



# IDSS COMMENTARIES (51/2005)

*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.*

---

## THE ROLE OF OPEN SOURCE INTELLIGENCE IN THE GLOBAL WAR ON TERROR

Jonathan Tow & Weimeng Yeo \*

3 August 2005

THE bombings in London have once again highlighted the seismic changes to the global security landscape. The world as we know has changed. Security agencies all across the globe have not been spared from these shockwaves and many have been undergoing restructuring efforts to meet these new challenges. In the context of the Global War on Terror (GWOT), there is great emphasis by security agencies to enhance their clandestine intelligence abilities.

However, many policymakers have reservations in using Open Source Intelligence (OSINT). They are critical of the analysis they receive from open sources and often share a frustration over its perceived lack of utility and hence impact. Thus, OSINT has been neglected as a valuable tool. This is a mistake; particularly in the GWOT where global Jihadists have used open source information such as the Internet as a mode of communication, information dissemination and interaction. Indeed, OSINT can play a pivotal role in the GWOT effort and should be considered as an important component in gathering tactical and strategic intelligence.

### WHAT IS OSINT?

"OSINT" refers to an intelligence gathering discipline based on information collected from the general public such as newspapers, the internet, radio and television broadcasts. Similar to other sources of intelligence, HUMINT (Human Source Intelligence), SIGINT (Signals Intelligence) and IMINT (Imagery Intelligence), OSINT has its own limitations and strengths. One limitation of OSINT is information overload. Short of a highly developed system able to consolidate searches, it is likely that time-consuming human intervention is still required to trawl information. A second limitation is the veracity of OSINT. With the amount of information open to the public, it is difficult to differentiate real information from disinformation. This raises a serious concern about the reliability of the information.

Nevertheless, while these limitations are valid, OSINT has its own strengths. In the context of GWOT, the value of OSINT is in providing an understanding of the ideological concerns and thinking of key personnel. In this context, analysing OSINT in the GWOT might offer strategic "barometers" of the adversary's intentions for policymakers to be made aware of. This "barometer" appears to be amply found in the Internet, which is the focus for assessing OSINT's role within the GWOT.

### THE ROLE OF THE INTERNET

Focusing on the Internet for OSINT offers an unique opportunity for analysts, as global

Jihadists have increasingly turned to cyberspace after the US-led GWOT destroyed many key logistics, operations and communications facilities. Given its easy accessibility, low cost, and wide distribution, the Internet has now been used by global Jihadist groups to disseminate ideology, operational strategy and instructions to both supporters and operational cells.

As an example of how credible the Internet resource can be, one can merely focus on the various online publications such as Al Qaeda's "Voice of Jihad." In its January 2004 issue, it carried statements from Osama Bin Laden claiming that American citizens will be the targets of a major attack in Saudi Arabia. The message stated that Al Qaeda hoped that such attacks would drive up oil prices, instigate the Americans to take over the Saudi oil fields and thereby provoke a split between both Riyadh and Washington. Heeding the call of Bin Laden, local militants started to increase their attacks on American targets in Saudi Arabia. In a span of 10 months after this issue of "Voice of Jihad" was released, there were three major attacks on American targets in Saudi Arabia, including one on the US consulate in Jeddah on 6 December 2004.

The case for examining the Internet for OSINT is compelling and it readily fulfills two important criteria in assessing the hypotheses -- the Internet is easily and openly accessible and there is credibility in the content. The final criteria will be an assessment of the value of strategic and tactical intelligence to the GWOT.

### **STRATEGIC INTELLIGENCE**

Strategic intelligence is defined as the understanding of long-term trends of an issue that shapes how a government conducts its national policies. It warns of immediate threats to vital national security interests. For the GWOT, closer examinations of credible jihadist websites reveal the potential for strategic intelligence collection and analysis. Counter-terrorism experts such as Reuben Paz assessed that within these websites, one will "find the early signs of ideological developments which will affect the West". For example, the global jihadist websites offer postings on strategic issues such as their political and military goals as well as their ideology. These ideas and strategies have been published to inspire and guide Al Qaeda followers and its global affiliates. Understanding this strategic picture will assist governments in adopting the appropriate responses to the Jihadist threat.

For example, in March 2005, a 113-page article in Arabic was posted on the Internet entitled "The Management of Barbarism" (*Idarat al-Tawahhush*). The originators were the Center for Islamic Studies and Research, a known Al Qaeda affiliate. This document provided a blueprint for a military strategy to defeat the US and its allies.

At the strategic level, the document called for a "Disruption and Exhaustion" phase based on the premise that attacks on softer-targets will force the US and its allies to disperse limited security resources and incur high economic and financial costs in the process. For example, the document called for attacks on tourist destinations frequented by westerners, banks in Turkey that offer interest payments and oil installations like pipelines, refineries and shipping. In the section on "The Most Important Principles and Policies", the document also noted that "a superior enemy is defeated by economic and military attrition". The document suggested conducting a protracted war of attrition against the US. This strategic document gives an indication of the mental distance the global Jihadists are prepared to go.

### **TACTICAL INTELLIGENCE**

OSINT acts as a way to collaborate with tactical intelligence by providing leads for follow-up law enforcement action. For example, OSINT collected from Jihadist websites can help provide leads to track the activities of groups such as Al Qaeda. It should be noted, however, that OSINT is rarely able to provide early tactical warning of impending attacks as such information will not be published openly.

While it is possible to track and apprehend Jihadists using OSINT, successful cases are rare. Counter-terrorism experts acknowledge it is difficult to track Al Qaeda and global Jihadists. While they have a strong presence on the Internet, they are known to be well trained and careful to avoid leaving “virtual” footprints. These Al Qaeda operatives use a combination of encryption and coded messages that often leave intelligence services struggling to expose them.

It is evident Al Qaeda uses the Internet for much of its “cyber planning” and coordination of terrorist activities, which is a highly secretive activity. Nevertheless, OSINT can take advantage of the inherent weak links global Jihadists encounter on the Internet. This weak link is that websites and chat-rooms need to remain open and accessible to all users as they act as gateways to allow would-be Jihadists to establish contact with Al Qaeda and its affiliates. Tracking the movement in and out of these portals can be targeted overtly and passed on to law enforcement agencies.

Lastly, the Internet has also been used by global Jihadists for funding, training and recruitment activities. Observing these on-line activities help create tactical intelligence leads by tracking their financial activities. For example, Qassam.net, a Hamas website actively seeks donations on-line. Donors are asked to send emails to an address on the website that provides a bank account number. By following this trail, law enforcement agencies can track such activities and assess how to shut-down the banking facilities.

## CONCLUSION

The exploitation of the Internet to aid the GWOT effort offers OSINT an increasingly pivotal role in the security community’s strategic intelligence assessments as well as developments in tactical intelligence requirements. The importance of these benefits should constitute a sufficient incentive to galvanise the security community to develop a keener sensitivity towards OSINT, and to establish a more equitable allocation of resources and priorities between open and secret resources. In the final analysis, better use of OSINT would greatly contribute to more effective exploitation of intelligence and help enhance international security and cooperation in GWOT.

---

\* Jonathan Tow & Weimeng Yeo are both graduate students at the School Of Foreign Service at Georgetown University. The latter was formerly a terrorism analyst at the Institute of Defence and Strategic Studies, Nanyang Technological University.