Chapter 25
Social Media Analytics for Intelligence and Countering Violent Extremism

Jennifer Yang Hui
Nanyang Technological University, Singapore

ABSTRACT

Social media analytics are increasingly incorporated into security practices due to the rise in online criminal and extremist activities. Social media research, however, has not become established in either intelligence practice or academic-based approach. This chapter aims to fill the gap by discussing collection methods and analytical tools for the study of social media data for intelligence and countering violent extremism: social network analysis, sentiment analysis, multilingual analysis, geo-coding, automated entity extraction, semantic search, and multimedia analysis. While technological capabilities of social media analytics are improving rapidly, it needs to be complemented with nuanced perspectives from the social sciences. Understanding of the epistemology of social media and dynamics between the online-offline interaction as well as data access will put practitioners in a better position to reap the benefits of the social media. Attention should be given to train practitioners in relevant technological skills while also incorporating social science knowledge.

INTRODUCTION

Traditional approaches to tackle violent extremism face limitations. One key area in which more effective countering violent extremism initiatives is needed is in the cyberspace. Online activities are increasingly impacting real world events as movements are organised, and communications conducted via the cyberspace. The cyberspace therefore makes up a crucial aspect of national security investigation. By 1999 most jihadist organisations had established an online presence, although the impact of radical websites and social media on radicalising individuals are debatable (Bartlett & Miller, 2013). Recent events had shown that terrorist movements around the world are increasingly aided by social media. For instance, the Islamic State in Iraq and Syria (ISIS) has proved to be extremely adept at utilising social media to

DOI: 10.4018/978-1-5225-7912-0.ch025

attract sympathisers and recruit members globally. The Europol has estimated that more than 50,000 Twitter accounts belong to ISIS supporters, and are used to send nearly 100,000 tweets every day. In Norway, the perpetrator of the 2011 attacks, Anders Breivik, distributed a manifesto via social media before committing the actual shootings. Given the role that the Internet plays in the processes of radicalisation and aiding violent movements, greater effort must be made to make sense of the vast amount of online data in order to be made into information that is actionable for security purposes.

This chapter examines various methodologies and analytical tools for online intelligence gathering and countering violent extremism on the social media. A part of the Web 2.0, social media is a series of online tools which facilitates social interactions among users as opposed to the monologue (one-to-many) approach of content delivery of the traditional media such as radio and television (Antonius & Rich, 2013). The practice of gathering data on social media in order to study patterns, sentiment of users and network is referred to as 'social media analytics'.

Social media analytics has long been utilised by private companies for gauging consumer preferences and behaviour. Its potential for analysing sentiment and conducting horizon scanning in the national security realm is similarly vast. Intelligence gathering increasingly incorporates online data in addition to traditional human resources. Social media intelligence or SOCMINT is used to refer to the gathering, processing, analysis and presentation of social media data for the purpose of law enforcement and security-related intelligence (Antonius & Rich, 2013). It comprised of a mix of open and classified sources. While sources from social media cannot replace those from traditional human sources or even from open source intelligence, they can complement the latter. Security practitioners recognised that proper harvesting of online information may yield data on events that may not have been paid attention to, which can later be confirmed through traditional collecting disciplines and news outlets (Gupta & Brooks, 2013). Security organisations such as the U.K. Ministry of Defence and the Federal Bureau of Investigation (FBI) have expressed interest in tools to monitor and analyse social media data for the purpose of enhancing situational awareness. Organisations such as the U.S. Defense Advanced Research Projects Agency (DARPA) are involved in research on advancing state-of-the-art technology in studying online data.

Using online information for intelligence and countering violent extremism, however, is not only about technological improvements, but also about the study of human interactions. The Internet and social media is a rich repository of data for the understanding of user behaviour and diffusion of information. For instance, Hal Varian, Google's chief economist famously noted the ability of Google search terms to reveal real world behaviours (Varian, 2011). Another study on the dynamics of Facebook 'likes' observed that even the most rudimentary digital records on social networking platforms can yield insights into user information and behaviours (Kosinski, Stillwell, & Graepel, 2013). There is a need for more subtle and human centric approach to studying the Internet, and the social sciences can contribute towards that end. In other words, effective mining of social media data for national security meant that there is a need to combine the data analytical capabilities of computer scientists with the ability to study human behaviour that social scientists are familiar with. Network scholar Robert Ackland (2012) noted that:

The challenge stems from the fact that social media sites such as Twitter are generating terrabytes of highly dynamic and semi-structured data each day. While computer scientists are comfortable with working at 'data scale', the behaviour that is being studied is innately social, therefore requiring behavioural models from outside of computer science. On the other hand, although social scientists have been studying social influences for decades in fields such as economics, political science, sociology