Intelligence Support to the Development and Implementation of Foreign Policies and Strategies

Ian Dudgeon

Australia, like most other nations, draws on intelligence produced by its human, signals and imagery collection agencies to assist government to develop foreign policies and strategies to protect and promote its national interests. Many governments also use the human and signals intelligence agencies to undertake covert action to assist to implement those policies and strategies, especially in war or other crises. However, despite the uncertain security environment in which we live, the Australian Intelligence Services Act has removed the option of ASIS directly undertaking special operations to combat any threat to Australia or Australian national interests, from hostile states or non-state terrorist organisations. The above Act should be amended to re-establish that option for government in war or other major crisis situations.

Introduction

All countries seek to develop and implement foreign policies and strategies to protect and promote their national security interests. These policies and strategies apply to relationships with other states and non-state organisations, in peace, crisis and war. The national interests involved may be strategic, military, economic or societal, or a combination of any of these, but in all cases will also be political.

A country's intelligence agencies are one of the resources of government able to provide input into such policies and strategies. The intelligence community normally comprises three functional groupings. The first are the collectors who feed their product to the second grouping, the assessors, or the all-source analytical agencies. The latter are the major intelligence contributors to government knowledge, decision-making, policy development and strategies. The third less-recognised grouping are the 'doers', those agencies that are empowered to undertake "secret" activities that support the implementation of policies and strategies. Normally, the input of intelligence agencies will complement those inputs by the other agencies and elements of government. However, in many circumstances, the intelligence input can be significant, and in some circumstances, unique.

The principal intelligence agencies reviewed in this paper are those responsible for the provision of human intelligence (HUMINT), signals intelligence (SIGINT) and imagery intelligence (IMINT) on foreign targets. Potentially, they are able to contribute in two ways:

- firstly, by intelligence support through the provision of secret intelligence during both the development and implementation phases. During the development phase, the focus of intelligence collection would be to contribute to the assessment and decision-making process and thus assist policy-makers to formulate the most effective policies and strategies to deliver national advantage. During the implementation phase, that focus would be to provide policy-makers with a continuing flow of secret intelligence to monitor the effects of their strategies, and assist them to make sound judgements about any need for changes to strategies.

- secondly, by undertaking Covert Action (CA) during the implementation phase. CA comprises a broad range of activities that seek to shape or influence behaviour and events that will help bring about the outcomes being sought.

Where two or more countries seek common-interest outcomes they will usually cooperate and coordinate their actions to their mutual benefit. Often that will include high levels of cooperation between their intelligence agencies, as is presently the case for countering both the threat of international terrorism and the proliferation of weapons of mass destruction (WMD).

In principle as well as practice, the activities of the intelligence agencies of all major and middle-ranking states, including Australia, must be undertaken in a policy context, and at the direction of government. They must also be coordinated with related activities by other agencies of government in the normal open or 'overt' domain.

All intelligence operations entail some risk. Generally, the greater the criticality of national interests involved, the greater the willingness of countries to employ their intelligence agencies in higher risk operations to protect and promote those interests. Government is responsible for setting the "politically acceptable" parameters of operations i.e. the "intelligence rules of engagement", and must take ultimate responsibility for those operations. However, the agencies are responsible for ensuring that government is fully aware of the risks when planning and approving such operations, and for the professionalism of their execution.

This paper reviews the collection and covert action activities of the intelligence agencies, and some general effects in support of the policies and strategies of various sponsors during and since WW II. The paper also reviews the status of relevant Australian intelligence agencies in the context of these activities, and recommends the government remove the legislative prohibition on the Special Operations aspect of Covert Action. Removal of this prohibition would give present and future Australian governments the option of greater flexibility of action, in appropriate circumstances, to counter

possible threats to Australia's national security interests, including traditional military threats, and non-traditional threats such as international terrorism and proliferation of WMD.

Functions of Intelligence Agencies

Although the HUMINT, SIGINT and IMINT agencies are all collectors of secret intelligence on foreign targets, only the HUMINT and SIGINT agencies have the capacity to engage directly in Covert Action.

SECRET INTELLIGENCE

Secret Intelligence is information obtained unilaterally, or through liaison, which the targeted organisation (state or non-state) has sought to deliberately withhold for national or self-interest reasons, from the collecting country(s). It is information obtained by clandestine means, that is, by activities conducted secretly (i.e. using "tradecraft" techniques) to hide the fact that they are taking, or have taken, place. Usually, that information is obtained by recruited agents, orally or in documentary form, or by technical means.

COVERT ACTION

Covert Action comprises activities undertaken to shape or influence a foreign situation or events in order to promote outcomes in the national interests of the sponsor. These activities usually will be covert, and often clandestine. Covert activities are those designed to hide the identity of the sponsor; ideally they are not attributable to the sponsor, but as a minimum they are plausibly deniable by the sponsor. Clandestine in this context can mean hiding the fact that such activities have occurred, or that any external sponsor is involved.

LIAISON

Where mutual interests and common goals apply, the beneficial effects of liaison with the intelligence agencies of other countries can be significant, for all parties. These include the benefits of access to a broader range of intelligence through exchange agreements[1], and often capability development through training or technical assistance. Operationally, the benefits can include access to more diversified resources, and greater access to targets that would be inaccessible, or difficult to access, through

[1] Three potential concerns with liaison intelligence are the reliability of reporting, particularly where source details are limited or unknown, reliance where no other substantial intelligence is available, and the possibility of a deliberate feed of selected intelligence that supports the national interests of the liaison agency and its government. The vulnerabilities of reliability and reliance on liaison intelligence, both raw and assessed, were uniquely demonstrated when some key parts of the "evidence" of Iraq's possession and intention to use WMD, presented to the UN on 5 February 2003 by then US Secretary of State, Colin Powell, were subsequently discredited or disproved. This "evidence" was a major justification for the US-led invasion of Iraq in March 2003.

unilateral operations. But the agencies that are recipients of new intelligence or capabilities may also use these to advance their own separate agendas, which may or may not coincide with the short, medium or longer term policy interests of the sponsoring agency or country. The intelligence agencies, and their governments, in such liaison relationships must be alert to any broader agendas, and the acceptability of policy implications involved.[2]

Intelligence Collection

REQUIREMENTS AND LEAD TIMES

It is not intended to go into detail here about the actual methods of intelligence collection by the respective agencies. But if secret intelligence is to support effectively both the development and implementation of policies and strategies, agencies must know what their government's foreign policies are, what national strategic outcomes are being sought, and the precise collection requirements relevant to those outcomes. Also, the intelligence collected must be reliable, timely, and ideally where CA is proposed, "actionable" i.e it can directly assist in the planning and implementation of CA.

The relative abilities of agencies to fulfil their customer's secret intelligence requirements will depend on the particular circumstances relating to each target (who, what, where, etc.) and each agency's capability against that target (including necessary expertise and target access). An important part of the intelligence process (the timely delivery of quality secret intelligence to meet customer needs) is anticipating the potential requirements and investing the necessary resources in advance in order to have the skills and assets in place when required.

GOVERNMENT RESPONSIBILITIES

Governments intending to collect secret intelligence must appreciate that without such prior planning and investment, developing the necessary resources from a cold start can take considerable time. Factors that could dictate lead times include the recruitment and training of new staff, technical infrastructure investment, deployment, and in the case of HUMINT for example, the identification, recruitment and training of agents. Government must understand how these lead times can constrain their options for use of secret intelligence to deliver national outcomes, in the short, and perhaps medium, term.

[2] This, for example, was a major concern of the US government after 11 September 2001 during their dealings with the 'tribals' in Afghanistan to eliminate al Qaeda forces based there, and the ouster of the ruling Taliban regime. See Bob Woodward, *Bush at War*, Simon & Schuster, NY, 2002, p. 35.

The agencies must also ensure government is aware of the risks involved in collection operations, especially where the activity involves new targeting or a significant change of the operational environment. But, ultimately, decisions about resource funding or risk acceptance, and their implications, are risk management decisions for which government, not the agencies, must take responsibility.

AGENCY STRENGTHS AND LIMITATIONS

It is important to understand the strengths and limitations of different collection methods when reviewing secret intelligence collection in support of policies, strategies and operations.

The strength of HUMINT is its ability to obtain intelligence directly from and about people; their intentions, plans, attitudes, and potentially, to network those assets to give a broader reach across multiple targets. In sum, its strength is in the so-called cognitive domain.[3] Also, its strength relative to overt human source collection is primarily access to information deliberately withheld from the (collecting agency's) sponsor by the targeted organisation or individual. The limitations of HUMINT can include source access and reliability. It is essential for both case-officers and customers to know these.

SIGINT's strength is its ability to provide intelligence from or about various forms of communications[4]. That may include the intercept, and decryption where applicable, of written and oral communications. It might also include, through network analysis, intelligence about a target's command and control systems, structures and deployment. Collection methods can include space, aerial, maritime or land-based intercept systems. They can also include computer network exploitation (CNE) i.e. penetrating IT networks and databases to extract the intelligence within. The major limitations of SIGINT can be the inaccessibility of some key communications, and its inability to deliver directly on intentions or other critical information that is not contained in intercepted communications.

IMINT's strength is the provision of optical and geospatial intelligence in its many forms, e.g. photographic, electro-optical, radar, infrared etc., i.e. intelligence that would not normally be available by other means[5]. As with SIGINT, imagery collection is possible from space, aerial, maritime and land-

[3] Some of the better known examples of HUMINT assets that provided key, timely and often actionable intelligence across the political, military and counter-intelligence spectrums include the British "Cambridge Five" (Kim Philby, Guy Burgess, Donald McLean, Anthony Blunt & John Cairncross) run by the KGB; Colonel Oleg Penkovsky and Oleg Gordievsky, both Russians run by CIA and UKSIS; and Gunther Guillaume, a member of East Germany's HVA (Main Intelligence Directorate) who worked within the private office of West Germany's Chancellor Willy Brandt.

[4] The breaking of German and Japanese codes during WWII provided the allies with critical intelligence about both countrys' military plans and operations, and contributed significantly to their ultimate defeat.

[5] IMINT was the key source of US intelligence during the 1962 Cuban missile crisis.

based platforms. Its major limitations, like SIGINT, can be providing direct intelligence about intent, and only being able to access targets that are "visible".

Both SIGINT and IMINT can also provide unique intelligence support to HUMINT operations, and vice-versa.

Depending on the circumstances, only one of the above methods might be capable of collection against a target. But where two or all three agencies are capable of target access and collection, they can usefully collaborate and complement one-another in terms of delivering different parts of the jigsaw, or providing collateral for the product of another agency, or other, including open, sources. Politically, HUMINT is generally more high-risk because of its intrusive collection methods, but because of the infrastructure costs of other collection methods, HUMINT usually is the least expensive method of collection. As indicated above, acceptable degrees of risk and cost are matters for governments to decide based on the criticality of relevant national interests.

WHOLE-OF-GOVERNMENT COLLECTION AND ASSESSMENT

It must be re-emphasised that secret intelligence collection is only one of the resources available to governments in the information/intelligence collection process. It does not and should not operate in a vacuum; it complements the continuing collection of information and intelligence through normal open or overt sources, both unilateral and third party/liaison (including, of course, the exchange of confidential information through diplomatic and other means). Usually, these open or overt sources will be the main sources of information and intelligence into the policy process. But the intelligence agencies can create their own unique niches of access and can be the main, and sometimes only, sources of intelligence input to government on some key requirements.

Finally, high quality intelligence collection alone is not enough. The broader needs of the national security policy-making process also require a high quality analytical and assessment capability, and other highly efficient integrated mechanisms, including comprehensively networked data bases and communications systems, to support the process.

Covert Action

Covert Action (CA)[6] may be divided into two categories:

- firstly, **Special Operations** (SO), which includes paramilitary and any other activities employing physical force in its many forms, and

[6] Referred to by the Russians and former Soviet Bloc nations as Active Measures.

- secondly, **Covert Influence,** i.e. activities that often use information and psychological methods to deliver outcomes through effects within the cognitive domain. These operations do **not** employ physical force.

SO is at the hard end of the CA spectrum. It is as much a fundamental tool of war as conventional military operations. It has also been employed extensively in warlike and crisis situations, including during the Cold War, and, currently, aspects of counter-terrorism and counter-proliferation.

Covert Influence is the soft end of the CA spectrum. As mentioned, it is used to shape and influence activities in the cognitive domain. It has an important role in war or warlike situations, but also can and has had broad applications in peace.

While SO and Covert Influence are two separate forms of activity, SO will rarely, if ever, be conducted without Covert Influence being an integral part of the action plan. Covert Influence, on the other hand, can be conducted independently of and without any requirement for SO.

Both SO and Covert Influence activities have been conducted routinely against hostiles during war and crises. Neutrals and allies, both state and non-state, have been Covert Influence targets in war, crises and also peace. However, in war or a crisis where national-interest stakes were high, some sponsors of CA have shown limited concern about their involvement in some of these activities being seriously unattributable, or even plausibly deniable, especially regarding hostile targets. But in times of peace, the norm is for such activities to be both covert and clandestine.

The conduct of CA, particularly in peace, has provoked debate about issues of necessity, justification (including political, strategic, moral) and effectiveness. How governments, or sponsors, view the need for these capabilities, and the circumstances in which they would be willing to use them, will depend in large part on their perception of the criticality of national interests involved, the availability of other options to deliver similar national interest outcomes, and the ideological and cultural values of the sponsor. These issues are addressed further below. But historically amongst countries, the issue generally has not been the principle of having a CA capability, but what that capability should be at any given time (with the ability to expand that capability if necessary), and if, when and how to use it.

Special Operations

Special Operations (SO) covers a broad spectrum of activities, both offensive and defensive. During times of conventional and unconventional war, SO includes organising, supporting and co-ordinating partisan warfare by resistance forces in strategic areas behind enemy lines, and establishing or supporting escape and evasion networks. Crisis (including Cold War) and

peacetime activities have included supporting so-called wars of national liberation, other civil wars or provoking popular uprisings or public disorder to create regime change for ideological or other national-interest reasons. Equally, SO activities have been mounted to support governments threatened by these activities, by containing and potentially neutralising the source of threat. Also within the SO spectrum is non-state terrorism or similar activities that employ the use of extreme and indiscriminate violence to pursue ideological (political, religious, societal) agendas. Aspects of counter-terrorism also fit the definition of SO.

SPECIAL OPERATIONS AND WAR

Military historians accept that partisan resistance activity in occupied territory in both Europe and Asia during WW II was a military and political necessity. Resistance movements were supported or raised by the allies to hasten a military victory over the Axis forces. They did this by waging war in the enemy's strategic rear, thus complementing fighting by conventional armies in the tactical area of operations. They sabotaged manufacturing facilities of war materiel, disrupted logistic supply lines, and forced the diversion of large numbers of Axis forces from tactical to strategic areas to contain and counter the resistance. According to some sources, the ratio of diversion of Axis soldiers in Europe from the front lines per resistance fighter was as high as 10:1; i.e. a telling example of asymmetric warfare. The justification for this activity, generally, was not in question. The allies were fighting a war initiated by the enemy; partisan warfare was directed against enemy military targets and simply employed less conventional means to do so.

In addition to pursuing this common military objective, many allied powers also separately sought to use those resistance movements under their control to shape and influence their post-war political agendas. Very high levels of long-term national interest were involved e.g. from attempts to re-establish political and economic influence in former colonial territories, to the expansion of political and ideological influence, regionally and globally. The Cold War was one product of this.

The reasons why the allied intelligence agencies (UK's SIS and SOE, the US OSS and then Soviet counterpart, the NKGB, later called the NKVD)[7] ran the resistance movements were primarily twofold. Firstly, this activity was then an acknowledged function of such agencies (albeit with considerable

[7] SIS is the UK's Secret Intelligence Service. SOE was the Special Operations Executive, created in 1940 by Prime Minister Churchill. Its primary role was paramilitary, to "set Europe ablaze", complementing SIS whose primary role was intelligence. SOE was disbanded in 1946 and its functions subsequently taken over by SIS. OSS was the US Office of Strategic Services, established in 1942 and forerunner of the Central Intelligence Agency (CIA). The NKGB was the People's Commissariat of State Security; the NKVD was the People's Commissariat for Internal Affairs. Both were predecessors of the KGB, the Committee of State Security, which was established in 1954. Russia's Foreign Intelligence Service (SRV), established in 1991, is the KGB's current successor.

direct or indirect military support) given the special covert and clandestine requirements of activities. And secondly, it was because of the broader and increasingly important political objectives involved. While many of the military-related activities undertaken by the resistance were neither particularly clandestine nor covert per se (many were very visible and the Axis powers knew who their supporters were) the manoeuvring in pursuit of longer-term political objectives was much less visible. Towards the war's end, the latter also assumed much greater priority.

SPECIAL OPERATIONS AND THE COLD WAR

Globally, the four or so decades of "peace" that followed WW II were dominated by the Cold War, where many of the wartime resistance skills were again actively used. This period was characterised by a clash of political ideologies between East and West, and the "covert" exploitation of any cause or "ism" as both sides competed for national power, and control or influence within the broader regional and global domain. This struggle saw the creation and countering of proxy revolutionary wars, popular front uprisings, and various peasant or social reform movements or the like, which reached across Europe, Asia, the Middle East, Africa and Latin America. Within Asia for example, the communist parties of China, Vietnam, Laos, Cambodia, Thailand, the Philippines, Malaya, and Indonesia sought both regime and ideological change through revolutionary guerrilla warfare and other political means, and were supported in these endeavours by other ideologically sympathetic states. And the West was as committed to preventing a communist take-over in these countries.

The intelligence agencies of stakeholder countries were deeply involved in the Cold War for various reasons. Supporters of revolutionary warfare sought to keep it as covert as possible, to deny and disguise any foreign military presence, in order to credibly project the conflict as a "people's war". Opponents sought to expose that presence. Where it suited, covert warfare could circumvent international agreements on guaranteed neutrality, the cessation of hostilities and withdrawal of foreign military forces or support.[8]

[8] The "secret war" in Laos during 1962-73 is an interesting study. The 1962 Geneva Conference that guaranteed Laos its neutrality required the withdrawal of foreign military forces from the country. US forces withdrew, the North Vietnamese army (NVA) did not. The NVA deployed to protect infiltration routes along the Ho Chi Minh trail into South Vietnam, and also supplanted the Pathet Lao in prosecuting the revolutionary war to defeat the relatively weak Royal Lao army (RLA) and overthrow the Royal Lao Government (RLG). At the request of the RLG, the CIA raised and supported an army of mostly hill-tribe irregulars to be the lead force to combat the communists, particularly the NVA. At the height of the war, some 33,000 irregulars successfully kept in check some 70,000 NVA regulars, although the outcomes of some major battles see-sawed late in the conflict. CIA support was withdrawn as part of the general US disengagement from Indochina following the 1973 Paris Peace Accord. The NVA did not withdraw, and paralleling Vietnam, the communists took over Laos in 1975. One reason advanced for the non-deployment to Laos of US regular forces was an alleged understanding between the USSR and US that the former would not come to the direct support of Hanoi if the US did not re-deploy conventional forces into Laos. (That understanding, however, apparently accommodated some limited USAF close air support to the irregulars). Although the most

Covert warfare could minimise supporters on both sides being compelled to match any overt military presence of the other, and that situation cascading to a much more costly conventional war. The Super Powers in particular sought to avoid any escalation of conflict which might have precipitated direct confrontation between their military forces, and potentially bring into play the threat of nuclear force. The covert card and shadow play of deniability during much of the Cold War, therefore, served an important function for national stakeholders, even where the level of deniability often was largely notional.

Was SO during the Cold War justifiable and effective? At the risk of being too simplistic, Cold War outcomes, in terms of relative political and social freedoms, and economic well-being generally, saw global hard-line communism fail.[9] From a Western perspective therefore, the use of SO, as one of the means employed to counter violent revolutionary communism in particular during the Cold War, was both justified and effective[10].

TERRORISM AND COUNTER-TERRORISM

At the far end of the SO spectrum are acts of terrorism, characterised by the actions of such non-state organisations as al Qaeda and Jemiah Islamiah (JI) whose tactics to achieve their political and ideological aims include acts of extreme indiscriminate violence. While both organisations are non-state in nature and without a homeland, they have received secret support directly and indirectly from some sympathetic countries and organisations. This has included financial and materiel support, and the provision of safe bases for training and other purposes.

While the terrorists see acts of extreme violence as necessary and justifiable, most countries including Australia see them as totally unjustifiable and morally repugnant. The quest to track down, pre-empt, disrupt and ultimately destroy al Qaeda and the JI has seen an unprecedented surge in counter-terrorist related political, military and intelligence cooperation amongst many stakeholder nations, and the authorisation of military, law enforcement and many intelligence agencies to use lethal force where necessary.

expensive CIA covert action operation up to that time, former CIA members claim that until its end, the “secret war” was very successful, and the overall cost very small, compared to any comparable operation by US conventional forces.

[9] China stands out as a significant exception, still communist, but increasingly a global economic power. However, China today it is much less ‘traditionalist’ ideologically than it was in the past.

[10] This outcome does not mean, of course, that all political, economic or societal inequities exploited by East or West during the Cold War were or have since been resolved. Nor does it mean that for any like-conflict, the end justifies all means. Given the diverse political, ideological and cultural values of the countries and organisations involved, activities employed by some could not be condoned by Australia or countries with similar values.

Countering most well organised and elusive terrorist organisations can be operationally difficult and politically challenging, especially where the threat is direct and continuing, and the terrorists are being supported and harboured by another country. In these latter circumstances, particularly where all open representations to that harbouring country have been unsuccessful, the options for effectively dealing with that threat are limited. One option is an overt act of cross-border military force. However, where national and/or international political constraints preclude such overt action, SO offers a covert option. The necessity and justification for SO action in such circumstances is a matter for government decision. But where a country faced a grave, direct and continuing threat of terrorism in these circumstances, few nations would see such action as unnecessary or unjustified. The same principle would apply to similar threats from other sources.

OTHER SITUATIONS

History is also witness to other non-Cold War/non-terrorist-related situations since WW II involving SO intervention. The reasons for such intervention have varied, but included the prevention and pre-emption of a major physical threat from a neighbouring country, or to protect or pursue important political or other interests threatened or unattainable while a particular regime remained in place. Many such interventions have involved regime change, or attempted regime change, through a 'popular uprising' by opposition elements that were organised, trained and armed covertly by a third country.[11]

Covert Influence

The major focus of Covert Influence is the use psychological methods to deliver national advantage through effects in the cognitive domain. Covert Influence is designed to shape or influence the perceptions, decision-making and actions of one, or more, foreign target groups. It does this by targeting factors that shape their emotions, attitudes, motives, thinking processes and ultimately, behaviour.[12] Those targets may be hostiles, neutrals or allies, being state, non-state, or other groups or significant individuals, in one or

[11] Examples are Libyan intervention in the Sudan, Chad and Tunisia, and Algerian intervention in the Western Sahara in the 1970s/80s. In Iraq's case, author Laurie Mylroie in her book *Bush Vs The Beltway*, Regan Books, 2003, pp. 72-104, claims that US Presidents Clinton and George W. Bush both considered programs of major covert support to Iraqi opponents of Saddam Hussein to help remove Saddam from government. Mylroie attributes the faltering of both programs primarily to a lack of agreement among the White House, Defense, State Department and CIA over which opposition groups to support. The resultant stalemate was overtaken by Bush's decision to invade Iraq in March 2003. Assuming majority Iraqi support for Saddam's removal, it is interesting to speculate on what the Iraqi internal and regional political and security situation might have been today, and the relative costs, including those of military and civilian casualties, had Saddam been removed by a covertly-supported successful Iraqi-led coup or 'popular uprising', versus the US-led war.

[12] Means used could range from subtle persuasion to blatant propaganda.

multiple countries. In the case of the latter, the specific targeted effects of Covert Influence might be to gain international understanding and support for the policies and actions of the sponsoring nation and its allies, while simultaneously neutralising or discrediting those groups (state and non-state) opposed to these.

In wartime, the primary focus of Covert Influence would be fourfold: firstly, to boost the commitment and morale of allies; secondly, to win the support or sympathy of neutrals, or at least keep those targets neutral; thirdly, within hostile nations, to demoralise and undermine popular or factional support for the war, and ultimately the commitment and will of their military, population and politicians to wage war; and fourthly, to shape post-war strategic outcomes.

Covert Influence operations would also be coordinated with and support the SO plan. They must also be coordinated with parallel action in the open or overt domain, especially public diplomacy.

METHODOLOGIES

The methods available to achieve planned outcomes through HUMINT and SIGINT resources in peace, crisis or war, are diverse. Selecting the most appropriate means of delivery to reach identified targets (eg the public generally, the government, political opposition, other specific influential interest groups) is important and can determine the success of an operation. In some aspects, these operations may parallel a sophisticated public relations campaign i.e. what is the product being marketed, why is it better than other products being marketed, who are the target audience(s), what variation of product best suits each audience, how do you access the audience, how do you monitor audience penetration and response?

HUMINT. Methods available within the HUMINT toolbox have included:

- Funding operations, targets being:
    - political parties, student groups, women's groups, organised labour, peace groups, professional groups, other thematic, ethnic, or religious groups.
    - media outlets including radio, TV, internet websites, newspapers, journals, magazines, films, posters
- Propaganda
    - white (directly attributable to the sponsoring nation), grey (attributable to source(s) sympathetic to the sponsor), black (unattributable to the sponsor or allies)

  - factual information or disinformation (including forgeries)
  - dissemination by media outlets, plus graffiti, SMS, leaflets etc.

- Protest activities (non-violent) within the target country, and internationally
  - domestic strikes, boycotts, demonstrations, other civil action
  - the same activities but in third countries, including strikes at foreign owned factories, boycotts of imported products, the cessation of or imposed restrictions on economic aid, financial credits, private sector investment, military aid etc.

- Other
  - the use of clandestine agents, and agents of influence

SIGINT. The SIGINT toolbox includes a range of radio/broadcast and non-kinetic electronic techniques:

- computer network attack (CNA), involving the penetration of computer systems within or outside a target/host country(s) in order to destroy and disrupt the primary and supporting systems, and deny access to, corrupt, alter or falsify data within. Such targets could include government or military critical information or command and control (C2) networks, control systems or the operations generally of selected public or private infrastructure or other production facilities within that/those country(s). Specific infrastructure and production facilities could include power supply, transport, media publishing or broadcasting facilities, or selected manufacturing facilities, especially where these are involved in the production of WMD components or other weapons.

- other computer network operations (CNO)[13] or electronic attack methods that destroy, disrupt or corrupt computer-based control systems and data-bases by the use of electronic pulse techniques e.g. concealable and mobile high-energy radio frequency (HERF) weapons.

- other denial operations using clandestine means that target specific radio communications or broadcast systems

- deception operations to protect other clandestine activity.

[13] Computer Network Operations (CNO) is the generic term used to cover all forms of such operations, and thus includes CNA and CNE.

- support to radio or electronic-based HUMINT propaganda activities

APPLICATION

Where the technology existed and operational circumstances were appropriate, the above HUMINT methodologies have been used by various foreign intelligence agencies during and subsequent to WW II. On the issues of deniability and unattributability of funding and media operations, it should be noted that an organisation or individual being used for these operations may not necessarily be aware of any intelligence connection, or even the true nationality, of the sponsor.[14] In addition, media organisations and/or individual journalists who are not known or suspected of having any undue affiliation with the sponsor, or that sponsor's government, may have greater credibility, and thus greater direct and indirect influence,[15] amongst their target audiences, particularly target audiences in third countries. It should also be noted that the use of disinformation is, potentially, two edged. It might achieve important short-term outcomes, but if, or often when, the truth emerges the source may lose credibility and be of lesser utility afterwards.

Many of the CNO methodologies in the SIGINT toolbox are still being developed, especially within the US, UK, China, Japan, India, and Russia, but within smaller technically advanced countries also. For the latter, one immediately identifiable advantage offered is an asymmetric warfare capability. In wartime, CNO also offers the advantage of reach into areas that may be inaccessible to military forces, and may also be inaccessible to HUMINT resources.

CNO operations have three other potential advantages: firstly, the ability to destroy or disrupt a target without the use and possible collateral effects of traditional physical or kinetic force; secondly, remote target access and thus a lower risk in terms of possible casualties; and thirdly, it can be much cheaper compared to other options. But two major potential disadvantages apply. One is the difficulty of limiting any non-physical collateral damage, especially where that damage might raise ethical issues e.g. shutting down an electricity power station to disrupt an arms factory in a target country but where that closure could also cut off power to hospitals and other essential services to the civilian population. The second are legal issues. These can apply where access to the target country, and the target itself, would necessitate hacking through computer networks in third countries, or where the facilities intentionally targeted or unintentionally affected, belong to third country shareholders. These issues might be less of a challenge to justify in war, but could be very sensitive politically in peace. But as for all possible

[14] Such situations are a form of "false flag" operations and the persons used are unwitting agents of influence.

[15] One form of indirect influence would be the further dissemination of a media article through its syndication to or carriage by other national or international media outlets.

covert action operations, their justification and risk acceptance are matters for government to decide.

The Intelligence Agency-Military Relationship

Defining the relationship between intelligence agencies and the military is important, particularly where SO activities involve raising, training, supporting or directing para-military forces. There is no set formula. Historically, the relationship has depended on various factors, including the structure and capabilities of the intelligence community within the sponsor country, its relationship with the national defence organisation and government, the nature of the target, the criticality of national interests involved, and outcomes sought.

Where deniability and unattributability have been politically important, where complex intelligence targets and high levels of tradecraft have also been involved, and especially where targets and outcomes were highly political, related activities have usually been run by the intelligence agencies. Depending on the scale of para-military operations in the target country, including logistic support operations, these aspects have been conducted either by military-trained specialists (usually ex-military) who were members of the agencies, or military personnel seconded to the agencies.

Where circumstances have escalated to the involvement of large-scale para-military activities, and/or the need for deniability has been of lesser importance politically, the activities usually have been run by the military, with the agencies conducting the more complex intelligence aspects. Other variations have also applied depending on sponsors and circumstances.[16] In all cases, overall policy direction and strategic co-ordination was exercised by government.

The Australian Agencies

Australia has HUMINT, SIGINT and IMINT intelligence agencies i.e. the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO). ASIS, DSD and DIGO have the collection of foreign intelligence as their prime function, and this is stated in relevant legislation i.e. the Intelligence Services Act

[16] Circumstances can also arise where such an operation could transfer from intelligence to military control. For example, where war-like hostilities were imminent, the recruitment and training of partisan "staybehind" intelligence and paramilitary assets within the potential aggressor country prior of the outbreak of hostilities, would be an intelligence agency responsibility because of deniability requirements. Once hostilities break out, deniability normally would no longer be a political issue. The military could then take over the paramilitary assets and, potentially, routine military-focused intelligence assets. The agency would continue to run and develop other intelligence assets in support of both military and broader government requirements.

(ISA) 2001, as amended. While ASIO's primary responsibility is the collection and evaluation of intelligence about the security of Australia and its interests, it is also mandated under the ASIO Act 1979 to collect foreign intelligence in Australia. In certain circumstances, the proposed means of collection must have prior authorisation by warrant.

As stated above, only the HUMINT and SIGINT agencies have the capacity to engage in CA. In Australia, however, none of the foreign intelligence collectors are mandated by legislation to conduct CA activities per se.

The legislation under which ASIO and DSD operate does not specifically prohibit those agencies from engaging in CA. Potentially, therefore, ASIO could become involved in Covert Influence activities involving agents or access in Australia where directed to do so by an appropriate authority. Section 7 of the ISA in particular enables DSD to provide "assistance" to Commonwealth (and State) authorities in the broad area of "cryptography and communications technologies." This would include assistance to ADF operational activity and, potentially, could include assistance to other intelligence operations approved by the Minister for Defence.

ASIS is different. When established in 1952, ASIS was modelled on the UKSIS which had both an intelligence collection and a covert action capability, a derivative from WW II.[17] Thus, CA became one of the initial functions of ASIS. Justice Hope, in his Royal Commission Report into the November 1983 Sheraton Hotel incident, described that function more fully as "to maintain a covert action capability for war-time or other very special circumstances" and "to be maintained only on a contingency basis."[18] Referring to special operations as a subset of covert action, Hope added that "it has always been clearly understood that any use of special operations would not be countenanced outside of special circumstances, and that prior ministerial approval would be required for any step at all into the special operations field."[19]

Hope said ASIS had made only limited and cautious progress in developing a SO capability up until the early 1980s when, with ministerial approval, it developed a new capability in-being, and recruited and began training a small cadre of part time agents for that purpose.[20] This initiative went badly awry during a training incident at the Sheraton Hotel in Melbourne's central business district in November 1983.[21] As a result of Hope's investigation

[17] See footnote 7.
[18] R.M.Hope,*Royal Commission on Australia's Security and Intelligence Agencies: Report on the Sheraton Hotel Incident*, Commonwealth Government Printer, Canberra, 1984, para 3.2. (public version).
[19] Ibid para 3.6.
[20] Ibid, paras 3.6, 3.7 & 3.9.
[21] This incident took place in the Sheraton Hotel in Melbourne on 30 November 1983 and involved a covert hostage rescue exercise in a notional overseas setting. The rescuers, who

into and aftermath of the incident, Hope recommended in his classified report that SO be removed as a function of ASIS. The government instructed ASIS to disband the capability accordingly. However, according to retired senior intelligence officials, it was not Hope's intention that Australia no longer have such a capability, but no other government agency then existed, or now exists, that could exercise that function on an unattributable or plausibly deniable basis.

That capability was not formally revisited until addressed by the 1995 Samuels' Inquiry into ASIS. The Inquiry report included the recommendation that the existence and functions of ASIS be defined in legislation, and that ASIS not engage in activities involving "force or lethal means".[22] This latter recommendation was not raised with ASIS officials during the Inquiry, nor were reasons for it given in the report.

In 2001 the Intelligence Services Bill (ISA) was submitted to parliament and defined the functions of ASIS, and DSD. It also included Section 6(4) which states that ASIS and its agents

> must not plan for, or undertake activities that involve (a) paramilitary activities or, (b) activities involving violence against the person, or (c) the use of weapons.

In an address to the House on 27 June 2001, Foreign Minister Downer described these activities as "not relevant to the functions of ASIS."[23] Both the Government and Opposition were keen for the Bill to have a smooth passage through Parliament, and for SO to be a non-issue in related parliamentary debate. The Bill was passed with bipartisan agreement.[24]

In 2004, in response to fundamental changes in Australia's national security interests and the ASIS operational environment,[25] Parliament amended Section 6(4) via Note 1, and a new Section 6(5) was added, both with bi-partisan agreement. Note 1 enables ASIS to be involved with the planning

---

wore masks and carried (unloaded) weapons, had not informed the State or hotel authorities about the exercise. Unintentionally, hotel staff and guests became involved and a police chase resulted in the arrest of some of the rescuers when fleeing the scene. At the request of the then Prime Minister, the Hon. R.J. Hawke, Justice Hope investigated the incident.

[22] Gordon J. Samuels & Michael H. Codd, Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service*, Public Edition, Australian Government Printing Service, Canberra, 1995, p. xxix, para 37.

[23] The Hon Alexander Downer, MP, House of Representatives, Intelligence Services Bill 2001. Second Reading, Hansard, 27 June 2001.

[24] The author, in his submission dated 20 July 2001 to the Joint Select Committee on the Intelligence Services, recommended that the decision of Government not to include SO as a function of ASIS be implemented by non-legislative means to ensure greater flexibility for policy change in response to any future national security crisis. See "Joint Select Committee on the Intelligence Services: An Advisory Report on the Intelligence Services Bill 2001, the Intelligence Services (Consequential Provisions) Bill 2001, and certain parts of the Cyber Crime Bill 2001", Submissions, Commonwealth of Australia, August 2001.

[25] House of Representatives Explanatory Memorandum to the ISA Amendment Bill 2003.

or undertaking of paramilitary activities *by other organisations* provided that staff members or agents of ASIS did not undertake those activities. Section 6(5) now enables members or agents of ASIS to carry weapons for self-defence.

The Government identified the changes to Australia's security interests and the ASIS operational environment responsible for the above amendments as being international terrorism, WMD, transnational crime, and the "imperative" of close cooperation with unspecified "other organisations".[26] While it was not the government's intention via Note 1 to enable ASIS itself to get involved in SO, this change would enable ASIS to cooperate with foreign liaison organisations actively engaged in SO-like operations in their own, *as well as Australia's*, security interests.

While ASIS's potential involvement in SO is limited as above, Section 6(1)(e) of the ISA enables ASIS

> to undertake such other activities as the responsible Minister directs relating to the capabilities, intentions or activities of people or organisations outside Australia.

In 2004, when asked by the Bulletin magazine what this meant, Foreign Minister Downer said it involved ASIS doing "work on things such as counter-terrorism, people smuggling, weapons of mass destruction, particularly trafficking in WMD, that sort of thing." Downer added that Australians "would expect a government agency to do that sort of thing on their behalf…they'd be surprised if we didn't."[27] Could that "work" involve Covert Influence activities? Potentially, yes; there is nothing in the wording of Section 6(1)(e) to preclude ASIS from engaging in such activities if directed by the Foreign Minister.

The most recent DFAT and Defence White Papers[28] have highlighted the uncertainty and complexity of Australia's external security environment. The Asia/Pacific region is home to some of the world's most volatile flashpoints, and to active and brutal terrorist organisations that have and continue to target Australia and Australians. Threats from unstable and, potentially, failed states as well as proliferation and other transnational causes, also exist. Wherever possible, Australia has and will continue to deal with these threats through cooperation with its neighbours, other allies and multinational organisations. And at times, Australia will be expected to take the lead role in such cooperative action. But Australia must also be able to act independently if required. In either case, Australia must have the best-

[26] Ibid.
[27] *The Bulletin*, 6 April 2004, p. 19.
[28] *Advancing the National Interest: Australia's Foreign and Trade Policy White Paper*, Commonwealth of Australia, Canberra, February 2003 and *Defence 2000 – Our Future Defence Force*, Commonwealth of Australia, Canberra, December 2000.

available knowledge, skill-sets and resources to pursue the most appropriate policies and strategies to combat these threats. A strong and flexible foreign intelligence capability is an essential inclusion in the related inventory of assets to deliver required outcomes.

It is not difficult to envisage a regional situation arising where a grave and direct threat to Australian security interests emerged, and where the Australian government found it necessary, and unavoidable, to take the initiative using all available means to protect its people and national interests from that threat. It may also be assumed that in such a situation, members of ASIS and its agents would be directly engaged in intelligence collection and other activities authorised under Section 6(1)(e) of the ISA to protect and support those interests. Yet members of ASIS and its agents are prohibited by law from direct involvement in any potentially critical SO activity to pre-empt that threat, to delay it thus providing valuable lead time for intense diplomatic and ADF intervention and prevention, to provide direct support to deployed ADF forces, and to assist in shaping post-conflict outcomes. In sum, the Australian parliament has denied Australian Governments this potentially vital SO option.

Removing the prohibition and enabling the inclusion of an ASIS SO capability amongst the inventory of national-interest options in war or major crisis does not mean that activity will be utilised, any more than some existing high-end Defence capabilities will be employed other than in special situations where warranted. Both are contingency options; the circumstances of their possible employment is a matter for government to decide. But if parliament authorises ASIS to re-establish a contingency capability in SO, it should do so before a crisis arises, not in response to a crisis. Timeliness is critical; adequate lead times are required to define and develop that capability, especially from a cold start.

Conclusion

Historically, the intelligence agencies have played an important role in supporting, shaping and influencing the development and implementation of the international policies and strategies of sponsor organisations, in peace, crisis and war. But they are not the primary drivers of policy. As collectors, each is only one contributor to the all-source information/intelligence pool that feeds into the assessment process. As doers of Covert Action, they operate within a policy context and complement the activities of the other open or overt activities of government.

The skill-sets required by these intelligence agencies to be able to deliver quality services and outcomes in the areas of both secret intelligence collection and CA, are complex and often require long lead times to develop and implement. Once these skill-sets have been attained, it is important that government at both the political and officials level understand what options

these resources offer, and the means and risks involved. Ultimately, the willingness of government to employ these resources, to approve the methodologies employed, and accept the risks and responsibility for doing so, will depend on the criticality of national interests involved, and national ideological and cultural values. These can and have varied significantly from country to country.

Australia has sophisticated and capable HUMINT, SIGINT and IMINT intelligence agencies. All have a solid reputation for delivering quality and timely intelligence to government on major intelligence requirements, and contributing to the national assessment process, to government knowledge, and the development and implementation of government foreign policies and strategies. The HUMINT and SIGINT agencies have the potential, under their current legislation, to contribute also to national security interests by undertaking Covert Influence activities, where approved by their respective Ministers.

In response to a changing and growing direct threat to Australia's security interests, the Government and parliament amended the ISA in 2004 from an absolute prohibition on any ASIS involvement with SO to limited involvement in the planning and undertaking of SO activities *by others*. In 2005 the government amended the ASIO Act and counter-terrorist laws to significantly upgrade the powers of the security and law enforcement agencies, and the courts, to combat a more serious and imminent threat from terrorism. That increased threat to Australian citizens and interests is as real overseas, particularly within the Asia/Pacific region, as in Australia. But members of ASIS and its agents remain prohibited by legislation from direct involvement in the conduct of any form of potential SO activity to lessen that risk. No such legislative prohibition applies to the other agencies.

It is recommended that the Government consider further amending the ISA to remove any prohibition on direct ASIS involvement in SO. This would enable consideration of SO as a potential optional tool for use in war or other crisis situations, such as combating terrorism. Whether that option is exercised, and if so, how, is a matter for government to decide.

Ian Dudgeon is the principal of a Canberra-based consultancy whose services include advice and reviews concerning national security issues. He has served in both the Foreign Affairs and Trade and Defence portfolios, and held senior appointments in the Australia intelligence community. He is the author of major policy studies for government on AIC support to military operations. information operations, and the national information infrastructure. iandudgeon@netspeed.com.au.