Professor Babak Akhgar tells Robert de la Poer how police and security services can use social media and other open source data to combat terrorism and organised crime

CROWDSOUR
COUNTER T

RP: Some of our readers may not be familiar with the field of informatics. Could you begin by outlining what it involves and how it can practically be applied to the policing of terrorism and organised crime?

BA: Informatics broadly speaking encompasses computing technologies and their diverse relations to the human and social worlds. By understanding informational phenomena – such as computation, cognition, and communication – we are able to forge technological advances. Informatics has many aspects but is generally about creating "value" from information through the utilisation of information and communication technology (ICT). In the context of informatics, "value" can be the knowledge and intelligence required in order to conduct an operation, or make sense of a large volume of data for decision making processes. Law enforcement agencies must constantly adopt a scientific, evidence-based approach to their work. Informatics is a key part of this, facilitating the acquisition of knowledge from a variety of different data sources. It is often hypothesised that "knowledge is power"; if this is true then informatics is a key enabler in creating the knowledge needed for effective modern data policing.

RP: You advocate the use of open-source social and mobile media data to advance public knowledge and assist law enforcement in the detection of terrorism. Can you give some examples of the sort of data you are referring to (eg geographical, biographical, inter-personal, communications, etc).

BA: In order to combat crime and terrorism effectively, there are a variety of data sources in the public domain that can be utilised by law enforcement agencies (LEAs). Despite the potential benefit of using as many sources and as much data as possible, LEAs must carefully consider the legal and ethical implications of using them. In combination, open source intelligence (OSINT) and more traditional closed source intelligence can provide LEAs with a holistic foundation of evidence for their operational needs. Furthermore, OSINT can help to underpin a more refined decision-making framework for command and control during incidents and crises. Of course, one of the key challenges in utilising OSINT in this way is how to represent and visualise information effectively so that it can be easily understood by decision makers.

©Getty Images

Public coverage: onlookers in Beirut photograph the aftermath of a terrorist attack

RP: In what ways can social media help LEAs in combating terrorism?

BA: Social media has the potential to assist LEAs in crisis situations – for example during a terrorism incident. The public make use of social media every day, so during crisis situations they naturally opt to use platforms like twitter to get real-time instant updates about what is happening on the ground and also contribute to the reporting of incidents. One of our

RCING TERRORISM

projects, ATHENA, recognises that the public are under-utilised crisis responders; they are often first on the scene, vastly outnumber the emergency first responders and are creative and resourceful in performing countless life-saving actions. The project will therefore explore how the huge popularity of new communication media can be harnessed to provide efficient and effective communication and enhanced situational awareness during a crisis for citizens and first responders. ATHENA is a three-year, €5m, grant-funded European Commission, 7th Framework Programme security-themed research project co-ordinated by West Yorkshire Police from December 2013 to November 2016.

The project will develop a set of best practice guidelines for first responders and citizens for the use of new media communications and supporting tools and technologies in crisis situations. It will also develop a suite of prototype software tools (the ATHENA app) to enhance the ability of first responders and citizens in their use of new media in crisis situations. In doing so, ATHENA will move the state of the art forward in two areas. Firstly, the use of social media during crisis situations by first responders and the public, and secondly by technologically exploiting social media in crisis management through the searching, acquisition, aggregation, filtering and presentation of knowledge from social media to support crisis management using smart mobile devices.

Applications of ATHENA may have been useful during incidents such as the 2008 Mumbai shooting and 2013 Boston Marathon bombing, where it has been widely reported that social media had a key role to play in the public's communication of the incident. Also potential future terrorist-related incidents carried out in public spaces – for example, incidents in which an active shooter or lone wolf is operating would benefit from the use of the ATHENA application, as it allows an instant communication channel between LEAs (including first responders) and the public. So, in short, social media potentially has a very important role to play in helping LEAs combat terrorism.

RP: Is such intelligence better suited to identifying previously unknown potential suspects or plots, or to supporting and corroborating ongoing investigations?

BA: A combination of open and closed source intelligence can provide LEAs with greater environmental scanning capability, giving LEAs the potential to identify the emergence of new crime trends and patterns. For example, we are currently working on the EU Project ePOOLICE, developing a platform to act as a medium to long-range radar for the identification of new and emerging organised crime activities such as human trafficking, and cyber crime and cyber terrorism. Applying open-source intelligence in this way provides LEAs with a new medium to support their intelligence-led activities in this area, and opens them up to new insights from open, public

sources such as social media and the web – sources that may not have been considered previously and which may aid in the identification of pertinent indicators of, and information supplementary to the emergence of organised crime.

It is increasingly being acknowledged that criminal entities themselves are taking to the web in order to facilitate recruitment, and the transfer of money and information for use in financing and co-ordinating their illicit activities. One of the key challenges faced by LEAs in applying OSINT in this way is need to identify pertinent and relevant information from the vast quantities of data made available from open-sources such as social media platforms, while simultaneously managing ethical expectations and societal privacy concerns.

RP: What other advantages and possibilities does open-source intelligence offer for law enforcement?

BA: The ubiquity and availability of internet-based products and services such as social media and mobile-based applications have significantly increased the volume of, and accessibility to, open source intelligence. Law enforcement agencies can use this intelligence to enrich their understanding of public sentiment in regards to their perception of security and threats. For example, in the context of community policing this intelligence can provide significant insight into community tensions, whereas when applied in the context of counter-terrorism, open source intelligence can aid in identifying potential instances of radicalisation.

RP: What are the drawbacks of crowdsourcing serious criminal or terrorist investigations? How can these best be managed?

BA: In medieval England, communities would assist in the apprehension of wrong doers and criminals using a "hue and cry" – raising the alarm and alerting other bystanders to the presence of said individuals. Today this process has evolved, with citizens taking to social media and smart technology to capture images and videos of, and to pass comment on, events. This content can spread a modern day "hue and cry" across communities around the globe. Active participation in this way can lead to an avalanche of information directed towards modern day police tasked with dealing with the incident or crime. The potential for information overload in this way can divert police resources towards untested, unverified information and slow down prospective investigations. Without the application of highly sophisticated analytical capabilities (such as those that deal with the analysis of big data), crowdsourcing information in this way can actually obscure the intelligence needed to resolve the incident. Worse still it can potentially incite citizens into making false accusations or provoke vigilant activity

RP: What do you hope to achieve at Counter Terror Expo 2014? What do you think are the main benefits of such events?

BA: One of the main benefits of attending events such as Counter Terror Expo is the opportunity to learn from others in the field. Networking with stakeholders from a variety of backgrounds helps us to keep up to speed with the dynamic, ever-evolving environment that surrounds counter-terrorism. Further, the threats themselves and the technologies used in order to mitigate and prevent them are developing at a rapid pace, and the Expo provides the perfect opportunity to keep up to speed with developments in the area.

Babak Akhgar is Professor of Informatics and Director of CENTRIC (Center of excellence in terrorism, resilience, intelligence and organised crime research) at Sheffield Hallam University and Fellow of the British Computer Society. He has extensive and experience in the development, management and execution of KM projects and large international security initiatives. His recent book is entitled "Strategic Intelligence Management". Prof Akhgar is a member of the academic advisory board of SAS UK. He will be speaking at Counter Terror Expo on Wednesday 30 April.

Mobile data could offer law enforcement agencies valuable intelligence about criminal or terrorist activity