Written by Per Andersson

"A proper analysis of the intelligence obtainable by these overt, normal and aboveboard means would supply us with 80 percent, I should estimate, of the information required for the guidance of our national policy."

Allen Dulles, 1947

INTRODUCTION

The role of intelligence is "to inform decision making – independently, impartially and with integrity." Intelligence itself is "the product resulting from the collection, processing, analysis, evaluation and interpretation of available information"; the important point being that raw information alone has no intrinsic value until analysed and filtered to meet the requirements of the customer. The key question then is, "How to find the best information to produce relevant and useful intelligence".

This paper will answer the question by examining the value of Open Source Intelligence (OSINT) primarily from the perspective of national security as it is at this level that intelligence efforts are focussed across the globe. It will be argued that Jardines is generally accurate in his statement that "OSINT should not be viewed as a panacea, but rather a highly effective component of the intelligence toolkit." The essay will consist of three parts, starting with a short background on the evolution from traditional to 'postmodern' intelligence before going into the details of OSINT. Mercado's criteria will be used to conduct an objective (albeit qualitative) comparison of the value of OSINT relative to other intelligence. Ultimately, "the only real measure of effectiveness must be the utility of intelligence to the customer," therefore this will be examined in the final section.

BACKGROUND

Traditionally the Intelligence Community (IC) has focussed on collecting information using clandestine methods and sources, from secret agents to covert technical surveillance. Within this institutionalised culture of secrecy and elitism, open sources where marginalised, despite the fact that, "OSINT produces the lions share of intelligence." Former CIA director, George Tenet, exemplifies this attitude with his description of the role of his agency as; "we steal secrets." This tradition was also responsible for the widely held misunderstanding that the value of intelligence is related to its classification; the protective handling of 'secret' information is purely to safeguard a sensitive source, human or technical. This prioritisation of the source over the customer often makes the intelligence product very difficult to utilise effectively, the greatest problem facing classified information, detracting immensely from its potential value. This led Colin Powell to comment, "I preferred the Early Bird with its compendium of newspaper stories

to the President's Daily Brief." Utilising expensive and susceptible secret sources as a first stop to gather information was illogical - as Teverton commented, "Assessing the value of secrets requires knowing what is already available publicly."

New trends within society

A number of trends have emerged since the demise of the Cold War re-shaping the world irreversibly. The information era, driven largely by the proliferation of the internet, and aided by the collapse of formerly denied areas, has resulted in information overload, to the IC, in a host of languages. The impact of globalisation is an environment far more unstable than before and for nation states the threats are ever expanding. Complex emergencies from traditional natural hazards are now matched by equally dangerous threats from transnational crime/terrorism with increasing frequency and lethality. Within this transformed framework, the requirements placed on the IC have dramatically increased, as has the cost of failure, yet the applicability of traditional secret collection methods have been called into question, particularly in areas of the developing world where little coverage exists.

During this time the IC has had to evolve into what Gibson describes as 'post-modern intelligence' – "a product of change and a tool to deal with it". He describes the intelligence function within a democratic society as a two-way relationship based on trust. With the reputation of western intelligence agencies at a low ebb post the failures of 9/11 and the Iraq WMD reports, transformation was inevitable. The 9/11 commission drove this in the USA, whilst in the UK the Hutton Enquiry led to a "desire for openness in civil society generally and the intelligence community in particular... to bring intelligence out of the closet." The IC are waking up to the reality that, "intelligence is about being in the information business, not the secrecy business... the IC does not have exclusive access to knowledge."

What is OSINT?

NATO defines OSINT as, "Unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question." It applies the proven intelligence process to a broad diversity of information legally available in public domain to create overt intelligence. Investigative journalists would recognise this process as very similar to the traditional operation of a newsroom. The use of open sources by various elements within the IC is nothing new; "in World War II, the Cold War and the Vietnam War, radio and print sources accounted for the majority of intelligence gathered." Reports from recent high profile commissions have led to a resurgence of interest in OSINT resulting in the creation of new organisations and appointment of executives specifically responsible for OSINT. Table one shows some of these landmark events involving OSINT organisations within the USA. The rapid expansion of the internet was another factor in the resurgence of OSINT, however the internet is, "not of itself a source but merely the means by which sources are accessed."

The principal open sources are:

Traditional media broadcasts.

Commercial 'on-line premium' services.

Specialist technical and tactical coverage (eg. Jane's).

'Grey Literature' – expert channels such as academia

Overt human observations – commonly NGOs

Commercial imagery

VALUE ANALYSIS

Speed

Timeliness is vital if intelligence is to result in successful action, particularly within dynamic situations such as the counter-terrorist game. "Even a partial intelligence picture with flaws delivered in a timely manner is more useful than the best intelligence picture provided after the fact." Hazards from emerging threats to natural disasters frequently manifest themselves 'out-of-area' where classified intelligence support is not readily available.

When a crisis erupts within a remote area, "intelligence analysts and policymakers alike will often turn first to the television and internet." When starting a cold search into a new area in reaction to a surprise event, OSINT will take time (proportional to the number and quality of skilled analysts dedicated to the task) to produce verifiable intelligence. Pro-active investment in OSINT, however, can provide an 'insurance policy' for areas of the world where classified resources are unlikely to be focused, resulting in almost instantaneous background information and possibly live links to observers in the area. Even when classified means are available, the dissemination of 'secret' intelligence is notoriously slow due to the sanitisation process. Technical means, such as Network-Centric systems, designed to increase the tempo of military operations, will not be able to overcome this obstacle where sensitive-sources are involved. OSINT, however, is unable to match the real-time surveillance, provided by covert means, that is required for specific law enforcement or military operations – particularly those leading up to the detention or elimination of dangerous criminals or terrorists.

Quantity

There is no shortage of potential open sources to interrogate for relevant information, therefore, "the odds are good that the composite bits of information assembled from the many can often approach, match or even surpass the classified reporting of the few." Those odds will increase considerably if investigators know where to look – if networks and databases have previously been established across a broad spectrum of areas. OS potential coverage is truly global and this information has a wide spectrum of applicability for, "operators, logisticians, acquisition mangers and all source intelligence professionals." Within this expansive ocean of information, OSINT collectors risk drowning in their attempts to identify relevant, reliable sources. Clearly the ability to understand, harness and exploit this potential is dependant upon the resources dedicated to this discipline, however there are technical solutions (such as complex Boolean

searches) that can assist with this.

Quality

Due to the large number of potential information 'feeds' and the difficulty in establishing the original source, OSINT is often accused of being hard to verify or evaluate, therefore producing an inconsistent product with reliability concerns. Worse still, a sophisticated adversary may use deliberate disinformation to confuse sources that are vulnerable to manipulation. But classified intelligence is also liable to contamination through poor quality secret sources, particularly HUMINT, relying on a small number of key informants, as has been demonstrated on numerous occasions. The veracity issues surrounding OSINT are associated with its perceived dependence on the internet, which is not a true reflection of its practice within professional intelligence agencies. When multiple independent sources are assessed and evaluated, the true picture emerges; quality will be assured through analyst expertise, and the passage of time engendering trust in the most reliable sources. The intelligence produced from OS has its limits; whilst it can provide very high quality background briefs and indications of trends and activity, it is, "rarely able to provide early tactical warning of impending attacks." This level of granularity can only come from highly focussed methods, targeted using the wider picture provided by OSINT.

Clarity

Whilst the original sources of OSINT can sometimes be unclear, reports will generally be well referenced, much like an academic paper, with citations identifying the sources creating a transparent, unambiguous product; "There is a clear path that shows how the analysis was arrived at, leading to greater reliability and accountability." Sensitive source intelligence, particularly HUMINT and SIGINT, lose much of their clarity in the sanitisation process resulting in "reports which were too general or broad to be of much use." This lack of clarity of confidential intelligence "contributed to the Iraqi WMD debacle in 2002-03."

Ease of Use

OSINT really distinguishes itself as superior to classified intelligence in its ease of use. As explained previously, the protective handling of classified material is its greatest liability, often rendering it useless for informing decisions or facilitating action by front line operators. OSINT can be rapidly disseminated to everybody who needs to know – from security operatives through first responder to the general public. Furthermore, the ability to share between departments, IOs, NGOs and nations not only ensures everybody has a common and up to date picture, it engenders trust and is partner forming, encouraging mutual support. This quality also gives it greater utility to law enforcement, particularly in court proceedings; not only is it generally admissible as evidence (having been obtained legally), it also protects classified sources that may also have been involved. However, whilst OSINT can provide leads for security operators to follow up, successful operations on this basis alone are rare – professional adversaries such as Al Qaeda are careful not to leave a trail (virtual or physical). Once again other specialist means are required to drill deeper into the layers of information.

Cost

The resourcing of specific intelligence methods is difficult to establish and the whilst the proponents of OSINT, generally people in the business or who are likely to benefit from involvement in research, will always claim it is relatively inexpensive, a quantitative comparison is rarely quoted. The 2005 allocation of one percent of the US intelligence budget to OSINT does appear disproportionately low, particularly given its track record and popularity with senior military and political figures. To be sure, establishing an independent OSINT capability requires significant money and effort to ensure sufficiently robust global coverage to cover most contingencies; skilled personnel together with subscriptions to a large number of targeted, quality sources comes at a price, but it still offers extremely good value when compared with the huge sums invested in secret intelligence. An alternative approach, advocated by Steele (a prominent figure in the OSINT private sector), is dependency on purchasing existing OS expertise, thereby negating the development and running costs. This is the preference of many businesses and NGOs but may not give sufficient, dependable coverage or resilience for governments. The expensive, secretive, technical means cannot be neglected in favour of OSINT; whilst these do not appear to offer the same volume of actionable intelligence, they deliver a unique capability which, in certain cases, is the essential ingredient in solving the intelligence puzzle.

PRACTICAL UTILITY

NATO is often cited as the model of a large security organisation leading the way in the practice of OSINT and General Kernan confirmed it is "a vital component of NATO's future vision." OSINT provides a "very robust foundation for other intelligence disciplines... (and) reduces demand on classified collection resources by limiting requests for information." The nature of the organisation and the contemporary operations it tends to get involved with calls for a common view, provided by validated OSINT, as the "most effective means of delivering decision-support." This compliments the all-source process, from strategic to tactical level, providing "tip-offs, context, validation and cover for information sanitisation."

But NATO is a special case and its enduring commitment to OSINT is due to two factors. First of all, "NATO staffs are unable to task classified collection. Second, the make up of NATO makes the sharing of classified intelligence very difficult, particularly amongst the partnership for peace and Mediterranean dialogue members, but also even within core nations.

Within the fields of proliferation, terrorism and counterintelligence, "the OSINT target is immense... with many paper trails winding around the world." It can also support the 'global war on terror' by providing a valuable "understanding of the ideological concerns and thinking," and perhaps even "a strategic 'barometer' of the adversary's intent." The internet is widely utilised by transnational criminals and terrorists – tracking online activity and financial activities has proven useful to law enforcement agencies. OSINT is certainly used by the enemies of the state, exploiting the openness within Western society and government. The internet alone provides unrestricted access to information that supports infiltration, targeting, weapon manufacture and evading detention; evidence from counter-terrorist operations confirms OSINT has been utilised in the planning of attacks.

OSINT continues to offer huge potential in other security sectors where secrecy is not required. From understanding and countering natural threats, affecting millions every year, to "generating resilience and competitive advantage... by returning decision-making and action to those individual decision makers." Steele proposes a concept of 'collective intelligence', with citizen as collector and consumer, relying on the combined brain power of large groups of people. This is already evident in the ways political parties or business boards decide policies and is inherent to cooperative services like wikipedia. Steele's vision of a citizen's intelligence network to enhance homeland security utilises existing cell phone technology as the means for passing data (voice, text or imagery) to a central cell which will corroborate then initiate an appropriate response. Similar situations have already occurred, post the 2004 tsunami and on the fourth aircraft on 9/11. Harnessing what everybody sees and knows can only enhance situational awareness and learning from the history of all people allows secret assets to focus more narrowly.

CONCLUSION

OSINT is not particularly new but after a long period of repression by the IC, its significance and relative importance has recently been rediscovered. It compliments conventional all-source methods, providing context for classified means to more effectively exploit 'difficult' targets. OSINT can also validate sensitive sources and provide cover for the utilisation of 'secret' intelligence. It has utility at all levels across the spectrum of security operations, particularly those involving multiple and diverse nations, IOs and NGOs. To exploit effectively, skilled analysts are required, supported by new technologies for searching through the plethora of data available – good quality OSINT requires money and effort. Used indiscriminately by amateurs it resembles a 'Google' search – useful, but unreliable and no basis for making important decisions.

Good intelligence is dependant upon the value of the original source, not the means of collection or the classification it is given, indeed secret material can be very difficult to utilise effectively. Verified OSINT is extremely user friendly as it can be rapidly disseminated to the customer (and all of his operators) or shared with security partners; it can even be communicated to the public, particularly where they may be exposed to a specific risk. This freedom from restrictive handling procedures is its greatest strength, facilitating effective action but also breeding trust within the wider community. In this respect, OSINT is responding to the new forces shaping our society and has much to contribute to the perception of security within a state.

It is not surprising that the cause of OSINT is being championed by those people standing to benefit from greater investment; eager to reap the benefits, many gloss over the effort required to identify relevant reliable sources within the plethora of raw data. Few mention the threat posed to security from the 'transparent society' they support. There can be no doubt that OSINT is of far more value to closed societies collecting information on open democracies than vice-versa. It is also undeniably of significant value to the terrorist organisations targeting the soft underbelly of Western society.