Employing a social media monitoring tool as an OSINT platform for Intelligence, Defence & Security

BY PAUL BRELSFORD
### TABLE OF CONTENT

1. Foreword
2. Introduction
3. The Intelligence Cycle: Modern Intelligence Tradecraft
   4.1. Direction – Stage 1
   4.2. Collection – Stage 2
   4.3. Processing – Stage 3
   4.4. Dissemination – Stage 4
4. The Intelligence Cycle:
5. Looking Forward
6. Summary
7. Glossary

---

**WHO IS PAUL BRELSFORD?**

Paul served for 23 years in the UK’s Military Intelligence. He is counter-terrorism and OSINT professional with global experience. Paul is an expert in Intelligence Management and analytical processes and was awarded the Intelligence Corps distinguished service award for his work in establishing the UK LAND Forces Intelligence Information Management section within the UK LAND Forces Intelligence Fusion Centre. Paul now advises on counterterrorism and intelligence management issues.

[UK.LINKEDIN.COM/IN/DECISIONSUPPORTSPECIALIST/](UK.LINKEDIN.COM/IN/DECISIONSUPPORTSPECIALIST/)
EMPLOYING SOCIAL MEDIA MONITORING TOOLS AS AN OSINT PLATFORM FOR INTELLIGENCE, DEFENCE & SECURITY

This whitepaper discusses how social media monitoring tools can be applied as powerful and cost effective Open Source Intelligence (OSINT) platforms; and how they can support collection and analysis of relevant and targeted information relating to counter-terrorism, criminal and political open sources. The use of such tools has wide application and benefits for a number of industries, including; Government and Defence Intelligence agencies, Law Enforcement, Commercial Risk Management companies, Private Security Companies (PMCs) and Non-Government Organisations (NGOs).

Over the last 6 months of 2013 a proof of concept exercise was undertaken. This exercise was conducted by a counterterrorism and OSINT expert to test the application of Talkwalker as an OSINT platform in the role of supporting the intelligence cycle and to provide a monitoring function as an Early Warning System (EWS). The capabilities and findings are discussed within this paper.

FOREWORD
Conducting OSINT for wider intelligence, counter-terrorism and risk management work has become a complex and increasingly resource intensive task for both Government and Defence Intelligence agencies and the commercial risk management sector alike. This paper covers some of the challenges involved in the collection and processing of OSINT and how a social media monitoring tool can exponentially enhance those processes when implemented as an OSINT platform. Moreover, not only do such tools enhance OSINT collection and processing but it also provides a vastly increased cost/benefit versus allocated resources ratio through a tool’s capability to crawl, filter and deliver increasingly relevant results from huge quantities of data on daily basis, the results of which are delivered via a consumable and easy to manage interfaces. These capabilities allow for the delivery of focussed results from a larger pool of raw information in a shorter timeframe. Concurrent to the delivery of results the overall processes requires less resources and personnel to manage and exploit the information in intuitive interfaces that have a virtually non-existent training burden to analysts.

Many readers will be familiar with the analogy that getting information from the internet is like taking a drink from a fire hydrant. This feature of information discovery, management and curating presents difficult challenges in terms of the allocation of resources, personnel and time constraints all combined with the challenge of being able to filter out the noise and irrelevant information from the river of information so that the relevant information can surface to be discovered, processed and delivered in a timely manner for action by decision makers.

Within Government and Defence intelligence agencies OSINT work has gained momentum to become recognised as a legitimate area of intelligence operation alongside the more traditional intelligence domains; such as HUMINT (agent handling) and SIGINT (signals intelligence) disciplines.

This is particularly true in the domain of counter-terrorism. Nearly all Government and Defence intelligence agencies have resources dedicated to the production of OSINT within the framework of the intelligence cycle in order to meet their intelligence requirements and to produce actionable outputs.
3. THE INTELLIGENCE CYCLE – Modern Intelligence Tradecraft

Supporting the intelligence cycle in the direction, collection, processing and dissemination of actionable intelligence is key in the discovery and validation of critical and relevant information from OSINT sources. This process requires much more detailed focus than blindly surfing the internet for clues or merely typing relevant or target oriented search queries into a search engine.

Moreover, even conducting manual cursory trawls for adversarial social media outputs or other online channels is likely to provide little value without the technology to cast and manage a wide net across the online space.

The modern intelligence tradecraft of exploiting OSINT requires the assistance of technology that will enhance the precision, relevance and speed in the collection and validation of meaningful insight from online sources.
4. THE INTELLIGENCE CYCLE

WHAT IS THE INTELLIGENCE CYCLE?
METHODOLOGY & APPLICATION

The intelligence cycle is the framework and methodology used by modern intelligence agencies and professional intelligencers for the production of intelligence outputs and reporting to support decision making. It is a proven concept that in more recent years has also been adopted across many commercial industries that have a requirement for information management and discovery to support business processes and decision making. The basic tenet of the process is that information requirements are prioritised and focused against the decision maker’s objectives. This allows resources to be matched and allocated accordingly for the collection and production of intelligence.

THE 4 STAGES OF THE INTELLIGENCE CYCLE

The intelligence cycle is comprised of 4 key stages (5 in the USA) with continuous review of each stage conducted throughout the process. For the purposes of this paper the UK model has been adopted to explain the framework, which consists of the components below:

- Direction
- Collection
- Processing
- Dissemination

The intelligence cycle is the classic intelligence management methodology and doctrinal tradecraft utilised for the production of intelligence to support decision makers. The chapters below discusses how a social media monitoring tool can support each phase of the intelligence cycle as a powerful and significant OSINT platform with application beyond its conceptual design of supporting brand protection and delivering competitive intelligence insights.
4.1 DIRECTION
Stage 1 of the Intelligence Cycle

Direction is the first stage of the intelligence cycle. This is where the decision makers define and prioritise their (business or mission) objectives. These requirements are then captured and form the basis of the Intelligence Collection Plan (ICP), allowing the analysts to design a series of highly focussed information requirements to answer specific questions or to maintain a horizon scanning (early warning system) for information that is critical in supporting decision making within the prioritised business or mission objectives. The following describes how a social media monitoring platform was employed in a counter-terrorism role.

TERROR GROUP WATCHPOINTS:

A series of terrorism watchpoints was designed to provide support in answering specific information requirements and to provide early warning of developing threat streams from horizon scanning. Watchpoints were based on a target series of known terrorist groups and threat actors to meet the intelligence requirements of the decision makers. This was achieved through setting defined search query parameters, established to collect against known terrorist organisations and associated persons of interest; and to monitor terrorism related event indicator query terms. The watchpoint query terms were generated in a spreadsheet and the specific information requirements to be answered were itemised. This formed the basis of the collection plan, the ICP which was then imported and implemented on Talkwalker.
4.2 COLLECTION

Stage 2 of the Intelligence Cycle

Once a collection plan was implemented on the social media monitoring tool. A series of profiles were setup to meet the intelligence collection plan requirements. The first profile was structured as a generic intelligence collection watchpoint of about 20 terrorist organisations. This defined the list of terror groups to be collected against (as illustrated above).

A secondary profile was then implemented with a list of known terror suspects (associated Persons of Interest (POI)) to be collected against. The POI were known terrorist suspects with links to terror organisations listed in the ICP. This second series of watchpoints allowed for the building of a deeper layer of linked, relevant information to be collected. This profile allowed for collection of information linked with the terror group watchpoints. The scale of collection from Talkwalker profiles exponentially increased in volume daily.

A third profile was developed as a set of potential event indicators based on very specific positive search query criteria and negative search query criteria. This watchpoint was designed to add a third layer of relevant information, which could be linked and cross referenced with the previous watchpoints. This profile also monitored pattern changes in these key terms, which could potentially surface signals that would highlight new or building threat streams. In essence this combined and layered watchpoint approach enabled the development of an intelligence picture and the provision of live situational awareness.

The key benefits of this initial multi-profile design was to provide a wide ‘capture all’ feature that could act as a total information repository to be subsequently exploited or analysed at any point in order to provide deep current understanding of events or to look back on historical events.

The ICP was implemented directly from the spreadsheet import function, a time saving and easy process in itself. Once implemented the social media monitoring tool then began to produce results from crawling and indexing hundreds of millions of online sources per day.

In summary, the following Watchpoints were established for collection, each Watchpoint was capable of independent research and analysis but had greater value through the ability to define patterns and conduct cross-referencing and deep link analysis between all three Watchpoints:

- Terrorist Groups & organisations.
- Known Persons of Interest (POI) associated to terrorist groups.
- Terrorist incident event indicators.
SURFACING RELEVANT INFORMATION RHYTHMS AND INTELLIGENCE

SOURCE VALIDATION AND INTEGRITY

Another key component to the collection stage of the intelligence cycle is ensuring source validation and integrity. This was achieved in combination by the selection and refining of negative search query terms to filter out the irrelevant results containing these terms. The ability to block persistent sources which delivered irrelevant information; and through fine tuning and grading positive search queries which returned the collected results.

The simple source management dropdown menu is also a highly efficient capability within social media monitoring tool used. This enabled users to grade or block sources. In addition, sources can be emailed, custom tagged or priority marked. They can then be filtered for subsequent analysis based on their grading. This functionality and process adds a high level of confidence to the source integrity as key sources are subjected to first line interrogation and grading by an analyst.

The source management functionality should not be underestimated and was a ‘force multiplier’ in providing and refining results and sources with a high level of confidence. Over time this builds up into a hugely powerful capability in its own domain. For example, by developing graded sources within each profile or Watchpoint the analyst is essentially developing a high quality reporting and monitoring function based on graded and judged sources with a higher level of integrity. This high grade source list can be segmented separately to run against search queries. In essence, this method removes a high volume of noise to leave highly focussed and relevant results for further analysis.

In addition to the above functionality other sources and files can be added to each project. External files and documents may also be uploaded instantly for indexing with the developing database.
THE BENEFITS FOR ANALYSTS IN THE COLLECTION STAGE

With the assistance of a social media monitoring tool, analysts are no longer physically limited to the number of online sources and searches that could be conducted on a daily basis through manual processes. Not only does it discover the content but it allows the vast array of content to be instantly searched, segmented and analysed. A further benefit of such tool are that they can automatically weed out much of the duplication in the results served and provide a plethora of new and previously undiscovered relevant sources and material, which would not surface from manual or semi-automated search efforts.

What does this mean for the collection process within the intelligence cycle? Using social media monitoring tools provides fast, relevant and intuitive platforms to load and align highly defined collection efforts based on the objectives and requirements of decision makers.
4.3 PROCESSING

Stage 3 of the Intelligence Cycle

With 4 million records (and growing) the possibilities of analysis, external to the social media monitoring tool you use are vast. Building in depth Social Network Analysis (SNA) charts, link analysis between POI and terrorist organisations, and geographic and threat financial linkages has also become an achievable concept.

However, utilising social media monitoring tools as OSINT platforms continues beyond the collection stage. With more than a million records to analyse users may require an external database due to the limitations of volume that spreadsheets such as Excel can manage.

Ideally, the tool must have the ability to interrogate the results and drill-down deep into the information in an extremely easy and intuitive way from the interface as was the case with Talkwalker. Data should be able to be segmented by a number of different attributes; such as source type and grade, language, region, country, date. The data can be further segmented by selecting individual Watchpoints, such as POI or by source (collection) channel (Facebook, Twitter, Blog, YouTube etc.). The data can also be segmented by Boolean search, keywords and date range.

This type of powerful functionality allows analysts to process and easily manage large volumes of data in a very short timeframe with ability to separate out highly relevant results from a substantially bigger repository of information than could be achieved from manual or semi-automated processes.

From a counter-terrorism viewpoint this enabled the rapid segmentation of POI and groupings as required for subsequent analysis. At the time of writing a significant number of networks and links have been developed by building Social Network Analysis diagrams based on collected data within the results that have been returned in the Watchpoints.

In addition, patterns and trends have also emerged in the both the cycle and sources of release of information into the OSINT environment. This pattern analysis allows analysts to further refine and target collection that would not be possible without the use of technology such as that provided by the Talkwalker interface. Snapshots of the ease with which results can be processed and analysed within the Talkwalker interface to provide an intelligence picture are highlighted on the next page.
The intelligence picture above shows the tempo and rhythm of terrorist related events. The snapshot above is based on over 2.7million results and shows the tempo, rhythm and effect of terrorist events between August & December 2013. Of note this strategic picture can be exploited in the future to understand and anticipate terrorism related events and activity to mitigate their impact.

**MONITORING PERSONS OF INTEREST**

The simplicity in which events can be visualised and interrogated is one of Talkwalker’s key strengths, allowing rapid analysis and understanding of events that take place. Moreover, by setting Watchpoints to monitor persons of interest (POI) any increase in activity related to those being monitored may be instantly viewed in a separate graph as an overlay.

The POI overlay below was instantly generated by selecting POI Watchpoint from the search query column in the intelligence picture interface below.
THE WESTGATE MALL ATTACK IN KENYA

Further illustration of the image below depicts a clear and expected spike in OSINT by the predicted surge in media and online user generated content following a major terrorist or crisis event. In this case, the Westgate Mall attack in Kenya by Al Shabaab in September 2013.

By analysing the results surrounding this surge in activity new leads and sources could be identified from within the content. Persons who generate content which indicates inside knowledge of the event or being close to a POI, or those who have connections to terror groups can be isolated through analysis of this data for subsequent addition into social network analysis (SNA) and link analysis.

Analysis of this segment of data also leads to further discovery and identification of source types that may be of further interest. An individual, even if using false credentials online will often have published other material which divulges essential elements of information or links to other online sources or individuals of interest that feed into building an increasingly accurate intelligence picture and horizon scanning function.
The tool can also collect against identifying threat streams at the tactical level, allowing for quick analysis and early warning.

The example below was identified against query terms for Al Shabaab, Al Mujahideen. On its own such open messaging may not raise significant interest. However, when combined with other specific OSINT signals following the Al Shabaab attack on the Westgate shopping Mall and the pressure faced by Al Shabaab from Kenyan forces in Somalia, it raises the probability that this is a developing threat stream surfacing the intent of Al Shabaab to cultivate an insider threat against the Kenyan government.
4.4 DISSEMINATION

Stage 4 of the Intelligence Cycle

Social media monitoring offers a number of different methods to distribute results and analysis. Alerts can be setup to immediately disseminate results from the Watchpoints or search query sets of interest that may be considered as triggers for information relevant requirements.

Export functions have the capability to segment results according to the requirements of the analyst and to generate the report into a number of exportable and consumable formats. Results may then be exported as CSV datasets, which can be imported into external databases or external analytical toolsets for subsequent exploitation. Reports may also be exported in Word and PDF formats for use as standalone reports or for inclusion in other reporting formats.

In sum, using a social media monitoring solution can significantly speed up the process of dissemination by packaging and aligning the collection results for export to database, email, PDF, Word or to other analytical toolsets and reporting formats.
LOOKING FORWARD

Prediction and the art of the future. At the time of writing, testing continues to extrapolate emerging patterns based on designated query term sets and phrases, which are common signals before terrorist events occur. This may highlight signals of changes in the online environment, such as a growing threat stream, or changes in tactical or strategic objectives of terror groups, or even the ability to predict an event in advance.

Watch this space!
6. SUMMARY

This white paper illustrated the relevance and efficiency of employing a social media monitoring tool application as an OSINT platform in support of the Intelligence Cycle. Whilst the proof of concept was focussed within the counter-terrorism domain it has equal application to other sectors; such as, law enforcement, NGOs, risk management and private security companies.

The implementation of such tools dramatically enhances the capability to discover, curate and analyse vast volumes of information to provide monitoring and early warning of developing threat streams. In addition, it also delivers deep datasets with rich, relevant content and sources for further processing to develop significant social network analysis on POI and link analysis charts of threat organisations.

The functionality of social media monitoring seamlessly integrates to support the requirements of each stage of the intelligence cycle. The implementation of collection plans and Watchpoints and the delivery of relevant, graded results with a highly intuitive source management capability.

Results can be layered and linked as overlays and datasets may be rapidly segmented or analysed using powerful drill-down options in the interface. The distribution of the results and analysis is easily disseminated in multiple formats and alerts settings allow dissemination of reports either across an organisation or direct to the key decision makers in a timely and efficient manner.

From an organisation viewpoint, a social media monitoring tool is a resource multiplier. It is cost effective, requiring less time to process more actionable insights which are derived from a much wider set of results than can be processed manually or by semi-automated approaches.