

Due to the heightened prevalence of Islamic extremism coupled with the wide acceptance of online social media platforms (Facebook, Twitter, Youtube, etc.), what was once a regional phenomenon established only in areas housing terrorist networks particularly the Middle East, has now found its way to the doors of many Western countries. Considering the extremeness of radicalisation, many ponder how an individual could adopt such a behavior and, or, beliefs that bolster his or her engagement in subversive and terrorist activity. Accordingly, what was formerly assumed to be the existence of a single, universally applied, terrorist personality, is now understood as a gradual process undergone by individuals motivated by separate agendas and incentives. Although the process of engaging in terrorism or violent extremism has been argued to be the product of radicalisation and the development of extreme ideologies; radicalising by developing or adopting extremist beliefs that justify violence is just one possible pathway into terrorism involvement (Borum, 2011).

Alternatively, it is important to note that most people who hold radical ideas do not end up engaging in terrorism, just as all terrorists may not be as deeply ideological as they are perceived to be. Likewise, though the rapid spread and influence of these individual occurrences seem to be, at first glance, precipitated by external terrorist organisations located abroad; the underlying influential component consists of a fundamentalist temperament supplemented with an online social outlet for self expression.

In many cases it has been argued that the Internet, operating through the medium of cyberspace (the total landscape of technology mediated communication), provides mechanisms (social media platforms and online services) by which individuals, who would otherwise not have conducted a terrorist attack, can self radicalise and access the information they require to carry out such attacks (Kebbell & Romyn, 2016, p. 92).

Additionally, extremists have been known to broadcast their views, provoke negative sentiment toward enemies, incite people to violence, glorify martyrs, and create virtual communities with like minded individuals in order to convey their message and groom new recruits on online social media platforms, such as:

Facebook, Twitter, YouTube and other online services (COPS, 2014). In contrast to terrorist networks such as the Islamic State (IS) and al Qaeda radicalising and recruiting individuals in the physical sense, the internet has the ability to shroud methodological steps taken in order for militants to connect with, communicate with, and muster, prospect radicals.

Technologies such as virtual private networks (VPN), onion routers (TOR) and other forms of encryption, provide what could be viewed as cyber camouflage; thereby strengthening evasive techniques employed by extremists. Securitising these online anonymity tools would essentially provide law enforcement and intelligence services with enhanced capabilities, thus reducing the overall discreteness found between extremists and their uploaded content in addition to the individuals they seek to influence and inspire. The purpose of this research topic of choice is to extend upon how digital platforms are used in order to strategically advance online self radicalisation, recruitment and enlistment (Khader and Neo, 2016). In addition to the latter, focus on features that are often highlighted in regards to modern examples of terrorism is the importance of rapidly advancing and accessible technologies.

Terrorists acquiring and using these technologies to more effectively promote their agenda is a grave national and international security issue (Terrorism

Analysis 2016). Furthermore, online self radicalisation is a source for concern which has virtually lead to difficulties withstanding, as well as unsuccessful domestic counter measures, within the United States of America. This dissertation aims to not only address the current ubiquitous phenomenon ensuing within the United States (U.S), additionally, it will also discuss, as well as investigate, why effectively combating such a harsh reality has momentarily proved to be unsuccessful. The theoretical framework of this document consists of a detailed literature review, further supported by a case study analysis. Implementation of

an indepth literature review appropriately seeks to conceptualise radicalisation, its causes, and the various existing models and pathways that have been developer beneficial to comprehend Ing its process. In contrast to previous radicalisation models, Angelini's online self radicalisation model (AOSRM) was developed to shed light on the radicalisation process as it occurs in the cyber domain. The model itself emphasises the individual's exposure to radical online content also referred to as echo chamber indoctrination as well as the social cultural transitions that subsequently take place. Furthermore, AOSRM's application is not only theoretical, but instead practical; as it provides transparency on how an individual(s) may progress towards radicalisation, online, min addition to exposing a possible outcome that does not necessarily lead to violence radicalisation into extremism (RE).

By analysing three cases involving online radicalisation and terrorism, the case study analysis examines the hardship and tedious procedural process U.S. authorities occasionally go through in order to fulfill their responsibilities during and following an investigation.

In each case the author exploits the backgrounds, interests and incentives, of the perpetrator(s). Criticism and admiration is impartially distributed towards the procedural steps taken, or not taken, in attempts to countervail online radicalisation and terrorism. Moreover, the author's recommendations are offered in hopes of improving a systemic problem found within the U.S. Furthermore, the first two cases undergoing analysis highlight the failure's and success' directed towards prevention and apprehension of a terrorist attack, with the third and final case exemplifying the success of a counter terrorism operation, in addition to incorporating the author's personalised online self-radicalisation model

-AOSRM. The overall rationale behind the case selection is to essentially reveal a variation of outcomes among similar, yet unrelated, incidents in addition to assessing the parallels and diversity between them. Accordingly, the first two cases that were selected, yield distinct infractions and obedience regarding the institutions involved (the FBI, Facebook, Apple, etc.), technologies and regulations confronted concerns critically addressed in the third chapter. Likewise, the two cases further provided an uncomplicated analysis on a particularly complex topic. The third case that was selected simply demonstrates a coherent pathway towards extremism by means of radical online material, and is therefore thoroughly analysed via compatibility with the author's radicalisation model, AOSRM. Incorporation of the author's model offers insight to the online

-radicalisation process; more specifically how it can facilitate preemptive awareness and, perhaps, intervention, in further support of successfully thwarting terrorism prior to its devastating aftermath. Considerably influenced by terrorist organisations, such as the self-proclaimed Islamic State (IS), the exploitation of social media and recruitment/enlistment of domestic extremists is the result of radical online propaganda varied with obsessive regularity and sympathy towards terrorist causes (Khader and Neo, 2016). As a result, criticism is impartially distributed towards the procedural steps U.S. legislature and private corporations have taken, and have not taken, in attempts to countervail the growing phenomenon of online self-radicalisation. As Michael A. Stefanone states in his expert analysis article, "The ultimate utility of social media is to connect like-minded individuals... Today, however, technology enables us to connect globally. Now that we can connect globally, there is also greater opportunity to connect with others who are increasingly extreme in their attitudes and beliefs"