IDSS COMMENTARIES (105/2006)

IDSS Commentaries are intended to provide timely and, where appropriate, policy relevant background and analysis of contemporary developments. The views of the authors are their own and do not represent the official position of IDSS.

It Sure is Dark in Those Classified Caves
Open Source Intelligence for National Security

Tom Quiggin[*]

27 September 2006

NATIONAL security intelligence requirements are increasing in both the subject matter required and the speed at which actionable reports are needed by senior leaders. An already uncertain and complex international environment is becoming increasingly unstable. Concurrently, the potential lethality of both known and unknown asymmetric threats is increasing, raising the overall costs in the event of warning failures.

The current national security threat is devolving downwards from systems threats (countries or large organizations) to the individual or small groups (such as self-forming terrorist groups). National security intelligence must provide for possible intra-state conflicts, but it must also deal with non-traditional threats from transnational terrorism or critical infrastructure disruptions. Unfortunately, most of the highly technological and classified intelligence systems were designed to operate against country-level Cold War-style threats. These highly classified systems work well against large scale threats such as armies or nuclear installations, but they cannot perceive individual level capabilities or intentions.

Need for the bigger picture

With a dynamic and complex threat environment, a developed country now faces the need for an increasing number of people who can see and understand the bigger picture. In Singapore, the past successes were made by a few key risk takers who had made closely calculated decisions that have proved successful. Now, decisions that will affect the future will require a broader range of inputs than similar decisions in the past. Furthermore, the decisions will have to build in more flexibility and scalability to adapt to developing external pressures and technological change. And they will have to be made faster.

Timeliness and accuracy are the two bywords of intelligence, whatever the particular area of leadership requirements. Of the two, however, timeliness is the most critical. A variety of political and military leaders have repeatedly stated that even a partial intelligence picture with flaws delivered in a timely manner is more useful than the best intelligence provided after the fact.

Looking behind the varied list of threats that could negatively impact Singapore's national security and economy, the most serious threat could be the information gap between what is known and what needs to be known. To be clear, the world is currently awash in data and has been since the late 1960s. Obstacles exist, however, in getting information from where it is, to where it is needed in a timely manner. A series of technological promises of the past have not fixed this problem, or at least not in governments.

Secrecy as a Liability

A globally observed obstacle to good intelligence is the obsession with secrecy. Repeated indications are that some 75% to 90% of classification is used to protect "turf" and reputations. Only a small minority of the information actually needs to be classified to protect sources, agents, or to prevent potential damage to the interest of the state. One result of over-classification is the building of bureaucratic bunkers or caves. In order to protect their classified information, bureaucrats build compartmented systems that in effect, cut off them off from the rest of the world.

A recent American case demonstrates how "dark" it can be in the bureaucratic caves of intelligence. In June of 2006, US government officials loudly complained that the New York Times reported the tracking of terrorist financial information. They believed that this would compromise efforts to track terrorists by alerting them to the fact they were being tracked. Most open source intelligence analysts and research institutions know that terrorists are aware they are being tracked. Terrorists have resorted to recruiting proxies, they are shying away from registered charities, they use non-formal transfer methods and they are increasingly self-financed either with their own funds legally obtained or through crime such as credit card fraud. The New York Times story, while wrapped up in the mystique of secrecy and intelligence, was reporting old news.

The products produced by classified agencies are also frequently beaten out by non-classified sources when they compete head to head. Various experiments in the past have embarrassed the classified intelligence communities badly. Even former US Joint Chiefs Chairman and former Secretary of State Colin Powell made a damning statement when he stated: "I preferred the Early Bird with its compendium of newspaper stories to the President's Daily Brief, the CIA's capstone daily product."

Closing the Gap – Open Source Intelligence

Open Source Intelligence (OSINT) can fill in most of the gaps immediately and at low cost. OSINT in not just open source information nor is it a substitute for all source analysis. OSINT is a distinct analytical process that integrates human expertise and open source information to produce policy relevant or actionable intelligence. If done correctly, it is as rigorous and timely as any other intelligence source. Currently, the majority of information and expertise are in the private sector – not government and the trend is growing towards more private sector dominance.

OSINT is particularly well-suited to national security work, even though it lacks the "cool factor" of classified intelligence and is seen as a threat by many centralized bureaucracies. Why is OSINT so well-suited to national security asymmetric threats? There are six main reasons:

1. Many of the contingences or surprises that arise tend to do so in both geographic and thematic areas that are not covered by classified sources, but the government leaders will need the information anyway. The expertise required usually exists in the private sector.
2. OSINT allows for a greater flexibility when dealing with politicians, bureaucrats, foreign

partners and with civilian agencies that lack clearances. Information can travel faster and more efficiently. OSINT can also be shared with supra-national organizations or non-government organizations. This is both a domestic and an international advantage.

3. OSINT-based information can be shared more readily with the media and the public in order to better inform them of actual or impending risks.

4. A small number of OSINT analysts (two or three) can track and provide warnings on global phenomena that are of interest to the state. This can be done using complex Boolean searches on databases such as Dialog or Lexis Nexis assisted by the WWW.

5. OSINT is low cost as the private sector has already developed and paid for the infrastructure needed to support it. There is no need to develop costly software or hardware.

6. OSINT relies exclusively on information gained through legal and ethical means. It can therefore be used in court proceedings, quasi-judicial hearings or other public venues. It is a means of informing the public about threats in an open manner,

Outlook

Knowledge is the critical component in defeating an asymmetric threat situation. A good defence in an asymmetric struggle can only come from an understanding of the threat (knowledge) and therefore an ability to combat it or stop the threat before it materializes.
The same can be said of natural asymmetric threats such as pandemics or climate change. Classification is an obstacle to the movement of information and may be more of a vulnerability than an asset.

Secrecy is the ally of the weaker party in an asymmetric conflict while knowledge is the friend of the stronger party. Singapore and other states should try to find more ways of sharing information, intelligence and methodologies of defeating asymmetric threats. As such, greater alliances should be explored with partners that offer OSINT knowledge on threats.

[*] *Tom Quiggin is a Senior Fellow with the Centre of Excellence for National Security (CENS), a constituent unit of the Institute of Defence and Strategic Studies, Nanyang Technological University.*