**NSM activities and behaviors as predictors of terrorism support and involvement**

The role of the internet in radicalization and recruitment processes has recently been the subject of much attention, discussion and debate. Such have downplayed the significance of the internet, arguing that traditional offline interactions play a more significant role in radicalization processes, although admitting that the internet acts as a ‘force multiplier’ or ‘radicalization accelerant’ (Sageman, 2004; Sageman, 2008; ICSR, 2009; RCMP, 2009). In a recent review of the state of the literature relating to criminological approaches to terrorism, Freilich et al (2015) identify the need to compare terror offenders with those who hold similar beliefs but have not committed any terrorism. Until now the trend has been to compare terrorists with other violent criminals, such as murderers. The need to compare terrorists with non-violent radicals should be intuitive. Both groups are exposed to the same types of information, materials and environments, they share certain core beliefs, outlooks and philosophies, and yet one group goes on to engage in violent acts while the other does not. Indeed, only a very small percentage of those who ascribe to extremist ideologies go on to be involved in terrorism, whether in supporting roles or by actually engaging in violence (Horgan, 2008; ICCT, 2016). There are also various levels of participation or involvement which can only be gauged on a case by case basis. Generally speaking, there are also many terrorists who have not strongly adhered to a radical ideology or been overly religious (Alarid, 2016), just as there are a great many adherents of radical ideology who have never engaged in terrorism. As such, the current study seeks to examine the differences in the NSM activity and behaviors of terrorists and non-violent radicals, specifically seeking to identify differences in online behavioral patterns, lexicon changes and network characteristics.

The current study uses Social Learning Theory, with an emphasis on the Differential Association processes in order to examine the key differences in NSM behaviors and activities. The study will employ experimental software provided by Terregence that offers a unique user interface for accessing the Facebook API and extracting user activities and page activities for open pages and profiles. The software also enables the automatic production of key trends and NSM metrics associated with these open pages and profiles. The software's abilities extend to conducting social network analysis and identification of lexical patterns and changes. This unique study seeks to shed light on the online predictors of online radicalization.While three distinct analyses will be conducted, this draft proposal presents the theoretical framework for only the first two of these analyses.

**Research questions**

R1: Can we identify differences in the patterns of NSM activity between: radicalized activists, supporters, sympathizers, and non-sympathizers?

R2: Can Social Learning Theory indicators help to predict differences in the expected NSM activities between activists, supporters, sympathizers and non-sympathizers?

R3: Can NSM activity be used to predict real world terrorism events?

**Social learning theory, differential association and online radicalization**

Social learning theory holds that deviant behaviors are learnt behaviors, with the individual learning such behaviors from important groups to which they belong to or are otherwise a part of to some extent. In this way, deviant behaviors are learnt in the same way that normative behaviors are (Akers 1985; 1998). Akers’ Social learning approach is an extension of Sutherland’s (1947) differential association theory, which remains an important aspect of social learning theory. Social learning theory consists of four primary processes or concepts, namely, differential association, definitions, differential reinforcement, and imitation (Akers, 1998). These elements are important to understanding the role that the internet plays in radicalization and recruitment processes and provide measurable variables of internet activity and behaviors.

Differential associations vary on a case by case basis, with the four important elements of priority, frequency, duration and intensity of associations differing for each individual (Akers, 1998).  The frequency of interactions is believed to play an especially vital role in social learning (Ellis & Walsh 2006, 114). It is said that individuals who are close to their networks and associations, and who engage in frequent contact over an extended period, are more likely to be effected by them (Freiburger & Crane, 2008). More specifically, Akers (1998) reiterates Sutherland and Cressey (1974, 76) in stressing the variability of frequency, duration, priority, and intensity in differential associations.

The advent of the internet, which has led to the creation of both imagined and real communities which are unbound by the limitations of geographic proximity, has contributed greatly to social learning processes. In this sense the internet has certainly acted as a force multiplier for social learning processes, especially differential association (Sageman, 2004; Sageman, 2008; ICSR, 2009; RCMP, 2009). Early studies that examined social learning of deviant behaviors focussed on the effects of passive exposure to television violence. The internet however provides active participation, which has a stronger influence than passive exposure (Pauwels & Shills, 2014). A USAID report explains that one of the primary roles of the internet and involvement in virtual communities is the “shortening of the time frames involved in embracing, and acting on, violent extremist beliefs” (USAID, 2009). Such observations have precedence in other areas, where membership in online communities has been found to help those with sexual identity, stigmatized or fringe beliefs, express themselves in real world settings (McKenna and Bargh, 1998). This has also been found with respect to internet based pedophile activities. In fact, Quayle & Taylor (2011) see a similarity in the processes of radicalization to pedophilia and terrorism. It seems quite possible that many of the same processes of differential association are present with respect to a number of phenomenon. There is a growing amount of research that suggests that using the internet for deviant purposes increases the chance of deviant behaviors being taken offline. Such findings have been made with respect to pedophilia and other sexual crimes, marital affairs, suicide, school shootings, and a host of other actions (Durkin, 2007).

As Hawdon (2012) explains, the four components of differential association are clearly seen with regards to online hate groups. He explains that differential association theory expects it to be more likely that an individual from these groups will be lead to violence when learning of violence has started early in life (priority), exposure to the pro-violent messages and associations occurs more frequently (frequency), over a long period of time (duration), and the associations are held in high regards (intensity). It is clear that other factors may also determine why some act violent and other do not, since different ideologies and trajectories may radicalize individuals differently (Borum, 2011, 2014). Thus there may be significant differences in the way the radical right-wing, left-wing or Islamists use the internet and in the ways in which the internet is a factor in their radicalization and recruitment.

Pauwels & Schils (2016) comment that “The idea that the Internet will increase extremism by splitting individuals into numerous groups of like-minded individuals is called the fragmentation hypothesis. Engaged in homogeneous conversations, people may be more inclined to believe that a violent extremist worldview is the only sensible one and are less likely to appreciate the position of someone who disagrees”. The internet, and especially social media, work as a force multiplier in such processes. Those that demonstrate increased frequency, duration, intensity and priority exposure to radical material, information and messages and connections are more likely to become radicalized and in turn be recruited to commit acts of terrorism.

With regards to *frequency*, recent studies of ISIS members and supporters’ online behaviors indicate that they post far more frequently to social media than average users. ISIS members who appear to have primary functions as online radicalizers and recruiters have even been termed hyper-posters (ISIS Twitter census). However, whilst some case studies show that terrorists increased their online posts prior to their attacks, others went 'dark' in the weeks and months prior to their attacks. Some believe that those who are hyper-posters are actually less likely to turn to actual violence since their online activities provide them with a non-violent outlet to voice their narratives. Frequency can be difficult to gauge in the absence of access to a user's entire computer and computer history. This is because passive exposure is not recorded by Facebook activity logs or user activity histories on other platforms. Therefore, frequency must be a measure of a combined metric that accounts for 'likes', 'posts', 'comments' and 'shares' made by the user.

*Imitation* can be inferred from when the commission of a behavior occurred after having observed someone else to commit the same or similar behavior (Akers, 1998; Rebellon, 2006). With regards to online radicalization and recruitment this could be attributed to a few different areas. Firstly there is direct imitation, what may even be referred to as copy-cat actions. A terrorist may copy the modus operandi of another terrorist whose attack was viewed as ‘successful’ (although this is subjective). Many scholars have noted that copy-cat attacks tend to occur in clusters, similar to other types of deviance (mass school shootings, suicide, drugs etc.). Another type of imitation may be when a terrorist employs the same type of weapons, tactics and/or modus operandi that they read about, such as from Inspire magazine (Perry, Hasisi, Clarke & Newman). Still, here there is a similarity with the previously described type of imitation in that they view another as having done it before them. A third type of imitation may be that in which an individual seeks to model themselves, their style and their image on that of another individual or type of individual. Furnell (2002) explains that the internet has changed the way in which imitation manifests on account of the increased reinforcement that is inherent in the internet and online communities. Akers and Sellers (2004) inform us that imitation in most important in the initial adoption of a behavior but less important in the maintenance or cessation of said behaviors. In the case of terrorism this is an important point, since initial adoption can mean a terrorist attack or attempt, which often leads to death or capture of the terrorist. However, it may be that imitation only leads someone to be a non-violent radical, rather than simply engaging in an act of violence. In imitating others, an individual may choose to imitate living individuals who may or may not advocate individual engagement in violence but who may expound radical ideology. This may mean changes in lexicon (which is also connected to definitions), changes in dress, behavior, body language and other stylistic or outward expressions imitation. In recent years there has been an increase in the attraction of pictures and videos of foreign fighters in Iraq and Syria in influencing imitation with regards to the image of the jihadist.

*Definitions,* broadly speaking, constitute how an individual defines, views and perceives a particular behavior and therefore how their attitude towards it is dictated. With regards to deviant behavior, definitions are what lead to the justification of the behavior(s) so that the perception of potential consequences and their significance is neutralized (Akers, 1998). Definitions play an important role in leading an individual to engage in deviant behavior.

There are however other processes at play here, namely *differential reinforcement*, and there is some overlap here with definitions. Since definitions ‘define’ an individual's perception with respect to their attitude towards a behavior and their perception of consequences, they also consider how their definitions will be supported by others in the future, as they do in the past and present (Holt et al). Differential reinforcement takes place when positive and negative reinforcements of a behavior are given to an individual, especially when it's by someone or a group of people to whom they give the ‘priority’. Positive reinforcement is the attaching of reward to behavior, such as money in the case of robbery, pride and honor in the case of gang violence, or religious achievements in the case of Islamic terrorism (72 virgins, martyr status etc.). Negative reinforcement is when something undesirable is claimed to be removed from the individual for engaging in the behavior. For example, someone who commits murder to remove shame or dishonor, or a terrorist who may be trying to remove past sins or even remove themselves from this living world if it’s defined as being undesirable, as is the case with a salafi-jihadi ideology.

The study also examines how social learning theory variables can predict an online user's position and progression from exposure to radicalization, to operationalization in the carrying out of terrorism. Here the issue is how a user's internet activity behavior and patterns indicate their level of radicalization and how their behavior and patterns may predict their upward transition on the radicalization pyramid (Victoroff, 2005; Pauwels et-al, 2014). It is important to understand what characteristics and online patterns of behavior and activity may predict an individual's progression from a non-interested observer to a sympathizer, or an active supporter to someone who goes on to carry out an act of violence. This is an important gap in the current knowledge since whilst there are a great many radicals, or individuals who adhere to a radical ideology and support radical groups, very few go on to commit acts of violence. The current study proposes to conduct three innovative analyses that seek to address these significant and important gaps in the knowledge.

**Advances in cyber radicalization research**

There have been an increasing number of important studies in recent years which seek to take advantage of the data rich environment of social media. Such approaches, which have had a tendency towards thinking that big data is better data. Berger & Strathear (2013) first examined white nationalist radicalization based on open source Twitter data. Their approach was to identify 12 ‘seed’ accounts (popular accounts of known radicals) and through this identify another 3000 relevant follower accounts.  They analyzed over 300,000 tweets/posts in total.  The inspection of the automated collected data took 3 months. They were able to classify and analyze the type, content, reach and influence of tweets and accounts, also comparing the analysis with a smaller N examination of anarchist accounts. Berger & Morgan (2015) took a similar approach examining Twitter activity of 20,000 accounts of ISIS members, supporters and followers.  They introduced new NSM metrics to analyze reach and influence of specific users, posts and types of posts. Post and view frequencies were significantly greater for these groups compared to average twitter users. Rowe & Saif (2016) recently used new data mining techniques to mine for radicalizing material on Twitter of ISIS supporters.  They examined about 154,000 users, finding these accounts through known ‘seed’ accounts. Ferrara et-al (2016) conducted prediction experiments based on the posts from 25,538 twitter accounts belonging to ISIS supporters and members and Mitts (2016) examined 15,000 accounts against socio-economic metrics. Despite these advances, some of the best information we have regarding the processes and effects of online radicalization and recruitment come from case studies.

For example, Gill, Corner, Thornton & Conway (2015) created a database of 227 individuals which they extracted from case studies contained in existing literature and also from open sources. They presented a Smallest Space Analysis for behavior clustering for different online activities/behaviors.  Gill & Corner (2015) conducted another study, utilizing the same data-set and looked at the type of usage of the internet and differences between those who used the internet for different purposes (IE learning/inspiration, communications, training, etc.). Additionally, Simcox (2015) examined 32 IS and AQ inspired or directed plots/attacks in the west by creating case studies through a variety of open sources.  With respect to the role of internet he found that in 84% of the cases the internet was relevant to the outcome in some way. In total, for 47% of the plots, online content and material acted as the inspiration. Additionally, in 41% of the plots the attackers publically declared their support or allegiance to engaging in terrorism. In only 19% of the cases was the internet used for obtaining instructions and guidance on how to conduct the attacks, and for the same percentage of the plots the internet enabled extremists to connect with each other to discuss their plans.

To date there has been little use of the Facebook API and open source data for examining that platform with respect to radicalization to terrorism. One of the reasons may relate to the difficulties in accessibility and user-friendliness of the API compared to Twitter.

**Study design**

*Analysis 1:* The study will conduct analysis on open profiles of terrorists, primarily lone-wolves, who were either caught or killed following their attacks (N=30) and compare their online activity with a comparison group of (N=30) radicals who have not carried out any terrorism. Additionally, the study will collect data from open profiles of terrorists who commit acts of terrorism during the course of the study's duration in order to increase the N. The study will conduct a factor analysis approach to examine the impact of variations in the independent variables (Lee et-al, 2004; Holt et-al, 2010). This study will seek to test the first hypothesis:

**H1**: In line with Social Learning Theory, it is expected that individuals whose NSM activities display higher levels of: differential association (priority, frequency, duration, intensity), imitation, differential reinforcement and definitions - will be situated higher on the radical spectrum (sympathizer, supporter, activist).

*Dependent variable*

Analysis 1: A dichotomous variable construction of "terrorism" with 0 being that an individual has not committed an act of terrorism and 1 being that they have not.

*Independent variables*

Frequency- A composite metric for both users and pages which includes all active activities such as 'likes', 'posts', 'comments', 'shares', 'views' etc.   
  
Duration- Measured from the time of the user of pages account being opened until the time of attack, or until the time of the analysis where no attack has been conducted.

Intensity- A measure based on a 1-3 scale that scores an associations intensity based on how the user or others refer to them, their position (IE politician, religious leader, family member etc.) and their closeness in the user's network.

Priority- A measure based on the time of when a user established contact with an association relative to the time that their account was opened.

Differential reinforcement- A ratio measure of reference to rewards/punishments, risk/benefits as mentioned in a user's posts made, received, or with which they interacted actively.   
  
Definitions- A measure based on the frequency of specific lexicon based on an existing dictionary of key words, phrases and hashtags.  
  
Imitation- A count measure based on the content of lexicon and images displayed by a user.

*Control variables*

Age, sex, employment, stated religion, stated political affiliations, marital status, family status, language.

*Analysis 2:*

The second analysis in this study will focus on "Hotspot" pages and groups (open) that exist on Facebook. These will be identified by using seed accounts to direct us to those pages and groups that have the most influence and reach/resonance with radical jihadist ideology in Israel. The study seeks to examine the makeup of the followers and participants, examining for differences in behaviors we will seek to fulfill gaps in the knowledge identified by Berger & Strathearn (2013). We will group the top 50, top 100, top 500, top 1000 and top 1000+ users who interact with these hotspots and check for differences in these users' behaviors and lexicon in order to classify the type of behaviors associated with those users that are more radical, and those less radical who may be prone for radicalization but are at a stage where they may be receptive to online interventions. This analysis will likely employ SNA to identify how differences in the independent variables predict a user's classification in the radicalization pyramid. This study will aim to test the second hypothesis:

**H2**: Individuals that are situated as activists or supporters will display stronger indicators of differential reinforcement and definitions in their NSM activities, than those situated as sympathizers or non-sympathizers.

*Dependent variable*

Level of radical: A variable in which a user is measured as either 1) non-supporter, 2) sympathizer, 3) supporter, 4) activist

*Analysis 3*

This analysis focuses on the usefulness of NSM data in predicting real world terrorism. We will create a database of keywords, phrases, hashtags and other user and network level metrics and use these to examine the potential to predict real-world terrorism based on online activities. This part of the study follows the work of Compton et-al (2014) who have shown that it is possible to use NSM activity to predict political violence of different varieties. More recently, Gerber (2014) and Williams (2016) have explored the utility of using NSM data for predicting crime patters. The current study will compare trends in radical NSM activity and compare it with trends and patterns in terror attacks in Israel, including low-level violence attacks such as stone throwing, firebombing and violent riots. The collection of data will be live rather than retroactive. Random effects and fixed effects models will likely be employed for this analysis. This analysis seeks to test the third hypothesis:

**H3:** New social media activity in radical online networks can predict real world violence at the local level and with respect to specific types of violence.

*Dependent variable*

The study follows the approach of Williams (2016) by constructing 9 categories of the dependent variable as representing different types of terrorism events, including low level-violence events that will occur during the course of the study.

**Innovation**

The proposed study provides significant innovation in finding new ways to exploit open source data from the data rich environment of social media. Until now, the largest and most important of NSM platforms, Facebook, has been perceived by most researchers as too difficult to use or access for the purposes of examining issues of radicalization on that platform. My employing experimental software that provides user-friendly and interactive access to the Facebook API, the current study will be able to conduct analyses on data sets previously unavailable. Furthermore, the three proposed analyses will lead to the production of new evidence with regards to radicalization processes and the ability to predict radicalization based on specific online behaviors. In general, the terrorism literature has suffered from a lack of quantitative analysis and very few studies produce new evidence. By combining the three proposed analyses, the proposed study will address issues relating to individual behaviors, the effects of online radicalizing agents, and the possibility of using online activity to predict real-world terrorism. The proposed study will be carried out by creating a joint initiative between the Institute of Criminology, the Cyber Security Research Centre, and by employing innovative experimental software developed by the private intelligence sector.