Leveraging on Digital Footprints to Identify Potential Security Threats:
Insights From the Behavioural Sciences Perspective

Loo Seng Neo
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

INTRODUCTION

The growing pervasiveness of the internet has revolutionised how individuals communicate and interact with one another. Despite being an effective channel for communication, it has also been exploited by individuals with malicious intent – such as criminals, violent extremists – for the purposes of fundraising, recruitment, propaganda creation and dissemination, sharing of vital information, data mining, etc. With the ease of accessibility and cloak of anonymity, individuals with malicious intent have reorganised their operations online to exist and operate in social environments that may not agree with their activities.

Violent extremists of all affiliations have exploited this technological advancement to transform the way they operate on a historically unprecedented scale. As Weimann (2004) posited, "Islamists, Marxists, nationalists and separatists, racists and anarchists all find the internet alluring" (p. 3). The internet and the opportunity it offers, allow violent extremists to expand the functionalities of their propaganda efforts beyond that the boundaries of the traditional, mainstream media (Europol, 2014). Violent extremists are no longer dependent on traditional media outlets to disseminate their propaganda. For example, it offers the opportunity for violent extremists such as Al-Qaeda in Iraq leader, Abu Musab al-Zarqawi to shape their audience worldviews. Before al-Zarqawi began his online propaganda campaign, it is essential to note that he would have to kill large numbers of people in order to grab the attention of supporters and media (Conway, 2007). However, through the online disseminations of video-taped beheadings of foreign hostages such as Nicholas Berg, al-Zarwawi was able to achieve greater impact and media publicity albeit using fewer resources. The internet has provided him with a readymade audience to exert his influence and presence. The use of the internet by individuals with malicious intent such as violent extremists therefore demands the attention of law enforcement agencies across the world.

In fact, the continuous advancement in information and communications technology can be envisioned to have a dramatic impact on the way such persons of interest may operate. Some recent examples include the online expression of hate during the 2018 Sri Lanka Kandy Riots (Gan, Neo, Chin, & Khader, 2018); acts of insider threats such as WikiLeaks data breach by Bradley Manning (Savage, 2013); online recruitment of members by violent extremist groups (Neo, Dillon, & Khader, 2017); ransomware attacks like 'WannaCry' (Tan & Wang, 2017); spread of fake news during the U.S. 2016 Presidential Election (Chen, Tan, Goh, Ong, & Khader, 2018); online circulation of upskirting photos (Luo & Wang, 2018); acts of cyberattacks (Dillon, 2016); and use of spear phishing to gain illegal access to computer networks (Vishwanath, 2016).

As the world witnesses an upward trend of such crime and security concerns in the online sphere, it places additional 'responsibility' on intelligence and law enforcement agencies to respond with the appropriate technological interventions (Abdul Rahman, 2019). Because the internet has played an im-

DOI: 10.4018/978-1-5225-9715-5.ch068

perative role in the way malicious activities are being conducted, these security agencies are therefore compelled to transform the way they identify potential persons-of-interest, collect usable intelligence, and conduct threat assessments.

In that case, how can individuals with malicious intent be identified in advance? How are they using the internet and social media to further their nefarious deeds? These questions can be addressed by examining how open-source digital footprints (i.e., one's online behaviours on social media and internet) should be harnessed to better identify and assess potential security threats. It is within these digital footprints where a potential perpetrator's intention and warning signs may manifest (Augenstein, 2017; Neo et al., 2017), which in turn can be utilised to assess the threat they pose. This chapter will discuss how digital footprints can be leveraged to identify potential security threats, particularly for crime and security issues that will result in negative repercussion at the national level, such as acts of violent extremism and hate crimes.

IDENTIFYING INDIVIDUALS WITH MALICIOUS INTENT USING THEIR DIGITAL FOOTPRINTS

The ability to disseminate information instantaneously and globally at very low costs provides these individuals with great opportunities to further their nefarious deeds. For example, on 29 October 2013, a video was released by an individual claiming to represent Anonymous via YouTube. It was addressed to the government of Singapore; the person threatened to disrupt key infrastructure in Singapore in an attempt to protest against the government's online regulatory framework (Neo et al., 2013). In another illustration, the Islamic State of Iraq and Syria (ISIS) spokesperson, Abu Mohammed al-Adnani, issued a call for attack on the 'enemies' of ISIS in 2014 via ISIS' repertoire of online platforms (Goh, Tan, Neo, & Khader, 2017). This led to an increase in the number of lone-wolf attacks by followers of ISIS in many parts of the world (Tee, Neo, Chin, & Khader, 2018). It is essential to note that such attempts to reach out and gain attention amongst the population would not have been possible without the internet. The internet has provided these individuals with a readymade audience to exert their influence and presence.

The use of information and communications technology inevitably leave behind publicly accessible digital footprints for intelligence and law enforcement agencies to follow. Personal information and stories (e.g., online expressions of personal sentiment, photographs of local places and happenings, geo-tagging a post, publicised social networks) are becoming easily available on websites and social media platforms (Whitty, Doodson, Creese, & Hodges, 2017). These changes in the access to digital footprints might be particularly useful for law enforcement and intelligence agencies who are increasingly drawing from online sources to assist in identifying potential security threats.

While this repertoire of open-source, highly personal and detailed cyber information can serve as leads for more technical means of intelligence gathering, the massive amount of these open-source digital footprints requires security agencies to be able to prioritise and focus their limited resources in their intelligence gathering endeavour (Skillicorn, 2009). There is also the need to ensure that the data points are reliable and credible. In the context of violent extremism, for instance, law enforcement agencies have utilised social media postings to incriminate individuals who are being radicalised online. In one case, Bilal Abood was arrested in Texas as a result of his Twitter activities. He used his Twitter account to pledge 'obedience' to ISIS leader, Abu Bakr al-Baghdadi, and had plans to travel to Syria to fight against the government of Bashar al-Assad. Although Abood originally denied that he had made the