must be unbiased and impartial. Intelligence practitioners must avoid letting personal beliefs, bias, or external pressure influence their analysis to ensure that their conclusions are based on accurate and reliable data. Objectivity requires the courage to challenge assumptions and beliefs, and to present evidence that may contradict popular views.
3. **Predictive.** Intelligence is relevant when it anticipates developments and provides early warning of future events. This proactive approach allows decision makers to prepare for possible outcomes and to take appropriate action to mitigate risks or seize opportunities.
4. **Timely.** Timeliness is crucial in intelligence work as it ensures that decision makers receive relevant and up-to-date information to act proactively. Intelligence practitioners must prioritise tasks and manage resources effectively to deliver assessments when they are needed, allowing decision makers to respond promptly to emerging developments, threats, or opportunities.
5. **Continuous improvement.** Intelligence professionals should regularly evaluate and refine assessments, tools, and processes to enhance the quality and effectiveness of both intelligence outputs and the intelligence system. This includes learning from past successes and failures, and adapting to new technologies, as well as evolving operating environments.
6. **Ethical.** Members of the New Zealand intelligence profession are trained and vetted to work on sensitive matters and in areas of high trust. The public and decision makers expect these privileges to be exercised responsibly. Therefore, intelligence work requires adherence to a strong set of moral principles and professional conduct. Practitioners must act with integrity, respect sources' privacy, and ensure the information they gather and disseminate is lawful, accurate, and used for legitimate purposes. Intelligence professionals must also speak honestly and openly to decision makers.
7. **Integrated.** Intelligence assessments involve the collaboration and coordination of various intelligence disciplines, sources, and organisations. Combining different perspectives and expertise can provide a more comprehensive understanding of complex issues. Furthermore, to be relevant, the intelligence system needs to be integrated into organisational decision making processes.
8. **Source protection**. Source protection involves safeguarding the confidentiality and safety of sources who provide sensitive information. Applying manaakitanga ensures respect for the public and individuals, and supports the prevention of unnecessary harm. This includes implementing strict security measures, anonymising information when appropriate, and ensuring that sources are not put at risk due to the disclosure of their identities, or association with intelligence activities.

The Intelligence Cylce and Intelligence Systems

The role of intelligence

Intelligence is the product resulting from processed information. It aims to enhance understanding and reduce uncertainty to support decision making about future courses of action. This applies equally to supporting ministers and chief executives as it does to frontline staff.

Analysts, as part of this process within a wider team, interpret the requirements of decision makers and assemble information (unprocessed or unanalysed knowledge or data). Context is then applied to enhance understanding of the information, producing key assessments supported by facts and logic. To be relevant to the decisions that need to be made, key assessments are predictive, timely, actionable, and accurate. This is then formed into a product to be communicated to the customer.

The intelligence cycle

The intelligence cycle describes the process by which the decision maker's needs are interpreted, and how information is subsequently collected and transformed into assessments that support the customer's decisions. In its simplest form, there are three functional components to the intelligence cycle (see figure 1).

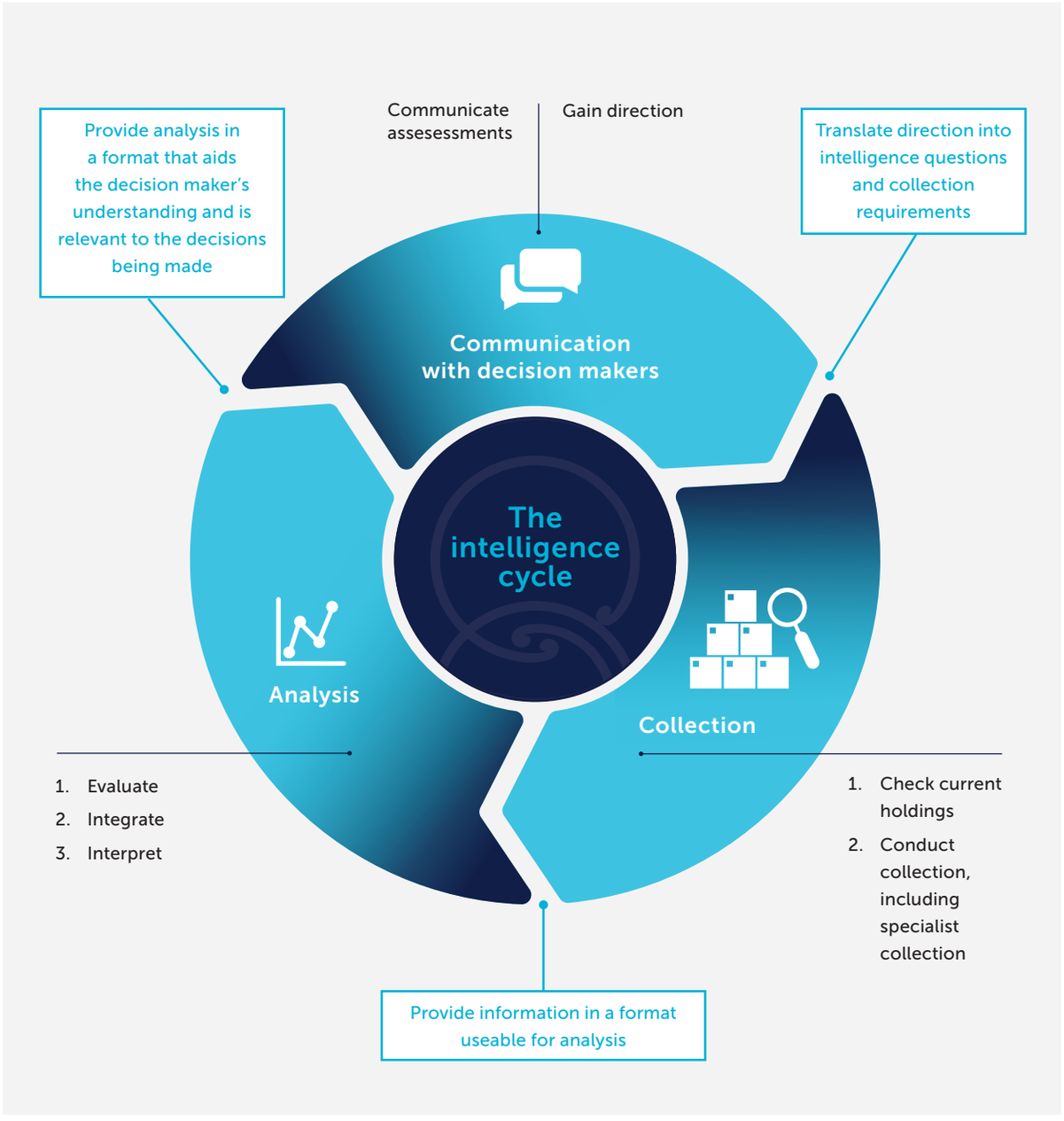
1. The intelligence cycle starts and ends at **communication with decision makers**. At the outset, intelligence analysts interpret what a decision maker has stated they require and transform it into tasks and terminology that all intelligence functional areas will understand. This initial step of understanding the customer's needs for content, timeliness, and their decision making context, is crucial to ensuring the final product is relevant and actionable.

2. During **collection**, information is gathered from a variety of sources. This can be through a review of current holdings and existing assessments, through tasking specialist collection elements, or a multitude of other methods available within the resources and authorities available to the organisation, including surveys, interviews, and a search of publicly available information.

3. As information is collected, **analysis** is conducted to answer the questions identified by the decision maker. This is done through several sub-steps to:
   a) Evaluate the individual pieces of information for accuracy and relevance.
   b) Integrate the individual pieces of collected information together, along with consideration of existing assessments and knowledge. This can be done through structured analytical techniques.
   c) Interpret the integrated information to identify patterns and predictions, and assess them against the decision makers' requirements and organisational goals to identify opportunities and threats.

4. (Or 1. again). The assessments resulting from analysis are **communicated to decision makers**. Further questions may arise from decision makers to initiate the cycle again. An implied task after the communication is to continue to use collection and analysis to monitor development of the predictive assessments. Based on this, updates can be provided about key milestones or changing trajectories, as well as the creation of new assessments. This phase provides the link between the intelligence system and the supported decision making process – between the intelligence cycle and the operations or policy cycle.

Figure 1. The intelligence cycle.



There are three linking actions that connect the different functional areas and phases of the intelligence cycle:

1. **Linking decision maker direction to collection.** Decision makers are rarely intelligence professionals. Intelligence professionals need to interpret the direction, needs, or concerns voiced by the decision maker into a format that can be used by both intelligence analysts and intelligence collectors. This begins by developing an intelligence question for analysts. Each intelligence question is then broken into collection requirements.[1] Intelligence questions can be either open or closed questions, while collection requirements are most effective when formed as closed questions. Closed questions (supported by the overarching context and intent) provide collectors with clear and achievable tasks and enable them to provide objective facts for the analysis phase. The overarching context and intent should be provided so some judgement can be applied by the collectors.

2. **Linking collection to analysis.** As information sets increase in size, the ease and speed of access and integration of information becomes more important. The output of collection should be in a format that is useable for the analysis phase, both immediate and for future intelligence tasks.

3. **Linking analysis to the decision maker.** For the analysis to be relevant to decision making, it needs to be timely and accurate, and provide a level of detail that enables action. Furthermore, it should be delivered in a manner that is appropriate to the individual style of the decision maker, making best use of verbal, visual, and written communication methods. Timely can also refer to the method of distribution – whether it is 'pushed' to decision makers as it is produced, or available for decision makers to 'pull' when needed.

There are variations of the intelligence cycle used by different New Zealand organisations. These usually add emphasis to functional areas by breaking them down into additional steps. The additional steps usually cover:

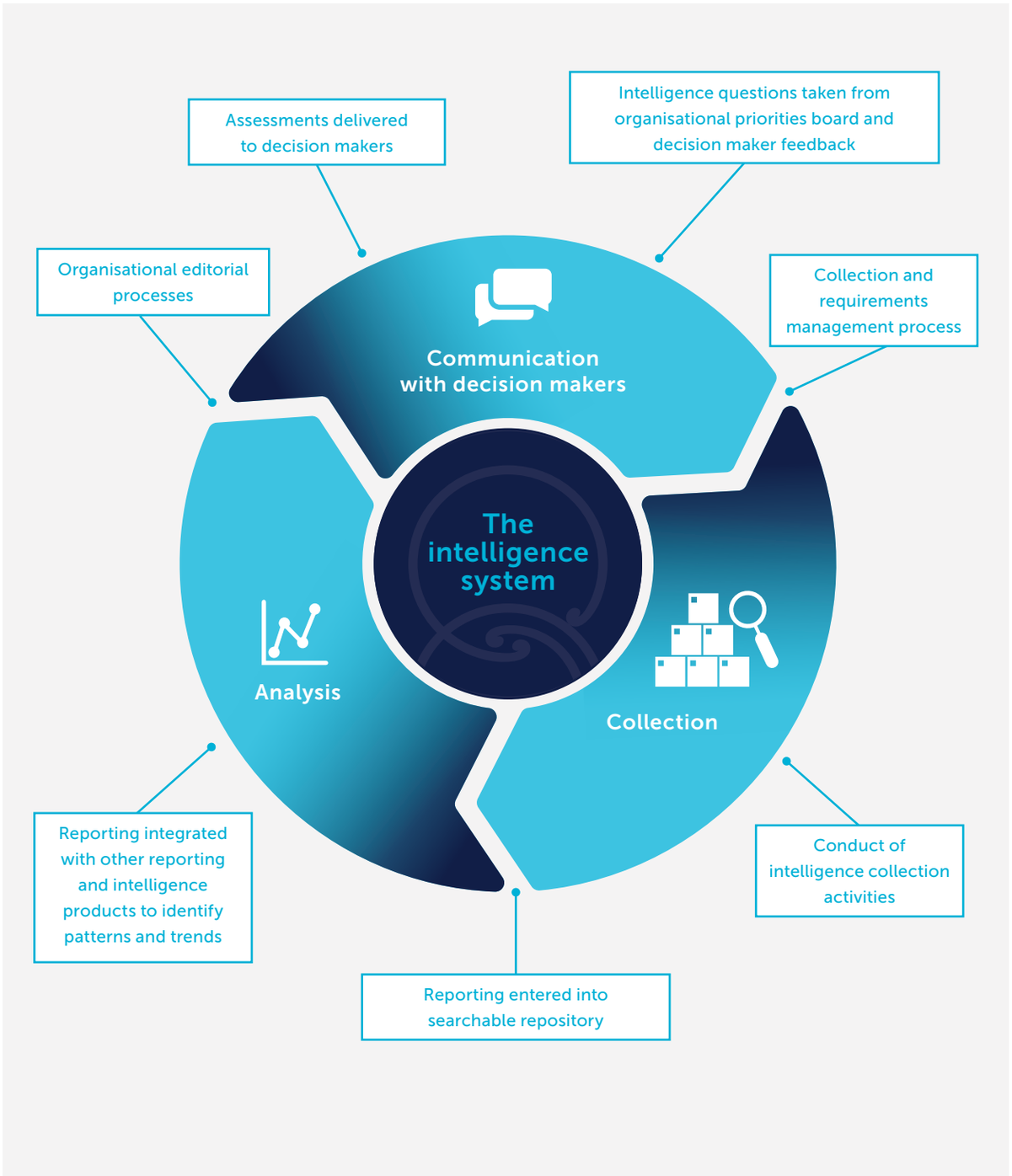
1. **Review.** To review the decision maker's guidance before starting collection or after communicating assessments. This can also mean to review assessments prior to communication to identify situational changes, and to ensure that they align with initial guidance. Furthermore, review of the overall process and final product, through feedback, group and self-reflection, ensures continuous improvement toward best practice.
2. **Requirements and planning.** Before collection occurs, a step is added to emphasise deliberate tasking and planning for intelligence collection operations.
3. **Processing and evaluation.** A step or multiple steps are added between collection and analysis to emphasise the evaluation of information before it is included in databases or integrated with other information. Here, processing refers to the broad process of evaluating and organising information.

1 For complex situations, an intelligence question may have to be broken into sub-questions or topics. These sub-questions can then be turned into collection requirements.

Intelligence systems

All systems are composed of three parts: components, interconnections, and a purpose. An intelligence system refers to the processes, tools, and people that are the practical application of an intelligence cycle. These systems can be permanent or can be assembled for certain events. In either case, they comprise people from multiple disciplines to cover each functional area. In larger organisations, each function may have its own internal systems.

Figure 2. Intelligence as a system. Linking disparate disciplines into a whole and linking that to the decision making process through effective communication.

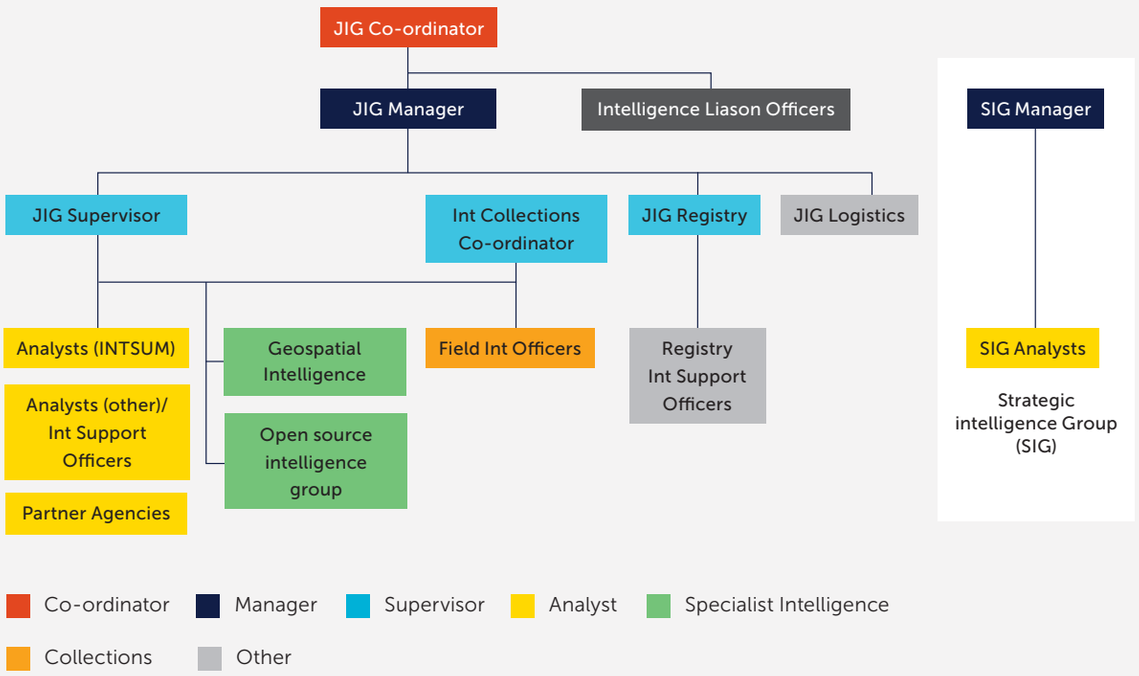


An Analyst's Role in the Intelligence System

Intelligence is a multi-disciplinary team endeavour to support decision makers. While an analyst specialises in the analytical functional area, they need to also understand how they fit into, rely on, and support the wider system. Key linkages are:

- Defining the problem. At the outset it is crucial to interpret the decision maker's needs. Have a clear understanding of what the final product will be used for. This will involve engaging with the customer and/or intelligence managers to start with the right question.
- Working with the organisation's collection requirements and management system to review current holdings and to task collection if required.
- Understanding the strengths and limitations of different types of collection disciplines to evaluate incoming information and reporting.
- Drawing on peers and deliberate analytical methods when integrating and interpreting information to reduce potential bias during the analytical stage.
- Submitting products to organisational review and editorial processes, checking for bias, accuracy, and relevance.
- Deliver assessments to decision makers and interpret further tasks.

Figure 3. The Joint Intelligence Group (JIG)



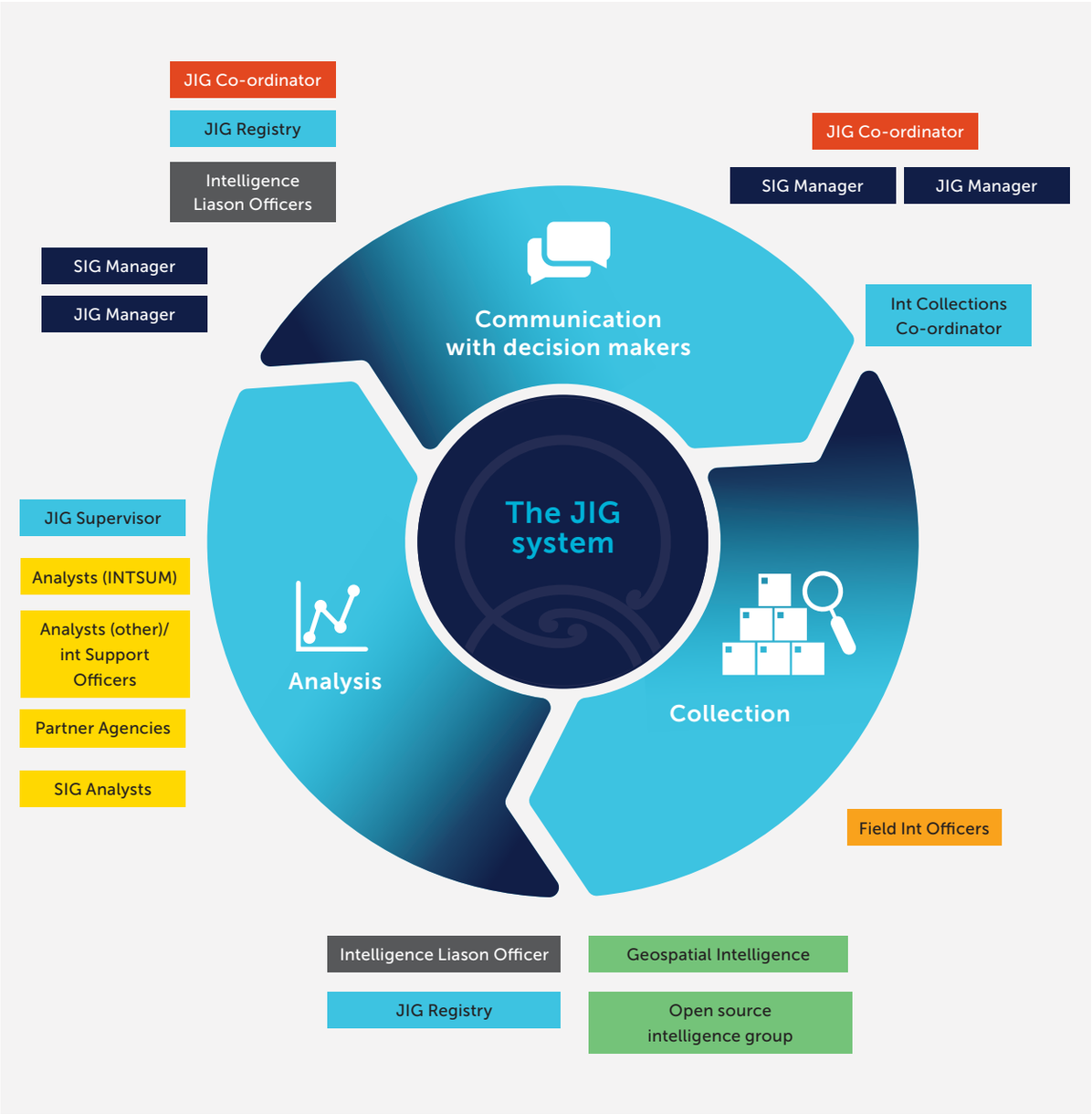
Case Study: The Joint Intelligence Group

The Joint Intelligence Group (JIG) is an example of a scalable multi-agency intelligence system that is established in New Zealand in preparation for or response to major events.

In March 2020, a JIG was set up to support the Operational Command and Coordination Centre (OCCC) as part of New Zealand's response to the Covid-19 pandemic. The JIG was led by the New Zealand Police and consisted of multiple agencies as diverse as the NZDF, MPI, Customs, DPMC, New Zealand Intelligence Community, Worksafe, and many more. At its peak, the JIG numbered 61 intelligence professionals, and continued its support throughout the pandemic.

It provided strategic and operational intelligence in support of national decision making through the crisis response phase in early 2020, adapting and scaling to decision maker needs as the response normalised. The JIG provided assessments on everything from infection rate projections, efficacy of various overseas response settings, the potential of different technologies to support tracing, impacts on mental health, and how the public would respond to potential scenarios.

Figure 4. The JIG depicted as an intelligence system.



Note: Analysts may be the ones carrying out the communication, but managers assist in initially defining the questions and providing guidance and quality control on how the resulting assessments should be communicated. (The arrangement of tiles here does not suggest a hierarchy within the JIG.)

Specialist areas of collection

Robust intelligence assessments result from the fusion of information from different sources. There are multiple disciplines within the collection function that require specialist training and governance. Intelligence analysts should understand the strengths and weaknesses of each collection discipline. This can be gained through formal or informal engagement with the collectors themselves, post-project evaluation of sources, and learning from the experience of senior analysts and managers. Furthermore, to prevent information overload it is important to have a clear and rapid evaluation process that determines the accuracy, relevance, and source of new reporting.

The main collection disciplines	
	**Human intelligence** (HUMINT) involves the collection of information through direct contact with individuals who have access to relevant information, either through overt or covert means. HUMINT operations can be risky and resource-intensive, and there is always the potential for human sources to provide false or misleading information intentionally or unintentionally.
	**Signals intelligence** (SIGINT) involves the interception and analysis of electronic emissions, such as radio signals, satellite transmissions, and digital communications. SIGINT is typically collected through a variety of methods, including passive and active interception of communications, analysis of communication networks, and decryption of encrypted messages. It is broken into two subsets, the interception of communications-based signals (COMINT) and non-communications based electronic signals (ELINT). There are ethical and legal considerations that must be considered when conducting SIGINT, particularly with respect to privacy and civil liberties.
	**Geospatial intelligence** (GEOINT) combines traditional intelligence methods with geospatial information, such as satellite imagery and maps, to produce intelligence products. GEOINT normally requires the components of data collection, data management, data analysis, and visualisation.
	**Imagery intelligence** (IMINT) is a subset of GEOINT and is often used in conjunction with other types of geospatial data. IMINT is specifically focused on the collection and analysis of imagery data, which can include satellite imagery, handheld imagery, full motion video, and aerial photographs.
	**Open source intelligence** (OSINT) sources include a wide range of publicly available information, such as news articles, social media posts, government reports, academic research, and public records. To conduct OSINT effectively requires specialist skills and training. OSINT is a valuable tool for gathering information that is not classified or restricted, which can aid in wide communication to decision makers. However, OSINT can also be subject to inaccuracies, biases, mis- and disinformation and other limitations, particularly when the sources of information are unreliable or unverified.

Types of Intelligence Output

Basic Intelligence. This provides foundational and factual reference material on a situation, event, entity, or issue. It can encompass such things as countries, people, geography, organisations, infrastructure, and culture. Basic intelligence is often referred to as encyclopaedic knowledge from which other types of intelligence are developed.

Current Intelligence. Current intelligence reports on new developments, providing up-to-date and timely information on unfolding events. It contextualises this information within broader trends and assessments, highlighting their significance, and warning of unexpected departures. The time period is tailored to the decision maker's urgency, ranging from monthly to real-time monitoring.

Estimative Intelligence. Estimative intelligence offers comprehensive, long-term assessments. It integrates analysis of past and present data, expert knowledge, and predictive analytical techniques to determine potential outcomes and their likelihood. Estimative intelligence assists decision makers in anticipating and strategically planning to shape future scenarios.

Case Study: Intelligence during the First Taranaki War, 1860 to 1861

The First Taranaki War took place from March 1860 to March 1861 between Te Ātiawa, led by Wiremu Kīngi and British colonial forces over disputed land sales and the wider issue of sovereignty. Te Ātiawa were supported by other Taranaki and Waikato iwi at various stages. Kīngi's forces were able to quickly lay siege to the nascent settlement of New Plymouth and continuously gain advantage over British troops until a negotiated settlement temporarily ended the conflict.

Te Ātiawa maintained very good knowledge of the location, numbers, and equipment of British forces, their commanders, and their preferred tactics. This basic intelligence was gained through human sources allowed to move around the British camps, from local newspapers, and from their own scouts. Additionally, all Māori had a good knowledge of the tracks and local geography in the region. These sources also reported when British troops left their camps, including the composition and direction of travel. When this information was added to their knowledge of the local geography and the weather at the time, it created a current intelligence picture of British intentions over the coming few days, including the likelihood of an attack at certain locations.

Te Ātiawa and supporting iwi were outnumbered by British forces throughout the conflict. However, their estimative intelligence enabled effective decision making to gain advantage over the larger force throughout the campaign. They maintained 20-30 fighting pā and fortified villages to effect the siege of New Plymouth, but would most often withdraw from these locations if a defeat was assessed as likely. Te Ātiawa had such a good understanding of British tactics that the battles that took place were regularly at a time and location of their own choosing, inflicting significant defeats and humiliation on the British forces and the wider colonial government.

Intelligence Support to Different Levels of Activity

The type of intelligence support provided to decision makers is influenced by their level of authority, available resources, and the effects they intend to achieve. Strategy, operations, and tactics form hierarchical levels of planning and execution used in government, security services, business, and other domains. Strategy sets the overall direction, and the operational level translates strategic goals into specific objectives and synchronises tactical actions to achieve them. The tactical level is where physical actions are carried out. The levels are interconnected with all actions directed toward a common purpose and clear outcomes. While accuracy is essential for intelligence outputs at all levels, the detail necessary for effective decision making and action varies across each level.

Distinctions between levels are not always strictly defined, and intelligence support may overlap depending on the situation. Strategic trends may influence the adoption of new tactics, and tactical outcomes may have operational and strategic effects. Tactical reporting collected over time can provide indicators of changing strategic trends. Flexibility and adaptability in intelligence are essential to meet the needs of decision makers at each level.

Figure 5. A guide to the different levels of activity and typical intelligence support.

	Level of Activity	Intelligence Support
STRATEGIC	• Strategy is the highest level of planning and focuses on long-term goals and objectives. • It involves formulating overarching plans and allocating resources to achieve those goals. • Strategic decisions are typically made by senior leaders and executives. • Actions at the strategic level include setting organisational direction, competitive positioning, and identifying key initiatives to achieve long-term success.	• Strategic intelligence support focuses on providing broad assessments and long-term trends. • Topics at this level often include high-level analysis of political, economic, social, and technological factors that can impact the organisation's strategic direction and positioning. • Communication may involve estimative assessments, risk analyses, and scenario-based reports that inform senior decision makers about the global, national, and macro-environment. • Timeframe is normally measured in years.
OPERATIONAL	• Operations sit between strategy and tactics, translating strategic goals into synchronised practical actions. • They encompass medium-term plans and actions to achieve strategic objectives. • Operations involve the coordination and deployment of resources and units. • Operational decisions are made by mid-level managers. • Actions at the operational level include developing campaign plans, organising resources, and coordinating large-scale actions to achieve specific outcomes.	• Operational intelligence support provides more detailed information to support planning and execution. • Topics at this level include analysis of specific regions, actor capabilities, and environments relevant to the organisation's plans and objectives. • Communication may involve estimative assessments, situational updates, and intelligence briefings that help mid-level managers and commanders make informed decisions and adjust plans as needed. • Timeframe is normally measured in months.

	Level of Activity	Intelligence Support
TACTICAL	• Tactics are the lowest level of planning and execution, focusing on immediate actions to achieve specific objectives. • They involve detailed plans for small-scale actions and engagements. • Tactics are implemented by front-line personnel, such as soldiers, employees, or individual teams. • Tactical decisions are made by those directly involved in executing the plans. • Actions at the tactical level include executing specific missions, deploying forces in the field, and employing specific techniques to achieve immediate objectives.	• Tactical intelligence support focuses on providing real-time or near-real-time information for immediate decision making at the frontline. • Topics at this level include geographical factors, situational awareness, and specific entity or mission-related information. • Communication often involves tactical reports, mission briefings, and intelligence updates that assist frontline personnel in executing their tasks efficiently and mitigating risks. • The timeframe is normally days to real-time.

Note: The timeframe is less important than the level of responsibility, resources, and authorities of the decision maker using the assessment.

Practical tips to apply the intelligence cycle

- For a number of reasons, intelligence teams will not always receive clear or timely direction from decision makers, particularly during times of crisis. To be proactive, intelligence professionals should use their experience to produce intelligence questions and initiate the intelligence cycle, and then clarify these at the earliest opportunity with the decision maker. Intelligence professionals should also use their judgement to interpret what a decision maker has stated they require into tasks and terminology that all intelligence functional areas will understand. This requires familiarity with those decision making processes being supported.
- Due to the different internal processes and outputs sought by analysts and collectors, communication and feedback is important. Communication and feedback between the two allows collectors to gain a better understanding of what information is relevant, making collection more efficient, and allows analysts to discover new information from collectors that may not have been formally reported.
- Similarly, evaluation of information is often done formally or informally by specialist collectors as part of their internal processes. Collectors will have good insight into the reliability of sources. However, analysts still need to evaluate information during the analysis phase to determine what information is relevant to the current problem. This can occur during the integration and interpretation sub-steps, particularly where one piece of information may separate two competing scenarios. Again, communication and feedback to collectors will help improve collection.
- Technology can be used during the transfer of information from collectors to analysts, enabling automation of the integration sub-step. This gives analysts more time to focus on interpretation. Additionally, where current holdings are easy to review, a collection and requirements manager can reduce the need to commit resources to collection. Speeding up the intelligence cycle gives decision makers more time to act.

The New Zealand Intelligence Landscape

The largest body of intelligence practitioners in New Zealand's government sector is devoted to national security. The Government's National Security System has in recent years taken an 'all hazards – all risks' approach to national security, encompassing internal, external, human, and natural challenges. More recently, there has been a move towards a more traditional – and more contracted – conception of national security focused on territorial, political, diplomatic, military and economic aspects of security. Led by DPMC, a wide range of agencies contribute to the national security system, and through it, the safety and prosperity of New Zealand and New Zealanders.

While government agencies play a central role, local government and the private sector are a growing component of New Zealand's intelligence landscape. As early as 2003, the Auditor General stated in a review of New Zealand's domestic security that "local government, quasi-government agencies, and the private sector have increasingly important roles". Moreover, New Zealand's private sector increasingly values intelligence to navigate complex markets, regulatory changes, and global economic shifts. Digital technologies and data analytics improve data-driven decisions, but also bring increased risk from cyber threats.

In a country of New Zealand's size, coordination and cooperation is crucial to effective intelligence outcomes. The National Security and Intelligence Priorities define where intelligence can support government decision making. As of 2021, Cabinet has approved 13 broad priority areas. Most agencies will participate in the National Security System through attendance at formal multiagency governance boards, and in times of crisis through Watch Groups chaired by a designated Lead Agency. These support the Officials' Committee for Domestic and Security Coordination (ODESC) attended by Chief Executives. Analysts may be asked to support their officials attending any of these groups.

At the operational level, a Joint Intelligence Group (JIG) may be established in preparation for or in response to major events to coordinate multi-agency intelligence efforts (this is described in more detail above). Analysts may participate as part of a JIG or may be supported by the JIG as they assist a local level response. In a country of New Zealand's size, even without these formal structures for major events, kotahitanga, through lateral communication and proactive cooperation between different organisations, is central to effective intelligence support.

An ongoing issue in the intelligence community is data collection, storage, and privacy. In particular, Māori data is a taonga that requires protection and care. As such, a Māori Data Governance Model has been co-designed by government agencies and Māori data experts for use across the Aotearoa New Zealand public service (Kukutai, et al., 2023). This is an example of adherence to the principles of Te Tiriti o Waitangi in action, a consideration for all public sector work from which the intelligence profession is not exempt. During a natural disaster, for example, communities in need may be unwilling to share their information and needs without trust and assurance that this data will be treated with respect.

Ethical Standards

The purpose of ethical behaviour

Professional ethics refer to the moral principles that guide conduct and behaviour in a particular field. They are a set of standards that govern actions and decisions and help to ensure that members act in a manner consistent with their profession's values and norms. Ethics, along with other professional standards such as training and education, are the foundation of a professional tikanga.

Members of the New Zealand intelligence profession are trained and vetted to work on sensitive matters and in areas of high trust. The public and decision makers expect these privileges to be exercised in an ethical manner. As the operating environment for the New Zealand intelligence community continues to evolve, the public deserve sustained high levels of safety and adherence to the principles of Te Tiriti o Waitangi, alongside greater transparency and assurances of privacy.

A code of ethics guides practitioners in situations of moral ambiguity, or where there is an absence of a legal requirement, set of rules, or protocol. In these circumstances, ethics promote responsible and trustworthy behaviour, protect stakeholders, and enhance public confidence.

While organisational values will overlap with professional ethical behaviours, they differ in purpose. Organisational values seek to align multiple professions and functions to its own vision and outcomes. Intelligence professional ethics guide common behaviour to maintain public trust in the intelligence community, and apply throughout an individual's career, regardless of the organisational context. Intelligence practitioners have a responsibility to uphold the values and outcomes of the organisation they support, as well as the professional body they represent.

At an individual level, ethical behaviour complements other wellbeing initiatives. Intelligence professionals often face challenging situations in the conduct of their work. Maintaining professional integrity and upholding ethical behaviours can promote personal satisfaction, reduce stress and anxiety, and foster positive relationships. With practitioners of varied backgrounds and experiences, a shared code helps to unite professionals across the intelligence community.

Ethical dilemmas are not black and white. Laws can answer the question "can we?" whereas ethics help to answer the question "should we?" and to identify where "the line" may be before it is crossed. By understanding who they have a responsibility to, the nature of that responsibility, and through application of ethical behaviour, intelligence practitioners are enabled to make professional and ethically sound decisions in diverse and difficult situations.

Responsibilities to stakeholders

Intelligence professionals have a responsibility to three key stakeholders: the public, decision makers, and the profession itself. The nature of the relationship is different for each stakeholder, but each place their trust in the intelligence practitioner to carry out their work in an ethical manner.

The Public. In both government and the private sector, intelligence activities are ultimately carried out in the public's interest. The public place a high degree of trust in the professionals who work in this sector, expecting their activities to be lawful and to contribute to public safety and wellbeing. There is an expectation that intelligence activities will be conducted only when necessary, with effective use of resources, respect for privacy, proportionality, and accountability for mistakes and failures.

Decision Makers. Decision makers provide resources, authority, and direction to intelligence professionals. In return, decision makers expect timely, accurate, and actionable intelligence that is relevant to their decisions. This intelligence assists them to achieve organisational goals, while also highlighting gaps in confidence and risks to those goals, resources, and personnel. Decision makers can include chief executives, operational staff, leaders outside an organisation, and sometimes individual members of the public. Intelligence professionals must be truthful and impartial to decision makers, regardless of the outcome of the decision, and have a responsibility to explain legal or ethical considerations relevant to an intelligence activity.

The Profession. Intelligence professionals perform a number of specialised and generalist roles that span many different organisations. Cooperation is required to carry out intelligence work, especially in New Zealand due to our small size. Furthermore, intelligence professionals rely on their peers to uphold ethical standards and maintain the credibility and trust granted them by the public and decision makers. This highlights the importance of trust and integrity within the intelligence profession.

Ethical behaviours

1. Kotahitanga

The concept of togetherness, kotahitanga is identifying as one. In an intelligence context, this means unifying as an intelligence team of many components and specialities and working with decision makers toward a task or organisational outcomes. Furthermore, practitioners should consider the need to share, where information or intelligence gained can assist another organisation or team. Kotahitanga also means participating in a community of practice, sharing skills, innovating, and providing support to other intelligence practitioners to advance the profession as a whole.

2. Manawanui

Intelligence problems can often be complex and more ambiguous than in other professions. Manawanui, as applied to the intelligence profession, emphasises the ideas of determination, thoroughness, persistence, curiosity, and resilience. It depicts the ability to work through internal and external uncertainty to continually provide high quality intelligence to support decision making.

3. Manaakitanga

The process of showing respect, humility, generosity, and care for others through propriety and a sense of responsibility. Respect for the public and individuals is exercised during collection and investigations by ensuring proportionality, necessity, and the prevention of unnecessary harm. Manaakitanga also closely supports kotahitanga. Respectful relationships, cooperation, and open mindedness encourage teamwork, and pursuit of higher standards. In each individual's pursuit of greater mana through learning and proper process, they enhance the mana of the profession overall.

4. Whakawā

The quality of being impartial and unbiased, providing assessments based on facts and evidence rather than personal opinions or beliefs. Intelligence professionals must speak honestly and openly to decision makers in positions of authority. Whakawā requires courage to challenge assumptions and beliefs – including self-awareness of one's own biases – and to present evidence that may contradict popular views. It supports the concept of 'speaking truth to power'.

5. Tapatahi

This encompasses the ideas of integrity, reliability, and diligence. In practical terms, tapatahi in the workplace means being honest in all interactions, maintaining confidentiality when required, respecting the authorising environment, avoiding conflicts of interest, fulfilling commitments, and taking responsibility for one's actions.

Analytical Techniques

The teaching of structured analytical techniques (SATs) as a deliberate package in New Zealand dates to the mid-2000s. This followed changes adopted by overseas partners to address flaws exposed in the intelligence analysis used to support the 2003 invasion of Iraq. Institutionalised instruction of SATs was introduced as well as a focus on understanding cognitive bias. Additionally, it became a standard requirement to record use of techniques in formal assessments as evidence of impartiality. Since then, additional checks have been built into intelligence workflows, such as peer and formal reviews, to confront bias systematically.

Structured analytical techniques (SATs) are one tool an analyst can use to integrate and interpret collected information to produce intelligence assessments. Analytical techniques aid in overcoming bias, encourage divergent or convergent thinking, and provide evidence to others for the conclusions reached. However, as with any tool, the quality of the final product relies on the knowledge, skill, and care of the people using it.

The benefits of structured analytical techniques	
	**For Analysts** • Help to organise seemingly disparate information. • Provide a tool to deliberately address human bias in the intelligence workflow. • Help to generate alternative interpretations. • Provide a guide to systematically step through an analysis from start to finish.
	**For Managers and Decision Makers** • Help to combine diverse viewpoints. • Aid in reducing bias. • Provide an audit trail to show how assessments were developed.

The following pages are an introduction only to cognitive bias and a quick reference guide to the most common SATs. There are many books, manuals, and training courses that cover these topics in further detail. Undergoing formal training to learn and practise SAT application is highly encouraged. One useful text containing over 50 SATs is *Structured Analytical Techniques for Intelligence Analysts* (Pherson and Heuer, 2020). Others are listed in the Further Reading section at the end of this handbook.

Bias and Heuristics

Bias in intelligence analysis refers to the influence of personal, organisational, cultural, or political factors on interpreting information. It can originate from internally held beliefs or be a product of the wider environment. Bias can result in a distorted or incomplete picture of the situation, which can cause serious miscalculation or errors in the allocation of resources when presented to decision makers.

In addition to bias, mental shortcuts can also negatively affect the interpretation of information. Mental shortcuts are also known as heuristics, taken from Richards J. Heuer, author of *Psychology of Intelligence Analysis* (Heuer, 1999). They are a natural part of how our brains have evolved to think and are used every day to simplify decision making and problem solving. Heuristics can be useful, allowing individuals to make quick and efficient decisions without having to engage in extensive analysis or evaluation. However, this simplistic and automatic decision making approach can lead to significant misinterpretations, particularly when the situation is complex or the information available is incomplete or ambiguous.

There are many types of bias and heuristics that can affect intelligence analysis, the most common ones include:

1. **Confirmation bias.** This occurs when an analyst selectively focuses on information that confirms their pre-existing hypotheses, while ignoring information that contradicts them.
2. **Cultural bias.** This occurs when an analyst's cultural background, values, or beliefs influence their interpretation of information. It leads to a distorted or incomplete understanding of the situation, particularly when assessing the interactions and decision making of other groups.
3. **Organisational bias.** This refers to the influence of an organisation's culture, structure, or incentives on the analysis of information.
4. **Political bias.** This occurs when political pressures influence the analysis of information, leading to a lack of objectivity.
5. **Mirroring bias.** Also known as projection bias, mirroring bias involves assuming that others think, feel, or behave in the same way that the analyst does. This bias can lead to inaccurate judgments or decisions, particularly where individuals from different cultures, backgrounds, or perspectives are involved.
6. **Hindsight bias.** The tendency of people to falsely believe after an event has occurred that they would have predicted the outcome beforehand. Hindsight bias can result in a distortion of memory, as people may unconsciously alter their recollection of past events to better fit with their current understanding. This bias can be particularly problematic for analysts as they may overestimate their ability to predict future events based on their knowledge of past events.
7. **Availability heuristic.** This involves making decisions based on the most readily available information, rather than conducting a thorough analysis of all available information.
8. **Representativeness heuristic.** This involves making decisions based on how well an individual, object, or situation matches a particular stereotype, rather than considering all available information.
9. **Anchoring heuristic.** This occurs when an initial value or piece of information is used as a reference point for making subsequent decisions, regardless of whether this value is relevant or accurate.

It is important for analysts to have an awareness of how their natural cognitive processes can introduce analytical errors into their thinking. Employing approaches that incorporate critical thinking and whakawā is crucial to reducing these errors.

SATs are one tool in the intelligence process to help analysts mitigate bias and heuristics. When conducted in groups, SATs further ensure that multiple perspectives and sources of information are considered. During all phases of the intelligence cycle, it is important to identify and address potential sources of bias, and to continually monitor and evaluate the reliability and accuracy of assessments and information sources.

Divergent and Convergent Techniques

Analysts generally face two common problems: combining seemingly unrelated pieces of information into a cohesive picture, and developing new perspectives regarding an established line of assessment. The former is common for analysts new to a topic, and the latter for those who have been involved in a topic for some time.

SATs can help analysts to think divergently or convergently about a problem.

- **Divergent techniques** help an analyst to think broadly and creatively. They generate a range of options, hypotheses, or scenarios. Brainstorming and scenario generation exercises are examples of divergent techniques, where the goal is to generate a wide range of outcomes or possibilities. Divergent analysis can be useful when there is a high degree of uncertainty or complexity in the situation, or to test established assessments.
- **Convergent techniques** help analysts to narrow down possible explanations to a single or reduced amount of options. They identify the most likely explanation from a particular set of information and data. Convergent analysis can be useful when there is a clear question to be answered, or when there is a need to narrow down a large number of possibilities. This is particularly useful where there are no established assessments, or when there is new or contradicting information.

SATs can be combined to first generate multiple hypotheses, before then converging on the most likely assessment. Some SATs contain both divergent and convergent steps within the same technique.

Key terms

Hypothesis. *A proposed explanation or prediction which is subject to further testing and validation.*

Bias. *Personal, organisational, or political factors that can influence collection and analysis of information leading to distorted assessments and lack of objectivity.*

Heuristic. *Mental shortcuts or simplified decision making strategies to quickly process and interpret information.*

Divergent thinking. *The process of generating multiple ideas or hypotheses that diverge from traditional approaches, to explore a wide range of possibilities.*

Convergent thinking. *The process of identifying the best supported hypotheses to converge on the most likely assessment.*

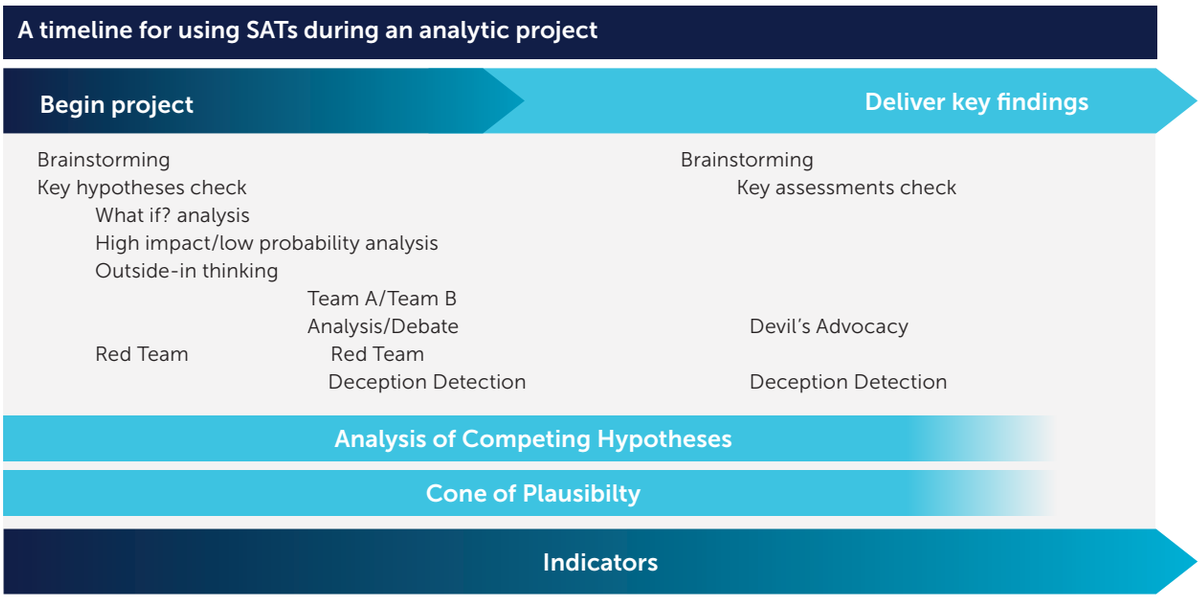
Selecting the right technique

Aside from situational factors such as time and resources available, the key selection criteria for which SAT to use is the intended outcome. There are four broad types of SAT by purpose:

- **Basic techniques** aim to organise information and are often used early in the analytical process. Examples are pattern analysis techniques, link analysis, and event mapping.
- **Diagnostic techniques** aim to critically analyse hypotheses, key assessments, the weight of evidence, and to identify information gaps. Examples include key assumptions checks, analysis of competing hypotheses, and back-casting.
- **Contrarian techniques** are used to deliberately challenge current thinking. Examples are red teaming and the six thinking hats.
- **Creative thinking techniques** support divergent thinking to generate multiple scenarios, new insights, or develop different perspectives.

Multiple methods can be used at different stages throughout an analytical project. Diagnostic and contrarian techniques directly challenge possible bias. Basic and creative thinking techniques help to organise thoughts and evidence, as well as promote new perspectives.

Figure 6. Adapted from A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis, Heuer and US Government, 2009



Additional tools to overcome bias

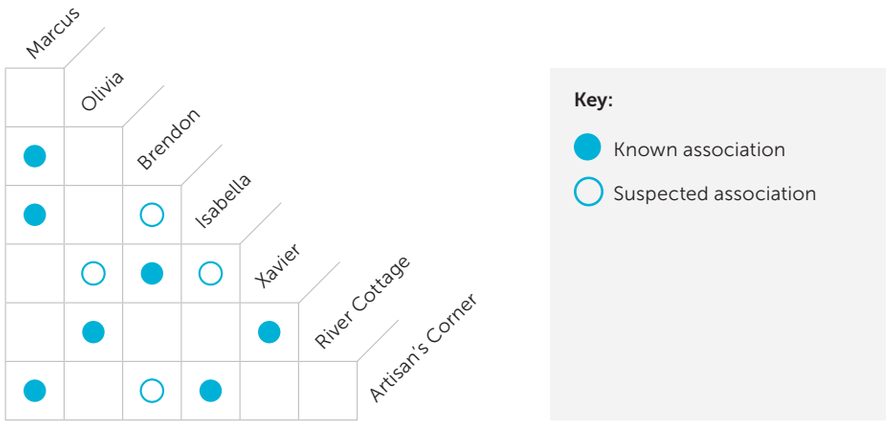
- Make a 'bias check' a deliberate action item as part of the quality control and editorial process when reviewing intelligence products.
- Consider discussion of bias as part of formal or informal performance management meetings, including deliberate self-reflection by analysts.
- Manawanui, whakawā, and tapatahi are all professional ethical behaviours that seek to address both external and internal bias.

Pattern Analysis Techniques

At the tactical level, there are a broad range of techniques that can be used to determine patterns. Plotting reports against time and space provides a visual which aids in the identification of trends, supporting understanding and prediction. Note that patterns will not always be present, and be aware of such biases as illusory correlation, where a link is seen between two unrelated events that does not exist.

Association Matrix. Useful for understanding organisations and networks, including the role and influence of different people and the relationship between different entities or events.

Figure 7. Example association matrix



Steps:

1. Gather information and data regarding people, places, items, or events.
2. Identify links between the entities or events from reporting and mark either known or suspected relationships at the box where the two entities meet on the matrix.
3. Interpret the links to make assessments. Consider which entity is central to the network, what role each entity plays in the network, the nature of relationships, and the gaps in knowledge.

Time Pattern Analysis. Useful for identifying patterns in time, particularly with data where there may be seemingly large gaps between similar events. Time pattern analysis tools can identify patterns in the time of day, day of the week, or time of the month.

Steps:

1. Gather information to be analysed.
2. Organise the information sequentially and into groups of similar types of activity.
3. Plot the events onto the various time pattern analysis tools.
4. Interpret the groupings to make assessments about clusters of similar events. This can include the time period in which the activity is likely to occur.

Consider additional information or make assessments about the causal relationship between the time and the activity.

Spatial Analysis. Involves the examination of geographic patterns and relationships. It aims to gain insights into spatial data by exploring how different elements are distributed or related geographically. Spatial analysis can be performed using Geographic Information Systems (GIS) or through manual methods.

1. Manual methods involve plotting the locations mentioned in reporting onto mapping. This can be useful for preliminary analysis or quick assessments.
2. GIS requires specialised software and is usually conducted by specialists with technical training.

Figures 8 and 9 below show the same information presented in two different time pattern analysis tools. The time wheel compares days of the month in concentric circles with the time of the day in segments. The analysis shows protests occur between 1400-1600 and intimidation occurs between 2000-2300. There is no clear pattern for robberies. The Day of the Week graph shows that protests occur exclusively on a Sunday.

Figure 8. The Time Wheel

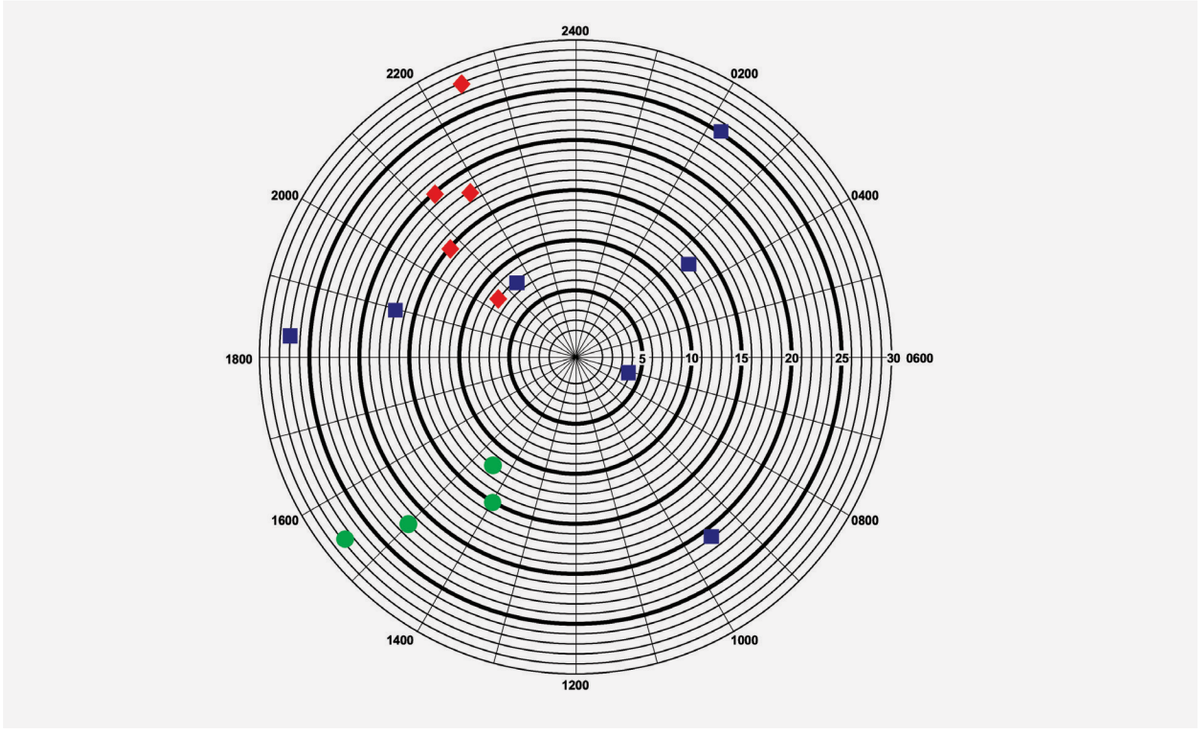
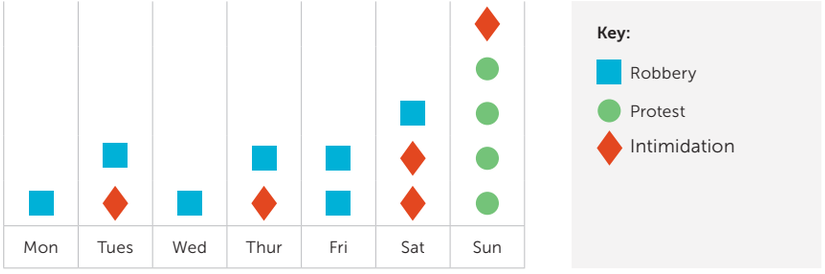


Figure 9. Day of the Week Graph



Brainstorming

Background: Brainstorming is a simple and often underrated divergent analytical tool. It can be used to generate a wide range of options, or simply to collect the thoughts of the group in a single space. It is a good technique to generate inputs prior to a more involved SAT, or even in the middle of a SAT to collect everybody's thoughts before moving on.

Steps:

1. **Define the problem or challenge.** Clearly define the problem that you are seeking to address. Include any context or background information but be wary of indirectly putting limitations on participants.
2. **Set the ground rules.** Establish ground rules for the brainstorming session. These could include encouraging all participants to share their ideas, refraining from criticism or judgment, and building on each other's ideas.
3. **Generate ideas.** Encourage participants to generate as many ideas as possible, without worrying about the quality or feasibility of the ideas. This can be done through a variety of techniques, such as free-form brainstorming, mind mapping, or idea cards.
4. **Categorise ideas.** Once enough ideas have been generated, group them into common categories or themes.
5. **Refine and develop ideas.** Once the ideas have been grouped, work on refining and developing the most promising ideas. This may involve further research, analysis, or collaboration with other stakeholders.
6. **Evaluate and select.** Finally, evaluate and prioritise the refined ideas and select the ones that will be taken forward.

Tips for a successful brainstorm:

- Conduct a short brainstorm with the group on an unrelated topic to 'warm up' prior to the main event. This can break down any stand-off behaviour, loosen up participants' minds, and set the tone for an open forum free from judgement.
- Conduct a silent brainstorm before opening the floor. Give each participant a few minutes at the start of the idea generation phase to write down their ideas and bring them to the facilitator or central display. Then proceed with an open floor verbal brainstorm. This allows people who may be nervous about speaking in a group to contribute, as well as avoiding the group being dominated by one or two people.
- The conclusion of the categorisation step can be a good place to stop and move to different techniques or reconvene later.

Analysis of Competing Hypotheses (ACH)

Background: ACH is a technique used to evaluate multiple hypotheses or scenarios against a set of available information. This is a convergent technique, helping analysts to determine which hypotheses are contradicted by the evidence and which are supported. The process forces analysts to systematically examine their initial working hypotheses against the evidence, while also critically evaluating the evidence itself. ACH output is also useful in identifying critical gaps to help plan further collection. Furthermore, the process aids in structuring the final product by providing a logical list of facts to support the assessment.

Steps:

1. Identify and clearly define the problem or question to be analysed.
2. Collect the evidence that will be used.
3. List all the possible hypotheses for the problem or question (this can be conducted through a brainstorm or other scenario generation SAT).

4. Evaluate each piece of evidence against the hypotheses and assign a value that indicates if the evidence supports, neates, or is not relevant to the hypothesis.
5. Identify any gaps in the evidence and determine what additional information or data is needed to fill those gaps.
6. Confirm or rule out the individual hypotheses.

Figure 10. Example ACH.

	H1	H2	H3	H4
Evidence 1	++	+	+	NR
Evidence 2	NR	++	NR	NR
Evidence 3	+	+	+	+
Evidence 4	-	++	+	NR
Evidence 5	NR	NR	++	++
Total	-	6	5	3

H each hypothesis being tested
\+ the evidence supports the hypothesis
(++ means the evidence strongly supports it)
NR the evidence is not relevant to the hypothesis
– the evidence negates the hypothesis

In this scenario:

- H1 can be discounted because E4 indicates contrary evidence.
- E3 is not useful and can be removed because it supports all hypotheses.
- H2 and H3 are close in total scores. The evidence should be re-examined to determine its accuracy and weighting, particularly E2. Further evidence should also be collected if possible.
- Consider if there are factors from H3 that support H2, such as an influential stakeholder working to support H2.

ACH is also a useful tool for monitoring the development of assessed scenarios. Determine what indicators are expected to confirm its trajectory, task these as collection requirements, and then record the information against the indicator as it is reported. The weight of positive indications will indicate the most likely developing scenario.

Tips for a successful ACH:

- The hypotheses that are being compared can be detailed or broad. The main factor is that they are distinguishable from each other.
- Where a piece of evidence negates a hypothesis, and you are confident in the accuracy of the evidence, this indicates that the hypothesis can be ruled out. Otherwise, the evidence should be recorded as not relevant or left blank.
- If a piece of evidence supports all hypotheses, then it is not a useful piece of evidence. However, you are unlikely to determine this until going through all steps above.
- At step 6, consider if hypotheses can be combined into a new assessment or hypothesis due to causality or stakeholder relationships.
- Revisit the ACH as new evidence arises. Be aware of the anchoring and availability heuristics.

Cone of Plausibility

Background: The cone of plausibility is a comprehensive divergent thinking technique. It is intended to help analysts overcome hindsight bias and generate a range of possible futures, including best case, worst case, and wildcard scenarios. It can be particularly useful in situations where the future is uncertain or where there is a need to anticipate potential opportunities and threats. Alongside intelligence analysis, it can also be used for futures thinking and risk management.

Steps:

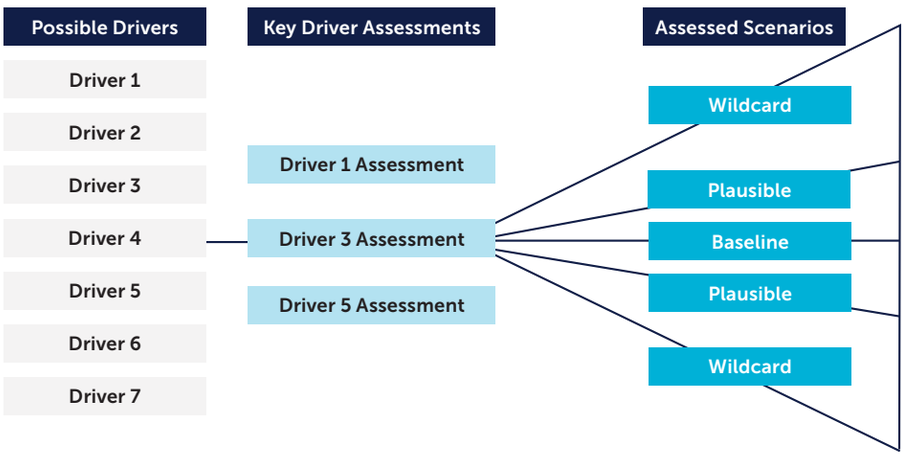
1. Define the parameters of the question to be answered. This should encompass how a situation or group will develop over a set timeframe.
2. Identify key drivers or influences on the issue in question. Consider other divergent thinking techniques, such as brainstorming, STEEPLED (social, technological, economic, environmental, political, legal, ethical, and demographic), or other methods relevant to the subject.
3. Make assessments about how these drivers are likely to individually develop over the chosen timeframe.
4. Generate a most probable scenario by extrapolating the interaction of the individual driver assessments into a single assessment. This is the 'baseline' scenario.

Generate one or more alternative scenarios by changing one or more of the driver's assessments, including plausible alternatives, worst case scenarios, and or low probability 'wildcard' scenarios.

Tips for a successful cone of plausibility:

- There is no minimum or limit on the number of drivers required to conduct the cone of plausibility analysis. It is recommended to use 5-7 drivers; complex situations require more, rather than less, for more robust assessments.
- The change in drivers to generate alternative scenarios provides useful indicators to task collection and monitor the development of baseline, worst case, and alternative scenarios.
- Completing this process can be time consuming as a group activity, particularly with multiple subject matter experts. Consider breaking the activity into different stages to avoid cognitive culmination of the group. A possible structure is to generate the drivers and their assessments, then formulate the scenarios as an individual effort before providing them back to the group for review.

Figure 11. Process Flow of the Cone of Plausibility



Step 1: Define the question and parameters

Intelligence Question:
How will the cyber threat environment develop in New Zealand over the next five years?

Step 2: Identify key drivers

- Supply chain attacks
- Growing Dependency on Cloud Services
- Cybercrime-as-a-Service
- Internet of things vulnerabilities
- Skill shortages in cybersecurity
- Collaboration and information sharing
- Attacks targeting small to medium enterprises
- Privacy and data protection regulations
- Heightened Focus on Critical Infrastructure Security
- Increased Digital Transformation
- Increased awarenes and education
- Sophistication of Nation-State Threats

Step 3: Make assessments about each key driver and how they will individually develop over the timeframe

Increased Digital Transformation: The ongoing digital transformation of various sectors in New Zealand, such as healthcare, finance, and government, may lead to an expanded attack surface and an increased risk of cyber threats.

Growing Dependency on Cloud Services: The adoption of cloud services by businesses and organisations in New Zealand may introduce new cybersecurity challenges, including data breaches, misconfigurations, and supply chain attacks.

Cybercrime-as-a-Service: The availability of cybercrime-as-a-service offerings on the dark web could lower the barrier to entry for potential attackers in New Zealand, leading to a rise in cybercriminal activities such as ransomware attacks and data breaches.

Sophistication of Nation-State Threats: New Zealand may face an increased risk of sophisticated cyber threats from nation-states seeking to gain access to sensitive government information, critical infrastructure, or valuable intellectual property.

Heightened Focus on Critical Infrastructure Security: As New Zealand's critical infrastructure becomes more digitised and interconnected, protecting essential services, such as power grids and transportation systems, from cyber threats will become top priority.

Targeted Attacks on SMEs: Small and medium-sized enterprises (SMEs) in New Zealand may be targeted by cybercriminals due to their potential vulnerabilities and limited cybersecurity resources. Such attacks could range from ransomware incidents to business email compromise (BEC) schemes.

Step 5B: Repeat Step 5A with another driver or multiple drivers to generate further scenarios, including 'wildcard' scenarios

Wildcard (successful international cybersecurity treaty): The international treaty forms the basis for increased international collaboration, with targeted efforts to dismantle the infrastructure supporting non-state actors. While some nation-states continue to use cyber attacks as a weapon of influence, they are increasingly easier to mitigate, particularly with shared cyber defence techniques and the ability for the government to shift investments into supporting the private sector.

Step 4: Combine the key drivers into a single scenario to determine the baseline

Baseline: Over the next five years, as New Zealand increases digital transformation, the convergence of increased digital connectivity poses significant cyber threats. Compliance with privacy and data protection regulations become challenging for SMEs, creating vulnerabilities for cybercriminals to exploit. Cybercriminals, including nation-state actors, exploit the expanded attack surface and limited cybersecurity resources of SMEs, launching sophisticated attacks such as phishing, ransomware, and supply chain compromises. These targeted attacks on SMEs result in financial losses, reputational damage, and disruptions, potentially affecting critical infrastructure and larger organisations.

Step 5A: Alter the assessment for a single driver (for example, 'flip' it to the opposite) and recombine the drivers into an alternative scenario

Alternative (no focus on critical infrastructure security): Over the next five years, New Zealand increases digital transformation and digital connectivity but pays no attention to cybersecurity or compliance with privacy and data protection regulations. Vulnerabilities in SMEs exacerbate attack surfaces for cybercriminals and nation-states. This leads to financial losses, disruptions, and risks to essential services. The cumulative effect undermines public confidence in service providers and the government in general, leading to the need for significantly more government spending in cyber defence for the private sector.

General tips for a successful analytical session

- **Clearly define the problem.** Some SATs are relevant to the analysis of specific situations only, such as the analysis of groups or scenarios. Ensure the problem being analysed is clearly defined before selecting the technique and is communicated at the beginning of the session. This normally includes a set time period that is being assessed.
- **Group size.** While working in groups supports diversity of thought, large groups can become unwieldy and lead to analytical inertia. As an anecdotal guide, an ideal group size is the number of people that can fairly share between one packet of biscuits and two regular pizzas.
- **Time limits.** As a guide, analytical sessions that are longer than one hour can result in cognitive culmination and risk introducing negative heuristics. However, some techniques or a large volume of content require longer periods of time to work through. Consider deliberate facilitation to keep the group on track, or breaking sessions into stages to ensure the time available is used effectively.
- **Group selection.** Diversity of thought is a great strength of SATs, leading to more robust assessments. Diversity can be achieved through inclusion of non-subject matter experts, including operational staff outside the intelligence function. These 'randomisers' can work to interrupt bias and heuristics related to status quo thinking. Availability of key participants is another practical consideration that will affect time factors.
- **Facilitating inclusion.** The facilitator has a key role in allowing every group member a chance to contribute. Groups can sometimes be overtaken by one or two strong voices. Methods to combat this include silent brainstorming (see brainstorming section), going around the room one by one for input, and singling out group members who have not spoken in a while, potentially through targeted questions on topics that have not been mentioned.
- **Equipment.** Post-its, coloured pens and whiteboards help to visualise information and promote divergent thinking.
- **Review and Acknowledgement.** Whether or not group members are included in the drafting phase post-SAT, including them in the peer review will help incorporate further thoughts that may arise following the SAT activity. More opportunities input will lead to greater buy-in.

Strengths and weaknesses of manual and computer assisted analytical techniques

Manual Techniques	Computer Assisted Techniques
• Allows for application of judgment, intuition, and experience • Can leverage experience and contextual understanding, particularly around the intent of individuals • Provides flexibility to adapt approach and techniques as the situation develops • Promotes creativity, enabling analysts to explore alternative perspectives or hypotheses. This is particularly useful when working in groups, allowing analysts to build off each other • Manual analysis is more effective at harnessing diversity that analysts bring to the table	• Can process, store, and analyse large volumes of data efficiently, providing speed and scalability • Automation of routine tasks, freeing up time for more complex analysis • Integrating multiple sources can generate a more complete picture • Databases can be manipulated in multiple ways, allowing queries to be rephrased and explored from different perspectives • Can help minimise human bias through predefined algorithms and rules • Consistency and standardisation
• Inherent subjectivity and bias, with a higher risk during crises • time-consuming, particularly when dealing with large volumes of data or complex scenarios • Lack of standardised approach or outputs across teams • Human error, oversight, or gaps in analysis are inherent risks	• Lack of human intuition, creativity, and contextual understanding that can be crucial in overwhelmingly opaque problem sets • Complexity and nuance may be challenging to capture • Heavy reliance on the quality and accuracy of input data, which can be compromised by misinformation or biases • The reasoning behind certain conclusions or predictions may not be easily explainable. • Overreliance on algorithms may limit the exploration of alternative perspectives or hypotheses • Technical limitations such as data privacy concerns, compatibility issues with certain formats, and vulnerability to cyber threats

Considerations for AI-Analyst Teaming on the near horizon

- Human oversight is still crucial to ensure accurate and ethical analysis. The public and senior decision makers will demand transparency of algorithms and audit trails of assessments.
- The performance of AI algorithms relies on the quality and relevance of the training data. Biases in training data can result in biased outputs.
- AI systems struggle with contextual understanding and the ability to consider complex social, cultural, or historical factors that human analysts excel at.

AI-assisted analysis offers the potential for enhanced processing power and efficiency. However, the limitations in data quality and contextual understanding, and the need for human oversight underscore the importance of striking the right balance.

Case Study: Joint Border Management System – intelligence data models

In 2016, as part of the Joint Border Management System programme, data analysts from Customs, MPI, and the Ministry of Business, Innovation and Employment formed a joint analytics team to better inform risk targeting at the border. The agencies used analytics software and data sharing to process the millions of border transactions and identify patterns in data representing border risk. At the time, MPI and Customs built predictive models to address risks particular to each organisation, with MPI's focus on the biosecurity risk of pest infestation in cut flowers and fresh produce, and Customs' focus on air cargo data to identify methamphetamine smuggling.

Making Assessments

Far from being a fascinating world of intrigue, much intelligence consists of the painstaking assembly of known facts and interpreting a pattern from them. Intelligence analysis is a skilled activity.[2]

The Rt Hon Sir Geoffrey Palmer
Prime Minister of New Zealand 1989-1990

The final stage of analysis is to interpret the integrated information. In its simplest form, intelligence is produced when information is put into context. The desired result is an understanding that reduces uncertainty for decision makers and enables action. There are three levels to understanding which, when followed sequentially, also form a step-by-step process to make assessments.

Figure 13. The levels of understanding

Step 1. Determine the facts. The first step to producing an assessment is to establish what information there is to make assessments from. As mentioned in earlier chapters, each report should be evaluated for its relevance, accuracy, and reliability. A clear and speedy evaluation process aids in dealing with information overload. In the initial stages of a crisis, simply collecting facts and separating out rumours adds value to decision maker understanding.

Too much or too little information?

Complex and rapidly evolving situations often have either too much or too little information. Too much information puts a heavier emphasis on evaluation. Facts do not have to meet 100% confidence at this stage, but source reliability and corroboration are useful checks. When there is too little information, the problem lies in generating enough to move forward. Here, the absence of information can be information itself – no knowledge about an incident from a normally active group may mean their involvement can be ruled out (at least until validated). Historical patterns are another useful tool – assumptions based on similar past incidents can be a stand in to keep moving assessments forward.

2 Sir Palmer, G.W.R. (2000). Needs and Safeguards. Securing our Nation's Safety. Security and Intelligence Group. P4

Step 2. Understand what is happening. This step answers the question "what happened?" or "what's going on?". Facts are joined together to illuminate the links between them. This allows interpretation of causal relationships, such as what led to an event occurring; or interpreting wider organisation and networks. At this level, you should have a good understanding of what has happened up to this point, although there may still be gaps on specific details.

Quick integration

Geospatial tools and timelines (putting things on a map or in sequence) are useful during Step 2 to visualise the linkages, breadth, and progression of a situation. They are also a useful briefing tool for decision makers.

Step 3. Assess future developments. Intelligence teams add the most value when they are predictive. Determining the facts and understanding what is happening are necessary steps to ensure that predictive assessments are grounded in logic. Drawing on previous assessments and historical information are helpful prompts and can add corroboration or illustrate the magnitude of a change in situation. The exact content of the predictions will depend on the needs of the relevant decision makers, but they should clearly identify any risks and/or opportunities.

Making it relevant

Relevance is made of up from three factors:

1. **Timely.** Timeliness in the delivery of the predictive assessment adds value by giving decision makers enough time to act and influence the outcome. A partially accurate assessment given as early warning is better than an accurate assessment given after the fact. Timeliness will be different at the tactical, operational, and strategic levels. In addition to delivery of the initial product, assessments should then address indicators of a developing trend to ensure the assessment remains relevant as time progresses.
2. **Accurate.** The assessment should also contain sufficient detail to enable the supported decision maker to act. Accuracy should ideally answer the questions: who, what, where, when, why, and how[3], or at least cover a time, place, what is known about who, and a description of how events will unfold. Again, the appropriate level of accuracy will be different for tactical, operational, and strategic level problems. The aim is an 'actionable level of detail', which should be clarified with decision makers if it is not known.
3. **Organisational context.** Intelligence assessments should aim to enhance an organisation's plan or objectives. This goes beyond simply providing a picture of the external environment. An understanding of the goals of the organisation and how it conducts business allows intelligence assessments to identify opportunities, threats, and assist with risk. The intelligence being briefed should address the questions or direction taken from the decision maker at the start of the intelligence cycle. If assessments are not answering the original questions, then they should have a clear link with organisational goals or relate to the actions available to the decision maker. For example, consideration of the time it could take for decision makers to organise the appropriate resources. Accuracy in an organisational context allows the action to be carried out with the efficient use of resources.

3 How refers to what actions will occur over time to achieve the 'what' – where the 'what' is the overall objective. An alternative structure is to place all the 'whats' necessary to occur sequentially to achieve the objective.

Case Study: Action against drift net fishing in the South Pacific

In 1989, Prime Minister Sir Geoffrey Palmer launched a campaign against driftnet fishing. Nets of up to 64km were strung out in a wall and left to drift across the open ocean. Known as the "wall of death," the nets killed most living things in its path. Fleets from Japan, Taiwan, and South Korea had large fleets at work in the South Pacific seriously depleting tuna stocks. Some of these nations would frequently deny the scale of the problem as argued by New Zealand. Information gathered by the GCSB disclosed the extent of their catches and allowed the Government to prove the massive scale of drift-net catches and to campaign on facts. This campaign in turn helped to bring about the Wellington Convention that entered into force in 1991 and effectively banned drift-net fishing in most of the Pacific (Palmer, 2020).

Assessing the Level of Threat – Capability, Intent, and Opportunity

Many intelligence teams are responsible for determining a level of threat as part of their assessment. Threat can be described as the potential for harm or damage to a person, group, or system. Threats come from natural disasters, accidents, or deliberate actions by individuals and groups.

The C-I-O method is an effective way to analyse and assess threat. Each category is analysed in isolation before being combined to determine the overall level of threat.

1. **Capability** refers to the ability of an actor or group to carry out a particular action. This includes factors such as access to resources, technical expertise, and organisational co-ordination. A group or actor with a high capability poses a greater threat than one with a lower capability, as they have the means to carry out more sophisticated and potentially more impactful actions.
2. **Intent** refers to the motivation or purpose behind a particular action. This includes factors such as ideology, politics, leadership, and personal beliefs. Again, a group or actor with a high intent is considered to pose a greater threat than one with a lower intent, as they are likely more committed to carrying out an action.
3. **Opportunity** refers to the conditions or circumstances that provide an opening or chance for an action to occur. This includes factors such as access to vulnerable targets; weak security measures; and social, economic, or political instability. A group or actor with increased opportunity is considered to pose a greater threat than one with less opportunity, as they have a better chance to carry out a successful action.

Figure 14. C-I-O matrix (adapted from Security Risk Management Aide-Memoire, Talbot, 2020)

Capability						
	Extensive	M	H	E	E	E
	Advanced	M	M	H	E	E
	Developed	L	M	M	H	E
	Moderate	L	L	M	M	H
	Low	VL	L	L	M	M
		None	Little	Expressed	Determined	Dedicated
		Intent				

Opportunity
• Can modify the capability by matching vulnerability to threat actor's capability • Can modify the intent by reporting or previous actions indicating the threat group's focus on target

Key

E Extreme H High M Medium L Low VL Very Low

When assessing threat using the C-I-O model, it is important to identify and communicate what you are considering the threat against. A group may pose a different level of threat to different targets and entities based on the opportunity at each. For example, the threats from a national disaster may be different in urban versus rural areas, or coastal versus inland areas. Or the threat of a group may be different against members of the public in open areas compared to members of security services in secure locations.

The threat level is taken from the combination of all three factors. A group or actor with a high capability and intent but low opportunity may still pose a significant threat if the opportunity arises. Similarly, a group or actor with a high opportunity but low capability or intent may not pose a significant threat if they lack the means or motivation to carry out an action.

Communicating for Influence

Communicating for influence is usually an iterative process that is underpinned by trust and credibility, both at a personal and organisational level. This iterative process reflects how trust, and subsequently influence, is achieved over time between decision makers and intelligence professionals through the timely and accurate communication of credible, concise, and balanced intelligence. In my personal experience with busy senior decision makers, once you or your organisation has a trusted 'brand', you are usually able to gain ready access to and communicate with (influence) decision makers about important issues or events that have time sensitivities attached to them.

John O'Reilly
National Manager: Intelligence and Analytics Group
New Zealand Police

A critical component of the intelligence system is where it interacts with decision makers. This link comes down to effective communication of assessments and the understanding of customer requirements. A significant amount of the organisation's time and resources are ineffective if the intelligence produced has little or no influence on operations or policy. Moreover, the communication of an intelligence product can have a lasting impact on the credibility of the overall intelligence team, regardless of the accuracy of the assessments.

The ABCs of intelligence communication

A **Accuracy.** Analysis should be accurate – factual errors will undermine the analysis.

B **Brevity.** Analysis should be clear, short, and to the point.

C **Clarity.** The reader should be able to understand the facts and follow the logic to the presented assessments.

Adapted from Delivering Effective Analysis, UK College of Policing, 2020

Recommended format of intelligence products

Communication of intelligence assessments are recommended in the following format:

- Heading: statement of key assessment.
- Fact (or facts).
- Assessment.

The above format offers a sequence for the audience to follow that also explains the logic of the assessment. It outlines the key takeaway up front for busy decision makers who do not have time to read full products or stay until the end of a brief. This format is applicable whether presented in verbal, written, or visual form.

Longer reports may contain multiple iterations of the 'fact(s) then assessment' structure, where each paragraph covers a key assessment supported by just enough evidence to give it credibility. Or one paragraph outlines facts with the following explaining the assessment.

Where facts are blended into the same paragraph as an assessment, there should be a clear indication of what is fact and what is assessment. This could be indicated by the assessment sentences beginning with "It is assessed that ..." or "Assessment: ..." Use of probabilistic language (see below) also indicates assessment.

Our clients are busy readers, and many don't feel as if they have to read our product. In talking to regular readers of intelligence about what they thought the problems with intelligence writing were, more often than not their issues were not about style but were related to structure. The main problem in intelligence writing is that it is often not well planned. It is the key messages that dictate the structure of a report, not the other way around.

Euan Staples
New Zealand Police and Creator of the Convincing Writing for Intelligence Course

Written intelligence products that are longer than one page should include an executive summary of the key assessments. Decision makers receive a lot of information in different forms each day; there are multiple anecdotes describing how senior leaders often do not read reports longer than two pages (Eley, 2018). A 2015 report by the US Office of the Director of National Intelligence found that senior policymakers often rely on summaries, oral briefings, and other condensed forms of intelligence reporting rather than reading full-length intelligence products. The report cited factors such as time constraints, competing demands, and the sheer volume of intelligence products as contributing factors (Office of the Director of National Intelligence, 2015).

It is the product's structure that helps guide the reader. To influence decisions, the case made in a report needs to be presented in a logical way. A poorly structured product with too much detail and hard to follow logic will ensure the message is unclear and unconvincing.

Think, plan, and only then, write

The main problem in intelligence writing is that it is often not well planned (Staples, 2020). Unplanned reports invariably bury key points in an overly long, unwieldy mass of words that are then impossible to re-plan.

One of the biggest mistakes analysts make is launching into full text before they know what the product's key messages will be. If writing starts under the presumption that the focus of the piece will emerge as the product evolves, the products will come up short. Analysts will write themselves into a problem, managers receive the product late and then have to re-work it.

Move away from a "write to think" approach toward a "think, then write!" framework.

- Start with a precise knowledge of what the report's key messages are. Know your customer's needs and have a clear understanding of what the final report will be used for.
- Next, plan an outline of all the points you intend to make and the order in which they will appear. The outline is constructed once the research and 'thinking' stage is compete, but before the 'writing stage' begins. Put onto paper the key messages and the logical points that support them, in as few words as possible. This will give you the report in miniature, without having to wade back through reporting or a poor first draft.

This approach makes writing the full report much easier and less time consuming. It becomes clear what is important, what can be left out, how far you need to go in pursuit of meaningful characterisation and how hard you need to make each sentence work. It may take time to produce a good outline, but this will save time in the actual writing, and subsequent re-writing.

Types of effective communication

Using the right method of communication plays a significant role in whether the assessments are understood and will have an influence on decision making. The communication of an assessment is as equally significant as the relevance of the assessments themselves.

Continuous Improvement

A common complaint from analysts is that they are beholden to existing organisational templates and methods of communication. This will never be the case in a proactive organisation. Continuous improvement in communication methods should be encouraged by intelligence leaders – each new decision maker will have their own individual preferences and reflect the constantly evolving way in which people receive information.

Analysts and intelligence leaders should conduct a deliberate assessment of the intended audience and their preferred way to receive information. Consider reading versus being briefed, whether they favour interaction and learn through questioning, or if they prefer to not voice opinions in large groups. Also consider where their schedule allows for a focus on intelligence products free from interruption. There are also situation dependent factors such as topics or issues that may be currently preoccupying their thoughts and how this may affect the way they are prepared to receive new information (although often there may be no choice due to the decision maker's schedule and the urgency of the reporting). And while style of the report can be adapted for better influence, it should always remain objective and have integrity toward the facts and assessments.

Each type of communication has its strengths and weaknesses. And often the most suitable method will be a combination of the three different types.

1. **Verbal Communication.** Verbal communication of intelligence assessments can occur in a variety of settings, such as face-to-face briefings, conversations, or video conferences. They can vary from formal to informal, the balance of which is important to get right in order to develop confidence of the decision maker in the analyst and intelligence organisation. Verbal communication can be effective for building rapport and establishing long term trust with decision makers, as the interaction allows for immediate feedback and clarification through questions and discussion. Informal briefings should still be well prepared and follow the ABC's. Verbal communication can also be undermined by environmental distractions and misunderstanding.

Tips for effective verbal communication

- Setting. Ensure the briefing area is set up ahead of time and free from distractions such as phones, awkward lighting, and sounds.
- Technology. Conduct a trial run of any intended technology to ensure you can log on, access, and run any electronic briefing aids.
- Opening remarks. Before briefing the main content of your intelligence product, introduce yourself, the topic of the brief, the length of the brief, security classification, and when there will be an opportunity for questions (remove any of the above criteria if it is not relevant).

- Rehearse. Gain confidence by practicing your brief. Check the coherence of the brief through speaking the content aloud; verbal communication is often less formal than the written form, so ensure the structure flows when vocalised at a deliberate pace. Also check that the briefing time matches the time the decision maker has available. Rehearsals are more powerful with a peer or manager acting as the audience to provide additional feedback.
- Write the briefing notes before supporting visuals. Producing visuals first tends to result in more words on the visual and can lead to briefing verbatim off the visual.
- Answer questions directly. Questions are a great way to add additional detail, but this should be focused on aiding understanding of the key assessments. Pause before answering a question to determine whether it is simply a question of fact (because it may have been misheard) or whether the decision maker is testing your assessments. If it is the latter, then the brief may not have been as clear as intended, so it is recommended to reiterate the logic trail by outlining key facts followed by the assessment. Consider if additional facts are required or an explanation of why an alternative assessment was discounted (with reference to the facts). If you are clearly uncertain of the answer, do not make something up, simply state, "I do not know the answer to that, but I will find out and get back to you."
- Troubleshoot likely questions. Anticipate what questions may arise, such as why you have not included something that may be topical to the decision maker, or why there is no further accuracy around the predicted time, place, or entities. It is helpful to do this with peers or managers.

2. **Written Communication**. Whether in long or short form, written communication can be highly effective for conveying detailed or complex information, as it allows for careful crafting of the message. It can also be easily stored and made available when convenient to the decision maker or for other analysts to utilise at a later date. However, it can be severely limited by the lack of immediate feedback or clarification, which can cause a break in the intelligence cycle.

Tips for effective written communication

- Be clear and concise. Use clear and simple language. Avoid using overly complex or technical terms that may confuse or alienate the audience. Use a professional tone and style, and avoid using slang or jargon, particularly for products likely to be distributed outside your organisation.
- Organise your writing. Use a clear and logical structure. Use the heading/fact(s)/ assessment structure above. This is recommended for each paragraph. Headings and subheadings can be used to break up long blocks of text and make writing easier to scan.
- Written intelligence products that are longer than one page should include an executive summary of the key assessments.
- Use specific examples to support your arguments.
- Peer editing. Take the time to edit and proofread your writing carefully. Use peer and managerial review to ensure your key assessments are logical and easily understood.
- A consistent organisational style helps readers know what to expect from written products and assists analysts when preparing their product.
- Avoid contradictory statements. Excessive use of 'however' statements to outline alternative explanations confuse the reader and lower their confidence in the assessments. For short pieces, use probabilistic language to outline the likelihood of the predictive assessment. Careful consideration should be made before including alternative scenarios or explanations in longer products unless this has been deliberately requested by the decision maker. The product should also make clear what the most likely assessment is.
- Avoid overuse of adjectives. Without careful selection, adjectives can skew the emphasis of key judgements and cause misunderstanding. They should be saved for when they are really warranted and there is a clear purpose to their use.

3. **Visual Communication.** This refers to the use of visual elements, such as images, graphics, and videos, to convey information and assessments. Visual communication can be highly effective to express complex or abstract concepts, as they are generally more readily understood. Visual communication can also be used to create a more engaging and memorable message. However, visual communication may be less effective for conveying nuanced ideas that require detailed explanation. Effective visual communication involves more than simply creating eye-catching graphics or images – it requires careful consideration of the message, audience, and purpose.

Visual communication can be a very powerful tool to assist understanding. In my view, employing a full-time infographics specialist and routinely using this medium to support both verbal and written briefs was one of the most significant communication developments undertaken at the National Assessments Bureau in at least the previous couple of decades.

Mike Hickman
Former NAB Chief Assessments Officer

Tips for effective visual communication

- Use visuals to support the message. The purpose of using visuals is to support the analytical message and its communication to decision makers, rather than simply adding decoration.
- Keep it simple. Avoid cluttering your visuals with too much information (visual or text). Use clear and concise language and limit the number of page elements.
- Consider using charts and graphs for numerical data and infographics for complex information.
- Use colour and contrast effectively. Colour and contrast draw attention to key elements and make visuals more engaging. However, too many colours or colours that clash can be hard to read and distract from the message.
- Write your briefing notes before producing supporting visuals. Producing visuals first tends to result in more words being placed on the visual and can lead to briefing verbatim off the visual.

Integrated Assessments

Busy senior leaders prefer to be presented integrated options to shorten decision cycles. In an organisation where each branch presents their own problems and advice, the senior must first integrate the information, complicating and slowing down the process of making a decision. Often the real decision making happens at the operations or policy manager level, with these people putting together the options that go before the senior. Intelligence is likely to have more influence on the organisation by being relevant to the operations or policy team and working with them to incorporate intelligence assessments into the operations or policy formulation at the outset. This results in an integrated assessment and options going to the decision maker and speeding up decision making.

During verbal briefings, some decision makers prefer to move on quickly from the intelligence brief to the question of "what to do" about the situation. This is not often the place of an intelligence analyst to provide advice on, but nor is it appropriate to brush it off with a "that's not our role" type of response. Integration of the intelligence process with the broader operations or policy decision making process will ensure briefers are prepared. This also contributes to the process of developing the decision maker's confidence in the intelligence and operations system supporting them.

Probabilistic language

Probabilistic language allows an intelligence analyst to convey the level of likelihood in a predictive assessment. As these events take place in the future, all assessments will contain an element of uncertainty.

Likelihood is a useful tool for decision makers to evaluate risk appetite, the balance between cautious or forward leaning options, and the amount of flexibility needed to react to an unexpected change in the environment. Should time allow, likelihood also indicates whether more time should be spent gathering further information before acting at all.

Likelihood can be expressed in words or numbers with some research suggesting that words are more useful to avoid a false image of accuracy (Friedman, Lerner, Zeckhauser, 2016). What is most important is that the audience understands the terms used, which is gained through deliberate explanation and consistent usage. Common practice is that decision makers are unlikely to remember the nuance of multiple probabilistic language categories and are also unlikely to flick between the body content and a language table at the end of a document. In the absence of existing standards in your organisation, the following categories are offered for consideration:

Figure 15. Probabilistic language

Term	Percentage Likelihood
Unlikely	Less than 35%
There is an even chance	40-55%
Likely or probable	Greater than 60%
Almost certain	Greater than 90%

Notes on the use of probabilistic language:

- It is recommended that "there is an even chance" is used sparingly. While this and other words such as "possible" are useful for analysts to hedge their bets, it can be unhelpful to plan against, except when considering contingency plans. For customers not familiar with the nuance of intelligence work, it can even be more confusing than useful, sounding as if it is predicted to happen, whereas there is actually a low level of likelihood. If this term must be used, it is recommended that the product is accompanied with indicators of the assessment developing one way or the other. Being a professional analyst means having the integrity to make an assessment and monitor its development.
- "Highly unlikely" and "highly likely" can be a useful modification to emphasise great levels of doubt or support for an assessment.
- There are deliberate gaps in the percentage ranges in order to encourage an assessment to be made about which term to use, rather than sitting on the border between two.

Reaction during a crisis

Figure 16. The Prepare-React-Adapt Model of Intelligence Support to a Crisis

Prepare	React	Adapt
• Establish standard processes • Conduct training • Maintain contact lists • Maintain IPOE	• Set up • Prioritise and plan • Balance collection and analysis • Determine the facts • Understand what is happening • Predict what will occur next • Understand the threat and how it will develop • Movement limitations • People's needs • Establish liaison officers	• Anticipate the organisation's future needs and identify opportunities • Establish sustainable personnel rotation • Establish scheduled delivery of assessments

The role of an analyst

What follows is a description of how the intelligence system should Prepare, React, and Adapt to a crisis. What is important for an analyst is to:

- Understand where you fit into the system at each stage, and to the overall success of the response. It is possible that you will be required to conduct duties outside of your regular role, such as liaison, verbal briefing, and logistics of the intelligence operation.
- Be proactive. Direction and guidance are unlikely to be clear or timely, especially at the outset. Anticipate what might be required and identify where you can add value.
- Keep your contacts updated – both your own and for key internal and external people.
- In line with the first point, you may find yourself leading the system. If this happens, follow the below and try your best – everyone wants you to succeed.

During a crisis decision makers require understanding of the situation to act quickly and regain control while also minimising danger to the public, staff, and resources. The role of intelligence is to make sense of the rapidly evolving environment and enable organisational action. Intelligence teams must make quick, informed decisions around where to prioritise effort and what to brief. The Prepare-React-Adapt model provides an effective way for intelligence teams to focus on the basics and perform to the expected level of decision makers during a crisis.

1. Prepare

These activities occur before a crisis event. They focus on establishing standards and processes in an environment where there is no immediate external pressure.

a. **Establish standard processes.** Outline how the intelligence system will operate during a crisis, including the roles and responsibilities. This also includes the tools – especially ICT systems – and the points where the intelligence system connects to decision makers. Established processes includes product templates. Product templates save time for analysts to focus on content and provide a guide on expected outputs.

b. **Conduct training.**

   i. Individual training. Individuals need to be trained in their role and responsibilities within the system, particularly where their role will be additional to their routine duties.

   ii. Collective training. To build a team that can come together and function in a fast and unpredictable environment requires repetition. Exercising practises both individual and collective skills, as well as familiarity with organisational processes. Going through a scenario translates the theory of the plan into skills, equipment, and processes to make it work on the ground with real people and systems.

c. **Maintain contact lists** of both personnel who will be called out during a crisis, and key external contacts for supporting or supported teams and organisations.

d. **Conduct and maintain intelligence preparation of the operating environment.** A crisis will have unique characteristics, but some aspects may be predictable in outline ahead of time, such as the physical environment and aspects of the threat. Generic decision maker questions may also be anticipated and addressed in outline. These models will not be perfect, but they can be reviewed and refined if there are indicators of a building crisis. They provide something to work off and avoid a cold start.

2. React

This occurs when the crisis happens and focuses on achieving understanding to enable the organisation to regain control. While there will be organisational processes for initiating a formal crisis response, intelligence personnel should use their initiative and be proactive to gain as much of a head start as possible within their authorities.

a. **Communicate with decision makers for direction.**

   i. Set up the team and the working area, including checking communications.

   ii. Prioritise where intelligence effort is needed for collection tasks and analytical focus. If decision maker intelligence questions are currently unknown, it is recommended that the intelligence leader assess what questions are likely to allow the intelligence system to keep moving. Check and refine these questions with the decision maker at the soonest opportunity.

   iii. Plan. Assign personnel to the priority areas and set timelines for tasks and briefs to be achieved. In the early stages, more personnel are likely to be needed to conduct collection and evaluation, including establishing the facts.

b. **Collection.** Part of the plan should include collection requirements to collectors. A running display of the overarching intelligence questions, as well as current gaps and lesser information requirements should be maintained and available for collectors to 'pull' at any time to enable them to work without direct tasking if required.

c. **Analysis.**
   i. The analytical effort should be focused on moving through the steps of understanding to determine the facts, understand what is happening, and to predict what is coming next.
   ii. Each crisis will have its own situational needs and decision maker requirements. Generic requirements during an accident or natural disaster situation revolve around these topics:
      (1) Understand **the threat and how it is developing**. (Who, doing what, where, when, why, and how[4]).
      (2) What **movement** is affected or unaffected in the environment.
      (3) What are the current and anticipated **needs of the public** or other relevant entities.
      (4) What are the threats, opportunities, or risks in the above.

d. **Communicate assessments.**
   i. Brief assessments at operations planning groups.
   ii. Make assessments available for operational or other teams to 'pull' without the need for direct briefing.
   iii. Establish Liaison Officers if required to keep other teams informed of key assessments. These will also feedback further intelligence questions.

3. Adapt

Once understanding has been gained, the intelligence system needs to adapt to a sustainable rhythm.

a. **Communicate with decision makers for direction.**
   i. Anticipate what the next phase of the response may be for the organisation and develop intelligence questions and intelligence plans to both maintain understanding and support future organisational planning, including how to exploit opportunities.
   ii. Personnel planning should move to a predictable rotation or other form of steady state, to allow ongoing sustainment and rest for both individuals and the team. It should also look for opportunities to move people back to their primary duties.
   iii. Conduct welfare checks on all individuals, not just those who may be experiencing a crisis for the first time. This should continue after the conclusion of the crisis, including referrals to formal counselling if not part of routine organisational processes.

b. **Collection.** Collection Planning Groups should move to a regular schedule.

c. **Analysis.** Continue to provide understanding and predictive assessments as per the React stage. Some analytical effort shifts to support future organisational planning.

d. **Communicate assessments.** This should now be on a regular schedule, but with constantly improving formats to suit the decision makers.

Crisis situations are often fast and unpredictable and require intelligence teams to be adaptable and resilient. Controlled exposure to likely events through exercises helps reduce the impact of shocks and surprises during a real-time crisis, building resilience as a key part of long-term mental welfare. Welfare checks should take place during the crisis when outputs allow, and continue after the conclusion of the crisis, including referrals to formal mental health support if required.

4 See the Making Assessments chapter, under 'Accurate'.

Coordinated Incident Management System (CIMS)

CIMS is New Zealand's official framework to manage an incident across multiple responding agencies. The framework outlines nine functions to provide effective command, control and co-ordination during the response (control, safety, intelligence, planning, operations, logistics, public information, welfare, and recovery). It allows for a scalable response appropriate to the incident, including first responders, local authorities, regional authorities, and finally national level authorities. A number of New Zealand agencies, essential service providers and community members will have received some level of training in CIMS.

The Prepare-React-Adapt Model provides more structure to the expected outputs of the intelligence function outlined in CIMS, demonstrating how effort changes over time, and adding additional tasks to the preparation stage.

Additional information on CIMS can be found in the further reading chapter.

Case study: Key findings from the Auckland Flood Response, January 2023

Over 27-28 January 2023, Auckland experienced a major flood event that caused significant transport and infrastructure disruption, mass evacuations, property damage, and loss of life. An external review conducted after the crisis highlighted weaknesses in Auckland Council's emergency management systems and community relationships, which impacted situational awareness and the ability to respond (Bush, 2023).

Early intelligence was limited due to low engagement with partner agencies outside the small group of first responders and the National Emergency Management Agency. Elected members and the Office of the Mayor relied on local communities, personal contacts, and public media for information instead of all source intelligence. The lack of structured intelligence reporting and delayed situation reports further hindered response efforts.

The review recommended developing a common ICT system for Auckland Emergency Management and partner agencies to improve real-time communications and decision making. Other opportunities for improvement identified were the development of more sophisticated data collection mechanisms, increased engagement with partners outside of a crisis, prearranged intelligence gathering protocols with Auckland Transport, Waka Kotahi, Auckland Airport, and lifeline utilities, enhanced engagement at the iwi and local board level for localised information dissemination, and clarity on sharing finished intelligence products with relevant stakeholders. Additionally, the use of physical Emergency Operations Centres was encouraged to facilitate real-time information sharing and monitoring from multiple sources instead of working from home.

The review also noted that within a week, the quality of reporting and intelligence improved considerably as Tropical Cyclone Gabrielle descended on the North Island.

Leading tasks as an analyst

Analysts rarely work in isolation and will often be required to informally lead tasks such as structured analytical techniques, multi-agency assessments, and coordinating with other elements of the intelligence system. Having broad input and working through analytical differences is a powerful way to gain access to further information, overcome bias, and arrive at more robust assessments. In most organisations, leading tasks will be a formal development goal for those seeking career progression to intermediate and senior analyst or managerial roles.

Successful leaders are those who can adapt their approach based on the needs of the task and the needs of the people involved. Situational leadership is a flexible model that suits the ad hoc tasks and groups an analyst is likely to lead.

Situational leadership allows for an adaptable approach based on balancing the following factors:

- **Task behaviour.** The extent to which a leader uses one-way communication to direct what each follower is required to do to achieve the overall task.
- **Relationship behaviour.** The extent to which a leader uses a facilitative and supporting approach. This can include coaching and mentoring.
- **Readiness of the individuals within the group.** The ability and willingness of a group member to act independently in relation to a specific task.

Crises or time sensitive tasks may require a more directive style of leadership to provide focus and achieve tasks on time. However, groups with highly experienced individuals may be better suited to a facilitative approach. The appropriate approach will rely on an appreciation of the time available and the understanding of the individual participants. The approach may also change throughout the task, with a more directive style to initiate action, moving to a more supportive style as participants gain a better understanding of the task and individual competence becomes apparent.

Recommended steps to lead an intelligence task

1. **Communicating with decision makers for direction:**
    a. Determine the time available to complete the product or output. Factor in the need to communicate tasks to the group, time for collection, structured analytical techniques, peer review and other editorial processes.
    b. Confirm the intelligence question or questions that need to be answered. Break out each question into sub-topics that would help to answer the question. This can be done as an individual or group activity.
    c. If other personnel are available, assess and assign them by topic or by functional area (collection, collection co-ordination, analysis, communication), or a mixture of both.
2. **Collection:**
    a. Consult current information and intelligence holdings.
    b. Task collection if required using organisational processes.
    c. Direct team members to carry out the above if appropriate or conduct their own collection within their authorities.

3. **Analysis:**
    a. Determine which personnel will add value to the SAT activity, consider factors such as subject knowledge, diversity of thought, and understanding of SAT processes. Assess the development level of each peer in terms of their skills, knowledge, and experience to tailor the leadership approach.
    b. Define the objective. Clearly articulate the objective of the analytical output, including what decisions are being supported, the intelligence questions, and any expectations about the form and timing of the product.
    c. Establish the group's process. Outline how the SAT activity will be carried out and ensure that each group member understands their role in the process.
    d. Apply the appropriate leadership style based on the development level of the peers and the objective of the analysis. It may be necessary to use a combination of leadership styles to achieve the desired outcome.
    e. Review the results. Once the analysis is complete, review the results with the group and provide feedback on the analysis process and outcomes. Canvas their opinions on possible ways to communicate the findings.
    f. Throughout the process, provide feedback in a respectful way to the group members to help them improve their skills and performance.

Figure 17. Different Situational Leadership styles (adapted from Schermerhorn, 1997)

Directing style	Coaching style
If some group members lack the necessary skills or experience, use a directing style to provide specific guidance and direction on how to approach the analysis. This is also appropriate if time is critical.	If some group members have some basic knowledge or experience but need to improve their analytical skills, use a coaching style to provide feedback and guidance to help them develop their skills further.
Supporting Style	**Delegating style**
If group members are more experienced but lack confidence or need some support, use a supporting style to build trust and encourage collaboration.	If group members are highly competent and independent, use a delegating style to allow them to take full responsibility for parts of the process while still providing support and resources as needed.

4. **Communication:**
    a. Consider delegating portions of the product to group members to draft. They are more likely to buy-in to the project the more points they have for input.
    b. Whether or not other group members were included in the drafting phase, including them in the peer review will help incorporate any further thoughts they may have had following the SAT activity.
    c. If appropriate, particularly in a multi-agency context, ensure acknowledgement of input of other group members in the final product.

Further reading

The following is a selection of books, articles, manuals, and documents on the topics discussed in this handbook. There are many more.

Andregg, M. (Ed). (2007). *Intelligence Ethics: The Definitive Work of 2007.* Center for the Study of Intelligence and Wisdom.

Beebe, S. M., & Pherson, R. (2017). *Cases in Intelligence Analysis: Structured Analytic Techniques in Action.* CQ Press.

George, R., & Bruce, J. (2011). *Analyzing Intelligence: National Security Practitioners' Perspectives.* Georgetown University Press.

Bush International Consulting (2023). Auckland Flood Response Review: Independent, external review of events, January 27-29, 2023. Auckland City Council. URL: https://ourauckland.aucklandcouncil.govt.nz/media/je3potln/auckland-flood-response-review_january-27-29-2023.pdf, accessed 23 July 2023.

Clark, R. (2013). *Intelligence Analysis: A Target-Centric Approach.* CQ Press.

College of Policing. (2023). *Intelligence Management.* United Kingdom College of Policing Authorised Professional Practice. URL: https://www.college.police.uk/app/intelligence-management, accessed 12 May 2023.

Department of Prime Minister and Cabinet (2016). *National Security System Handbook.* New Zealand Government. URL: https://www.dpmc.govt.nz/sites/default/files/2020-10/National%20Security%20System%20Handbook%202016.pdf, accessed 23 July 2023.

Filer, D. (2019). Signals Intelligence in New Zealand During the Cold War. *Security and Surveillance History Series* (2019/1).

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

Friedman, J, and Zeckhauser, R. (2012). Assessing Uncertainty in Intelligence. *Intelligence and National Security*, Vol. 27, No.6, 824-847. URL: https://scholar.harvard.edu/files/rzeckhauser/files/assessing_uncertainty_in_intelligence.pdf, accessed 12 May 2023.

Heuer, Jr, R. (1999). *Psychology of Intelligence Analysis.* Center for the Study of Intelligence, Central Intelligence Agency.

Heuer, Jr, R. (2009). *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis.* US Government. URL: https://www.stat.berkeley.edu/~aldous/157/Papers/Tradecraft%20Primer-apr09.pdf, accessed 23 May 2023

Higgins, E. (2021). *We Are Bellingcat: An Intelligence Agency for the People.* Bloomsbury Publishing.

Jones, M. (1998). *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving.* Crown Business.

Kahneman, D., Egan, P., Loewenstein, G., Fredrickson, B. L., & Schreiber, C. A. (2011). *Thinking, Fast and Slow.* Farrar, Straus and Giroux.

Kukutai, T., Campbell-Kamariera, K., Mead, A., Mikaere, K., Moses, C., Whitehead, J. & Cormack, D. (2023). *Māori data governance model.* Te Kāhui Raraunga. URL: https://www.kahuiraraunga.io/_files/ugd/b8e45c_803c03ffe532414183afcd8b9ced10dc.pdf, accessed 23 July 2023

Lowenthal, M. M. (2017). *Intelligence: From Secrets to Policy.* CQ Press.

Moore, D. (2012). *Critical Thinking and Intelligence Analysis.* CQ Press.

National Emergency Management Agency (2020). Coordinated Incident Management System (CIMS) third edition. National Emergency Management Agency. URL: https://www.civildefence.govt.nz/resources/coordinated-incident-management-system-cims-third-edition/, accessed 23 July 2023.

National Security Workforce. (2023). *National Security and Intelligence: The role of government agencies.* New Zealand Government. URL: https://www.dpmc.govt.nz/sites/default/files/2023-04/National-Security-and-Intelligence-Role-of-Government-Agencies-updated-February-2023.pdf, accessed 23 July 2023

New Zealand Police. (2021). *Enabling the New Zealand Police Deployment Model: National Intelligence Operating Model.* New Zealand: New Zealand Police. URL: https://www.police.govt.nz/sites/default/files/publications/national_intelligence_operating_model_2021.pdf, accessed 12 May 2023.

Sir Palmer, G.W.R. (2000). Needs and Safeguards. *Securing our Nation's Safety.* Security and Intelligence Group. URL: https://www.dpmc.govt.nz/publications/securing-our-nations-safety, accessed 24 July 2023.

Pherson, R.H., and Heuer Jr., R.J. (2020). *Structured Analytical Techniques for Intelligence Analysts.* CQ Press.

Pherson, K., & Pherson, R. (2016). *Critical Thinking for Strategic Intelligence.* CQ Press.

Tetlock, P., & Gardner, D. (2016). *Superforecasting: The Art and Science of Prediction.* Broadway Books.

Tufte, E. (2019). *Visual and Statistical Thinking: Displays of evidence for making decisions.* Graphics Press.

US Department of the Army. (2020). *Intelligence Analysis* (Army Techniques Publication 2-33.4). US Government Publishing Office.

Walton, T. (2010). *Challenges in Intelligence Analysis: Lessons from 1300BCE to the Present.* Cambridge University Press.

Research, drafting, and production supported by Astro Intelligence Systems
astrointelligence.co.nz