THE REGIONALIST
INSTITUTE FOR REGIONAL SECURITY

IS TODAY’S NATIONAL SECURITY INTELLIGENCE TOO RELIANT ON TECHINT SOURCES AT THE EXPENSE OF HUMINT SOURCES?

Alexandra Apse

SYNOPSIS

The Intelligence Community (IC) equally values and utilises techint and humint sources for national security intelligence because only when they are used together do they create a solid and useable intelligence. The IC’s balanced method is appropriate for the current international climate, as it provides the most comprehensive and experienced approach to intelligence collection. The Australian government should continue to encourage government agencies to work together to provide both types of intelligence through interagency cooperation.

NATIONAL SECURITY INTELLIGENCE AND THE INTELLIGENCE CYCLE

The purpose of intelligence agencies such as the Central Intelligence Agency (CIA) or the Australian Security Intelligence Organisation’s (ASIO) is to collect and analyse intelligence to anticipate, prevent and mitigate the impact of threats and attacks against a nation and its people. In 1991, the CIA referred to national security intelligence as ‘knowledge and foreknowledge of the world around us – the prelude to Presidential decision and action’. ASIO’s concept of security intelligence highlights the

Australian government’s definition of national security intelligence, including threats to Australia’s national security that:

- have consequences which, if not countered, could potentially cause grave harm to Australia’s people, institutions and interests;
- may involve Australian citizens or residents or have some link to Australia;
- may be directed by, influenced or otherwise linked to factors outside Australia, including foreign governments; and
- may require the use of special capabilities and measures to detect and respond to effectively.

The intelligence cycle is made up of the following phases: direction, collection, analysis, dissemination and feedback and review. The Humint and Techint collected as part of the collection phase is analysed to produce intelligence for key decision-makers responsible for national security.

WHAT IS HUMINT AND TECHINT?

Humint ‘refers to an intelligence discipline that bases its analysis and interpretations on information obtained through interpersonal relationships’. This method is primarily clandestine in nature and is generally associated with espionage. Humint has proved invaluable to the US, UK, Soviet Union and Australia throughout history, especially during the Second World War and the Cold War Era. The themes and targets, such as the evolution of conflict, emphasis on national security, and emergence of home grown threats have changed since the Second World War. But the basic principle of Humint remains constant and relevant in this contemporary era.

Techint differs from Humint as it incorporates Signals Intelligence (Sigint), Imagery Intelligence (Imint) or Geospatial Intelligence (Geoint) and Measurement and Signatures Intelligence (Masint). Technological developments over recent decades have led to a rapid growth in the Techint collection industry, as a result security and intelligence agencies are placing a growing dependence on Techint. Common technologies in the collection of Techint include satellites, aircraft, decryption software, wiretapping, communication, unmanned aerial vehicles and drones, data monitoring and remote sensors.

Humint and Techint independently experience limits of exploration. For example, in a study conducted by Mugavero, Benolli and Sabato into the benefits of a relationship between Geoint and

Humint specifically, 'it is clear that integrating images and geospatial data on a map as well as using devices capable of operating in three or four dimensions while integrating typical forms of intelligence collection, as Humint, judgement and discernment of activities and events would be consequently expanded, providing a most updated and accurate context to final decision-makers'. As such, single intelligence collection methods cannot be considered an adequate enough source to provide intelligence to analysts for decision-makers. This collaborative approach to intelligence collection and analysis adds to the argument that Techint sources are not too relied upon at the expense of Humint sources in today's national security intelligence.

BENEFITS OF HUMINT

Although Techint possesses many advanced capabilities, Humint has the ability to fill the intelligence void left by Techint. For example, one limitation of Techint is that satellites and other Imint assets cannot gain access and "see" into buildings, caves or underground structures. This limitation meant that agencies did not possess full situational awareness in their area of operations in places such as Afghanistan and Iraq. Another benefit of Humint is the interpersonal nature of the intelligence collected. With regards to foreign terrorist organisations that pose a significant threat to national security such as al Qaeda, 'one would prefer to have a human agent well situated inside the Qaeda organisation'. Being adept at identifying the weaknesses of one discipline and being adaptive and flexible enough to compensate and complement with another, is a prime example of the persistent relevance of both intelligence-gathering methods. Without this flexibility and experience in both disciplines, intelligence agencies have the potential to become irrelevant or forced to change. Therefore, maintaining both capabilities is beneficial to national security intelligence.

The benefits of Humint far outweigh its limitations and issues. However, they still exist and have sometimes contributed to intelligence failures. As agents are dealing directly with human beings, often recruiting foreign assets can be difficult. Agents cannot always overcome language barriers, cultural differences and personality characteristics when building an interpersonal relationship. Training a field agent also takes a significant amount of time and money, with no guarantee that an agency's investment will pay off in the field. Additionally, as with any person, recruited foreign assets have the potential to be untrustworthy and there is always a high chance that information provided to agents may not be credible or reliable. Humint is a high risk method and as the Director-General of ASIS stated in his ASIS at 60 speech, 'HUMINT, by its nature, is an imperfect art'.

BENEFITS OF TECHINT

With so many advancements and new technologies on the market, the possibilities of threats against national security, and the ability to combat those threats are almost endless. For example, with more communications being conducted via technology rather than in traditional writing or face-to-face methods, Sigint provides an important gateway to communication intelligence. Due to the extensive usage of communications technology, communications intelligence allows one to gain an insight in the most personal thoughts, plans, opinions and discussions with others both friend and foe. Technological advancement in networking, file sharing and social media etc has enabled information sharing to be conducted in real-time on a global scale. Techint has the ability to identify, process and analyse large quantities of data, and provide images and surveillance information at a much greater rate than what Humint can achieve.

Another contributing factor in the argument that national security intelligence *is not* too reliant on Techint sources at the expense of Humint sources lies in the issue of ethics and legislation. It is well known that the ethics behind Techint collection has raised both public and private concerns, especially in the US, about the legitimacy of Techint (and on occasion, Humint) collection. Both have been subjected to increased scrutiny in recent years as a result of intelligence related scandals such as WikiLeaks and the Edward Snowden leaks. With the intelligence profession and agency activities needing to become more transparent and accountable to the public, the question of ethics surrounding all types of intelligence has been raised. As national security is such a high-profile agenda, national security intelligence is often in the spotlight for varying reasons including operations and actions that may seem ethically questionable to the general, uninformed public.

Due to questions being raised in the US about the bulk collection of telephone data and the PRISM program, the Office of the Director of National Intelligence made a public statement denying that the data collection and PRISM programs were illegal. This statement was required in order to justify and provide legitimacy for these operations to the public. The statement clearly illustrates the challenges agencies currently face with regards to continuously scrutinised Techint collection, in pursuit of successful national security intelligence.

ARE WE TOO RELIANT ON HUMINT OVER TECHINT?

The nature of global threats posed to nation-states has changed significantly since the intelligence agency era began. It is important that key decision makers acknowledge this, as the changes and developments in types of threats have a direct link to current national security and national security intelligence. For Australia, the 2008 National Security Statement to Parliament identified 'twenty nontraditional national security "issues" – ranging from terrorism to organised crime to climate change – that influence national security planning'. The changing threat environment means there is no strict delineation for the use of Humint and Techint collection. The type of intelligence needed is directly dictated by the threat posed at that time. A particular situation may require Techint collection initially, then may develop to require Humint collection. An example could be suspicious online activity by an individual relating to potential terrorist activities. Techint would initially be utilised and relied upon to gather the initial intelligence, then Humint could be drawn on to form a relationship with individuals involved for further information. Agencies should not rely more on Techint sources when Humint sources are required. When the sole purpose of an intelligence agency (such as ASIO for example) is 'the protection of Australia and its citizens from: espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence systems, acts of foreign interference and serious threats to Australia's territorial and border integrity', it would be hard to imagine that an agency would risk this responsibility to rely upon one intelligence collection method at the expense of another.

Current national security intelligence *is not* too reliant on Techint sources at the expense of Humint sources. The characteristics and purpose of Humint and Techint are far too different for one of them to be solely relied upon by an agency. Both are required to gather the full range of information to analyse and disseminate to decision-makers for matters of national security. Both Humint and Techint have limitations but both equally have value for national security intelligence. Noting the reassurance by agencies that Humint is still a high priority, and that government funding has not leant more toward one particular method, it would be difficult to argue that Techint sources are being relied upon more at the expense of Humint sources in today's national security intelligence. Government agencies should continue to utilise the best intelligence collection method available for the given national security situation.