

ISIS social media propaganda – could it be their Achilles heel?

ISIS or simply Islamic State (IS), led by Abu Bakr al-Baghdadi is a jihadist militant group in Iraq and Syria and are responsible for mass terror attacks globally. According to a [New York Times analysis](#), more than 1,200 people outside of Iraq and Syria have been killed in attacks inspired or coordinated by the Islamic State¹.

IS has proven that in addition to their capabilities for brutality, torture and murder, they have a talent for social media. It has consistently and efficiently exploited online platforms, and most notoriously Twitter, as its modus operandi, to send its propaganda and messaging out to the world. They use it to broadcast their gruesome successes and to draw in people vulnerable to radicalisation. This is a successful ploy to use the internet to spread the ideology, promote the mission and recruit new fighters.



Source: [War on the rocks](#)

Can we fight ISIS online with data?

With the massive amount of content generated online, growing by the second, it is humanly impossible for data scientists to keep up with the rate of data generation seen on platforms like Twitter and Facebook. Instead, they must rely on advanced analytics that uses complex algorithms to intelligently sort and parse the data. So, how do we fight ISIS online? Advanced Analytics can deliver a real game changing capability in fighting ISIS. Combining analysis through data mining, anomaly detection, predictive analytics and network analysis is a highly effective, yet highly technical solution that many intelligence organisations do not have the depth of experience to comprehensively implement. In order to stay ahead of the growing ISIS influence online, we quickly need to ascertain the skills and technology required to make this possible.

How can online data provide insights?

A demographic snapshot of representative twitter data reveals official account information, display name and the date on which the account was created; supporters/non-supporters based on the content and top links followed, location metadata, time-zones, language preference, Avatars i.e. nom de plume, most popular hashtags, smartphones used, tweeting patterns, interaction within the network, number of followers, bots and app which are third-party services designed to promote content from a Twitter account automatically, without a human being manually sending tweets.

This goldmine of information is a solid foundation for predicting which of the available metrics best correlate to a user being identified as an ISIS supporter or not. Predictive Analytics ties the social behavior using those hashtags, phrases, etc., with the imminent behavior of the user. By looking at trends, it becomes easy to assess the number of fighters, as they are conscripted by ISIS, and answer questions like “Where does it get its money from?” This information can be deciphered by looking at network interactions which extrapolates information about private donors who fund IS operations, regions where sales of crude oil were made, kidnapping, extortion, abduction cases data, and areas where minorities are based (as they are forced to pay a special tax). This is only an iota of the insights that can be derived from the big data available.

¹ [New York Times - Map ISIS attacks around the world](#)

What Advanced Analytics techniques can we use to fight ISIS?

Counter-terrorism authorities are interested in questions like:

- Who are the IS recruits and who is likely to be next?
- How do we discover implicit links between users?
- Who are the major players in the pro-ISIS twitter network?
- Which keywords are most commonly used by ISIS fanboys?

In order to adopt a coherent approach to thwart the reign of terror, let us look at tangible techniques that authorities need to employ:

- 1. Social Network Cluster Analysis:** Who are the major players in the pro-ISIS twitter network? Where do they get their money from? Social network analysis (SNA) aims to discern the nature, intensity, and frequency of social ties, often as complex networks. By modelling these ties, social network analysts attempt to explain and indeed predict the behaviour of the individuals who comprise the network.

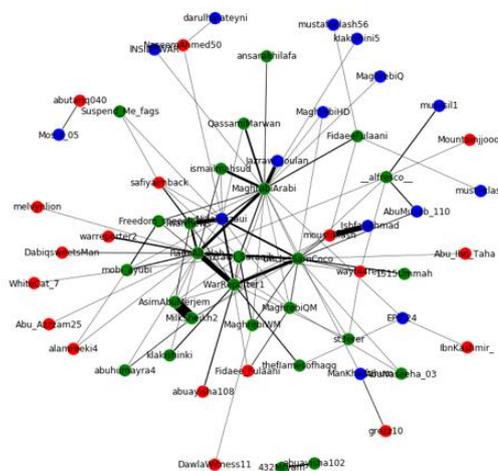
Studies have found that ISIS sympathisers used the same hashtag as another terrorist body, but still interacted with each other in identifiable and largely separate clusters. This demonstrates that SNA can be used to investigate the potential nuance and particular allegiances between the sympathisers of specific extremist groups. This allows us to identify accounts which fulfil important roles in specific groups within the wider flow of information.

Following the money trail helps find who they are, what they are doing and who their associates are.

Collecting and analysing social media data disseminated by ISIS presents the opportunity to understand more about the organisation, and other online jihadists. Intelligence agencies, diplomatic, and military strategic planners and operators would be able to use this information to develop and execute effective influence and kinetic campaigns against ISIS.

- 2. Geo-Spatial Analysis:** Geo-location enabled twitter analysis can help model global epidemic. There are situations where ISIS buildings and hotspots have been targeted by Western military forces, after users had accidentally pinpointed their location on social media. Geo-spatial analysis can characterise social media posts for health-related analysis, combining text features (e.g. tags as a prominent example of short, unstructured text labels) with spatial knowledge (e.g. geo-tags, coordinates of images and videos).

Analysis conducted by V.S. Subrahmanian and the [University of Maryland](#)² on 20 years' worth of monthly data including 770 variables on terrorist group Lashkar-e-Taiba (LeT) revealed the different



SOCIAL NETWORK GRAPH CREATED BY KAGGLE USER [HUWFULCHER](#) IN [SCRIPTS](#)
Source: [The Official Blog of Kaggle.com](#)

² [University of Maryland Institute for Advanced Computer Studies' Research - Computational Analysis of Terrorist Groups: Lashkar-e-Taiba](#)

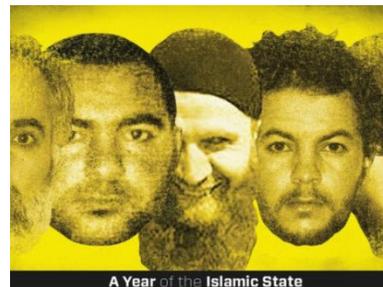
- 4. Keyword Analysis & Links Categorisation:** Which keywords derived from the name, username, description, location, and tweet were the most commonly used by ISIS fanboys? Examples include: “baqiyah”, “dabiq”, “wilayat”, “amaq.” Which websites are pro-ISIS fanboys linking to? Categories include: Mainstream Media, Altermedia, Jihadist Websites, Image Upload, Video Upload.

The reality that caused the British news headline on 3 girls from London travelling to Syria to join ISIS could have been prevented if these methods were employed. One of the three girls was in contact with another girl on twitter, who was known to the authorities for joining ISIS. A model can be developed for the purpose of storing and recording suspicious entities and incidents in the system which can be linked to various other events or people many numbers of times to build a network of associations and keep track of suspicious people. This data can be retrieved and updated quickly in real time.

IS sympathisers use blogs to write narratives on the caliphate; the process of its establishments, its theological and political underpinnings, its enemies and so on. Based on an analysis of 1700 pieces of propaganda produced by the group, Charlie Winter of Quilliam Foundation in his [Jamestown Foundation publication](#)⁴, distilled the messaging into six narratives: brutality, mercy, victimhood, war, belonging and utopianism. By adhering to this categorisation of data, resources can be optimised by targeting specific segments when planning discomfiture.

- 5. Facial Recognition and Video Analytics:** Focusing efforts on a facial recognition method based on imagery collected from available sources, be they high resolution cameras, or mobile phones, and even devices with less reliable resolution or lighting can lead to important predictions and aid to foil terror attacks.

Analytics results based on online video searching does not simply target tag words or user-generated content, but scans the video itself for elements that can describe what the movie is about. While terrorists may be clever enough not to tag videos where, for instance, they explain how to make explosives in view of a potential terrorist attack, their videos would be easily inspected and tracked down if a search method non-reliant on tags is developed.



Source: [Business Insider](#)

These movie samples may provide very valuable insight to national security experts, using advanced analytics to extract information from video material.

We know enough to be able to knock ISIS down!

The monstrous reality of our milieu has engendered an urgent need to tackle terror in an organised way.

Social Media Analytics shows that ISIS recruits tend to be predominantly young and male and the ones originating in the EU and the US tend to come from a middle class background, with a high level of education. This data can be mined to answer even more granular questions. There is data that can help security agencies

⁴ [The Jamestown Foundation - Charlie Winter Islamic State Propaganda: Key Elements of the Group's Messaging](#)

identify who is financing and feeding the group, who are the people supporting the group, who is supplying weapons to the group and similar data points.

Advanced Analytics can be our greatest ally in fighting ISIS, if the tangible techniques illustrated above are consciously implemented. Is there enough being done to circumvent this lawlessness? The insights from advanced analytics, if acted upon, can knock ISIS down. Are we ready for this challenge?

About Presidion

Presidion have operated for over 20 years and have been the pioneers in implementing cutting edge predictive analytics solutions with top UK and Irish organisations. We specialise in helping organisations leverage their data to deliver tangible practical returns on investment, aligned with their strategies.

Presidion works with both government and commercial clients, currently partnering with hundreds of organisations enabling them to understand what has happened in the past, anticipate what may happen next to take appropriate and timely strategic decisions for their organisation.