Understanding Online Radicalisation Using Data Science

Yeslam Al-Saggaf, Charles Sturt University, Albury, Australia

ABSTRACT

What characterises social media radicals? And why some people become attracted to radicalisation? To explore answers to these questions, a number of tweets posted by a group of suspected radicals tweeting in Arabic were analysed using social network analysis and machine learning. The study revealed that these suspected radicals’ networks showed significant interaction with others; but this interactivity is only significant quantitatively as the interaction is not reciprocated. With regards to why these suspected radicals became attracted to radicalisation, Topic Modelling revealed these suspected radicals’ tweets underpinned a perceived injustice that they believed the Secret Police and the Government inflicted upon them. Overall, the study has shown that data science tools have the potential to inform our understanding of online radicalisation. It is hoped this exploratory study will be the basis for a future study in which the research questions will be answered using a larger sample.

KEYWORDS

Data Science, Extremism, Machine Learning, Radicalisation, Social Network Analysis

INTRODUCTION

The extremist who took part in gunning his solider cousin in Saudi Arabia in 2015 was as young as 18 years old and the gunner himself was only 21 years old. All of the four suicide bombers who carried out attacks on mosques during the Friday prayers in Saudi Arabia in 2015 aged between 20 and 23 years. The fact that these attackers were this young suggests that radical groups can easily infect young people with the ‘radicalisation virus.’ Radicalising young people, who may not yet fully understand the grey areas surrounding right and wrong and who may not have the skill to reason and rationally analyse the outcomes of their actions, can have devastating consequences for people’s safety worldwide.

Radicals live by the rule ‘divide and conquer’. After dividing people into groups, they move to establishing their credibility to the groups they target (Al-Saggaf, Himma & Kharabsheh, 2008). Once this is achieved, they progress to communicating their ideology, explaining where they differ with others and providing the ‘justification’ for their thinking, which they often back up with ‘evidence’ (Al-Saggaf & Kharabsheh, 2009). However, their attempts to advocate violence in Saudi online communities, i.e. before the widespread adoption of social media, achieved limited success, as evidenced by fewer and smaller magnitude terrorist activities compared to the multiple, large attacks post the social media era.

One reason for this is because radicals were not alone in the Saudi online communities in which they operated (Al-Saggaf & Kharabsheh, 2009). The results of one study showed that there were voices louder than theirs in these online communities, which to some extent drowned their voices.
out (Al-Saggaf & Weckert, 2006). Other reasons for the limited success of these types of campaigns were that the radicals were either busy fighting in Iraq, killed during that war, serving time in jail or because the online communities’ moderators regularly removed their contributions (Al-Saggaf & Kharabsheh, 2009). Even those contributions that escaped the moderators culling tended to be met with heavy criticism from other online community members (Al-Saggaf, 2007).

However, the widespread adoption of social media sites has completely changed the environment in which radicals operate. Social media sites like YouTube, Facebook, Twitter, Instagram and Snapchat have allowed them to create their own channels to spread their messages and advance their agenda instead of, as before, competing with others for attention over shared mediums (Al-Saggaf & Simmons, 2015). The revelation that extremists now use the secure messaging App Telegram, which emerged while investigating those responsible for the November 2015 Paris attacks, highlights radicals’ technological sophistication and their ability to take advantage of the high-tech resources at their disposal. With more than 3.366 billion using the internet worldwide, which is nearly half of the world’s population, and 1.65 billion alone are active on Facebook, recruiting sympathisers via social media has never been easier (Torok, 2013).

There is a dearth of research studies that focus on online radicalisation (Torok, 2013), ostensibly because of the risks associated with this type of research (Reynolds, 2012). For example, there is no study in the literature that has investigated, using naturally occurring data (i.e. real social media data), the characteristics of social media radicals. Similarly, there are no studies on why unsuspecting people fall victim to the ‘radicalisation virus’. Yet the need to understand the profile of social media radicals and the reasons why vulnerable individuals fall victim to the ‘radicalisation virus’ has never been more critical.

The aim of this study is to address these gaps in the literature. In order to fulfil this aim, the study will attempt to explore the use of data science tools to collect and analyse social media data to address the following research questions: (1) What characterises social media radicals? (2) Why some people become attracted to radicalisation? The present study will address these research questions empirically but using a small sample to meet the overall aim of the study which is to explore the potential of data science tools in understanding the characteristics of social media radicals and what attracts people to radicalisation. It is hoped that this exploratory study will be the basis for a future study in which the research questions will be answered using a larger sample.

The study makes two contributions to the literature about online radicalisation. First, it attempts to study online radicalisation using naturally occurring data. In their review of the literature on Facebook, Wilson, Gosling & Graham (2012) noted that studying how users choose to portray themselves in their personal profiles presents an excellent opportunity for social scientists to study, as these profiles elicit accurate impressions. Wilson et al. (2012) asked social scientists, who underappreciated social media profiles as a source of data, to take advantage of this unprecedented opportunity to study the social phenomenon in its natural setting where it occurs. This study answers this call. Second, and arguably the most important contribution, is that this study attempts to explore the use of data science tools such as the Twitter Packages in R to collect this naturally occurring data from Twitter. From a dataset that contains records of naturally occurring data from Twitter, several social network analysis packages, text analysis packages and machine learning tools were used to address the above two research questions.

ONLINE RADICALISATION

Social Network Sites (SNS) are among the most popular sites on the internet. According to recent rankings from Alexa.com, of the top 500 sites globally, YouTube is ranked second from the top (in terms of the total number of page views), followed by Facebook in third place and Twitter in eighth place respectively. This suggests that social networking is one of the most favoured activities among internet users; with YouTube and Facebook being the most popular and widely used SNS.
Related Content

Critical Infrastructure Systems: Security Analysis and Modelling Approach
[www.igi-global.com/article/critical-infrastructure-systems/69771?camid=4v1a](www.igi-global.com/article/critical-infrastructure-systems/69771?camid=4v1a)

Hacking and Hacktivism as an Information Communication System Threat
[www.igi-global.com/chapter/hacking-and-hacktivism-as-an-information-communication-system-threat/140516?camid=4v1a](www.igi-global.com/chapter/hacking-and-hacktivism-as-an-information-communication-system-threat/140516?camid=4v1a)
Analysis of Possible Future Global Scenarios in the Field of Cyber Warfare: National Cyber Defense and Cyber Attack Capabilities
www.igi-global.com/chapter/analysis-of-possible-future-global-scenarios-in-the-field-of-cyber-warfare/140522?camid=4v1a

Terroredia: Exchanging Terrorism Oxygen for Media Airwaves
Mahmoud Eid (2014). Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia (pp. 1-12).
www.igi-global.com/chapter/terroredia/106144?camid=4v1a