University of Glasgow

Faculty of Social Sciences
Charles University in Prague

OTH OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

Terrorism: Difficulties in Countering U.S. Phenomenon of Self-radicalisation in the Digital Era

July, 2017

2224901A

34746078

Presented in partial fulfilment of the requirements for the
Degree of

MSc International Security, Intelligence and Strategic Studies

Word Count: 24,071

Supervisors: Dr. Adrian Florea & Dr. Nik Hynek

Contents

Page

Acknowledgments

This dissertation is dedicated to the following individuals: my mother and father, for supporting all of my aspirations; my grandmother, Uncle Paul and Uncle Robert, for moral and financial support; and my girlfriend, Ariel, who has been my dawn to end all nights. I love and thank you all.

Introduction

Research Question: **How can online self-radicalisation be successfully countered?**

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 doorstep 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 discreetness 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 in-depth literature review appropriately seeks to conceptualise radicalisation, its causes, and the various existing models and pathways that have been developed beneficial to comprehending 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, in 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 **s**tates 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" (2015).

Chapter 1

Principles of Radicalisation: Literature Review and Introduction to Angelini's Online Self-radicalisation Model (AOSRM)

1.1Defining Radicalisation

Due to 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. According to Randy Borum, "early efforts attempting to solve this enigma merely took the narrow approach by solely focusing on studying the individual(s) behavior" (2011, p. 14). Since the 1960's, however, academia has further analysed a multitude of terrorist activities, as well as their sectional subordinates. Accordingly, focus of analysis has, rather than stay fixated on observing individual behavior, broadened and concentrated on various criteria, such as: the individual, group interaction, social networks, organisations, mass movement, socio-cultural contexts, and even international and interstate contexts. Therefore, the prior assumption that radicalisation of an individual was once due to their aberrant behavior reflecting some sort of mental or personality abnormality, has been disproven. Randy Borum states, "Fortunately, with very few exceptions, most contemporary social scientists studying terrorism have moved past these early, naïve assumptions" (2011, p. 14). Comparable with Borum's statement, John Horgan asserts, "for a long time, there was a widespread assumption that there may exist a terrorist personality, and there have been many efforts to engage psychology in a technical sense in terms of the development of profiles (e.g. of particular types of terrorists such as suicide terrorists, or hijackers, for instance, and more recently whether suicide terrorists for example might resemble other kinds of mass killers such as school shooters), but as a *discipline*, psychology has had little to say about terrorist behavior" (2014, p. 3). As a result, radicalisation foreshadowing acts of terrorism, is no longer considered a "condition", so to speak. Instead, terrorism, in relation to its constituent 'radicalisation', is now viewed as a *dynamic process*.

Many who attempt to further understand the concepts and definitions of radicalism, face the probability of unintentional conflation between the various terminologies and contexts of the word, given the ubiquity of its usage. Instances such as this become seemingly recognisable when discussion surrounding radicalism and violence start to arise. The number of attempts on creating an absolute definition of the term "radical" are as indistinct as they are innumerable. Similarly, the clarity between the terms "radicalism" and "threat radicalism" is also lacking. According to the National Institute of Justice (NIJ) the definition of *threat radicalism* is as follows: "Extreme views, including beliefs that violent measures need to be taken" (2008, N.p). However, aside from the focus surrounding and interrupting the radicalisation process, also referred to as radicalisation into violent extremism (RVE), others oppose or, to some degree, question the cases involving radicalism and the lack of violence associated with them. In contrast to NIJ and in the context of radical Islam, Scott Atran acknowledges a poll taken from 'Pew and Gallup', which reports that although there is an existence of tens of millions of Muslims worldwide who are sympathetic towards Jihadists, most of them do not end up engaging in violence (2010, p. 5).

Although the term "radical", in addition to "radicalism" and "radicalisation", is often used in discussions regarding terrorism and extremism, the word essentially has two types of meaning; one relative and one absolute (Sedgwick, 2010). The relative meaning of the term "radical" is most appropriately understood from the *Oxford English Dictionary*, and states, "representing or supporting an extreme section of a party" (2009). It is in this sense, the term may be synonymous with the term "extremist" (Sedgwick, 2012). However, when seeking to define "radicalism" in its absolute context, the onset of confusion is often common. When comparing some of the earlier forms of the absolute definitions, such as, ‘‘radicalism is a unified and internally consistent interpretation of the world’’ or “when medieval man rebelled, he rebelled against the abuses of the lords”, one cannot help but feel as though the absolute definition of radicalism is still under development (Bittner, 1963; Ortega y Gasset, 1923). Therefore it is best to refer to its relative subordinate for purposes of conceptual clarity.

Radicalisation as a concept and in terms of violence, also referred to as radicalisation into violent extremism (RVE), could essentially be described as the processes by which people come to adopt beliefs that not only justify violence but compel it, and how they progress—or not—from thinking to action (Borum, 2011). The distinction that should be made when comparing radical acts of violence to regular, non- radical, acts of violence, is the presence of ideology as a motive. 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). Furthermore, as research shows that there is not a single pathway to RVE, and that the process undergone by one individual may not be the same process undergone by another; it is apparent that a single theory or discipline will not encapsulate a definitive pathway. Needless to say, identifying and interacting with mechanisms on the micro (individual) and macro (social/cultural) levels on a case by case basis is critical in providing edification to the radicalisation process, overall (Borum, 2011).

In addition to the lack of clarity attributed to radicalisation, in terms of extreme ideology versus extreme acts of violence, other areas facilitating discourse on the topic harbor similar aspects of contextual perplexity (the intricate use and context of the term); in that they disagree with how the term “radical” is used. As Mark Sedgwick concedes, the three most important official and semi-official contexts in which the term ‘‘radicalisation’’ is presently used in Western nations are *the security agenda*: intelligence and police agencies who are both concerned with radicalisation as a direct or indirect threat to the security of the state or of individual citisens of the state; *the integration agenda*: promoting equal membership through desegregation and prevention of segregation of previously segregated groups, with specific emphasis on avoiding residential and market- segregation; and lastly, *the foreign-policy agenda*: policy makers who are concerned with radicalism both directly (similar to the security agenda) and indirectly - through the involvement surrounding various benign and allied governments, as well as friendly Arab regime (2012, p. 485- 487). In accordance with the contextual perplexity surrounding "radicalisation", as Sedgwick had observed; Veldhuis and Staun from the Netherlands Institute of International Relations, Clingendael, argues that it is, in fact, the apparent absence of a lucid and universally accepted definition of the term (radicalism) that has caused so much confusion (2009, N.p). To illustrate this, Veldhuis and Staun state: "Although radicalisation has increasingly been subjected to scientific studies, a universally accepted definition of the concept is still to be developed. Nevertheless, faced with pressure to tackle radicalisation, policy makers have developed a few definitions. Definitions of radicalisation most often centre around two different foci: (1) on violent radicalisation, where emphasis is put on the active pursuit or acceptance of the use of violence to attain the stated goal, and (2) on a broader sense of radicalisation, where emphasis is placed on the active pursuit or acceptance of farreaching changes in society, which may or may not constitute a danger to democracy and may or may not involve the threat of or use of violence to attain the stated goals" (2009, p. 4). Respectively, as one enters the realm of differing contextual agendas, it is important to note that the author will be embracing and focusing on the first out of the two varying definitions.

1.2 Defining the Causes and Concepts of Radicalisation

The central argument behind the concepts of radicalisation is that there are various existing contexts (security, integration, and foreign policy) that inadvertently convolute the meaning of the word "radicalisation", or what it means to be "radical." What tends to be problematic is not the word itself, but the suggested "absolute concept" of how the word is applied within the discourse of said contexts. This can be supported by the increase in frequency of use of the term "radicalisation" by the press, in years 2005-07 due to the emergence of homegrown terrorism (Sedgwick, 2010, p.480). Previous discourse on topics relating to radicalisation leading up to years 2005-07 consisted of circumstances, ideology, the group and, or, individual. However, over the course of time, negligence to the subject of wider circumstance has led to the conflation of groups and individuals. An example of this would be the parallel drawn between Islam and violence, as well as the observable prejudice towards how all Islamists are driven by religious principles. Such assumptions aren't entirely true, therefore, we shall extend upon the differentiating factors pertaining to *Islam* and *Islamism*, in the context of radicalisation, downstream.

The number of attempts on creating an absolute definition of the term "radical" are innumerable. Similarly, the clarity between the terms "radicalism" and "threat radicalism" is also lacking. The definition of *threat radicalism* given by the National Institute of Justice (NIJ) is as follows: "Extreme views, including beliefs that violent measures need to be taken" (Hamm, 2008). This is true, however, the opposing argument or question that has been formed, rather, is that of the cases that don't involve any violence. What about cases that do not lead directly to violence, or do not necessarily lead to violence at all? For these cases it's best to rely on the relative yet conceptual meaning of the term "radical", which, in one's own opinion, happens to be most appropriately understood from the *Oxford English Dictionary* – as previously mentioned, and states, "representing or supporting an extreme section of a party" (2009). It is in this sense, the term may be synonymous with the term "extremist" (Sedgwick, 2012). Such a case will be recognised, as well as analysed later on in Chapter 2.

When discussing the causes of radicalisation, the intentional and systematic principles of *recruitment* often times coexists within the majority of discourse taking place. Although it is lucid that the topic of recruitment shares a unique place in the radicalisation into violent extremism (RVE) discussion, it would be prudent to note that not all individuals who are in fact radicalised fall under the process of being recruited. To illustrate this, Mark Sadgewick goes as far as to say, "There is no recruitment per se to armed jihad or Al- Quida" (2010, p. 479). Sedgewick continues to argue that contrarily to recruitment, *enlistment* is predominantly the contemporary mechanism for the emergence of new recruits (2010, p. 479). Despite the synergy between radicalisation and recruitment, the radicalisation process is far more intricate. In essense, recruitment may or may not be a specific phase within the overall process towards radicalisation, the process itself is entirely unique to individual(s) undergoing it.

Notions relating to radicalisation and involvement in terrorism are proposed as an ambiguous set of processes. To illustrate these processes, theories consisting of: social movement, social psychology, and conversion, would be the most practical to review, if the objective is to gain tautological understanding and comprehension to frameworks that may bare influence over terrorism – this will be discussed in further detail later on. In comparison to this, the use of the "radicalisation into violent extremism (RVE)" term may be apparent to illustrate and extend upon the process by which people come to adopt beliefs that they feel justify violence (Borum, 2011, p. 4). Alternatively, people should not apply the term RVE so carelessly. This is due to the fact that most people who hold radical ideas do not engage in terrorism, just as all terrorists may not be as deeply ideological as they are perceived to be. For instance, a poll taken from 'Pew and Gallup' reveals that although there is existence of tens of millions of Muslims worldwide who are sympathetic towards Jihadists, most of them do not end up engaging in violence (S. Atran, 2010, p. 5).

Theoretical Processes of Radicalisation

There are many pathways through which radicalisation occurs, each of which is affected by a variety of factors. Within this "pathway" or "developmental" approach, radicalisation is observed not as "the product of a single decision but the end result of a dialectical process that gradually pushes an individual toward a commitment to violence over time" (McCormick, 2003, p. 475). An example of this could the online consumption of radical material or propaganda by an individual who is sympathetic to extremists abroad. Simply put, prolonged exposure to such material may incentivise an individual to take action in favor of violent extremism, thereby self-radicalising and pursuing efforts of acceptance among a terrorist organisation – such as IS or Al' Quida – to then carry out similar acts of violence at home or abroad. Moreover, extensive research confirms the general proposition that no single pathway or explanatory theory exists that would apply to all types of groups, and, or, individuals who in fact have become radicalised or are currently on the path towards radicalisation (Borum, 2004, N.p). As Walter Laqueur states, "Many terrorisms exist, and their character has changed over time and from country to country" (2003, N.p). Such a transformation is equally recognised in the process of radicalisation, however, what is even more crucial than the existence of this process is the 'how' factor. According to Borum, "how do individuals come to not only accept, but advocate such violent extremist ideologies, to translate them—or not—into justifications or imperatives to use terrorist violence, and choose (or choose not) to engage in violent and subversive activity in service of those ideologies" (2011, p. 11)? In comparison to this, various frameworks and theories do exist that may support and elaborate on particular pathways throughout the radicalisation process, additionally providing a broader outlook on said pathways. Furthermore, subsequently concluding this section and the process of observing such theories, the following information will then be applied to home grown radicalisation in the west.

- Social Movement Theory (SMT): Also referred to as "Strain Theory", according to Borum, this movement arose from irrational processes of collective behavior occurring under strained environmental conditions, therefore producing a mass sentiment of discontent (2011, p. 17). Due to passively succumbing circumstances as well as overwhelming social forces, individuals find no other outlet other than joining such a movement. SMT researchers in the 1980s and 1990s determined that the primary task of any organisation and, or, movement is to maintain its own survival, thus requiring adherents to collect and maintain a body of supporters (Borum, 2011).
    - Klandermans and Oegema suggests that to survive and sustain itself, any Social Movement must attend to the following tasks: forming mobilisation potential, forming and motivating recruitment networks, arousing motivation to participate, removing barriers to participation (Klandermans, 1987, p. 520). SMT's can be applied to cases of isolated individuals self-radicalising online, due to similar procedural steps taken by extremists to replenish expired members by expanding the organisation/ movement's influence and capacity via online platforms.
- Social Psychological: Primarily concerns itself with relationships, influences, and transactions among people, and particularly group behavior. Because violent extremism is most often a group-related phenomenon, social psychology attempts to understand and explain how the thought, feeling, and behavior of individuals is influenced by the actual, imagined, or implied presence of others (Allport, 1954, p. 5).

Accordingly, there is a correlation between this theory and echo-chamber indoctrination, a phase within Angelini's online self-radicalisation model which will be discussed shortly. Essentially, however, the template is the same: individuals isolate themselves in an online community surrounded by other individuals with similar issues, only to reaffirm their own and avoid criticism.

- Conversion Theory: Devotes less focus on the collective movement, and more so on the individual process of transforming beliefs and ideologies – personal "Coversion" (Borum, 2011, p. 22). It has been speculated that theoretical perspectives on conversion have polarised into one of two categories: *passive*, which views the convert as a passive target who has been damaged by trauma and, or, has unfulfilled psychological needs, and whose will is overpowered by a form of brainwashing for indoctrination purposes; and *active*, which views the convert as a rational actor and active seeker, whose decision to join an organisation or movement of any kind is an act of uncompromised volition. (Borum, 2011; Richardson, 1989). The application of both mentioned perspectives can also be acknowledged in an online atmosphere. Resulting in the radically influenced individual to associate with what they perceive is the official message of Islam and, or, physically converting to the religion as a display of devotion.

Home Grown Radicalisation in the West

Home grown terrorism in the Western part of the world has been on steady incline for the past decade and a half. Moreover, home grown terrorism can be defined as: acts of violence against civilian and, or, military targets that are primarily orchestrated in Western countries – such as Europe and the U.S. - in which those committing violence have been born and raised; hence the term 'home grown'. Apart from these individuals being naturally integrated into their respected Western societies, with the exception of some remaining isolated in ethnic and religious enclaves, public locations, such as: metro stations, airports, restaurants, and night clubs, have all been unfortunate victims of their abhorrent agenda. Alternatively, the more recent immigration of Muslims in Western parts of Europe has led to rampant immigration failures. As a result, one notices a prevalence of discriminatory acts against Muslims throughout large portions of these modern societies. Although failure of integration does not exacerbate home grown terrorism, it does, however, boost jihadist recruitment efforts towards disaffected and marginalised young European Muslims. As for radicalised tendencies, there is no single factor to be considered 'standard' in the radicalisation process. What is understood is that personal identity, group dynamics, as well as one's particular values, all play an essential role in the transformation process. In other words, home grown radicalisation in the West could be observed as a sociological process. However, to further explain the emergence of home grown radicalisation, a combination of factors must be taken into consideration.

Despite the existence of other forms of radicalisation, Islam seems to be the most concerning issue throughout Western society. Similarly, Islamic ideologies are currently prominent and may consist of anti-western propaganda. Consequently, it is important to differentiate between both Islam and Islamism. In modern day, Islam is said to be a religion that does not promote violence, nor encourage hatred on none Muslims (Borum, 2010, p. 10). Contrarily, Islamism has been declared a totalitarian political ideology driven by potent anti-western goals, with the intended "conquest of the world by all means" (Borum, 2010, p. 10). Be this as it may, radicalisation is inherently personal, as well as may be influenced by political, social and, or, religious goals, that are justified by the individual as they, he, or she, seem fit.

As Borum suggests that it seems reasonable to assert that traditional recruitment—as the military does with a dedicated budget and personnel—may not be notable, it seems nearly indisputable that Islamist militants seek new personnel and that they engage in active efforts to influence others to adopt their extremist ideology, which is arguably a broader conceptualisation of recruitment (2011, p. 14). If genuine, Borum adds, “perhaps some of the contested differences really lie in how they do it rather than whether they do it. The issues cannot be resolved here, but the notion of recruitment has been raised both to distinguish it from radicalization and to suggest—as a policy matter—that there may be some value to considering a broader, rather than a narrower, definition of recruitment as it relates to violent extremism” (2011, p. 14).

As inquiry into radicalisation throughout the west persists, the inclination that the process of becoming radicalised and committing acts of terrorism is predominantly male oriented is a deceptive outlook. If one were to dive deeper into more contemporary cases of individuals becoming radicalised in the Western part of the world, one may notice a recent spike in female recruitment to terrorist organisation, Islamic State in Iraq and Syria (IS) (Saltmans, 2016, p. 174). Although this may seem like a new phenomenon, it has been discovered that women have taken up supportive roles in the revolutionary efforts of terrorist groups by virtue or recruitment or enlistment, thereby supporting the possibility for further radialisation into extremism or violent extremism. Such information reinforces previous claims that for many years’ women have long been a blind spot for security, academic and think tank sector, in relation to the growing threat of global extremism (Saltmans, 2016, p. 174). “The number of Western foreign terrorist fighters (FTF) and female migrants joining ISIS in Iraq and Syria was last estimated at upwards of 4,000, with 550 women within this figure” (Barrett, 2014, N.p). While the internet cannot be considered a sole cause of these figures, there is no doubt that online platforms, such as: various chat rooms, YouTube, Facebook, Twitter, and so on, have facilitated extremist recruitment and enlistment by virtue of fanatical online material and socialisation, in turn stimulating the processes of radicalisation (Saltmans, 2016, p. 175). In order for one to fully conceptualise the psycho-social influence terrorist organisations – like IS and Al’ Qaida– bare over their future adherents, analysis of various case studies is considered to be ideal. In the forthcoming chapter, Chapter 3, such case studies to which pertain to the United States will be analysed.

Challenges Sustained Online

The number of Foreign Terrorist Fighter (FTF) and female migrants leaving from Western countries to join IS is unprecedented. Although radicalisation in the U.S. is relatively new, the methods these radicalised individuals adopt in order to facilitate their migration is congruent with the digital era. According to Saltman, "The complexities of deciding to migrate to join a conflict and planning the logistics of this act, which is inherently illegal in the case of IS, is one that is currently facilitated by online communications and Internet tools" (2016, p. 183). With deference to radicalisation by violent extremist organisation, it has been observed that the Internet is used in three primary ways (Hussain & Saltman, 2014):

1. Firstly, indoctrination of individuals is achieved through deconstructing previous ideology in order to proselytize and re-educate individuals towards a particular extremist worldview (Saltman, 2016, p. 180).
2. Secondly, the Internet serves as a tool for educating the curious about extremist ideologies, further providing quick and easily accessible learning tools, lectures and educational resources (Saltman, 2016, p. 180).
3. Lastly, the Internet is used as a socialisation tool by recruiters, solidifying the radical violent ideology by providing a sense of community, or echo-chamber; a like-minded social environment and propagandised media that conform to various radicalised narratives (Saltman & Winter, 2014).

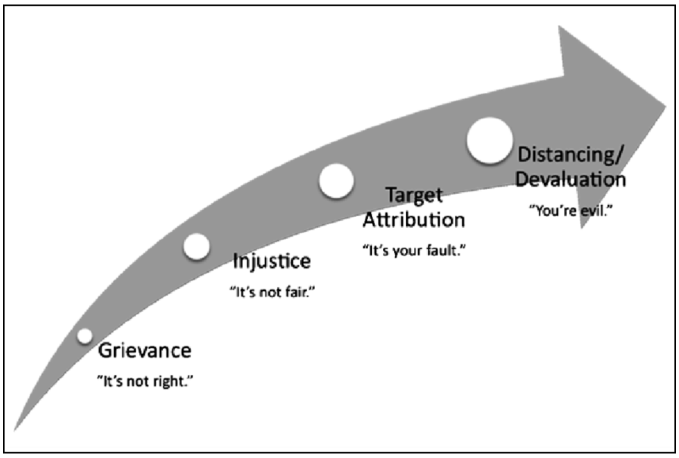
Janbek and Steinfatt insist that the biggest advantage of such communication, is that the messages reach their intended audience, unfiltered, by bypassing traditional media outlets (2016, N.p). However, Neo claims that the transition from online to offline violence exposes a grey area that remains poorly understood (2016, p. 201). Moreover, while many members of violent extremist online communities exist, it is only the small minority that become engaged in violent extremism (Neo, 2016). Opinions aside, social media has now become the mainstream recruitment platform for online radicals and extremists, allowing many IS recruits to find their way to the group in web forums and on Twitter, where they can easily connect to fighters and networks in Iraq and Syria (Dickinson, 2015; Torok, 2016). In 2015 alone it was estimated that IS had successfully recruited between 16,000 and 17,000 fighters from 90 countries ("Legion of Fighters", 2015). However, other estimates are certain that the number of foreigners joining IS as well as other groups was instead around 20,000 ("20,000 foreign fighters", 2015). The Internet enables one to bypass certain media outlets, thus allowing for terrorist organisations to unimpededly broadcast their message. According to Vidino and Hughes, "as of the fall of 2015, U.S. authorities speak of some 250 Americans who have traveled or attempted to travel to Syria/Iraq to join the Islamic State in Iraq and Syria (ISIS) and 900 active investigations against ISIS sympathizers in all 50 states" (2015, p. ix). Although the number of recruits from the United States represents a very small percentage of the overall number of foreign recruits, it remains significant and alarming.

1.3Existing Models and Pathways of the Radicalisation Process

As mentioned earlier, the pathway to radicalisation is a dynamic process. Similar to other existing processes that are extraneous to ones that could eventually result in acts of terrorism, the progression towards radicalisation can be divided into segments, or individual phases. These phases in their entirety demonstrate what most researchers refer to as a 'gradual process'; in which individuals' progress through multiple stages of a particular chain of events at varying timeframes, leading up to radicalisation (Borum, 2003; Moghaddam, 2005). Many of these models have been developed over the years, however, their content and structure differ greatly due to perceived variance in the radicalisation process, key aspects of radicalisation sought to be emphasised and exposed, in addition to differences of opinion among a number of scholars. Despite this, many of these models fail to accentuate the process as it exists in the cyber element, rather than its conventional one. In other words, existing models cater to a more generalised form of the process towards radicalisation instead of focusing on a contemporary approach, thereby incorporating the role of the Internet and the influential use of its numerous online platforms. Furthermore, the reviewed models are deficient in unmasking other facets of radicalisation distant from committing acts of terrorism, or 'Jihad', which seems to be the 'final phase' in frequent models. Nevertheless, the models that are to be discussed provide vital insight into the radicalisation process, whilst simultaneously unveiling multiple viewpoints on the topic as a whole.

Borum's four stage model was initially developed to convey to law enforcement officials insights into the radicalisation process (Borum, 2003). As shown below in Figure 1, Borum's model demonstrates a more conceptual outlook on the radicalisation process, rather than an empirical one.

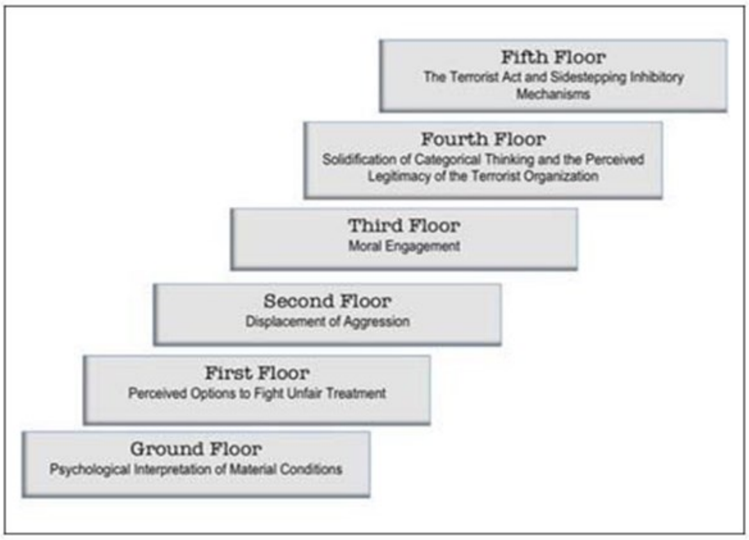
Figure 1. Borum's four-stage model (Borum, 2003, 2011).



The first and second phase of the model, grievance and injustice, set the tone for forthcoming discursive markers, target attribution and distancing/devaluation, and can be perceived as a common foundation that is acknowledged in various existing models. Moreover, Borum's model insists that grievances, in addition to exposure to radical discourse, generate hatred towards certain groups, ensuing a final outcome that allows the individual to embrace ideologies pertaining to jihad and martyrdom (Borum, 2011). In contrast however, the transformation into violent extremism is primarily a product of consumption of radical discourses pertaining to jihad and martyrdom, rather than ascribing to hate as the main influential factor. Although Borum's model accomplishes what it initially sought out to achieve, the model itself is overly simplistic and incompatible with online self-radicalisation as it does not include interaction with the Internet or its platforms. Furthermore, the purpose for its creation – to provide a general radicalisation template to law enforcement – hinders the model's practical application. Nevertheless, the first phase of the model is widely accepted as a sound starting point in the radicalisation process.

Moghaddam's terrorism staircase model (see Figure 2) describes the path to terrorism as a set of progressive stages with fewer and fewer individuals progressing onto each stage within the staircase (Moghaddam, 2005). Unlike most models, Moghaddam solicits that the first stage an individual embarks on in the radicalisation process is a product of personal adversity; subsequently outlining violence of action as a first floor option rather than a conclusive one. The implication that violence immediately succeeds personal adversity is a flaw in the model, due to the sense of idiosyncrasy circulating each particular case involving an individual becoming radicalised and, if need be, engaged in violence of jihad. Another issue with this model, again, pertaining to the first floor, is that violence of action is considered an *option* rather than an *obligatory crusade.* However, in contrast to the efficient staircase structure of the model, further supported by the moral aspects related to the transformation into terrorism, the psychological connotation throughout this model seems outdated if and when applied to contemporary processes of radicalisation. Therefore, the process of radicalisation is no longer focused around an individual's aberrant behavior, but instead has been broadened to encompass a diversified set of social and cultural influencing factors.

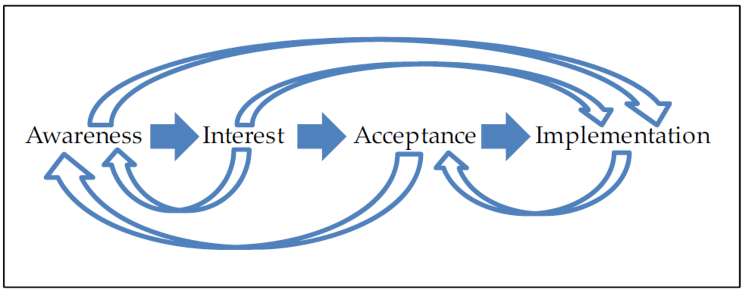
Figure 2. Moghaddam's Terrorism Staircase (2005)


Fifth Floor
The Terrorist Act and Sidestepping Inhibitory Mechanisms
Fourth Floor
Solidification of Categorical Thinking and the Perceived Legitimacy of the Terrorist Organization
Third Floor
Moral Engagement
Second Floor
Displacement of Aggression
First Floor
Perceived Options to Fight Unfair Treatment
Ground Floor
Psychological Interpretation of Material Conditions

Helfstein's four stage model, contrary to older models, views the phases of radicalisation as a dynamic series, similar to a cycle of events. This contemporary model (see Figure 3) was created based on case studies of radicalised individuals and plots of terrorism in the U.S. (Helfstein, 2012). In contrast to previous models, Helfstein argues that radicalisation cannot be independently viewed as a social or ideological process; but instead suggests it is a "coevolutionary" process that maintains interest in both streams of influence (2012, p. 2). Accordingly, as this model is more recent than the latter, it emphasises that Internet sites, YouTube and online magazines convey radical ideology, particularly focusing on Facebook and how interaction with the online platforms seem to facilitate the institutional process of socialisation (Helfstein, 2012). Another important factor can be attributed to individuals who are radicalised or prone to radicalisation often had a *counterculture* background (Helfstein, 2012).

The uniqueness of Helfstein's model can be credited not so much to the sequential order of discursive markers, but rather its regressive characteristics as well as its ability to revisit previous stages within the model. The first stage, awareness, involves exposure to radical ideology. Thereafter, individuals progress to the interest phase, willingly permitting the metamorphosis of their belief system. Here the individual(s) supposedly indoctrinates themselves into online institutions, similar to social networks and chat rooms housing people with related interests and perspectives. The acceptance stage, Helfstein claims, is where social norms are internalized and violent actions are sanctioned (2012, N.p). Lastly, the implementation stage is where universal action appears. Although Helfstein distinguishes between radical and violent radical norms on paper, his phase model unsuccessfully makes this distinction (2012, N.p). Furthermore, the ceaseless regressive and revisiting function of stages within Helfstein's model can be widely interpreted as ambiguous and controversial. One could argue that the model subliminally displays the procedural steps of de-radicalisation process without officially recognising its existence through inscribed explanation.

Figure 3. Helfstein's four stage model of radicalisation (Helfstein, 2012)



Torok's explanatory model utilising psychiatric power, interestingly enough, is not a phased based model (Torok, 2011, 2013). Alternatively, it examines power relationships online in addition to how discourses are formed and propagated online (Torok, 2016, p. 65). The assumptions underlying this model are based around Foucault's (2006) research; acknowledging the utilisation of circular and networked nature of power, in addition to significant discourse formation (Torok, 2011, 2013). The model itself was formulated to focus on three critical foundations: outlooks on social media platforms regarded as online institutions seeking to isolate and expose individuals to one-dimensional discourse; normalisation of extremist discourse, conveyed with authority and truth; and, lastly, power is networked with individuals being radicalised by various sources consisting of homogenous extreme discourse, rather than a single entity (Torok, 2016, p.65).

Notwithstanding, Torok's explanatory model is possibly the most contemporary model to date. However, it is unclear whether the model continues to follow the individuals' induction into extremist thinking. Moreover, similar to the lack of transparency surrounding the models outlook on extremist thinking, the overall depth of the explanatory model does not actually extend that far. Critical points have been address, like the social media environment and its influential power, yet provide no description on how individuals interact within it. Despite the importance of discursive markers and how they are related to the process of radicalisation – as Torok points out - this model could benefit from an attached phase model, for it would provide visual clarity towards the current explanatory model. Although Torok's model could be more descriptive and visually drawn out, it does refer to current issues other models seem to overlook, such as how online institutions tend to isolate people with identical interests. For that reason, Torok's model seems to be better equipped than the other aforementioned models to address radicalisation in its contemporary element.

I propose an alternative model, Angelini's online self-radicalisation model (AOSRM), which seeks to interpret online radicalisation as a process leading up to radicalisation into violent extremism (RVE), yet exposes the possibility of an individual not partaking in violent acts of any kind; thereby allowing the individual to branch off into what is referred to as radicalisation into extremism (RE). AOSRM was created to provide transparency on the online self- radicalisation process. The phase model starts off with *exogenous conditions*, also referred to as 'triggering factors'. These factors, whether they are motivations of any kind (economic frustration; political, social, and, or cultural injustices) are completely unique to the individual and may lead to curiousness and, or, self-education on matters relatable to oneself. Sequentially, *echo-chamber indoctrination* follows suit and provides insight into the individuals' online consumption of radical discourse through isolated online communities. This phase goes on to explain that disaffected individuals searching for an outlet to self-educate or socialise with people that possess similar or identical ideologies and, or, grievances actually turn out isolating themselves, in turn, reinforcing commonly held ideas that are safe from criticism. Subsequently, *conversion*, the third phase in AOSRM, introduces a conscious, or sometimes sub-conscious, decision involving identification or association with what is to be believed as the message of Islam – also referred to as Islamism – and is the radical tipping point in the process. *Justification* is essentially the last phase in the AOSRM model which ensues radicalisation, however, it is the divisions within the phase of justification – RVE and RE - that distinguish it from other models. The divisions establish a precedent that reveals how extremists do not always result to violence. Nevertheless, individuals who have progressed to this stage of the model, though they may not end up committing or supporting acts of violence, may not necessarily disagree with them. A comprehensive introduction of the author's contributions will be discussed further into the chapter.

1.4 Angelini's Online Self-radicalisation Model (AOSRM)

The author's model is a phase based model, similar to many of the aforementioned models (see Figure 4). However, inconsistent with most models, the premise for which it was devised is to provide perspective on the process of online radicalisation, primarily in the context of radical Islam. The model itself is in fact a portable model that can be applied to many existing cases of online radicalisation, however, the particular case the model will be applied to in the following chapter highlights an overlooked, if not completely neglected, feature of the radicalisation process altogether. The feature(s), or emotions, which go unrecognised in nearly all phase models, is *sympathy* and *empathy* portrayed outward towards acts of terrorism. What differentiates AOSRM from alternative models is that it exposes the possibility of the individual becoming radicalised, yet not partaking in violent acts of any kind and instead branching off into what is referred as *radicalisation into extremism (RE)*. The model also incorporates the radicalisation process leading up to radicalisation into violent extremism (RVE), however, it is the radical, non-violent, aspect of the model, supported by its cyber application that distinguishes it from previous models.

One of the most common trends pertaining to the radicalisation process and also discovered at the foundation of the many radicalisation models that were covered in the literature review, is the common trend of grievance or 'exogenous conditions' initiating the process. Although this is a very broad starting point in the process, one could argue that the initial reasons for an individual to begin down the path of radicalisation is, in itself, contingent upon the disturbances interpreted and, or, received by that person(s) at any given time. It is for this reason why the author has also included it as the first phase in his personal model. In every case, trigger factors are personal and diverse; consisting of, but not limited to: injustices (political, economic, social, cultural, etc.), personal adversity, or even something as simple as loss of status, such as change in occupation (Bartlett and Miller, 2012). Vulnerability incites susceptibility. It is imperative to include all possibilities of entrance into the radicalisation process, no matter how ambiguous, rather than limit the assumptions to only a handful of circumstances. Notwithstanding, development and refinement of these circumstances increases as the individual embarks further into the radicalisation process.

Taking into account that the development of this model has been to satisfy online radicalisation, the second phase dwells on the what is arguably the most influential and galvanising echelon above all others; the scope of ‘echo-chamber indoctrination’. Simply put, an ‘echo-chamber’ is a metaphorical term used to describe communities that have been formed online. Additionally, these communities are occupied by like-minded individuals who interact with one another in order to validate a particular set of beliefs (Bowman-Grieve, 2013; Thomas Mcgarty, & Louis, 2014). Similarly, echo-chamber indoctrination is the phase when the individual begins to isolate themselves online in order to further one’s radical perspective. Due to the fact that online social interaction is considered to be more compelling and persuasive than physically receiving information, further supported by one-sided narratives that bolster imperviousness to contrary sources and opinions, the echo-chamber indoctrination phase strengthens the bond between the individual and the wider radical movement (Duarte, 2007; Hussain & Saltman, 2014; Neo, 2016). An example of this is Facebook’s ability to suggest posts that are congruent with a user’s standpoints, allowing the technology to align itself with preexisting beliefs favored by the individual (Bermawy & Mostafa, N.d). Nevertheless, to facilitate the transmittance of factual information, one could argue that diversity of opinion is necessary for impartiality and objectivity to occur; echo chambers, like those occurring in Facebook, inhibited this type of outlook. Analogous to other phases within the radicalisation process, the length of echo-chamber indoctrination is determined by the individual undergoing the overall process.

As Torok demonstrates, “embedding an individual within a group of radicalised individuals and beginning the intensification process is critical in gaining a full commitment or self- identification” (Torok, 2016, p. 64). Likewise, many of the sites utilised by terrorist organisations, including various forms Western social media, have become much more media savvy; targeting and appealing to marginalised and disaffected youths (Torok, 2016, p. 41). Thus, “given that the Internet is difficult to regulate and censor, the creators of radical online medium are therefore able to portray an image which will inculcate a more extreme perspective of the enemy by generating more arguments favoring their biased position and isolate the community members from any alternative moral interpretation" (Neo, 2016, p. 210). This sort of enclosed atmosphere is well suited for recruiting and radicalising individuals who insist on continuing forward.

Although it has been argued that indoctrination and conversion are synonymous, in order for one to justify a particular set of actions, whether it be consciously or subconsciously, the individual must first be indoctrinated in order for full commitment and self- identification to occur. However, conversion, the identification or association with what is to be believed as "the message of Islam", is also a phenomenon that is consciously or subconsciously driven by the individual, yet distinct to the outsider. Interestingly enough, studies show that it is in fact individuals who misunderstand Islam who are more susceptible to radicalisation alternatively to those with a more detailed understanding (Schmid, 2013). Conversely, however, another case study exhibited radicalisation of an individual who possessed extensive knowledge of Islam (Torok, 2016).

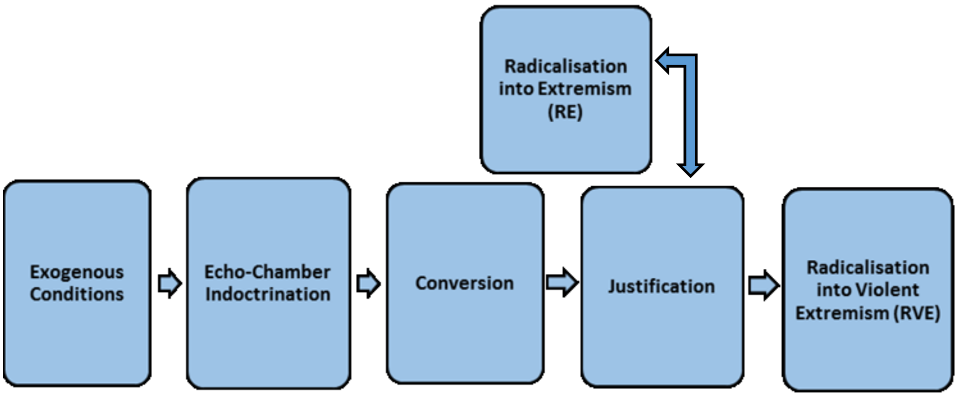
Conversion, the third phase in the author's model, is the radical tipping point leading up to justification. It is the final phase prior to being morally or physical engaged in acts of terrorism. This stage normally results in consolidating one's thoughts and, or, the possible subscription to radical Islam. Also referred to as a 'cognitive opening', the individual contemplates the need to change one's worldview in order to make sense of one's existence (Schmid, 2013). Conversion is an intermediate stage assembled in a very imprecise and lengthy process, whilst occupying an unaccountable amount of the individual's time. However, clear indications that someone may possibly be approaching this segment in the online-radicalisation process could be the public notion of religious convergence, similar to practicing and preaching the doctrine of Islam on a public forum; uncommon adjustments in social interactions, corresponding to possible radical topics of conversation; relative deprivation, parallel to personal isolation; and, or, alteration to one's social identity, which is identical to disconnecting from those who do not support one's ideology and, or, do not hold the same religious values (Precht, 2007; Veldhuis & Staun, 2009).

The last phase in the author's model, 'justification', is the final phase of the online radicalisation process which illustrates the now inherent decision the individual is faced with. Dissimilar from other models, the author's model essentially emphasises that the individual who manages to justify his or her radical ideology, is confronted with an ultimatum which allows the model itself to branch off into: active physical engagement – radicalisation into violent extremism (RVE) – or heartfelt sympathy and, or, empathy directed towards the vicious acts of terrorism committed and, or, the terrorist(s) themselves - radicalisation into extremism (RE). Despite the comparable traits among the two terms, the overall distinction between RVE and RE is the functions associated with their application. From the justification phase, RVE can take an upwards of several weeks or months to consummate, and ultimately results in all aspects of physical engagement in terrorist activities; whether it's an infantry role (direct engagement with the alleged enemy) or combat support (medical expertise, propaganda distributor, communications specialist, etc.). Furthermore, the candidate(s) who are attracted to the physically engaged role of extremism typically possess the following characteristics: a strong emotional pull to act in the face of injustice, a strong sense of thrill or excitement with action, an internal code of honor, and, or, they have been affected by peer pressure (Horgan, 2014, p. 79).

RE on the other hand, applies to the cases that don't involve acts of violence. Seemingly enough, an individual may accept his/her duty to jihad or terrorism in general, yet might not progress to the vengeful branch of RVE. Recent studies show that roughly 300 American and, or, U.S.-based IS sympathisers active on social media, distributing propaganda, and interacting with like-minded individuals (Vidino & Hughes, 2015). Moreover, some members of RE eventually transition from keyboard warriors to RVE candidates; however, lack of opportunity, contacts or resources, insufficient expertise, or even surveillance concerns from law enforcement, are just a few reasons why an individual would be unsuccessful in plotting acts of terrorism, or not even attempt to plot such acts in the first place; thus depriving them of reaching RVE (Torok, 2016; Vidino & Hughes, 2015). In other words, as Torok states, "a radicalised individual will not necessarily become a terrorist" (2016, p. 62). Inversely, the steps an individual must take to reach RVE are those that would essentially restrict individuals in RE to progress forward; whether the reasons be voluntary or compulsory. Furthermore, the model is unidirectional due to the dogmatic aspect of extremism. Once an individual justifies his/her initiate, the only methods to reverse their way of thinking would need to be found in a de-radicalisation program and, or, from cooperation within the community to which they newly identify and support. In the context of the U.S., both options seem equivocal and unstable.

What is normally affirmed in most radicalisation models is the notion that all individuals who fall under the umbrella term 'radical' or 'extremist' must, at some point during the radicalisation process, partake in acts of violence. Contrary to the following misconception, as stated earlier, the opposite is true: most people who hold radical ideas do not actually engage in terrorism. This excluded talking point is well-represented in the author's model, thus contributing to its overall originality and uniqueness as a model pertaining to the galvanisation of Internet radicals. The author's model does not seek to provide a definitive answer of predisposition; rather, it aspires to provide insight into a crucial yet inattentive element of the online-radicalisation process. One that is mission-critical when making decisions based on how to reduce, or at least efficiently identify, the individuals who are most likely to travel down this vindictive path.

Figure 4. Angelini's Online Self-radicalisation Model


Radicalisation into Extremism (RE)
Exogenous Conditions
Echo-Chamber Indoctrination
Conversion
Justification
Radicalisation into Violent Extremism (RVE)

Chapter 2

Obstacles in Countering Online Self- radicalisation: Case Study Analysis and Implementation of "AOSRM"

By analysing three cases involving online- radicalisation and terrorism, this chapter examines the hardship and tedious procedural process U.S. authorities occasionally go through in order to fulfill their responsibilities during and following an investigation. It also brings to light the unfortunate outcome when said officials are deprived of quintessential resources, inclusive of confrontation with obstinate behavior and refusal of entry into private technologies produced by private corporations. Moreover, the case study analysis seeks to essentially unmasked and emphasise the harsh reality of when civil liberties interfere with the future safety of the American people.

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. Correspondingly, the first two cases that were selected, in one's own opinion, 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.

2.1 San Bernardino Massacre (Failure)

The San Bernardino terrorist attack, which took place in San Bernardino, California, on December 2, 2015, is arguably one of the most unsuccessful counter-terrorism operations having ever taken place in the United States (U.S.). As one fully examines the substantial evidence that was gathered from this unfortunate case, the overwhelming preservation of civil liberties and Fourth Amendment rights, in addition and in relation to the United States' obligation to uphold and maintain the highest levels of national security, could instead be viewed as a systemic problem within the U.S., as preference to improve upon one issue inadvertently interrupts the progress of the other. Littered throughout this case are aspects of: preemptive negligence; advanced technological features owned by private corporations that decelerate proper evidence procurement; and failure of compliance by reason and in interest of customer privatisation as well as protection against implicit surveillance. The analysis of this study does not set out to demonstrate which party is right or wrong, rather it exploits certain flaws in the current U.S. system; flaws that could make the difference between successful prevention of future terrorist plots or enduring repetitive outcomes of belated investigations.

Rizwan Farook: male, 28 years of age and Chicago native; and Tashfeen Malik: female, 29 years of age and Pakistani native; were individuals who underwent a 'sham' marriage in order to carry out what is to be considered one of the most deadly mass shootings and acts of terrorism to ever take place in the U.S. (Chang, 2016). Armed with .223 AR-15 semi-automatic rifles, 9mm semi-automatic pistols, pipe bombs and a rented sports utility vehicle (SUV) they used as a getaway vehicle, together the couple managed to claim the lives of fourteen innocent people, whilst injuring an upwards of twenty-four (Rosenfeld, N.d, N.p). The targeted attack took place at a San Bernardino County Department of Public Health training event and Christmas party. Leading up to the shooting, Farook himself was a health inspector for the company. Up until recently the motives for the attack were still under investigation. Now, however, authorities claim that the perpetrators were inspired by Islamic terrorists and terrorist organisations, more specifically by means of 'online propaganda' (Mozingo, 2016). Although the events leading up to final outcome of the attack are inherently significant, our main focus of analysis will be fixated on the pathway to radicalisation and terrorism, the investigation, and the U.S. policy response.

In mid- December, 2015, James Comey, director of the FBI, had stated, "We can see from our investigation that in late 2013, before there is a physical meeting of these two people [Farook and Malik] resulting in their engagement and then journey to the United States, they are communicating online, showing signs in that communication of their joint commitment to jihadism and to martyrdom. Those communications are direct, private messages" (Baker, 2015; Lewis, 2015). Comey went on to speak about how the FBI's investigation had revealed that the perpetrators were "consuming poison on the Internet" and both had become radicalised "before they started courting or dating each other online" and "before the emergence of ISIL" (Lewis, 2015; Martinez, 2015). What the investigation also revealed and what has been a controversial topic of discussion since publicised, was Apple's rejection to meeting the demands of the FBI, essentially preventing the bureau from gaining access into Farook's IPhone.

As with most modern telecommunication devices, Apple's IPhone is protected by state of the art encryption. The encryption that the company uses is so advanced and privacy oriented, Apple itself cannot access an individual's phone without the individual personally divulging his/her four-digit pin number. In terms of privacy, Apple upholds the security of all customers to the highest regard. For law enforcement officials, however, this type of security is a serious inhibitor for successful procurement of all, relative, information pertaining to this case and future speculated cases. That being said, the content on Farook's phone was considered highly valuable and mission-critical to the then ongoing investigation conducted by the FBI. In spite of the four-digit PIN set up on Farook's phone, there had been 10,000 possible combinations one would need to input in order to gain access to the phone (Williams, 2016). "Yet once a device is locked, the only way to unlock it is by entering a passcode; thus, the data will be erased once ten incorrect attempts have been made" (Williams, 2016). The FBI's inquiry about the matter was simple: alter the phone's security protocol, allowing for an unlimited amount of passcode attempts and, or, allow the bureau the option to "brute force" attack the phone in furtherance of speeding up the PIN deciphering process (Williams, 2016).

The government went as far as to invoke the 'All Writs Act of 1789'. Consequently, Apple contested and rejected the court order that was issued to them, as they are more concerned with the long term effects of creating a back door in the phone's operating system, thereby entertaining the possibility of unpermitted investigative intrusions for future cases that are similar in nature. Drafted as 'A Message to Our Customers', a letter produced by Tim Cook, CEO of Apple, says, "The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand" (2016). Respectfully, Wayne Williams, author of the article 'Why apple is right to reject the order to unlock a killer's phone', agrees, "Apple is right to reject this court order, because what is at stake is too valuable to lose. The government is essentially asking Apple to eliminate a crucial feature of iPhone security, and create a master key that can unlock any Apple device… The government wants us to trust that it will only use this power for good -- to protect its citizens from the bad guys -- but there's no way this backdoor won't be misused and abused" (2016). This is a logical argument that does raise concerns that were previously discovered to have happened in the past. In reference to Chapter 1, the ambiguity surrounding the NSA's informal ability to use 'back door' approaches in support of breaking through and autonomously monitoring domestic encrypted traffic, had many Americans, especially the American Civil Liberties Union (ACLU), openly distraught (Schneier, 2007; Soghoian, 2010).

As Time Cook further states, "the government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers -- including tens of millions of American citizens -- from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe" (2016). Interestingly enough, Apples' refusal to remove security features and add new capabilities to the operating system, in the sense of protecting their customers data, only incited the FBI to take matters into their own hands by hiring professional hackers – grey hats - to do it for them. All data and privacy breaches Apple aimed to prevent, was, in fact, self-induced by their noncompliance. Moreover, rather than provide technical oversight and hands on expertise on issues related to the security bypass, they were instead excluded and no longer consulted during the investigation on account of insubordination. This is problematic for one major reason: The professional hackers who discovered the previously unknown software flaw, along with the FBI, have now found a back door into Apples' operating systems that Apple itself was unaware of. As it stands, both parties can choose whether or not to disclose the vulnerabilities to Apple. However, since the U.S. is vastly interconnected and dependent of digital infrastructure, when these types of vulnerabilities are in fact discovered and could potentially compromise mobile devices owned by many law abiding citizens, it is safe to assume a very strong bias towards disclosure (Nakashima, 2016; Williams, 2016). Consequently, however, by disclosing such information, the FBI and elected officials risk the chance of Apple patching the flaw, subsequently deteriorating any progress made.

When having to balance civil liberties and national security, one could make the justification on both national security and on law enforcement grounds and argue that the software flaw could possibly amplify surveillance capabilities, allowing law enforcement to discretely sift through tele-communicative extremist behavior, in turn, protecting more people in the near and distant future (Nakashima, 2016). The urgency for national security and privacy are two constitutional precepts. However, in contrast to the U.S' dependency on digital infrastructure, if some form of partisanship is to exist, it will most likely be focused towards national security. To illustrate this view United States Congressman, Trey Gowdy, concedes, "you *do* have the freedom to speech, you *do* have the right to have the government seek a warrant in most instances, and you *do* have the freedom of a jury trial and afforded council; and not a single one of those rights is much use to you if you're dead" (2017).

As further stated in Cook's letter, "the implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge" (2016). Despite the fact that the NSA was guilty of similar intrusive acts, crafting the comparable narrative that the FBI will follow suit is highly improbable for a number of reasons. Firstly, given the nature of work that is actually required by qualified, properly vetted, individuals and agents, the amount of resources needed to do what is implied by Apple is unrealistic. The FBI is already perplexed with attempting to focus on one key element of investigation(s): the conservancy of all possible resources dedicated to the cause of threat prevention. Secondly, it would be wise to assume the FBI, when faced with the same responsibility, need not be compared, nor share the same fate, as the NSA. Rather, they would most likely improve upon past failures and mistakes, whilst simultaneously upholding the utmost integrity associated with the privacy of individuals.

Accordingly, one of the arguments referenced on numerous occasions is the complex legal issues and obscurity surrounding the federally invoked 'All Writs Act'. Eric Limer states, "The legal issues around the All Writs Act are complex, but at its core, it gives federal judges the power to issue orders to compel people to do things within the limits of the law" (2016, N.p). What is considered to be of larger concern for most, however, is the age and broadness of the statute itself. The statute being applied to the Apple case reads, "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law" (All Writs Act 1789). Furthermore, the act was originally apart of the Judiciary Act of 1789, and, aside from being signed into law by President George Washington himself, it has been argued to be outdated if and when applied to cases regarding modern technology (Limer, 2016, N.p). Contrarily, the broadness of the law seems to preserve its relevance and overall application, thereby allowing it to keep up with technological advancements, such as universal encryption. Nevertheless, The All Writs Act does have its limits. To illustrate this, back in 2005, a federal judge ruled that The All Writs Act was prohibited from forcing a phone company to allow real-time tracking without a warrant (Benner & Lichtblau, 2016).

In reference to The Economist article, "The myth of cyber- security", terrorist attacks such as this, often yield debate directed towards weakening encryption methods so that security services, like the FBI, can better monitor what individuals are doing (2017, p.9). It is an impossible task, however, to weaken encryption on devices used solely by terrorists (The Economist, 2017). Moreover, computer and mobile security is best served by encryption that is strong for everyone, not just the presumable benign (The Economist, 2017). Alternatively, the government revealing the founded vulnerabilities within Apple's operating system, is a double-edged-sword. Naturally, Apple is going to repair any and all bugs, thereby forcing law enforcement officials to have no choice but to start from a foundational level of cracking mobile encryption in future cases (Nakashima, 2016).

Apple's uncooperativeness towards assisting the government with evidence procurement in this particular case, underlines one of the main issues the law enforcement agencies are faced with when conducting investigations. An increase in communication and cooperation between public and private partnerships (PPP's) is critical in efforts to successfully combat online-radicalisation and terrorism. Private corporations, like Apple, must be more consciously aware of the vindictive sentiment and violent dialogue being exchanged and communicated via use of their product(s) and, or, platforms. Perhaps establishing privately funded corporate counter-terrorism unit(s), outfitted to combat, reduce, or flag extreme dialogue held between individuals and serve as a buffer to law enforcement, would be the most feasible and efficient approach in reducing the domestic mobilisation between radicals. Such an establishment would serve to avoid expending unnecessary funds granted by U.S tax payers that cannot seem to neutralise the demand at an equal rate as these instances occur.

2.2 Boston Beheading Plot (Successfully Thwarted)

In June, 2015, Boston- area resident, Usaama Rahim, 26, plotted to behead Pamela Geller, an American political activist and commentator, known for her anti-Islamic writings. Preceding his plotted attack, Rahim divulged to his nephew, David Wright, also known as Dawud Sharif Abdul Khaliq, that he instead planned on beheading Massachusetts police officers, as his initial target proved too difficult of a task. However, leading up to the attempted arrest and fatal neutralisation of Rahim, the FBI conceded that Rahim was in fact under twenty-four hour surveillance since late May, 2015, after he bought three knives on 'Amazon.com' (Bidgood & Philipps, 2015). A third man, Nicholas Rovinski, was later discovered, arrested and convicted alongside Wright, for conspiracy to support IS (Bidgood, 2015; Brumfield, 2015; Ryan, 2015).

Similar to the San Bernadion case, the prevented attack originated from the perpetrators consumption of extremist material via online social media platforms. As the chairman of the House Homeland Security Committee, Representative Michael McCaul, points out, Rahim had been under investigation in consequence of "communicating with and spreading ISIS propaganda online" (Bidgood & Philipps, 2015). Furthermore, in accordance to CNN, "an analysis of his Twitter feed indicates he actively reached out to individuals connected with ISIS, including Mujahid Miski, the online alias of Mohamed Abdullahi Hasan, a Minnesotan believed to be fighting with Al-Shabaab in Somalia" (Brumfield & Sanchez, 2015). Dissimilar from the San Bernardino Case, however, aside from this case over accentuating the influence foreign extremists impose on homegrown radicals, the inquisitiveness of the FBI, further supported by their ability to successfully neutralise a confronted hostile - which resulted in no collateral damage or casualties – can and is attributed to a collective approach towards auspiciously combating online-radicalisation.

In contrast to the FBI's success in this particular case, many arguments can be developed when comparing the intricacy of variables confronted in the

San Bernardino case verses the Boston Beheading Plot. For example, in the San Bernardino case, the perpetrators were well-organised and possessed a translucent, strategically conducted, plan on how they were to execute their attack as well as how they were to subsequently flee the scene of the crime. Moreover, the perpetrators in San Bernardino, in addition to garnering semi-automatic weapons, pipe bombs and a getaway vehicle, were more precautious on how they communicated to one another leading up to the attack. Although online communications held between the married couple were monitored attentively, the prolonged de-encryption of encrypted devices produced by a leading global telecommunications provider –Apple, along with the formulated concerns pertaining to the government's infringement on civil liberties, played a significant role in obstructing the swift investigations of the FBI. On the contrary, in regards to the Boston Beheading Plot, the assailant, Rahim, had a highly anticipated and one dimensional variation of assertiveness. From his initial flagged purchase of three knives off of 'Amazon', to his frequent monitored calls to his nephew, revealing his volatile arrangements focused towards "those boys in blue" (referencing police officers), Rahim was scrutinised from the very beginning of his hopeful endeavor. Therefore, one could argue that the investigative efficiency of the FBI recognised throughout the Boston Beheading Plot, in opposition to San Bernardino, originated from the exiguous amount of variables and depth encountered throughout the cases existence (Allen & Valencia, 2015).

The insufficient resources, impulsive attitude and disorganisation of Rahim precipitated a great degree of carelessness, to which culminated the precision and sufficiency of the bureau. Intentions initially discovered via online-surveillance, followed by successful roving wiretaps, accelerated the prevention of what could have been a gruesome terrorist plot. As an appropriate result, the 'Boston Beheading Plot' is, in one's own opinion, the textbook example of how counter-terrorism/online-radicalisation operations should be conducted, in addition to providing conclusive transparency focused around the results induced by the proper amount of cooperation and resources distributed to all necessary areas of the *then* ongoing investigation. It comes with no surprise that the successfulness of this investigation and absent attrition of the targeted individual(s) – in this case, the police officers - can be attributed to procedural excellence, swift methodologies applied by law enforcement officials and the avoidance of impeding factors through public and private partnerships.

2.3 Mississippi Islamic State Recruit, Jaelyn Young (Applied Radicalisation Model)

In this particular case study, former Mississippi chemistry major, Jaelyn Young, had more than most could dream of. Back in high school, Jaelyn had been a cheerleader, a distinguished honors student, and homecoming maiden. However, despite all of her accolades, the ubiquitous patriotism existing in her family – her father being a police officer and U.S. Navy veteran - and to what some may consider a privileged upbringing, all of it was unsatisfactory in the alluring efforts of the Islamic States (IS) agenda. On March 28th, 2016, the former Vicksburg, Michigan, resident pleaded guilty in federal court to one count of conspiring to provide material support to IS, and was to be sentenced at a later date (Fox News, 2016). Her fiancé and fellow extremist sympathiser, Muhammad Dakhlalla, was also sentenced for personal charges filed against him. "After Jaelyn converted to Islam in March, 2015, is when she began wearing a burqa and distancing herself from non-Muslim friends. Prosecutors said she "began to express hatred for the U.S. government" and expressed "support for the implementation of Sharia Law in the United States"" (The Associated Press, 2016).

What is apparent and stated in the previous paragraph is this sort of self-manifested hatred and spitefulness Young forcefully directs towards the west, particularly the United States. What is uncertain, however, is what methods were used in recruiting or coercively enlisting Young into the ranks of IS.

Nevertheless, it would be safe to assume – seeing as Young had no prior affiliation with any foreign or domestic jihadists – that she was in fact influenced by IS propaganda through open source information retrieved via online platforms. Interestingly enough, the pathway in which Young took to become radicalised fully developed in under a twelve month period. Although Young and her fiancé were arrested on the 8th of August, before boarding a flight from Columbus, Mississippi, with tickets for Istanbul and the incentive of traveling to Syria; she did not present any future signs of amenability towards committing violent acts of terrorism. However, Young was in fact sympathetic towards jihadists with extremely violent aims towards the U.S. Per Young's social media account, "What makes me feel better after watching the news is that an akhi (the Arabic word for "my brother") carried out an attack against US marines in TN! Alhamdulillah, the numbers of supports are growing…" (Fox News, 2016). Furthermore, "prosecutors said Young approvingly cited a video of a man accused of being gay being thrown off a roof to his death by militants. She also expressed joy at the shooting of five members of the military in Chattanooga, Tenn., by an Islamic militant in July" (The Associated Press, 2016).

In addition to this type of mentality, along with Young's incentive of traveling to Syria with hopes of becoming a medic for IS, it is irrefutable that 'Angelini's Online Self-radicalisation Model', also referred to as AOSRM, is the most practical phase model for this case (see Figure 1). Despite her initiative drafted purely by international events as well as political narratives, Young's behavior towards individuals was influenced by the actual, imagined, and implied presence of others – in the context of her relationship with her fiancé, as well as connoted extremist propaganda found online (Fox News, 2016). Young was arguably less focused on the collective movement of IS, and more so involved in the individual process of transforming beliefs and ideologies. Furthermore, Young's case *does not* engage in any form of Islam. It *does*, however, introduce the fundamental stages of Islamism. Consequently, although Young held radical ideas and with that should be held accountable for her actions, one should have never anticipated her being awarded a combat position within the ranks of IS; but instead, a supportive role (medic) – as stated earlier. Though one can only speculate, Young reinforces the notion that all terrorists may not be as deeply ideological as they are perceived to be. Therefore, in accordance with AOSRM, I believe this classifies Young as *radicalised into extremism* (RE).

By examining this case in a more detailed manner whilst simultaneously applying the AOSRM phase model, a synergistic clarity is recognised. In order to understand how Young reached the point of RE, and why she is in fact classified as RE and *not* RVE, one must first observe the *exogenous conditions* Young was faced with at the very beginning of her delinquent path towards radicalisation. As it turns out, Young was primarily influenced by the consumption of open source material found via online sites. It was acknowledged that Young increasingly complained about the mistreatment of Muslims in the United States and United Kingdom (The Associated Press, 2016). To support this, The Associated Press states, "Prosecutors said that, after watching pro-Islamic State group videos, she began to view the fighters as liberators" (2016). Appropriately and conveniently understood in this precise moment, Young is considered to be fluidly matriculating from the exogenous conditions to which she has been exposed - in this case what is to be her interpretation of various injustices associated with the mistreatment of Muslims, domestically and abroad – thereby fueling her with the incentive to stay well-read on the subject and progress further into the radicalisation process.

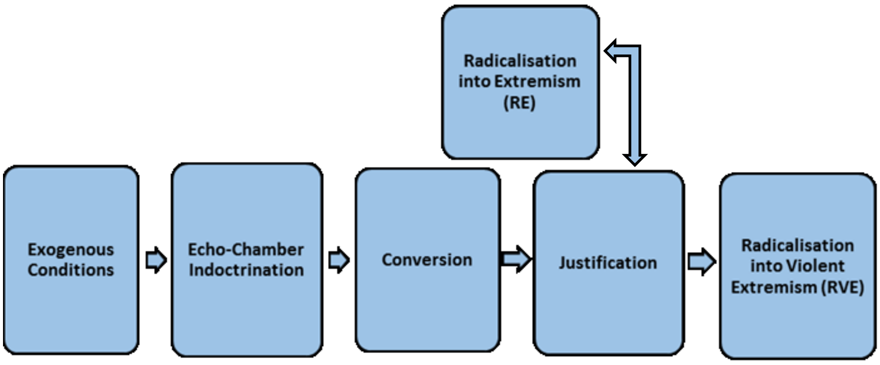
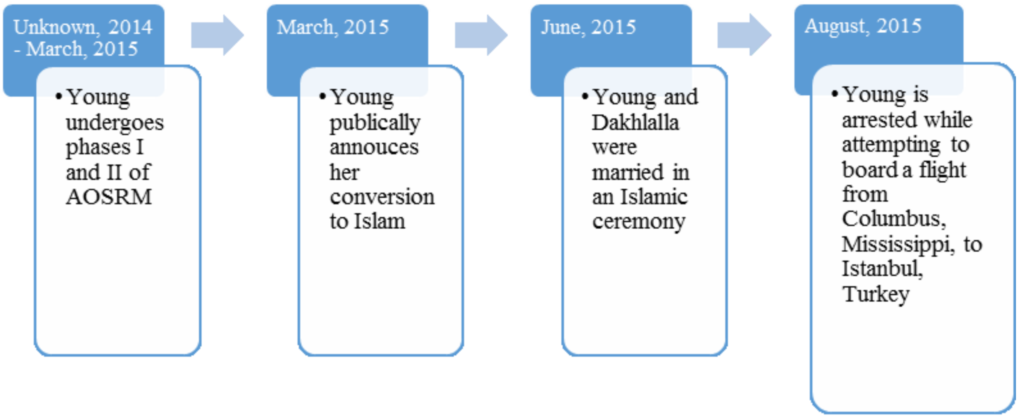

Radicalisation into Extremism (RE)
Exogenous Conditions
Echo-Chamber Indoctrination
Conversion
Justification
Radicalisation into Violent Extremism (RVE)

Figure 1. Angelini's Online Self-radicalisation Model

Continuing onward from the initial triggering factor(s), Young reinforces her growing concerns with online IS propaganda, much like the pro-Islamic State group videos that were previously mentioned, thus becoming self-absorbed. It would be wise to assert that at this point in time, either consciously or subconsciously, Young has entered *echo-chamber indoctrination*, the second phase of AOSRM. In this phase of the process, there is limited information available on how Young's situation progressed leading up to her religious conversion. What is known, however, is that the entire radicalisation process took Young less than twelve months to complete (see Figure 2). To illustrate this, "an FBI affidavit filed in the Young/Dakhlalla case does not discuss how the two came to form their positive views about the extremist group. But it does suggest that they failed to make contact with an actual recruiter, or at least that any Islamic State recruiter they did make contact with did not believe they were genuine in their desire to join group" (Richey, 2015). With echo-chamber indoctrination being the most influential stage in the radicalisation process, it is presumably where Young spent the majority of her development.

Echo-chamber indoctrination is when the so called ‘enlisted’ and, or, ‘recruited’ individual(s) begins to isolate themselves via online with like-minded individuals in order to validate a particular set of beliefs from others that do not share their evolving perspective. In correspondence with this tenant, Young followed suit when she met Mohammad Oda Dakhlalla and the two first started dating November, 2014. Moreover, it is *doubtful* that Dakhlalla did not further compel Young to convert to Islam, or at the very least support her decision, as it has been revealed by means of testimony that he himself is a Muslim and had been accused of being Young’s “hijjrah” partner - a common reference to journeying to the Islamic State (U.S.A v. YOUNG & DAKHLALLA, 2015). To support this claim, The Associated Press reports, “by the time Young began dating Dakhlalla in November 2014, she was already interested in converting to Islam. She announced her conversion in March and began wearing a burqa, a garment worn by some Muslim women to cover their face and body” (2016). In reference to AOSRM, in addition to what is gathered from the evidence at hand, one notices that Young’s progression from echo-chamber indoctrination to *conversion* takes roughly three months to undergo. This step not only demonstrates her overall commitment to what she believes is the true and undisputed message of Islam, given the online material she has been exposed to, it further solidifies her self-manifested path towards becoming an extremist.



Unknown, 2014 - March, 2015
Young undergoes phases I and II of AOSRM
March, 2015
Young publically annouces her conversion to Islam
June, 2015
Young and Dakhlalla were married in an Islamic ceremony
August, 2015
Young is arrested while attempting to board a flight from Columbus, Mississippi, to Istanbul, Turkey

Figure 2. Young's radicalisation timeline

Young's misinterpretation of Islam and its doctrine is overwhelmingly attributed to her prompted susceptibility towards the pertinent fundamentalist mentality. Proportionately, this form of Islamism has situated her in the third phase of AOSRM, thereby yielding the radical tipping point leading up to justification. “"After her conversion, Young distanced herself from family and friends and felt spending time with non-Muslims would be a bad influence," prosecutors wrote in a statement of facts regarding Dakhlalla's plea” (The Associated Press, 2016). Jaelyn Young's subscription to radical Islam exacerbated her rational, extending it passed dialogue into a cooperatively devised plot to abet IS. Therefore, Young's perpetual yearn to join IS, expressed support for Sharia Law to be implemented in the U.S and belief that IS had established a genuine caliphate, allows her to justify the path she feels destined to be on.

Justification, as observed in AOSRM, branches off into the following divisions: radicalisation into extremism (RE) and radicalisation into violent extremism (RVE). With that said, in regards to the transpired events facilitated by Young leading up to her and Dakhlalla's airport arrival, in attempts to board a flight to Istanbul, Turkey, classifying this case as ‘RE’ is the most appropriate assessment. Comparable to the AOSRM phase model, Young willingly and undisputedly accepted her duty to jihad and terrorism, however, did not progress to the branch of RVE. This can be supported by Young admitting to organising the entire operation: “I found the contacts, made arrangements, planned the departure,” prosecutors said she wrote to her family in a “farewell letter” last August. “I am guilty of what you soon will find out” (Fox News, 2016). The argument that is to be made is not one that favors the Young’s intentions, but instead focuses on the final outcome of her radicalised journey as a whole. The moral acceptance of atrocities, identical to Young’s expressed joy towards the shooting of five members of the military in Chattanooga, Tennessee, by an Islamic militant, and her cited video of a man accused of being gay being thrown off a roof to his death by militants, certainly classifies her as RE (Fox News, 2016). However, her failed attempt to follow-through with her departure to Turkey, due to the successful online-surveillance and physical apprehension conducted by the FBI, eliminates all possibilities of categorising her as RVE. To be clear, albeit the lack of opportunity for Young to board her flight is accredited to surveillance tactics enforced by the FBI, had she boarded the flight to Turkey, followed by a second flight to Syria, she would have unquestionably been categorised as RVE; for her and Dakhalla would have been physically engaged militants situated in a combat support role.

Jaelyn Young was initially attracted to physically engaged extremism by virtue of her strong emotional pull to act in the face of injustice and her internal honor, conflated with her misinterpretation of Islam. Though unlikely, during and, or, subsequently after her incarceration, Young could theoretically maintain her RE mindset. Though, attempting to transition from RE to RVE post-incarceration is highly improbable (Torok, 2016; Vidino & Hughes, 2015).

Chapter 3

Environmental Qualities of Online *vs* Offline Radicalisation & Recruitment, and its Relation to U.S. Policy

In this chapter, what is to be discussed is the differentiating factors between online and offline radicalisation and recruitment conducted by terrorist organisations, with a focus surrounding the United States of America (U.S.). Contrary to what some may perceive, in terms of terrorism, the process of online radicalisation and recruitment drastically differs from methods of its offline subordinate. According to the Community Oriented Policing Service (COPS) of the U.S. Justice Department, "Online radicalization to violence is the process by which an individual is introduced to an ideological message and belief system that encourages movement from mainstream beliefs toward extreme views, primarily through the use of online media, including social networks such as Facebook, Twitter, and YouTube" (2014). This chapter in particular will expound upon the latter, in addition to incorporating and critically analysing existing U.S. legislation and policies meant to countervail this homegrown terrorism phenomenon. More importantly, this installment will concurrently attempt to deduce policies and improve upon their strategic transparency. Finally, chapter three will conclude with a final discussion and summary of the topics that have been covered throughout the section.

Since its emergence in the 1990's, the World Wide Web has provided many opportunities to advance globalisation as well as the interconnectedness between people. Such revolutionary developments that are normally praised for their innovative attributes, are now viewed – at least in the security sector - as potential radicalisation and recruitment incubators which may produce unforeseeable circumstances of extremism and violence. Similarly, in terms of radicalising and recruiting individuals to assist in and, or, commit heinous acts of violence, the internet – more specifically the social media platforms that reside in it – is cause for concern in the efforts to combat this now widespread phenomenon.

What was once a regional phenomenon, most prevalent in territories housing existing terrorist networks, has now transcended into random acts of homegrown violence spilling over into the United States (U.S.). Although this discussion is focused around self-radicalisation (a phenomenon in which an individual(s) may progress towards committing a terrorist act or not necessarily disagree with the intentions of such an act, with or without affiliating oneself with a radical group, although may be influenced by its ideology and message) and homegrown terrorism (acts of violence against civilian and/or military targets primarily in Western countries in which those committing violence have been born and raised) within the United States, it is important to note that such events could possibly take place in any other existing country, and, in some cases, has already – in reference to the murder of Lee Rigby, which took place in Woolwich, southeast London, back in 2013.

3.1 Differences between Conventional and Online Radicalisation

When discussing the causes of radicalisation, the intentional and systematic art of *recruitment* often times coexists within the majority of discourse taking place; thus, preventing a deeper perception of the terms otherwise found when discussed independently and separate from one another. Although it is clear that the topic of recruitment shares a unique place in the radicalisation into violent extremism (RVE) discussion, it would be prudent to note that not all individuals who are in fact radicalised fall under the process of being recruited. Illustrating this and in reference to 'Understanding Terror Networks', Marc Sageman goes as far as to say, "There is no recruitment per se to armed jihad or Al- Quida" (2011). Sageman continues to argue that contrarily to recruitment, *enlistment* is the mechanism for the emergence of new recruits; subsequently depicting friendship to be the catalyst for about 70 percent of armed Jihad, kinship for about 20 percent, while discipleship comprises the remaining 10 percent (2011). Although one may argue that enlistment is most prevalent in regions that possess various terrorist networks, such as: Iraq, Syria, and Afghanistan, a similar argument could be made surrounding implemented methods of transnational radicalisation and recruitment regarding the nature of its exclusiveness conducted via online platforms (videos, images, and articles, containing violent material and, or, radical ideology).

Unlike the primitive, more conventional methods of radicalisation and recruitment, or enlistment, – previously touched on by Sageman – the Internet provides various avenues for terrorists to display and advance their agendas in order to communicate their ideologies on a massive, unfiltered scale. According to the Homeland Security Project's proposal, *Countering Online Radicalization in America*, "terrorists have embraced the technology's communicative aspects, helping them to spread their message and create (virtual) constituencies, and that such (virtual) communities are the places in which extremist behaviors are learned and normalized, enabling mobilization into violence to become possible" (2012, p. 15). In many respects, as Neo suggests, these online communities form what is referred to as an 'echo chamber' which reinforces the commonly shared ideology of like-minded individuals (2016, p. 210). Similarly, Janbek and Steinfatt write, "terrorist organisations that maintain an online presence use the Internet today to communicate or to inform, to radicalise and to recruit, to educate and to plan, and to fundraise" (2016, p. 30). To emphasise this, Bates and Mooney observe terrorist organisations' online efforts to online education: "Al – Qaeda and other jihadist organisations are offering their own form of distance learning" (2014, para. 22)… "These online training facilities are mostly offered for free and are accessible through semi-centralised, password-protected forums" (2014, para. 24). Moreover, the Internet provides terrorists with a centralised form of useful information, including instructions for bomb assembly, poisoning, weapons construction, and mixing lethal chemicals (Martin, 2006, p. 542). Furthermore, research shows that today, an estimated 42 percent of the world is connected to the Internet (Internet World Stats, 2014). In addition to the 42 percent of Internet users that exist globally, research shows that 84 percent of American adults possess Internet competency (Pew Research Center, 2015). Therefore, with globalisation on a steady incline, in conjunction with Internet usage and the dilating progression of technically competent individuals, the likelihood of such repugnant online content receiving recognition by curious individuals and potential radicals is much greater now than it was in recent years.

Alternatively to the boundless communicative features of the Internet, Janbek and Williams instead argue that, although one cannot isolate the Internet as the main or only factor that causes individuals to commit an act of terrorism, through documented cases, one can confirm that the Internet has been used in various ways to facilitate different aspects of terrorism (2014, p. 302). Accordingly, Benson insists that, "merely establishing that the Internet played a role does not preclude the possibility the terrorists were first motivated offline to attack and only later used the Internet as one tool among many to attempt to carry out that attack" (2014, p. 311). In contrast to Benson, Duarte concedes that online social interaction is considered to be potentially more compelling and persuasive than passively receiving information, due to communication through an isolated environment of like-minded individuals (2007, p. 173). What can be concluded is that it is imperative to understand that the radicalisation process and radicalism in general is not, and therefore has never been, generated by online platforms. Rather, the access to the Internet and various online platforms has unquestionably enhanced the transmission of radical ideologies and extremist behaviors transnationally; thus inciting negative sentiment toward enemies, or self-proclaimed enemies, in addition to undertaking potential recruit mobilisation by means of online propaganda.

3.2 The Complex Challenges of the Digital Era

When discussing the universal complexities encountered online, the most arguably controversial components associated with the cyber domain, synonymous to terrorist propaganda and extremist ideologies, are the various forms of communicative provisions (social media, chat rooms, video uplinks etc.) as well as the ambiguous civil liberties of the individual(s) operating within them. To what some may conceive as *cyber governance*, or generally what I like to refer to as *transferable law* – when existing national laws are equated the same within each operational domain (cyber, land, air, space and sea) – is entirely fictional. For example, in order for cyber governance to exist, there needs to be some sort of governing entity to enforce its regulations. However, as there is presently no single entity to enforce cyber governance, nor is there a current multinational approach among states to enforce a sense of online orderliness, the outcome results in none other than cyber lawlessness. Furthermore, as each state possesses differing laws and statutes to accommodate its citisens, the inconsistent geographical borders of cyberspace creates implications as well as uncertainty throughout the discussion of applicable legislation, in turn, making it difficult to impose any form of law.

As Peter Neumann from the National Security Project observes, the rise of the Internet in addition to the massive expansion of data storage over the past two decades has significantly overwhelmed and reduced the ability of policy makers to formulate rules for what law enforcement and intelligence agencies can and cannot do in terms of surveillance (2012, p. 39). This statement suggests that the reason in which government agencies are often unsure to what extent they can interact with open source information on the Internet, is because of undefined and unspecified guidelines. Moreover, as mentioned previously, cyberspace is as borderless as it is utterly lawless. As Neumann emphasises, "from surveillance to engagement, U.S. government rules for counter-terrorism and counter-radicalization distinguish between domestic and foreign. The transnational nature of the Internet, however, makes such distinctions difficult: A website may be registered in one country, its content hosted in a second, the producer based in a third, and the user in a fourth" (2012, p. 40). In addition to violent extremist online platforms being geographically disarranged, altering the Uniform Resource Locator (URL) associated with said platforms – as most of these platforms are notorious for doing - promotes further challenges towards the successful removal of turbulent content. Despite how intricate the Internet is, it comes with no surprise that terrorist groups such as Al-Qaeda and IS seem to capitalise on its current uncivilised state.

In accordance with the difficulties surrounding violent extremist messages circling the Internet, Neo and Dillon state, "successful disruptions of prominent violent extremist online platforms can be quite useful in signaling the types of content that the country regards as offensive or harmful… Restricting the access to some of these attractive violent extremist online platforms presents the opportunity to prevent Internet users from chancing upon these online platforms." (2016, p.11). Contrarily however, Peter Neumann disagrees; arguing that censorship over the Internet is rarely effective, except in the most repressive countries, which restrict and supervise Internet access and devote massive resources to policing its general use (2012, p. 24). In the United States, constitutional, political, and practical constraints make censorship impossible, given that constitutional free speech protections in the United States are as extensive as they are explicit (Neumann, 2012).

Although censorship is currently not an option of interest, others seem to focus on much more practical methods pertaining to content oversight online, such as surveillance. Schneier acknowledges that, in recent years, the U.S. National Security Agency (NSA) has incorporated "back door" programming in order to deconstruct encryption services (2007, N.p). With uncertainty attributed to the encrypted traffic the NSA is or is not able to access, the notion that governments are able to analyse encrypted information suggests inducement of apprehensiveness towards some individuals using services such as virtual private networks (VPN) when using the Internet (Torres-Soriano, 2012). Thus, as Kebball & Romyn state, "while the Internet can give the perception of anonymity to those who use it, it is still possible for law enforcement to race where information has come from and where it has gone" (2016, p. 92). Needless to say, however, the vast majority of the content that qualifies as 'extreme' or 'radically driven' would be protected under the First Amendment (freedom of speech) of the United States Constitution (Neumann, 2012). Unless of course a statement contains a direct and credible threat against an identifiable individual, organization or institution, in addition to fulfilling legal test for harassment; or constitutes incitement to imminent lawless action (Anti-Defamation League, 2000, p. 3). As a result, one can gather that exploiting the Internet by virtue of intelligence collection and/or evidence retrieval is the most effective way of dealing with online radicalization in the short term. Therefore, the government should pursue this approach more systematically.

3.3 Obstructive Characteristics of the Internet & Cyberspace

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). "Using a combination of traditional websites; mainstream social media platforms like Facebook, Twitter, and YouTube; and other online services, extremists broadcast their views, provoke negative sentiment toward enemies, incite people to violence, glorify martyrs, create virtual communities with like-minded individuals, provide religious or legal justifications for proposed actions, and communicate with and groom new recruits" (COPS, 2014). When incorporating these mechanisms into the discussion encompassing the variance of online versus offline radicalisation, the results are apparent. 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. Interestingly enough, individuals progressing through this online path towards radicalisation are most likely to be identified when they begin to speak out in favor of a terrorist group, religiously convert, and, or, publically support the brutality behind violent extremist acts. As it stands, law enforcement and domestic intelligence services *do* possess capabilities needed to trace where information has come from as well as where it has gone. Despite this, however, the internet can grant the perception of anonymity to those that operate inside its domain via the services in which it provides; such as, virtual private networks (VPN) and onion routers (TOR).

In theory, securitising online anonymity tools would essentially provide law enforcement and intelligence services with enhanced capabilities, thus reducing the overall discreetness found between extremists and their uploaded content in addition to the individuals they seek to influence and inspire. The anticipated outcome of establishing this level of security welcomes a number of positive results. Firstly, identifying and conducting online reconnaissance on suspected targets and, or, material would create a certain level of paranoia and apprehensiveness within the community of extremists and distributors of online propaganda. Lastly, accessing specific extremist-related information online would allow law enforcement to systematically identify those planning an attack, those attempting to galvanise others to commit acts of violence, and, or individuals who are excessively curious towards radical content (Torres-Soriano, 2012). Considering the material maintained on these sites is designed to radically motivate others as well as facilitate a terrorist attack, "the monitoring of IP addresses of people who access these sites could assist in identifying those who are planning an attack" (Kebbell & Romyn, 2016, p. 97).

Therefore, by securing online anonymity, the evasiveness of uploading volatile material without being discovered lessens while the chances of disrupting terrorist plots and radicalisation pathways improve.

Not excluding terrorism, usage of VPN in particular has been involved in many cases related to piracy, and, according to Kebball, "is a reasonably robust method to ensure online anonymity" (Kebball & Romyn, 2016, p. 92). Moreover, all traffic sent between a user and a VPN is encrypted, allowing the content of this traffic to remain hidden from the Internet service provider (ISP) or any other agency that may be collecting metadata (Larsson, 2012, p. 264). Furthermore, in terms of singling out and identifying which individuals have accessed particular information online, all compiled information as a result of investigation will refer to the VPN itself, rather than the person who was using that VPN (Kebball & Romyn, 2016, p. 92).

Much like a VPN, an onion router, or 'TOR', is another commonly used method of maintaining online anonymity. TOR is a method of online browsing that systematically randomizes a user's internet traffic through multiple points, or 'nodes', before it reaches its online destination (Antoniades, 2010, p. 134). Although it has been suggested that moving large quantities of data through TOR is less sufficient than if one were to use a VPN, however, one of the numerous advantages of TOR is that it's free, it is easy to install, and requires minimal information technology (IT) competency. Similarly, unlike a VPN, TOR bypasses the use of a single service provider, allowing the user to remain elusive in the attempt to facilitate avoidance of scrutiny directed towards Internet traffic; which, in turn, would prevent the retrieval and dissemination of information from reaching the hands of domestic authorities (Kebbell & Romyn, 2016, p. 93). Thus, the assertion pertaining to the ability to monitor and trace malicious internet traffic throughout the vastness of cyberspace could result in the user (in this case, the terrorist or potential radicalised individual) avoiding detection and sequestering their identity, as well as their intentions, from law enforcement officials.

Alternatively, as the Internet in many ways does provide some form of cyber camouflage to the individual looking to abusively take advantage of its function, it also promotes opportunities for authorities to systematically stalk and identify potential criminals, terrorists, potential online radicals, and, or, recruits. As for VPN, although the ISP may be *unable* to identify the individual utilising their service, it is possible in some jurisdictions of government to require a locally – based ISP to block customers' access to a VPN, if found that the service itself is facilitating terrorism related activities (Edman & Yener, 2009, p. 20). Per Kebball, "another possible solution, where user access to the VPN itself cannot be controlled, is for governments to block the actual VPN service from being able to access key services. In that instance, while users would still be able to access the VPN, any traffic identified as being from that VPN would be blocked from accessing those services" (Kebball & Romyn, 2016, p. 93). In comparison to counter measures taken to repel suspicious usage of VPN, similar procedural steps are taken by authorities to appropriate the same preventive response one would find in TOR.

In contrast to the steps taken to monitor and eliminate pernicious VPN usage, the process to observe comparable data within TOR is quite different. According to Murdoch and Danezis, "note that while it is impossible to observe traffic and identify a particular source, it is possible to identify which traffic has come from the same source and attempts to use the content of that traffic to identify the source itself" (2005, N.p). Through observational methods, the essential objective in regards to online traffic monitoring authorises the investigator to construct a profile of a particular user, and sift through the content of their traffic for identifying information (Kebball &Romyn, 2016, p. 95). As stated earlier, although IT competency is not a critical component when operating TOR, maintaining an online presence without revealing identifying information can be exceedingly difficult. Numerous domestic law enforcement agencies and organisations have taken note of this weakness and have begun to capitalise on it.

“As online traffic passes through TOR, it must exit TOR through what is known as an exit node, which is a random router that can be set up by anyone who wishes to be a part of TOR” (Kebball & Romyn, 2016, p. 96). It has been determined that by controlling the exit node(s) of TOR, government agencies that specialise in cyber security are now able to insert malicious code into the original user’s traffic in order to identify the origin from which it came (Kebball & Romyn, 2016, p. 93). Albeit the identity of individuals using TOR is hidden from investigative onlookers, the identity of the exit node that the traffic is originating from can be determined. One method in particular that grants admittance to the necessary precision government agencies need in order to identify, overload, and shut down these specific exit nodes, is known as ‘sniper attack’ (Jansen, 2014, N.p). A sniper attack has been described as a tactic which can be used to exploit exit nodes and identify individuals using TOR, thusly, proceeding to force the individual’s traffic to re-route through a disparate exit node (Jansen, 2014, N.p). With respect to Kebball & Romyn, “by overloading the exit node that has been monitored by the government that the individual is using, the user’s traffic can eventually be routed through an exit node that is being monitored by the government agency. At this point, the original user can be identified” (2016, p. 94).

Apart from VPN and TOR, there are many other online tools accessible for jihadists to take advantage of in order to mask their intentions and strengthen their cause within and throughout the cyber domain. The process of avoiding detection in a physical environment in comparison to its online subordinate, however, is seamlessly straight forward. Online platforms aside, extremists affiliated with terrorist networks cannot avoid detection by hiding behind some disfigured emoji, avatar, VPN, and, or, TOR. Instead, terrorist networks that are IT incompetent operating abroad and offline, or, interestingly enough, do not take advantage of the Internet conducive to other, more notorious terrorist organisations – such as the Islamic State - must instead avoid: physical disruption of terrorist networks, constant surveillance from unmanned aerial vehicles (UAV), espionage, and even death. Moreover, the art of which radicalising young men and women in countries that inherently breed terrorist networks, such as: Iraq, Syria, Lebanon, and Afghanistan – to name a few - are detached from the West by miles of land and sea. Despite the Middle East being isolated from the West, one of the main reasons why online radicalisation and recruitment is so prevalent within the U.S., is due to the influential extension the Internet provides in addition to the controversial narrative currently surrounding Islam and the establishment of IS.

Cyberspace, inconsistent with geography, is essentially borderless. The network and interconnected information systems that occupy its vastness, reside simultaneously in both physical and virtual space, and within and outside of geographical borders (Kuehl, N.d, p. 3). As important as interconnectivity is, a consequence of its global adherence has led to the inter-transmittance of social and regional phenomenon's. This isn't necessarily a bad thing, however, with and increase in homegrown radicalisation due to online propaganda and extremist ideals weighing in on the U.S. and its citisens, it would hardly be surprising if one were to find themselves debating the pros and cons to which the Internet and cyberspace produce. Over the course of time, IS has gained superiority, or dominance rather, in cyberspace. They have exemplified their objective and have influenced mass amounts of individuals via online platforms, such as: Facebook, Twitter, and various online chat rooms. A movement that would have only been reported on because of the sinister theme it upholds, has now infiltrated and affected the United States in a way that is unfamiliar to its domestic authorities as well as its elected officials.

What would have otherwise remained in its conceived location has now influenced and dispersed into neighboring states. Without the contemporary use of online platforms, IS, in regards to the influence it has been able to maintain for an extended period of time, may have shortly dissolved due to insufficient demographic support and gain within and outside its region(s) of operation, or would have exhausted all of its resources as a result of inadequate material goods. Instead, as a consequence of global interconnectivity via cyberspace, in addition to deficiencies surrounding U.S. policies installed for sake of weeding out malevolent behavior online, IS has been provided an outlet which enables them to popularise and bolster their purpose within the U.S., in absence of its physical presence. Accordingly, much of IS' success, in relation to appealing to and galvanising certain individuals, can be credited towards efforts of establishing false 'anti-Muslim' or 'Islamophobic' sentiment aimed towards Western states by means of online platforms they continuously take advantage of. Similarly, what has been unintentionally overlooked and, to some extent ignored, is pragmatic congnition - how changing the mindset of someone else can still be considered an attack. Cyberspace is a key operational medium by which "strategic influence" is conducted, and references to "Jihad.com" have become ever more inflated (Kuehl, N.d). The U.S government, as well as existing terrorist networks – such as IS and Al' Qaida – are both using cyber power as a crucial capability in the struggle for minds and ideas. "Recent studies indicate that 90 percent of terrorist activity on the Internet takes place using some type of social networking tool" (Weimann, 2012). Unfortunately for the U.S., by means of cellular encryption, neglecting to amend current legislation, as well as online persuasion and propaganda, the modern cyber extremist is ahead in this exchange.

One would assume that given all of the technological methods authorities have at their disposal, terrorist organisations, as well as the individuals influenced by them, would be more apprehensive to conduct to what some could argue is a public predilection of ones intentions and agenda. Whilst some argue it would be disadvantageous for terrorists to conduct operations via the Internet due to the likelihood of being monitored and identified, the possibility of the extremist(s) involved being able to effectively conceal his or her identity and further impede identification and reconnaissance procedures conducted by law enforcement, is an unfortunate certainty. One could argue that this is a consequence of the cyber domain in and of itself, as it is vast and to some degree intangible; or the result of unenhanced and, or, limited legislation currently existing within the United States. Let us now observe some of the policies and strategies the U.S. adheres to.

3.4 U.S. Regulations, Policies & Strategies

Passed on October 25th, 2001, the United States Patriot Act was essentially designed to amplify the power and jurisdiction of the Federal Bureau of Investigation (FBI) as well as other domestic intelligence collectors, generating enhancements to their ability to monitor and collect intelligence on suspected terrorists. However, due to its primary function of universal scrutiny directed towards suspected international terrorism, counterespionage, or foreign intelligence investigations; the document raises further concerns about civil liberties and human rights violations (Holm, 2004, p. xxvii). Lacking required Congressional approval, sections of the Patriot Act expired on June 1st, 2015. With the passage of the USA Freedom Act on June 2nd, 2015 – a document that aided restoration of several parts of the Patriot Act which had expired on the previous day - the expired sections were restored and renewed through 2019. Despite the documents reestablishment, Section 215 of the law was subsequently amended in order to stop the National Security Agency (NSA) from continuing its mass phone data collection program (Kelly, 2015, N.p). Instead, it has been implied that phone companies will retain the data and in order for the NSA to obtain desired information pertaining to targeted individuals, they must first request permission from a federal court (Kelly, 2015, N.p). The obstruction of intelligence collection techniques for purposes of installing a second party intermediary – the federal court - is a decelerating step on ladder that must uphold an efficient level of alacrity.

As stated in Title II: Enhanced Surveillance Procedures, in Section 215 of the Patriot Act, coinciding with highly controversial provisions initiated by human rights and civil liberties groups, is a regulation that allows the FBI to make an order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Similarly, the scope and availability of wiretapping and surveillance orders were expanded under Title II. The Act allowed any district court judge in the United States to issue such surveillance orders and search warrants for terrorism investigations. In congruence with Title III of the *Stored Communications Access Act*, search warrants were also expanded. Such steps now allow the FBI to gain access to stored voicemail's by means of search warrant, rather than through the more stringent wiretap law.

The issue surrounding the success of current and future counter-terrorism operations is not necessarily a question of how much information has been obtained; but instead, what methods, policies, and strategies are readily accessible in order for law enforcement of every caliber to efficiently facilitate evidence procurement, in addition to successfully counter homegrown radicalisation. Due to its intricacy, this extremist phenomenon is far too overwhelming for law enforcement to combat on their own without infringing on lawful Internet use, as well as the privacy and civil liberties of individual users. Technology and how it is applied is becoming just as increasingly affluent as it is adaptive. Current U.S. legislature, however, seems reluctant to follow this revolutionary trend and, as a result, has been exposed to certain vulnerabilities in the technology realm that hinder its application.

According to Peter Neumann, report author for the *Homeland Security Project* (HSP), "In its 2011 counter-radicalisation strategy and the subsequent implementation plan, the White House acknowledged that 'the Internet has become an increasingly potent element in radicalisation to violence' and promised to 'develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalisation and leveraging technology to empower community resilience'. One year later – referring to 2012, this still hasn't happened, and this report's first and most important recommendation is for the White House to complete its work on the strategy, make it public, and begin its implementation with alacrity" (p. 45). In compliance with Neumann and his ongoing project, the quintessential tools and resources needed in order to facilitate progress in all the necessary areas of policy, do in fact exist. However, a formal American domestic counter-radicalisation strategy has yet to be produced. U.S. strategies aside, *de-radicalisation* programs have started to surface all over the world, some of which having been initiated in Muslim majority counties, in hopes of reducing this socially inhibiting phenomenon. For instance, nations, such as: Yemen, Saudi Arabia, Northern Ireland, Colombia, Indonesia, Malaysia, and Singapore, have witnessed the development of its own particular approach to promoting disengagement of some form of terrorism (Horgan, 2008, N.p). Consequently, these countries seem less interested in facilitating de-radicalisation and more interested in attempting to promote disengagement and desistance from terrorist activity in the limited sense. Therefore the radical ideology an individual maintained throughout their service in a terrorist organisation may still remain even if and when he/she is detached from terrorism. Nevertheless, multiple strategies within these programs have also been developed involving the process of de-radicalisation. For instance, the 'Child Combatant program', part of the Ministry of Interior and Justice's Reincorporation Programme in Colombia, goes as far as attempting to reduce the size of terrorist movements by requiring incarcerated perpetrators to demonstrate symptoms of behavioral shifts

(Horgan, 2008, N.p). In other words, adolescents admitted into the program on the basis of the ideology they retain, may not be out-processed until there is a noticeable change in moral outlook.

Since the attacks of September 11, 2001, the United States has solidified itself as the lead entity in countering terrorism worldwide and, with its proclaimed status, has employed a variety of tools—military oriented and diplomatic—to pursue this objective adamantly. Despite its undertaking, Washington has been exceedingly apprehensive towards devising a solid cohesive strategy to counter radicalisation. Negligence has resulted in Washington's inability to accommodate the atrocious characteristics of radicalisation, particularly taking place within the cyber domain. Contrary to several European countries, which have invested substantial human, financial, and political capital in extensive, long-term, centrally-crafted counter-radicalisation strategies with multi-agency implementation, the United States possesses disorganised initiatives that fail to amass into a well-designed plan (Vidino, 2010, p. 2). For example, in comparison to CONTEST, the United Kingdom's counter-terrorism strategy, the American equivalent seems to be undiscovered. Inverse to the latter and contrary to Neumann, the United States does possess somewhat of a counter-radicalisation strategy. This strategy, however, lacks proactive components, such as the preemptive efforts observed in Colombia's 'Child Combatant Program', in addition to hardly extending beyond the art of research and engagement.

In August 2011, the White House issued a paper entitled 'Empowering Local Partners to Prevent Violent Extremism in the United States', which outlined the country's plan to counter radicalisation. The August document was followed in December 2011 by the release of another document entitled 'Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States', which expanded on the previous document's provisions (Neumann, 2012, p. 4). The August 2011 strategy, as

Neumann points out, “acknowledged “the important role the Internet and social networking sites play in advancing violent extremist narratives”” (2012, p. 4). Furthermore, in Washington’s Implementation Plan, released December 2011, it was stated that “the Internet has become an increasingly potent element in radicalization to violence” and that new “programs and initiatives” had to be “mindful of the online nature of the threat” (White House’s Counter-radicalization Strategy, 2011, p. 20). Interestingly enough, however, the two documents - if compared to strategies that have been long implemented in Europe - outline initiatives that are not nearly as aggressive as they should be (Vidino, N.d, p. 2). Moreover, the White House acknowledging that “the Internet has become an increasingly potent element in radicalization to violence,” has made imperceptible strides. Furthermore, six years later, the White House has fallen short of their promise to “develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience.” Instead, current U.S. ‘strategies’ are mostly limited to constructing an extensive knowledge base for understanding characteristics related to the radicalisation process and engaging the American Muslim community. Doubtless, these two aspects are unquestionably important, and certainly all European counter-radicalisation strategies similarly adopt them as integral components comprised into a larger agenda (Vidino, N.d, p. 2). However, as Vidino perspicuously points out, “the American strategy stops short of outlining the many and more proactive and ambitious measures that characterize the European approach to counter-radicalization beyond research and engagement” (N.d, p. 2). An ideal U.S. strategy would advocate an increase in communication and cooperation between public and private partnerships (PPP’s), in addition to encouraging private corporations – like Facebook, Apple and Twitter - to establish privately funded counter-terrorism units. Sufficient PPP’s are critical in efforts to successfully combat online-radicalisation and terrorism.

Although the U.S. Government, particularly the Department of Homeland Security (DHS) - which in 2007 was designated by Congress as the lead department to counter radicalisation - espouses awareness through Internet safety initiatives, educating the profuse amount of institutions in place (school districts, Parent Teacher Associations, local government, etc.) isn't, on its own, going to successfully ward off future terrorist attacks. Rather, in addition to these informative seminars, DHS must also devise and further expand upon preexisting *pilot programs*, similar to the three current programs that stand in several U.S. states (Vidino & Hughes, 2015, p. 1). The Boston Marathon bombing, followed by the rise of IS, triggered a renewed focus on Counter Violent Extremism (CVE) (Vidino & Hughes, 2015, p. 1). As a result, "a part of the revamped effort includes pilot programs in three cities, each with a distinct approach: Minneapolis-St. Paul's focused on societal-level concerns, Los Angeles' on community engagement, and Boston's on interventions with radicalized individuals" (Vidino & Hughes, 2015, p. 1).

As stated by Vidino, "The United States has lagged behind many European countries in creating a comprehensive CVE approach, largely because its homegrown violent extremist threat is relatively low. Only in 2011 did the U.S. launch a formal CVE strategy and its implementation has been disjointed and underfunded. Moreover, successful implementation of CVE initiatives faced key challenges during the Obama administration. These challenges consisted of: lack of funding and resources devoted to CVE; lack of a lead agency appointed to appropriately manage CVE efforts at the national and local levels; and, lastly, resistance from Muslim communities (Vidino & Hughes, 2015, p. 1). In order for any constructive progress to develop, these challenges must be attended to and overthrown, promptly. Furthermore, the amount of funding invested in community engagement should, in one's own opinion, be deferred and redirected elsewhere. Instead, corresponding with Europe's posture, individual interventions are not only easier to evaluate – as the focus has been tightened, they also produce a cost-effective solution that would replace large, more expensive, programs.

What is certainly present within the U.S., is tactics failing to emulate proper strategy. Furthermore, there is great obscurity surrounding how the U.S. should proceed with approaching these issues. More so, by virtue of former President Barack Obama transferring power over to his successor, President Donald Trump, and his administration. Although tending to this national security matter is most pressing and imperative, how one administration chose to manage risk does not necessarily transfer over to the succeeding administration – especially when the current administration is represented by the opposing political party of the former.

State action is an important form of strategic communication and therefore significant to CVE initiatives on and offline. Contradicting its altruistic purpose, however, are non-state actors who are, more often than not, eager to use state action (and sometimes inaction) to incite and legitimise violence against the state and its citizens (Cheong, 2016, p. 283). In comparison to this, counter-radicalisation programs are an immensely complex and controversial subject which, in one's own opinion, requires gradual application (Vidino, 2010, p. 10). Such programs touch on – what some may consider - extremely sensitive issues, such as religion, identity, and integration (Vidino, 2010, p. 10). According to Lorenzo Vidino, "they can be highly intrusive, impinge on civil liberties, and risk further alienating the very group they seek to reach" (2010, p. 10). Nevertheless, the ubiquitous use of the Internet has made it possible for terrorist groups to remotely foment attacks with little risk of capture. With that said, it is imperative for policymakers to indoctrinate innovative ways to prevent this radicalisation process from occurring - on and offline - in addition to implementing strategies designated to eliminate the ideology entirely from individuals who suffer from its cognitive infliction.

Conclusion

Research Question: How can online self-radicalisation be successfully countered?

For a long period of time, early efforts of attempting to understand radicalisation had been psychologically driven and primarily focused on research involving the individual(s) and his or her behavior. Since the 1960's, however, academic analysis pertaining to the phenomenon of radicalisation has now broadened and further includes observation into: group interaction, social networks, and affiliated organisations; thus disproving that radicalisation of an individual reflects mental and personal abnormalities. As such, radicalisation foreshadowing acts of terrorism is no longer viewed as a "condition", but is instead viewed as a *dynamic process* lacking a definitive terrorist personality. Moreover, definitions of "radical" "radicalism" and, or, "radicalisation" face conflation if not used in the proper context. Therefore, it is crucial that one identify which context best suits their agenda and, or, interests. In this paper two variations of the word "radicalism" were discussed: one absolute and one relative. Although both provided invaluable insight into the phenomenon of radicalisation, it was decided that the focus should embrace the words relative definition, taken from the *Oxford English Dictionary*: "representing or supporting an extreme section of a party" (2009). It is in this sense the word may be synonymous with the term "extremist", thereby providing clarity and awareness to the reader (Sedgwick, 2012).

Radicalisation in terms of violence, also referred to as radicalisation into violent extremism (RVE), could essentially be described as the processes by which people come to adopt beliefs that not only justify violence but compel it (Borum, 2011). However, the distinction that should be made when comparing radical acts of violence to regular, non- radical, acts of violence, is the presence of ideology as a motive. 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* of many possible pathways into terrorism involvement (Borum, 2011). Furthermore, as research shows that there is not a single pathway to RVE, and that the process undergone by one individual may not be the same process undergone by another; it is apparent that a single theory or discipline will not encapsulate a definitive pathway. In addition to the lack of clarity attributed to radicalisation, other areas related to the topic harbor similar contextual perplexities. Accordingly, the term "radical" is carelessly used to satisfy the context in a number of differing agendas, such as: the *security agenda*, *integration agenda*, and *foreign – policy agenda* (Sedgwick, 2012). The various existing contexts (security, integration, and foreign-policy) inadvertently convolute the word "radicalisation", or what it means to be radical. What tends to be problematic is not the word itself, but the suggested "absolute concept" of how the word is applied within the discourse of said contexts. An example of this would be the parallel drawn between Islam and violence, as well as the observable prejudice towards how all Islamists are driven by religious principles.

Similar to the lack of clarity surrounding "radicalism", the term *threat radicalism*- extreme views, including beliefs that violent measures need to be taken – follows suit (Hamm, 2008). Overemphasising the violence associated with radicalisation, the definition of both 'radicalisation' and 'threat radicalism' ignore the majority of cases that do not lead directly to violence, or do not necessarily lead to violence at all. Accordingly, the intentional and systematic principles of *recruitment* often times coexists within the majority of discourse pertaining to radicalisation. However, although recruitment shares a unique place in RVE, *enlistment* is the dominant mechanism for the emergence of new recruits (Sedgwick, 2010).

There are many pathways through which radicalisation occurs, each of which is affected by a variety of factors. Within this "pathway" approach, it has been determined that radicalisation should not be perceived as the product of a single decision, but rather the end result of a dialectical process that, overtime, gradually pushes an individual toward violence (McCormick, 2003). To illustrate this process and other processes , the following theories were reviewed in order for the reader to gain tautological understanding and comprehension of various frameworks that bare influence over terrorism: *social movement theory*, which focuses on the irrational processes of collective behavior occurring under strained environmental conditions; *social psychology theory*, which concerns itself with relationships, influences, and transactions among people, and particularly group behavior; and *conversion theory*, which devotes less focus on the collective movement, and more so on the individual process of transforming beliefs and ideologies.

Apart from individuals being naturally integrated into their respected Western societies, 'home grown' terrorism in the Western part of the world has been on steady incline for the past decade and a half. Home grown terrorism has been defined as: acts of violence against civilian and, or, military targets that are primarily orchestrated in Western countries – such as Europe and the U.S. - in which those committing violence have been born and raised. Despite the existence of other forms of radicalisation, Islam seems to be the most concerning issue throughout Western society. Similarly, Islamic ideologies are currently prominent and may consist of anti-western propaganda. Therefore, it is important to differentiate between both *Islam* - said to be a religion that does not promote violence, nor encourage hatred on none Muslims, and *Islamism* - a totalitarian political ideology driven by potent anti-western goals (Borum, 2010).

Although radicalisation in the U.S. is relatively new, the methods these radicalised individuals adopt in order to facilitate their migration is congruent with the digital era (Saltman, 2016). Moreover, online communications and Internet tools have reduced logistic complexities and provided an outlet for individuals seeking to coordinate and organise their own migration to join a conflict in order to gain acceptance into terrorist organisations, like IS (Saltman, 2016). These same tools are also applied to radicalise users by: indoctrinating individuals through deconstruction of previous ideology, providing the curious with quick and easily accessible educational resources, and acting as a social platform in order to further reinforce radical ideology and extremist propaganda. It is understood that the biggest advantages of these communications, is the sending of unfiltered messages received by the intended audience (Hussain & Saltman, 2014). Unfortunately social media openly contributes to the mainstream recruitment platform for online radicals and extremists, thereby allowing many recruits to virtually connect with IS fighters located in Iraq and Syria.

As previously mentioned, the pathway to radicalisation is a dynamic process. However, within that process it was learned that one's progression towards radicalisation can be divided into individual stages. Likewise, an individual(s) progressing through these stages, leading up to radicalisation, inherently does so at varying timeframes (Borum, 2003; Moghaddam, 2005). In order to comprehend the radicalsation process as well as the many avenues within it, we examined a diverse set of existing radicalisation models developed by a number of experts. Through observation it had been discovered that the content and structure found within the discussed models differ greatly, due to: perceived variance in the radicalisation process, key aspects of radicalisation sought to be emphasised and exposed, in addition to differences of opinion among a number of scholars. Despite this, many of these models failed to accentuate the radicalisation process as it exists in the cyber element, rather than its conventional one.

Correspondingly, the reviewed models illustrate different outlooks on the radicalisation process. For example, Borum's four stage model was originally developed to provide beneficial insight of the radicalisation process to law enforcement officials. Moreover, the model insists that grievances, in addition to exposure to radical discourse, generate hatred towards certain groups; ensuing a final outcome that allows the individual to embrace ideologies pertaining to jihad and martyrdom (Borum, 2011). Although the model itself is overly simplistic and incompatible with online self-radicalisation - as it *does not* include interaction with the Internet or its platforms - the first and second phase of the model, grievance and injustice, provide a common foundation that is acknowledged in other existing models. The second model that was examined was Moghaddams terrorism staircase model, which suggests that the path to terrorism is a set of progressive stages with fewer and fewer individuals progressing onto each stage within the staircase (Moghaddam, 2005). Dissimilar from most models, Moghaddam insists that the first stage an individual embarks on in the radicalisation process is a product of 'personal adversity'. Although the staircase structure of the model is efficiently laid out, the psychological connotation throughout the model was determined to be outdated if and when applied to contemporary processes of radicalisation. Helfstein's four stage model, contrary to older models, views the phases of radicalisation as a dynamic series, similar to a cycle of events. The model was created based on case studies of radicalised individuals and plots of terrorism in the U.S. and argues that radicalisation cannot be independently viewed as a social or ideological process, but instead suggests it is a "coevolutionary" process (Helfstein, 2012). Dissimilar from other models, Helfstein's model emphasises that Internet sites, YouTube and online magazines, convey radical ideology, further conceding that interaction with the online platforms seem to facilitate the institutional process of socialization (2012). Lastly, Torok's explanatory model utilising psychiatric power, examines power relationships online in addition to how discourses are formed and propagated online (Torok, 2016). The model itself was formulated to focus on three critical foundations: outlooks on social media platforms regarded as online institutions seeking to isolate and expose individuals to one-dimensional discourse; normalisation of extremist discourse, conveyed with authority and truth; and, lastly, power is networked with individuals being radicalised by various sources consisting of homogenous extreme discourse, rather than a single entity (Torok, 2016, p.65). Although Torok's model is the most contemporary model to date, it is unclear whether the model continues to follow the individuals' induction into extremist thinking. Furthermore, this model lacks transparency surrounding the social media environment and influential power, in addition to a visual interpretation of the models structure.

In pursuance of improving and extending upon self-radicalisation and how it is regarded in its cyber element, the author proposed an alternative model. Angelini's online self-radicalisation model (AOSRM) seeks to interpret online radicalisation as a process leading up to radicalisation into violent extremism (RVE), whilst simultaneously exposing the possibility of an individual not partaking in violent acts of any kind; thereby allowing the individual to branch off into what is referred to as radicalisation into extremism (RE). AOSRM was created simply to provide transparency on the online self- radicalisation process. The phase model starts off with *exogenous conditions*, also referred to as 'triggering factors'. These factors, whether they are motivations of any kind (economic frustration; political, social, and, or cultural injustices) are completely unique to the individual and may lead to curiousness and, or, self-education on matters relatable to oneself. Sequentially, *echo-chamber indoctrination* follows suit and provides insight into the individuals' online consumption of radical discourse through isolated online communities. This phase goes on to explain that disaffected individuals searching for an outlet to self-educate or socialise with people that possess similar or identical ideologies and, or, grievances actually turn out isolating themselves, in turn, reinforcing commonly held ideas that are safe from criticism. Subsequently, *conversion*, the third phase in AOSRM, introduces a conscious, or sometimes sub-conscious, decision involving identification or association with what is to be believed as the message of Islam – also referred to as Islamism – and is the radical tipping point in the process. *Justification* is essentially the last phase in the AOSRM model which ensues radicalisation. Accordingly, it is the divisions within the phase of justification – RVE and RE - that distinguish it from other models. The divisions establish a precedent that reveals how extremists do not always result to violence. Nevertheless, individuals who have progressed to this stage of the model, though they may not end up committing or supporting acts of violence, may not necessarily disagree with them.

Preceding the introduction of AOSRM, three cases involving online-radicalisation and terrorism were analysed. Coupled with the unfortunate outcome when officials are deprived of quintessential resources, inclusive of confrontation with obstinate behavior and refusal of entry into private technologies produced by private corporations, the case study analysis essentially sought to unmask and emphasise the harsh reality of when civil liberties interfere with the future safety of the American people. In each case the author exploited the backgrounds, interests and incentives, of the perpetrator(s). Criticism and admiration was 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 – the San Bernardino Massacre and the Boston Beheading Plot - underwent analysis to the extent of highlighting the failure's and success' directed towards prevention and apprehension of a terrorist attack. The third and final case exemplified the success of a counter-terrorism operation, in addition to incorporating the author's personalised online self-radicalisation model - AOSRM. Correspondingly, the first two cases that were selected generated distinct infractions and obedience regarding the institutions involved (FBI, Facebook, Apple, etc.), technologies and regulations confronted

– concerns that were critically addressed in chapter three. The third case that was selected simply demonstrated a coherent pathway towards extremism by means of radical online material, and was therefore thoroughly analysed via compatibility with the author's radicalisation model, AOSRM. The overall application of the author's model offered insight to the online self-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.

To conclude, the third and final chapter discussed the differentiating factors between online and offline radicalisation and recruitment conducted by terrorist organisations, with a focus surrounding the United States of America (U.S). Moreover, a critical analysis was conducted on U.S policies and legislation installed for the purpose of countervailing homegrown terrorism. Since its emergence in the 1990's, the World Wide Web has provided many opportunities to advance globalisation as well as the interconnectedness between people. Such revolutionary developments that are normally praised for their innovative attributes, are now viewed – at least in the security sector - as potential radicalisation and recruitment incubators which may produce unforeseeable circumstances of extremism and violence. As a consequence, what was once a regional phenomenon – radicalisation and recruitment - most prevalent in territories housing existing terrorist networks, has now transcended into random acts of homegrown violence spilling over into the United States (U.S.).

It is clear that the topic of *recruitment* shares a unique place in the radicalisation into violent extremism (RVE) discussion, however, it is important to note that not all individuals who are in fact radicalised fall under the process of being recruited. Alternatively, *enlistment* is the mechanism for the emergence of new recruits; subsequently depicting friendship to be the catalyst for about 70 percent of armed Jihad, kinship for about 20 percent, while discipleship comprises the remaining 10 percent (Sageman, 2011). Unlike the primitive, more conventional methods of radicalisation and recruitment, or enlistment, the Internet provides various avenues for terrorists to display and advance their agendas in order to communicate their ideologies on a massive, unfiltered scale. Access to the Internet and various online platforms has unquestionably enhanced the transmission of radical ideologies and extremist behaviors transnationally; thus inciting negative sentiment towards enemies, or self-proclaimed enemies, in addition to undertaking potential recruit mobilisation by means of online propaganda. Moreover, the Internet provides terrorists with a centralised form of useful information, including instructions for bomb assembly, poisoning, weapons construction, and mixing lethal chemicals (Martin, 2006, p. 542).

Considering there is presently no single entity to enforce cyber regulations, nor is there a current multinational approach among states to enforce a sense of online orderliness, the idea of cyber governance maintains its status as an unemployed perception. In conjunction with each state possessing disparate laws and statutes to accommodate its citisens, the rise of the Internet in addition to the massive expansion of data storage over the past two decades has significantly overwhelmed and reduced the ability of policy makers to formulate rules for what law enforcement and intelligence agencies can and cannot do in terms of surveillance (Neumann, 2012, p. 39). Although preferential censorship in some cases may be considered ideal, the United States' constitutional, political, and practical constraints make censorship impossible, given that constitutional free speech protections in the U.S are as extensive as they are explicit (Neumann, 2012).

It was formerly discussed that securitising online anonymity tools – such as VPN's and TOR - would essentially provide law enforcement and intelligence services with enhanced capabilities, thereby reducing the overall discreetness found between extremists and their uploaded content in addition to the individuals they seek to influence and inspire. Moreover, all traffic sent between a user and a VPN is encrypted, allowing the content of this traffic to remain hidden from the Internet service provider (ISP) or any other agency that may be collecting metadata (Larsson, 2012, p. 264). Comparable to VPN, an onion router, or 'TOR', is another commonly used method of maintaining online anonymity. TOR is a method of online browsing that systematically randomizes a user's internet traffic through multiple points, or 'nodes', before it reaches its online destination (Antoniades, 2010, p. 134). Furthermore, TOR bypasses the use of a single service provider, allowing the user to remain elusive in the attempt to facilitate avoidance of scrutiny directed towards Internet traffic; which, in turn, would prevent the retrieval and dissemination of information from reaching the hands of domestic authorities (Kebbell & Romyn, 2016, p. 93). Despite the cyber camouflage provided by the Internet, its various functions also promote opportunities for authorities to systematically stalk and identify potential criminals, terrorists, potential online radicals, and, or, recruits. For example, As for VPN, although the ISP may be *unable* to identify the individual utilising their service, it is possible in some jurisdictions of government to require a locally – based ISP to block customers' access to a VPN, if found that the service itself is facilitating terrorism related activities (Edman & Yener, 2009, p. 20).

Cyberspace, inconsistent with geography, is essentially borderless. The network and interconnected information systems that occupy its vastness, reside simultaneously in both physical and virtual space, and within and outside of geographical borders (Kuehl, N.d, p. 3). As important as interconnectivity is, a consequence of its global adherence has led to the inter-transmittance of social and regional phenomenon's. What would have otherwise remained in its conceived location has now influenced and dispersed into neighboring states. Without the contemporary use of online platforms, IS, in regards to the influence it has been able to maintain for an extended period of time, may have shortly dissolved due to insufficient demographic support and gain within and outside its region(s) of operation, or would have exhausted all of its resources as a result of inadequate material goods. Accordingly, much of IS' success, in relation to appealing to and galvanising certain individuals, can be credited towards efforts of establishing false 'anti-Muslim' or 'Islamophobic' sentiment aimed towards Western states by means of online platforms they continuously take advantage of. Naturally, the Internet is the perfect environment to convey such a message; seeing as cyberspace is a key operational medium by which "strategic influence" is conducted (Kuehl, N.d).

The issue surrounding the success of current and future counter-terrorism operations is not necessarily a question of how much information has been obtained; but instead, what methods, policies, and strategies are readily accessible in order for law enforcement of every caliber to efficiently facilitate evidence procurement, in addition to successfully counter homegrown radicalisation. Due to its intricacy, this extremist phenomenon is far too overwhelming for law enforcement to combat on their own without infringing on lawful Internet use, as well as the privacy and civil liberties of individual users. Unfortunately, current U.S. legislature seems reluctant to follow the revolutionary trend of technological innovation and has thereby been exposed to certain vulnerabilities in the technology realm that hinder its application. Consequently, the White House has fallen short of their promise to "develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience." Instead, current U.S. 'strategies' are mostly limited to constructing an extensive knowledge base for understanding characteristics related to the radicalisation process and engaging the American Muslim community.

In contrast to the White House strategy that seeks to prevent violent extremist online radicalisation by leveraging technology to empower community resilience, I suggest a U.S. strategy which advocates an increase in communication and cooperation between public and private partnerships (PPP's), in addition to encouraging private corporations – like Facebook, Apple and Twitter - to establish privately funded counter-terrorism units. Sufficient PPP's are critical in efforts to successfully combat online-radicalisation and terrorism. Accordingly, they would increase the efficiency of mitigating potential threats through a bilateral approach. Moreover, implementation of de-radicalisation programs, similar to the ones found in Muslim majority countries, such as: Yemen, Saudi Arabia, Northern Ireland, Colombia, Indonesia, Malaysia, and Singapore, should be investigated further. Likewise, preexisting *pilot programs,* identical to the three current programs that stand in several U.S. states – Minneapolis, Los Angeles, and Boston - should expand and continue to focus collectively on societal concerns, community engagement, and interventions with radicalised individuals (Vidino & Hughes, 2015, p. 1).

In hindsight, state action is an important form of strategic communication and therefore significant to counter violent extremism (CVE) initiatives on and offline. Contradicting its altruistic purpose, however, are non-state actors who are, more often than not, eager to use state action (and sometimes inaction) to incite and legitimise violence against the state and its citisens (Cheong, 2016, p. 283). In comparison to this, counter-radicalisation programs are an immensely complex and controversial subject which, in one's own opinion, requires gradual application (Vidino, 2010, p. 10). However, as a testament to topics covered, other intriguing avenues of research I am open to explore in the future involve online deradicalisation and methods of a counter – ideological response (CIR), more specifically Ramakrishna's developed CIR model. Firstly, online deradicalisation acknowledges the increasing use of how online platforms influence and aid violent extremism. The online deradicalisation to which I am referring, seeks to implement psychotherapeutic techniques by predominately employing cognitive behavioral therapy (CBT) online (Shi, 2016). The rationale behind such an idea, is that it provides an outlet to what would be considered as professional communication held between a qualified counselor and a radicalised individual. Moreover, the concept offers user convenience, opportunities to elaborate on manifested thoughts via physical disconnect, in addition to therapeutic reflection (Shi, 2016). As a result, the dialogue held between both parties could be facilitated over great distances; thus minimising the need for physical exposure as well as simultaneously assuring safety (Shi, 2016).

A second avenue of interest would most likely be familiarising one's self with what is referred to as a 'counter- ideological response' (CIR). CIR essentially consists of five conceptual spaces (sender, message, mechanism, recipient and context) to which violent extremism is sought to be countered by means of appropriate, ideological –relevant, policy interventions (Ramakrishna, 2016). In essence, a counter- ideological response customised for each of the five spaces seeks to negatively impact the overall reach and influence of violent extremism by intervening through the medium of legislation (Ramakrishna, 2016). CIR insists that 'ideology' as the centre of gravity within all violent Islamist terrorist networks. Moreover, CIR recognises that neutralising violent extremism online requires something more than a model strictly applied to the online space as well as its many platforms. Additionally, CIR further suggests that its five conceptual platforms within the counter- ideological response also be implemented into various offline contexts. When employed in unison, CIR stands to engage a comprehensive strategy to prevent further proliferation of violent extremism on and off- line (Ramakrishna, 2016).

Bibliography

20,000 foreign fighters flock to Syria, Iraq to join terrorists. (2015, February 10). CBS News. Retrieved from http://www.cbsnews.com/news/ap-2000-foreign-fighters-flock-to-syria-iraq-to-join-terrorists/

"28 U.S. Code § 1651 - Writs." LII / Legal Information Institute. N.p., n.d. Web. 05 May 2017. <https://www.law.cornell.edu/uscode/text/28/1651>.

Allen, Evan, and Milton J. Valencia. "Prosecutors Detail Roslindale Man's Decapitation Plot - The Boston Globe." BostonGlobe.com. N.p., 03 June 2015. Web. 22 May 2017. <https://www.bostonglobe.com/metro/2015/06/03/everett-man-face-charges-connected-with-tuesday-shooting-roslindale/A4GN3KGxekIvQG4JljKMUP/story.html>.

Allport, G. W. "The historical background of social psychology," in G. Lindzey and E. Aronson (eds.), Handbook of social psychology (New York: Random House, 1954), 5.

Anti-Defamation League, Combating Extremism in Cyberspace: The Legal Issues Affecting Internet Hate Speech (New York: ADL, 2000), p. 3.

Antoniades, D., Markatos, E.P., & Dovrolis, C. (2010). MOR: Monitoring and measurements through the onion router. In A. Krishnamurthy & B. Plattner (Eds.), Passive and active measurement (pp. 131 – 140). Berlin: Springer-Verlag. Doi:10.1007/978-3-64212334-4_14

Atran, S. "Pathways to and From Violent Extremism: The Case for Science-Based Field Research," Statement before the Senate Armed Services Subcommittee on Emerging Threats & Capabilities, March 10, 2010.

Baker, Al; Santora, Marc (December 16, 2015). "San Bernardino Attackers Discussed Jihad in Private Messages, F.B.I. Says". The New York Times.

Bartlett, J. & Miller, C. "The Edge of Violence: Towards Telling the Difference between Violent and Non-violent Radicalization," Terrorism and Political Violence, 24, 1 (2012), pp. 1-21

Barrett, R. (2014). *Foreign fighters in Syria*. New York, NY: The Soufan Group.

Bates, R., & Mooney, M. (2014). Distance learning and jihad: The dark side of the force. *Online Journal of Distance Learning Administration*, 17(3).

Benner, K., & Lichtblau, E. "Apple Fights Order to Unlock San Bernardino Gunman's IPhone." The New York Times. The New York Times, 17 Feb. 2016. Web. 05 May 2017.

Benson, D. (2014). Why the Internet is not increasing terrorism. *Security Studies*, 23(2), 293-328. doi: 10. 1080/ 09636412.905353

Bidgood, Jess, and Dave Philipps. "Boston Terror Suspect's Shooting Highlights Concerns Over Reach of ISIS." The New York Times. The New York Times, 03 June 2015. Web. 15 May 2017.

Borum, Randy. Psychology of Terrorism (Tampa, FL: University of South Florida, 2004).

Borum, Randy. "Radicalization into Violent Extremism I: A Review of Social Science Theories." Journal of Strategic Security 4, no. 4 (2011): 1-36.

Borum, Randy. (2003). Understanding the terrorist mindset. *FBI Law Enforcement Bulletin*, 72(7), 7-10.

Bowman-Grieve, L. (2013). A psychological perspective on virtual communities supporting terrorist & extremist ideologies as a tool for recruitment. *Security Informatics*, 2(9), 1-5

Brumfield, B., & Sanchez, R. "Usaamah Rahim Is Buried, Terror Questions Loom." CNN. Cable News Network, 05 June 2015. Web. 15 May 2017.

Chang, Cindy (December 26, 2015). *"San Bernardino shootings cast a somber tone over Muslim conference in Chino". Los Angeles Times. Retrieved April 5, 2017.*

Cheong, Damien. "Countering Online Violent Extremism: State Action as Strategic Communication." *Combating Violent Extremism and Radicalisation in the Digital Era*. Hershey, PA: Information Science Reference, An Imprint of IGI Global, 2016. 283-301. Print.

Clark, Matthew. "There's No Such Thing as a." *American Center for Law and Justice*. N.p., 28 Oct. 2014. Web. 04 Aug. 2016. <http://aclj.org/jihad/self-radicalized-islamic-terrorist>.

Cook, Tim. "Customer Letter." Apple. N.p., 16 Feb. 2016. Web. 03 May 2017.

Crossett, Chuck, and Jason A. Spitaletta. "Radicalization: Relative Psychological and Sociological Concepts." (2010): 1-94. US Army Asymmetric Warfare Group. Web. 3 Nov. 2016. https://info.publicintelligence.net/USArmy-RadicalizationConcepts.pdf

Duarte, C. (2007). The seductive web: Technology as a tool for persuasion. In B. Ganor, K. Von Knop, & C. Duarte (Eds.), *Hypermedia seduction for terrorist recruiting* (p. 169-187). Washington, DC: IOS Press.

Edman, M. & Yener, B. (2009). On anonymity in an electronic society: A survey of anonymous communication systems. *ACM Computing Surveys*, 42(1), 1-35. doi:10.1145/1592451.1592456

Egon Bittner, ‘‘Radicalism and the Organization of Radical Movements,’’ AmericanSociological Review 28 (1963), 932.

El-Bermawy, Mostafa M. "Your Filter Bubble is Destroying Democracy". WIRED. Retrieved 16 March 2017.

“Empowering Local Partners to Prevent Violent Extremism in the United States,” White House, August 2011, p. 6.

Farrell, Michael B. "Obama Signs Patriot Act Extension without Reforms." *The Christian Science Monitor*. The Christian Science Monitor, 01 Mar. 2010. Web. 31 Jan. 2017. <http://ezorigin.csmonitor.com/USA/Politics/2010/0301/Obama-signs-Patriot-Act-extension-without-reforms>.

Habeck, M., Knowing the enemy: Jihadist ideology and the war on terror (New Haven, CT: Yale University Press, 2005).

Hamm, Mark S. "Prisoner Radicalization: Assessing the Threat in U.S. Correctional Institutions." Www.nij.gov. N.p., 27 Oct. 2008. Web. 15 Jan. 2017. https://www.nij.gov/journals/261/pages/prisoner-radicalization.aspx

Hannon, Elliot. "Former Cheerleader and Mississippi State Sophomore Pleads Guilty After Trying to Join ISIS." Slate Magazine. N.p., 29 Mar. 2016. Web. 23 May 2017.

Helfstein, S. (2012). *Edges of radicalization: Ideas, individuals and networks in violent extremism.* Retrieved from https://www.ctc.usma.edu/v2/wpcontent/uploads/2012/06/

Hoffman, Bruce. *Inside Terrorism*. Revised and Expanded ed. New York: Columbia UP, 2006. Print.

Holm, Richard L. *The American Agent: My Life in the CIA*. London: St Ermin's, 2004. Print

Horgan, John. "Deradicalization or Disengagement?" *Perspectives On Terrorism*. Terrorism Research Initiative, 2008. Web. 20 Feb. 2017.

Horgan, John. "From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism," The ANNALS of the American Academy of Political and Social Science 618 (2008): 80–94.

Horgan, John. *The Psychology of Terrorism*. London: Routledge, 2014. Print

Hussain, G., & Saltman, E. (2014). *Jihad trending: Online extremism and how to counter it*. London: Quilliam Foundation.

Ibid.

Internet World Stats. (2014). *Internet usage statistics: The internet big picture.* Retrieved from http://www.internetworldstats.com/stats.htm

Janbek, Dana, and Thomas Steinfatt. "Chapter 2: Persuasion and Propaganda in War and Terrorism." *Combating Violent Extremism and Radicalization in the Digital Era*. Hershey, PA: Information Science Reference, An Imprint of IGI Global, 2016. 16-36. Print.

Janbek, D., & Williams, V. (2014). The role of theinternet post-9/11 in terrorism and counterterrorism. *The Brown Journal of World Affairs, 20*(2), 297-308.

Jansen, R., Tschorsch, F., Johnson, A., & Scheuermann, B. (2014). The sniper attack: Anonymously deanonymizing and disabling the Tor Network. Arlington, VA: Office of Naval Research.

Jose´ Ortega y Gasset, ''El ocaso de las revoluciones'' (1923), 2, pazfuerzayalegria.net_IMG_pdf_D8_el_ocaso_de_las_revoluciones.pdf

Kebbell, Mark. And Romyn, David. "Chapter 5: Using the Internet to Plan for Terrorist Attack." *Combating Violent Extremism and Radicalization in the Digital Era*. Hershey, PA: Information Science Reference, An Imprint of IGI Global, 2016. 91-103. Print.

Kelly, Erin. "Senate approves USA Freedom Act". (2015) USA Today. Retrieved January 31, 2017.

Kilbourne, B. and Richardson, J. "Paradigm conflict, types of conversion, and conversion theories," Sociological Analysis 50 (1989): 1–21.

Klandermans, B. and Oegema, Dirk. "Potentials, Networks, Motivations and Barriers: Steps Towards Participation in Social Movements," American Sociological Review 52 (1987): 519–531.

Kuehl, Dan. "From Cyberspace to Cyber Power: Defining the Problem." *CHAPTER 2*. N.p.: n.p., n.d. 1-17. Print.

Laqueur, Walter. End to War: Terrorism in the Twenty-First Century (New York: Continuum, 2003).

Larsson, S., Svensson, M,. Ronkko, K,. & Olsson, J.A. (2012). Laws, norms, piracy, and online anonymity: Practices of de- identification in the global file sharing community. *Journal of Research in Interactive Marketing*, 6(4), 260-280. doi: 10. 1108/17505931211282391

Legion of fighters battles for ISIS. (2015, May 20). Al-Arabiya. Retrieved from http://english.alarabiya.net/en/perspective/features/2015/05/20/Legion-of-foreign-fighters-battles-for-ISIS.html

Lewis, Danny. "What the All Writs Act of 1789 Has to Do With the Iphone." Smithsonian.com. N.p., 24 Feb. 2016. Web. 24 Apr. 2017.

Lewis, Paul (December 16, 2015). "San Bernardino attackers did not post about jihad on social media, FBI says". The Guardian.

Limer, Eric. "Why Is the FBI Using a 227-Year-Old Law Against Apple?" Popular Mechanics. N.p., 14 Oct. 2016. Web. 05 May 2017.

Martin, G. (2006). *Understanding terrorism: Challenges, perspectives, and issues* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Martinez, Michael; Shoichet, Catherine E.; Brown, Pamela (December 9, 2015). "San Bernardino shooting: Couple radicalized before they met, FBI says". CNN.

McCormick, G. H. "Terrorist Decision Making," Annual Review of Political Science 6 (2003): 473–507.

McManus, Brian. "An Experts Analysis: How Social Media Can Lead to the 'Self-Radicalization' of Terrorists." *VICE*. N.p., 07 Dec. 2015. Web. 04 Aug. 2016. <http://www.vice.com/read/we-asked-an-expert-how-social-media-can-help-radicalize-terrorists>.

"Mississippi Woman Who Attempted to Join ISIS Pleads Guilty to Terror Charge." Conspiracies - Plots. *Fox News*. N.p., 30 Mar. 2016. Web. 13 Jan. 2017. <http://www.foxnews.com/us/2016/03/30/mississippi-woman-who-attempted-to-join-isis-pleads-guilty-to-terror-charge.html>.

Moghaddam, A. (2006). Suicide terrorism, occupation and the globalization of martyrdom: A critique of dying to win. *Studies in Conflict and Terrorism*, 29(8), 707-729. doi: 10.1080/10576100600561907

Mozingo, Joe (2016). "'The worst thing imaginable:' Bodies and blood everywhere after San Bernardino terrorist attack, DOJ report shows". The Los Angeles Times. Retrieved April 5, 2017.

Murdoch, S. J., & Danezis, G. (2005). *Low-cost traffic analysis of TOR.* Paper presented at the 2005 IEEE Symposium on Security and Privacy, Oakland, CA. doi:10.1109/SP.2005.12

Nakashima, Ellen. "FBI Paid Professional Hackers One-time Fee to Crack San Bernardino IPhone." The Washington Post. WP Company, 12 Apr. 2016. Web. 02 May 2017.

Neo, Loo Seng. "Chapter 11: An Internet- Mediated Pathway for Online Radicalisation: RECRO." *Combating Violent Extremism and Radicalisation in the Digital Era*. Hershey, PA: Information Science Reference, An Imprint of IGI Global, 2016. 197-223. Print.

Neo, Leo, Leevia Dillon, Priscilla Shi, Jethro Tan, Yingmin Wang, and Danielle Gomes. "Chapter 1: Understanding the Psychology of Persuasive Violent Extremist Online Platforms." *Combating Violent Extremism and Radicalisation in a Digital Era*. Hersey, PA: IGI Global, 2016. 1-12. Print.

Neumann, Peter. *Countering Online Radicalisation In America*. London, England: ICSR, King's College London, 2012. *Bipartisan Policy Center*. Web. 2 Feb. 2017. <http://bipartisanpolicy.org/blog/whats-new-homeland-security-project/>.

"Online Radicalization to Violent Extremism." Responding to the Threat of Violent Extremism: Failing to Prevent (2014): 1-4. Www.cops.usdoj.gov. U.S. Department of Justice, 2014. Web. 12 June 2017. <http://www.theiacp.org/portals/0/pdfs/RadicalizationtoViolentExtremismAwarenessBrief.pdf>.

Paloutzian, Raymond F., and Crystal L. Park. *Handbook of the Psychology of Religion and Spirituality*. 2nd ed. New York & London: Guilford, 2013. Print.

Precht, T. (2007). *Home grown terrorism and Islamist radicalization in Europe: From conversion to terrorism.* Denmark: Danish Ministry of Justice.

Press, The Association. "Jaelyn Young to Plead Guilty to Terrorism Charge: Mississippi Woman Planned to Join ISIS." AL.com. N.p., 29 Mar. 2016. Web. 23 May 2017.

‘‘Radical, adj. and n.,” Oxford English Dictionary, September 2009.

Ramakrishna, K. (2007). *Self-radicalisation: The case of Abdul Bashee Abdul Kader. RSIS Commentaries (61/2007).* Singapore: S. Rajaratnam School of International Studies

Ramakrishna, Kumar. "Chapter 13: Towards a Comprehensive Approach to Combating Violent Extremist Ideology in the Digital Space: The Counter - Ideological Response (CIR) Model." *Combating Violent Extremism and Radicalization in the Digital Era*. Hershey, PA: Information Science Reference, An Imprint of IGI Global, 2016. 260-78. Print.

RAND: National Security Research Division. *De-radicalizing Islamists Extremist.2010*

Richey, Warren. "Eight Faces of ISIS in America." The Christian Science Monitor. The Christian Science Monitor, 29 Sept. 2015. Web. 23 May 2017.

Rosenfeld, Everette. "Upwards of 14 people dead in San Bernardino mass shooting: Police department chief". CNBC. Retrieved March 23, 2017

Ryan, David L. "Prosecutors Detail Roslindale Man's Decapitation Plot - The Boston Globe." BostonGlobe.com. N.p., 03 June 2015. Web. 15 May 2017.

Sageman, Marc. Understanding Terror Networks. Philadelphia: U of Pennsylvania, 2011. Print.

Sageman, Marc. Complex Social and Value Networks: The Jihad Case. N.d

Saltman, Erin Marie. "Chapter 10: Western Female Migrants to ISIS:Propaganda, Radicalisation, and Recruitment." *Combating Violent Extremism and Radicalisation in a Digital Era*. Hersey, PA: IGI Global, 2016. 174-93. Print.

Schmid, A.P. (2013). *Radicalisation, de-radicalisation and counter-radicalisation: A conceptual discussion and literature review.* The Hague: ICCT.

Schneier, B. (2007). Did NSA put a secret back door in new encryption standard?*Wired*.Retrieved:http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115

Sedgwick, Mark (2010) 'The Concept of Radicalization as a Source of Confusion', Terrorism and PoliticalViolence, 22: 4, 479 — 494

Shi, Priscilla. "Chapter 20: A Supplementary Intervention to Deradicalisation: CBT- Based Online Forum." *Combating Violent Extremism and Radicalization in the Digital Era*. Hershey, PA: Information Science Reference, An Imprint of IGI Global, 2016. 410-19. Print.

Soghoian, C. (2010). Caught in the cloud: Privacy, encryption and government back doors in the Web 2.0 era. *Journal on Telecommunications & High Technology Law*, 8, 359-423.

"Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States," White House, December 2011, p. 20.

"Terrorism Analysis: Mason Learning Solutions." *Terrorism Analysis: Mason LearningSolutions*. Web. 06 Sept. 2016. <http://ls.gmu.edu/programs/health_public_safety/terrorism_analysis.php>.

The Economist. *"The myth of cyber-security."* Volume 423. Number 9035. 2017.

Thomas, E. F., Mcgarty, C., & Louis, W. (2014). Social interaction and psychological pathways to political engagement and extremism. *European Journal of Social Psychology*, 44(1), 15-22. doi: 10.1002/ejsp.1988

Torres-Soriano, M. R. (2012). The Vulnerabilities of online terrorism. Studies in Conflict and Terrorism,35(4),263-277.Doi: 10.1080/1057610X.2012.656345

Torok, Robyn. "Chapter 3: Social Media and the Use of Discursive Markers of Online Extremism and Recruitment." *Combating Violent Extremism and Radicalisation in a Digital Era*. Hershey, PA: IGI Global, 2016. 39-66. Print.

Torok, Robyn. (2013). Developing an explanatory model for the process of online radicalisation and terrorism. *Security Informatics*, 2(6).

Torok, Robyn. (2011). *The online institution: Psychiatric power as an explanatory model for the normalisation of radicalisation and terrorism.* Paper presented at the European Intelligence and Security Informatics Conference (EISIC), Athens, Greece. doi: 10.1109/EISIC.2011.43

"Two Men Charged with Conspiracy to Provide Material Support to Islamic State." The United States Department of Justice. N.p., 12 June 2015. Web. 15 May 2017. <https://www.justice.gov/opa/pr/two-men-charged-conspiracy-provide-material-support-islamic-state>.

USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 215.

U.S.A v. JAELYN DELSHAUN YOUNG and MUHAMMAD ODA DAKHLALLA. 22. United States District Court. 21 May 2015. *The United States Department of Justice*. N.p., n.d. Web. 21 June 2017. <https://www.justice.gov/opa/file/705906/download>.

Veldhuis, Tinka, and Jørgen Staun. *Islamist Radicalisation: A Root Cause Model*. Den Haag: Netherlands Institute of International Relations Clingendael, 2009. Oct. 2009. Web. 16 Mar. 2017.

Vidino, Lorenzo. "Countering Radicalization in America: Lessons from Europe." *Special Report* 262 (2010): 1-16. *www.usip.org*. United States Institute of Peace, Nov. 2010. Web. 23 Feb. 2017.<https://www.usip.org/sites/default/files/SR262%20%20Countering_Radicalization_in_America.pdf>.

Vidino, Lorenzo. *Explaining the Lack of an American Domestic Counter-radicalization Strategy.* N.d, 1-10. < http://www.mei.edu/sites/default/files/Vidino.pdf>

Vidino, Lorenzo, and Seamus Hughes. *"Countering Violent Extremism in America." Center for Cyber and Homeland Security (2015): 1-23. The George Washington University. Web. 23 Feb. 2017*

Vidino, Lorenzo, and Seamus Hughes. *"ISIS In America: From Retweets to Raqqa."* Program on Extremism (2015): 1-50. The George Washington University. Web. 1 May. 2017

Weimann, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research*, 3(2), 75-90. doi: 10. 15664/jtr.405

Weinberg, Leonard et al., "The Challenges of Conceptualizing Terrorism," Terrorism and Political Violence, vol. 16, no. 4 (2004), pp. 777-794.

Williams, Wayne. "Why Apple Is Right to Reject the Order to Unlock a Killer Phone." Betanews.com. N.p., 2016. Web. 2 May 2017.