

# **Online Violent Radicalisation (OVeR): Challenges facing Law Enforcement Agencies and Policy Stakeholders**

*Bruce McFarlane*

*Researcher, Global Terrorism Research Centre and Politics Department  
Monash University*

## Abstract

This paper highlights contemporary challenges faced by law enforcement agencies and policy makers (stakeholders) relating to online violent radicalisation (OVeR). The aim of this paper is to generate and stimulate further discussion, debate and dialogue with stakeholders; and to assist future pro-active management strategies relating to this phenomenon. Focusing on the ‘online’ element of violent extremism, this paper will examine themes such as online anonymity, manipulation of online media, online violent messages and content and will explore these issues via the case study of Roshonara Choudhry.

Keywords: Radicalisation, Violent Extremism, Internet, Online, YouTube, Inspire Magazine

(Note: The author recognises the assistance received from Professor Greg Barton, Chris Heffelfinger and Dr John Horgan in framing this paper. All online references were accurate and accessible at the time of paper submission.)

*‘The growth of the internet has dramatically transformed the structure and dynamic of the evolving threat of global Islamist terrorism by changing the nature of terrorists’ interactions. The nature of this influence is still misunderstood both by the terrorists themselves and by the people who are fighting them.’*

*– Marc Sageman (Sageman, 2008: 109)*

## **1. Introduction**

It is unquestionable that the internet has had a profound and dramatic impact on how we interact and communicate with each other around the world. As consumers, we demand faster bandwidth speed, higher usage caps and increased connectivity to everyday items, ranging from mobile phones, gaming consoles to even refrigerators. We utilise the internet to conduct research, communicate with friends, manage businesses and network with likeminded individuals. Therefore it should be to no one’s surprise that the violent extremist utilises the internet in much the same manner.

The use of the internet in facilitating terrorism and violent extremism has been previously well documented by academics and authors such as Sageman (2008) and Weimann (2006). This paper will explore contemporary challengers facing law enforcement agencies (LEAs) and policy makers (both referred to herein as stakeholders), within Australia and abroad, in combating online violent extremism. Specifically, using the case study of Roshonara Choudhry this paper focuses on drivers such as online anonymity, manipulation of online media, and the interaction of individuals communicating online violent content. By focusing on the uses and drivers that motivate individuals to utilise online communication to facilitate violent acts, we place ourselves in a better position to identify the challengers and barriers stakeholder's face in combating this growing phenomena.

The specific nature of terrorism and violent extremism can take on many forms. Ecological, ethno-nationalist, State sponsored, animal rights or ideological/political/religious based violent extremism can all fall under the banner of terrorism. However, this paper will primarily concentrate on and refer to Neo-jihadist<sup>1</sup> forms of violence and extremism, noting that '78% of all global neo-jihadi terrorist plots in the West in the past five years came from autonomous home grown groups without any connection, direction or control from al-Qaeda Core or its allies.' (Sageman, 2009: 11) This is not to say that the themes explored in this paper are not applicable to some, if not all, other forms of violent extremism such as the ones mentioned above.

This paper predominately focuses on the 'online' component of violent extremism. It is important to note that radicalisation via online interaction, in the majority of cases, is not the sole determining factor that leads to an individual to commit acts of violence for their cause. (Bergin et al., 2009a: 4) Physical real world interaction and networks is, and still remains a vital ingredient for this development to foster and propagate. The internet is however, becoming an ever increasing and important tool, as a means to facilitate this process. (Stevens and Neumann, 2009: 11, Wilton Park, 2011: 9)

---

<sup>1</sup>The term *Neo-jihadism*, coined by Lentini, within the context of this paper refers to "simultaneously a religious, political, paramilitary and terrorist global movement, a subculture, a counterculture, and an ideology that seeks to establish states governed by laws according to the dictates of selectively literal interpretations of the Qur'an and the traditions of the Prophet Muhammad (normally) through enacting violence' and 'combines modern and postmodern re-interpretations of jihad that emphasize and elevate violent, offensive military actions over other forms of struggle which have been established in over a millennium-and-a-half of Islamic theology and jurisprudence.....(t)hey claim that all their actions are defensive, and that non-combatants are legitimate targets.' BRASHER, B. E. 2004. *Give Me That Online Religion*, New Brunswick, Rutgers University Press.

The physical and psychological development of radicalisation itself falls outside the scope of this paper; however the term, and use of the term, ‘radicalisation’ (as a definition and a process) is briefly discussed. It is also acknowledged that the number of individuals radicalised to point of committing violent acts, is in fact, quite rare. The number who are radicalised purely as a result of the online content they consume, is rarer still and therefore in-depth details surrounding these individuals are limited.

## **2. Online Violent Radicalisation (*OVeR*)**

To better understand the concepts outlined in this paper, the term ‘*Online Violent Radicalisation*’ (*OVeR*), requires defining. The definition of *OVeR* within this paper is intentionally narrow and restrictive in order to practically discuss the phenomena and the associated challenges facing stakeholders; not to enter into exhaustive theoretical debate in relation to the use of these terms.

*OVeR* may be best defined if broken down into its three broad themes: “online”, “violent (extremist)”, “radicalisation”.

This paper defines the ‘*online*’ component as: *human communication, exchanging information and connectivity via: emails, websites, peer to peer networks, bit torrents, Internet Relay Chat (IRC), Voice Over I.P (VoIP), social networking sites and online forums.*

The term ‘radicalisation’ is the most difficult of the above terms to define within this paper. Just as the term *terrorism* is subjective and dynamic in nature, so to, is the term *radicalisation*. Radicalisation is a term that is used liberally and generally within law enforcement and security stakeholders alike and creates much debate.

Within the scope of this paper, we are obviously referring to the, ‘radical as extremist’ notion of radicalisation that leads to violence. ‘To be radical is to be extreme relative to something that is defined or accepted as normative, traditional, or valued as the status quo.’ (Mandel, 2010: 9)

Radicalisation refers to *an individual, or group, developing, adopting, supporting and/or advancing belief systems and behaviours which conflict with normative societal behaviour.* (Monash Radicalisation Project, 2011) Radicalisation, or radical behaviour/thoughts, without the use or threat of violence, may not necessarily be considered problematic within society as

it underpins the notion of free democratic speech. However when individuals/groups utilise or incite acts of violence to further their cause, stakeholders are required to act.

The radicalisation process, as a process, is well documented and recognised by counter terrorism scholars. Pyramids, staircases and funnels (Moskalenko and McCauley, 2009: 241, Moghaddam, 2005, Silber and Bhatt, 2007: 10, Clutterbuck, 2010: 157) have all been utilised as metaphors to conceptualise radicalisation as a *process*, however ‘there is not complete agreement over what such a process, or indeed the term radicalization, actually entails’. (King and Taylor, 2011: 212) Scholars have debated whether the use of the term merely adds to the confusion in the development of counter terrorism (Richards, 2011) and that ‘[n]o one model can be distinguished as being more accurate than the other.’ (King and Taylor, 2011: 615) Despite these failings, these current models of understanding have made significantly contributions in conceptualising our understanding of the radicalisation process, albeit possibly raising more questions than answers.

‘Violent extremism’ can encompass a multitude of behavioural characteristics and be defined in many ways. For this paper ‘violent extremism’ is defined as: *any behaviour that encourages, seeks, promotes or justifies the use of violence of any kind in furtherance of particular beliefs.*(Crown Prosecution Service, 2010)

In light of above, *OVeR* can best be described as: *the use of online communication systems as a means to facilitate, and/or influence individuals or groups, in developing, adopting, and/or advancing belief systems which lay outside the relative norms of mainstream society resulting in the advocacy of threats, and/or physical acts, of violence, to further that belief system.* The use of the term ‘*mainstream society*’ is once again a subjective term and refers to Australian ‘*mainstream society*’.

### **3. Drivers Associated with OVeR:**

Violent extremists predominately utilise the internet for the following five<sup>2</sup> operational purposes:

1. Recruitment;

---

<sup>2</sup> The sixth use ‘cyber-terrorism’ has been omitted due to lack of evidence that the use of the internet has been used by violent extremist organisations in any significant way as a weapon or means to seriously disrupt critical infrastructure to cause fear in any population. This is not to say that cyber-terrorism will not be an operational tactic by violent extremist groups in the future as they become more sophisticated in their tactical methodology.

2. Propaganda;
3. Fundraising;
4. Information/Intelligence, and
5. Communications (Weimann, 2004, Sageman, 2008)

Each of these uses have remained relatively unchanged over the past decade, however the drivers and online content associated with these categories are dynamic in nature and provide stakeholders with a window on the issues that affect *OVeR*. Examples of such drivers include: anonymity on the internet, the manipulation of online media and *OVeR* content. Some, if not all, of the above categories and drivers can be present at some stage during *OVeR* development. (*See Appendix 1 for further online drivers*) It is these drivers which are proving difficult for LEAs to police effectively and legislate against.

### **Anonymity on the Internet:**

In utilising the internet, violent extremism varies little from other online crimes such as online fraud, online child sex offending or even the selling/distribution of drugs in utilising new and emerging technology. Criminal elements, including violent extremists, utilise the internet in similar ways in exploiting new technologies to assist them in committing crimes, communicating with each other and to assist in avoiding detection.

Due to the decentralised nature of the online world, merely communicating online lends itself to individuals to believe they are anonymous. ‘Because of its apparent anonymity, people are more likely to self-disclose via computer mediated technology, which contributes to feelings of greater intimacy.’ (Sageman, 2008: 115) This phenomenon is not new nor confined to *OVeR*. ‘Anonymity is a unique aspect of the internet that may help potential offenders’ [online child sex offenders] ability to commit sex crimes against minors.’ (Mitchell et al., 2010: 417) The internet has the ability to create a perception of deeper, more personal relationships where users report an increased ability to be confident; self-disclose and take interpersonal risks online. (Bergin et al., 2009b)

Seemingly intelligent and astute individuals who would never normally engage in criminal or risky behaviour in the physical world, appear to confide in the safety of their surrounding online environment, whether it be at home or at an internet café, and can form strong online relationships over a period of time or even in just a few hours. ‘People engage in these tasks through the internet because its qualities allow for anonymity, its uniqueness of socialising means, and its ability to close geographical and time constraints.’ (Lennings et al., 2010)

The utilisation of Internet Protocol address (IP address) cloaking and obfuscation techniques add to the notion of anonymity.<sup>3</sup> Online anonymity can, and does, play a vital and legitimate role in assisting and promoting political free speech within in nation States wishing to suppress dissent or anti-government opposition. However these same techniques are employed by criminals, and violent extremist alike, in an effort to mask their physical location and avoid detection from LEAs as the following examples illustrates.

Figure 1 and 2, below, depict a user on the pro-violent jihadist website, *Ansar Al-Mujahideen*. The user of the website encourages other online users to use caution when downloading ‘The Explosives Course’ instruction manual and for users to utilise anonymising software when downloading the file in order to prevent LEA in identifying the physical location of the user accessing the material.

Even with limited knowledge of the internet, users can quickly access and utilise IP anonymising technology to obfuscate their physical IP address in an attempt to evade LEA detection.

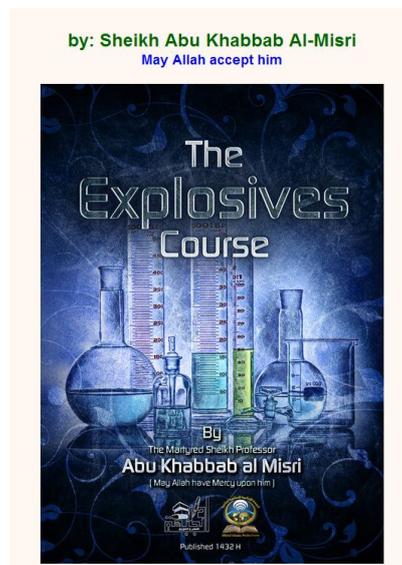


Figure 1.(Unknown Author, 2010)

---

<sup>3</sup> An IP address is a numerically unique identifier allocated to each online device (computer, mobile phone etc) in order for the device to communicate with the internet, similar to a telephone number. Individual Internet Service Providers (ISPs) keep a register of allotted IP addresses assigned to individual users for billing purposes, which enables LEA, with the correct authorisation, to determine who utilised an IP address and any given date and time.

To Download: PDF 5 MB  
Please use precautions when downloading by using appropriate anonymizing software

*Figure 2. (Unknown Author, 2010)*

For criminals and violent extremist this anonymity (or perceived anonymity) and safety net extends the feeling of security as the chance of being detected and prosecuted by LEA is made more unlikely by the use of such methods.

Whether perceived or real, anonymity on the internet presents itself as a major challenge to LEA in combating online criminal activity. Users are under the perception that they are operating in a safe and secure environment and that there will little or no consequences in their extreme online engagement and therefore little deterrence to cease from doing so. The result is potentially large numbers of users who would not normally engage in accessing this material, comforted by the fact that their behaviour will go unnoticed and undetected. For the more security conscious who utilise IP anonymisers, it not only intensifies this perception, but also in reality will inhibit LEA in conducting timely and effective online investigation enquiries.

Even when ‘users of interest’ are identifiable within their own jurisdiction, LEAs then face the challenge of establishing whether the individual poses a threat to the community or simply expressing radical ideology and stop short in promoting violent means.

### **Manipulation of Online Media**

The ease with which information can be manipulated and distributed via the internet is also an attractive feature for violent extremists and it plays a critical role within *OVeR* development. The nature of the internet lends itself to little, at best ‘self’ regulation where the violent extremist message can be published to a global audience in an instant with limited opportunity for stakeholders to counter the message. Radical ideology, belief systems and skewed interpretation of facts can be disseminated globally to a wide and varied target audience with very little if any counter narrative.

The Special Edition of the Yemeni based ‘Inspire Magazine’ illustrated this point after the 2010 attempted bombing of commercial and cargo UPS flights originating out of Yemen. In terms of propaganda and psychological warfare outcomes, Al-Qaeda in the Arabian Peninsula

(AQAP) claimed the operation a complete success. The magazine quoted one of the attackers saying the aim of the operation was to cause maximum disruption and financial loss within the aviation and security industry: ‘We knew that cargo planes were staffed by only a pilot and a co-pilot so our objective was not to cause maximum casualties but to cause maximum losses to the American economy.’(AQAP, 2010b p.7) Yet, if the devices on-board each flight had detonated, there is no doubt the AQAP would have also celebrated their achievements to the world as an overwhelming success. For AQAP, this operation was a win-win situation.

However paradoxically in this same edition of Inspire Magazine, AQAP claimed responsibility for the downing of a similar UPS cargo plane resulting in the death of two crew members in October 2010 stating, ‘We, in the al Qaeda of the Arabian Peninsula would like to convey to our nation the glad news and the awaited surprise: We have been enabled by Allah to blow-up a UPS cargo plane on the 3rd of September, 2010, after its take-off from Dubai International Airport.’ (AQAP, 2010b p.4) This statement contradicts their earlier statement of their aim was not cause casualties but to inflict maximum losses to the US economy.

### **Distribution of Violent Extremist Material**

The easy and mass distribution of online violent extremist material, such as the ‘Inspire Magazine’, is another driver that poses considerable problems for stakeholders.

*Figure 3* presented below represents a snapshot that illustrates how online violent extremists disseminate their message, in this case the ‘Inspire Magazine’ to multiple online depositories.



Figure 3. (AQAP, 2010a)

By utilising multiple source depositories for their material, violent extremists create difficulties for LEA in disrupting the distribution of such material due to the vast circulation networks over multiple free file sharing services. Violent extremist material is also offered in various digital resolution qualities (High, Medium, Low) as well as in a variety of formats (PDF, Word, movie and audio formats) to cater to the preference of the user.

### **OVeR Content/Message/Audience**

Online instruction, tuition and violent ideological rhetoric is not new to online jihadist material distribution networks, however *Inspire Magazine's* combination of contemporary content, message and targeted audience does represent a distinct change in target audience, physical appearance, content and message. Traditionally, online neo-jihadist propaganda has only been available in Arabic, has been visually unappealing, is text heavy to read and difficult to source online. Examples such as *Al-battar Training Camp* and the Taliban *al-Somood* online journals have been available since 2004 and 2006 respectively however, have gained little media attention outside scholarly, LEA circles. However, the publication of the first and subsequent issues of *Inspire Magazine* has brought with it, its own unique challengers for stakeholders.

The magazine was initially released in English but is now available in Arabic, Russian, Indonesian and Urdu to engage with the widest audience possible. Given this trend, it is highly likely that the magazine will continue to expand the number of languages published, possibly to include other European, African, Asia and Pacific languages.

The magazine is also a break away from traditional violent extremist texts. Its main target audience focuses on a young Western Muslim diaspora, utilising visual eye catching fonts, banners and backgrounds to complement the contemporary content of its extremist message. Magazine message content often comprises of simplistic, concise narratives to explain

complex global problems. Messages that appeal to those seeking quick answers to injustices (or perceived injustices) occurring around the world.

The magazine contains articles of detailed personally narrated stories calling on the all Muslims to pursue personal jihad on Western targets and civilians, as well as stories of global events, that can be attributed to the West coupled with specific detail on how to attack and kill the 'kuffar'. Other examples include Figures 4 and 5, as follows:

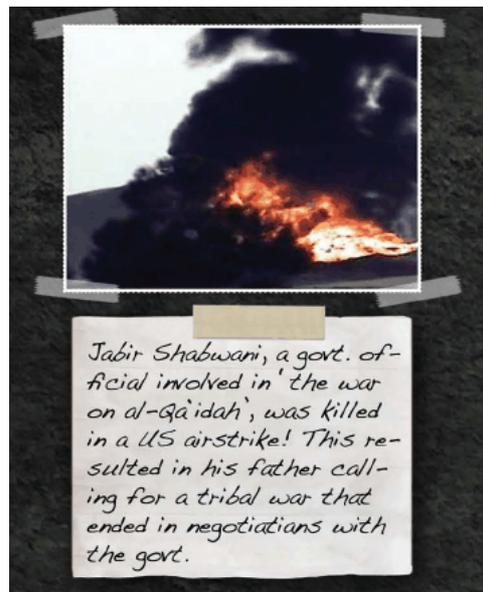


Figure 4. (The AQ Chef, 2010)

Afterlife. My Muslim brother: we are conveying to you our military training right into your kitchen to relieve you of the difficulty of traveling to us. If you are sincere in your intentions to serve the religion of Allāh ﷻ, then all what you have to do is enter your kitchen and make an explosive device that would damage the enemy if you put your trust in Allāh ﷻ and then use this explosive device properly. Here are the main qualities of this bomb:

- Its ingredients are readily available.
- Buying these ingredients does not raise suspicion.
- It is easily disposed of if the enemy searches your home. Sniffing dogs are not trained to recognize them as bomb making ingredients.
- In one or two days the bomb could be ready to kill at least ten people. In a month you may make a bigger and more lethal bomb that could kill tens of people.

Figure 5. (The AQ Chef, 2010)

A worrying finding from a study conducted by Lee and Leets (2002) relating to the persuasiveness of online hate groups on young adolescent teens noted, 'Of additional concern, neutral adolescents appear vulnerable to hate groups' persuasive strategies. Both high-narrative (text rich) and implicit message (graphical rich) approaches swayed them, with the two strategies interacting for greater persuasion.' (Lee and Leets, 2002) It is argued by academics such as Sageman (2008), that violent extremist material is traditionally sort after

by those who have already ascribed to, or biased toward, the cause and stakeholders should be concentrate their efforts in countering the narrative to prevent individuals or groups from getting to this point of radicalisation development. Lee and Leets study suggests that neutrally adolescent youth who are uncommitted, but curious, may be particular vulnerable to such material. It is noted that this study was conducted with teenagers between the ages of 13 and 17 years and did not focus on jihadi specific websites however, the study highlights the risks of online violent content may pose to stakeholders in the development of *OVeR* due to its high profile and ease of online access. Lee and Leets' research also highlights the lack of research in area of online viewing habits and its behavioural and cognitive effect on individuals of time.

Unlike traditional Islamic violent extremist material, the magazine is relatively easy to locate and access online via numerous non-jihadist based websites. In distributing online violent extremist material, individuals are encouraged to spread violent extremist material to as far and wide as possible within mainstream media jihadist based websites and within likeminded online social networks. This serves three main purposes.

First, it allows for a wide distribution network to reach the largest audience possible, with or without the assistance of mainstream media. 'The increasing use of the internet by reporters and journalists serves to create a "two-step flow" of information: terrorist to journalist, via the internet, to the public.' (Weimann, 2006: 109) It raises further global awareness and exacerbates the distribution of this material through the "journalist, via the internet, to the public". (Weimann, 2006: 109)

Second, it self-promotes, highlights and, in the eyes of the violent extremist, legitimises their violent message via mainstream media distribution, online or otherwise, by acknowledging their message. Previous online jihadist based material has been relatively difficult to locate with users having to locate and gain access to *source* documents via pro-violent Jihadi ideologist websites. These websites regularly restrict access, close down and reappear under different domain names making it difficult to track or be located if the user is not an active user within the network. However, due to wide spread mainstream reporting and online publishing of *Inspire*, it is widely available online and possible to obtain the material quickly from any number of non-jihadi specific websites promoted as *for educational purposes only*. (See Figure 7. below)

Finally, in combination with the above two points, the mass distribution and mass media attention could indirectly act as a recruiting tool. For individuals who are searching for religious/political alternatives or individuals who hold non-violent radical ideological beliefs and encounter this material, the magazine could act as one more piece of the jigsaw in the radicalisation path in encouraging the individual to take the next step toward legitimising violent behaviour. (Lenhart et al., 2011, The Message, 2012, Brasher, 2004)

Figure 6 and 7 below are two snapshots of conversations between a Junior Member and Moderator from a mainstream online Australian political forum, “OzPolitic”. This brief, but worrying conversation illustrates the above observations.

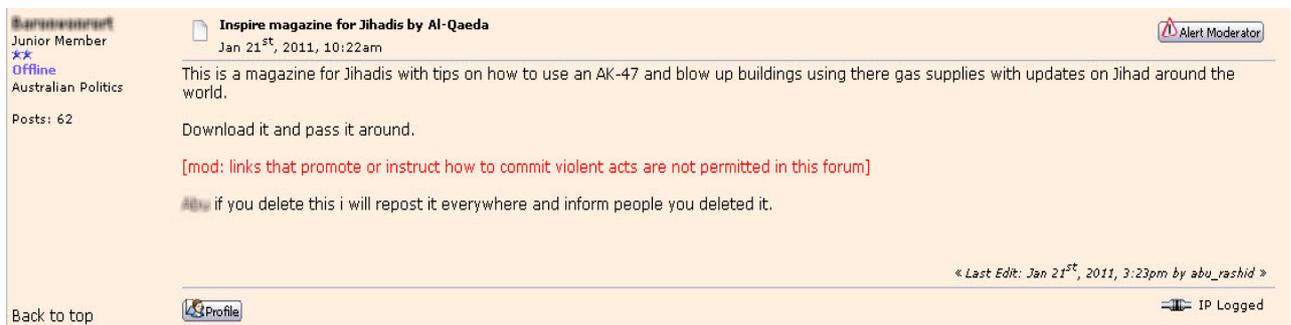


Figure 6. (Junior Member, 2011)

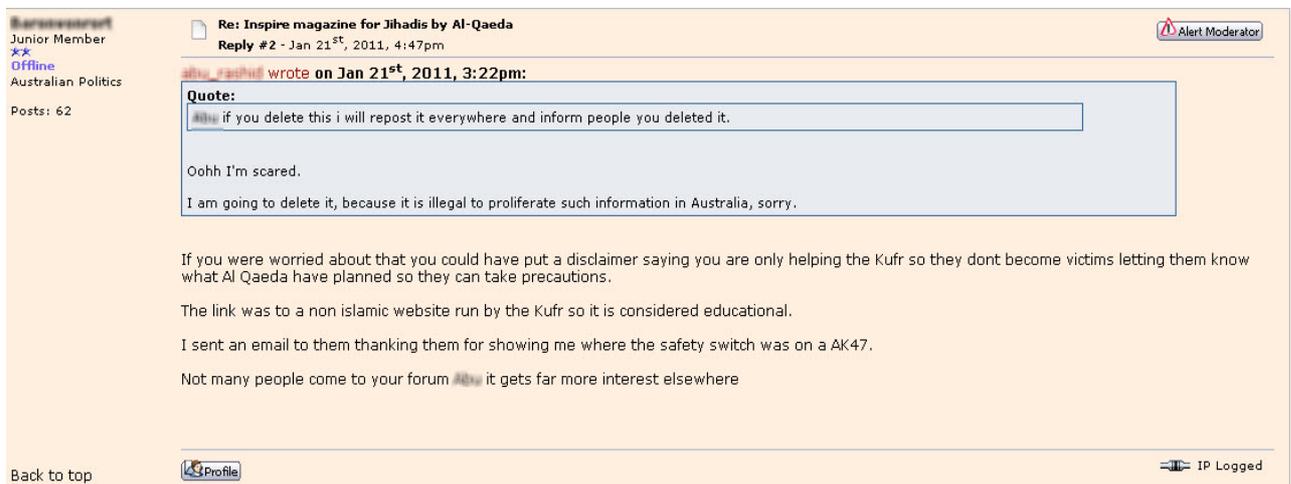


Figure 7. (Junior Member, 2011)

What is clear from the conversation, the Junior Member is attempting to distribute the *Inspire Magazine* within the forum website which is blocked by the site Moderator. The Junior member points out that he obtained the file via a ‘non-Islamic’ website and he therefore

considers it to be ‘educational’ material and claims he even thanked the site for showing him where the “safety switch was on a AK47.”

### **3. Case Study – Roshonara Choudhry**

Earlier this paper outlined that *radicalisation via online interaction, in the vast majority of cases, is not the sole determining factor that leads to an individual to commit acts of violence for their cause.* The number individuals who are radicalised purely as a result of the online content they consume, is exceptionally rare. However the case of 21 year old Roshonara Choudhry is one of those exceptions and raises a number of questions and provides an insight into the complexities of exploring cognitive biases and violent extremism in the online world. Roshanara Choudhry met with, and then stabbed, British Labour MP, Steven Timms, due to his endorsement of the coalition invasion of Iraq.

A report by the International Centre for the Study of Radicalisation and Political Violence stated: ‘It will be shown that the internet can play a role in radicalisation, but that so far it has not been the principal driver of the process. Furthermore it will be demonstrated that the process of radicalisation – even where it has a virtual dimension – remains rooted in the real world.’ (Stevens and Neumann, 2009) The role of the internet, in Choudhry’s case, demonstrates that this is not always the case and the internet appears to have played an instrumental role and substantial driver in the attempted murder of Steven Timms.

By her own admissions<sup>4</sup>, Choudhry became radicalised by viewing the online lectures of Anwar al-Awlaki on the social networking site, YouTube. After viewing al-Awlaki material and researching websites promoting violent extremism, she discontinued she studies at Kings College, London, purchased several kitchen knives, and then met and stabbed Mr Timms at an official function. Again by Choudhry’s own account, from beginning to end, this radical development resulting in violence took place in within a six month time frame.

Excerpts from her formal police interview reveal that Choudhry, a second generation UK citizen with Bangladeshi heritage, appeared to have self-radicalised purely as a direct result of her online viewing habits.

Sageman (2008) argues that individuals viewing static or *passive* website information, such as a general informational website, do not suddenly consolidate their views into extreme

---

<sup>4</sup> For detailed police interview extracts see: DODD, V. 2010. Roshonara Choudhry: Police interview extracts. *The Guardian*, 16/12/2010.

thoughts which materialise in extreme violent behaviour just in a same way that by reading newspapers articles or books will not change a social behaviour. ‘They usually read what conforms to their original bias, and thereby only confirm their views, which were created *elsewhere*’ (Sageman, 2008: 144) Choudhry’s interview reveals how the nature of User Generated Content (UGC) online social networking forums, such as YouTube, is changing the way individuals interact online and the possibility of its content influencing their cognitive behaviour or at very least, their online viewing behaviour. Sageman’s ‘*elsewhere*’ is YouTube, Facebook, MySpace and Tweeter.

In analysing the comments Choudhary made during her interview, she claims to have accessed YouTube to view how other individuals found their path to Islam and she wasn’t actively searching for al-Awlaki sermons. (Dodd, 2010) Users of YouTube quickly discover that the original search term entered into the site, compared to the end result of what the individual actually ends up viewing, can be two totally different subject topics and not related at all to the original search term at all. This can be due to many different variables such as YouTube’s site presentation of providing related subject movies down the right hand side of the site, the site algorithm used to search for keywords and the searchable tags users can attach to their uploaded movie.

Choudhary initially had no conscionable interest in viewing sermons by al-Awlaki. ‘I wasn’t searching for him, I just came across him’ (Dodd, 2010) What is not yet clear from these excerpts is the process used by Choudhary when interacting with the YouTube site. Was Choudhary a registered user of the YouTube site? Did she interact and upload her own movie files to the site or did she merely just view the content posted by others? What were the exact search terms she originally used to locate the content she was looking for within the site? And how did these search terms vary over the time period she claims to have being radicalised online?

The use of the internet to reinforce, or even develop, violent extremist ideological biases is a disturbing feature that may pose stakeholders with even more difficulties in the near future. We are now entering the era of Generation Z (individuals born after 1990), or the *NetGeneration*, and it is a generation that is already finding it difficult to distinguish between the online and physical world as the two worlds are become increasing blurred. Within

Western society, Generation Z users dominate the online world within social networking.<sup>5</sup> Sites such as Facebook and Twitter are fast becoming the primary source of social contact between online ‘friends’. In only seven years since its inception Facebook has over 800 million *active* users (Facebook, 2011), for comparison if Facebook was a country it would be the third largest country in the world, behind India and China.

It is important for academics, and investigators alike, to discover the user’s relationship with each site visited, and detail their online activities, when attempting to understand the true drivers and motivations behind individuals espousing views of a violent extremist nature online. Research that explores these questions will provide insight to individual cognitive thought processes, and better equip LEA to develop an effective, pragmatic approach to deal with the *OVeR* phenomena.

Choudhary’s case highlights the evolution of what is referred to as the ‘*Sheikh Google*’ phenomenon. Individuals living in the West find themselves more and more time poor, but still require answers to complex global problems instantly or are simply too embarrassed to ask. Individuals are increasing turning to search engines and websites for answers, bypassing independent or third party clarification regarding scholarly issues. (The Message, 2012)

A comparable phenomenon of information quest can be found in other areas such as the medical profession.

'Doctors are warning of catastrophic consequences after new research revealed four in five Australians are turning to the web for health information and nearly half of those are using Dr Google to make a self-diagnosis. Dr Steve Hambleton, federal vice-president of the AMA, said the "information explosion" on the internet had spawned many great sources of medical advice but also copious amounts of bad information.'

(Moses, 2011)

The same analogy can be used for individuals seeking religious answers to their ever complicated lives. (Brasher, 2004, Lövheim, 2004) Individuals seeking scholarly religious advice online are all too often presented with extreme political and ideology views backed by simplistic self-justified, strict religious interpretation which may appeal to the individual,

---

<sup>5</sup> A 2011 Pew poll found that ‘95% of all teens ages 12-17 are now online and 80% of those online teens are users of social media sites.’ LENHART, A., MADDEN, M., SMITH, A., PURCELL, K., ZICKUHR, K. & RAINIE, L. 2011. Teens, Kindness and Cruelty on Social Network Sites: How American teens navigate the new world of "digital citizenship". Washington: Pew Research Center’s Internet & American Life Project.

leaving little narrative to counter such interpretations. (The Message, 2012, Leuprecht et al., 2009)

In 2010, AQAP made numerous online pleas for neo-jihadists around the world to kill the 'kuffar' (disbelievers) regardless of its permissibility or sanctioning within the Islamic religion. An article from the second edition of *Inspire Magazine* states, 'It is a simple idea and there is not much involved in its preparation. All what is needed is the willingness to give one's life for Allah. ....The idea is to use a pickup truck as a mowing machine, not to mow grass but mow down the enemies of Allah.' (Ibrhim, 2010) In November 2010, al-Awlaki released a 23 minute online movie file, in Arabic, in which he calls on Muslims to kill Americans regardless of whether they are military forces, civilians or otherwise. (Raddatz and Wong, 2010) He encourages Muslims not to seek religious guidance and states, "Don't consult with anybody in killing the Americans. Fighting the devil doesn't require consultation or prayers seeking divine guidance. They are the party of the devils". (AFP, 2010)

These pleas create a perception of self-proclaiming, self-sanctioning fatwa's (religious opinion within Islamic law). Individuals or groups seeking undertake violent acts in the name of religion would normally seek scholarly advice, discussion, debate and authority in order for the act to be sanctioned. (Pantucci, 2011) Al-Awlakis' tactical call for violent extremists to self-sanction, may lead to a considerable decrease in the timeframe of individuals or groups seeking and planning a violent act, to actually carrying out the act. This will ultimately result in diminishing LEAs ability in detecting, disrupting or preventing such acts. This timeframe is diminished even further when scenarios such as the 'pick-up truck idea' are encouraged as the tools, methods and strategies to execute such acts require little planning and are simple, quick and effective.

#### **4. Conclusion**

In this paper we have discussed how the internet plays an ever increasing and vital role as a means of communication within society and that we should expect violent extremists to utilise the internet in much the same manner. Therefore we should also expect the internet to play an ever increasing role in the development of *OVeR* in the future. The use of the internet in facilitating acts of terror is widely documented, and stakeholders should be mindful of its role in facilitating terrorist acts. However there is limited research on *OVeR(adical)* behaviour, how the internet affects individuals in the development of violent extremist

ideology and why some individuals may be more susceptible than others to online violent messages.

Individuals radicalising to the point of committing violent acts in the name of their cause facilitated solely via their online interaction, is rare and the internet's role in radicalising individuals may be overemphasised to some extent. However as physical battlegrounds diminish and online content such as *Inspire Magazine* becomes more prominent, case studies such as Roshonara Choudhry may represent the changing face of violent extremism in a younger generation that is increasingly looking toward the internet for answers.

The ever changing face of online communication and online social networking will continue to challenge law enforcement and policy makers in the years to come in all areas of criminality. Anonymity, information manipulation/dissemination and the relationship between individuals and online content all contribute to the development *OVeR* which can violently spill over into the real world. As these drivers change and evolve with the advancements in online technology and internet user interaction, stakeholders must place themselves in a position to change and evolve with it in order to combat online violent extremist content in the years to come.

**Appendix 1**

**Drivers influencing the use of online communications to facilitate Online Violent Radicalisation (*OVeR*), (McFarlane, 2010)**

FACTORS	DRIVER	ANALYSIS APPLICATION	
Political	Freedom of expression; Manipulation of information; Mass distribution networks, global audience.	RECRUITMENT	O V e R  D E V E L O P M E N T
Economic	Economically affordable to set up, access and maintain; Affordable access to vast amounts of information.	PROPAGANDA	
Social	Access to targeted global audience; Loss of traditional, physical environment; Improved social networks; Re-enforces ideological cognitive bias.	FUNDRAISING	
Technological	Various ways sharing information in secure/covert environment; Access to encryption software, proxy servers; Multiple methods of distribution; Capitalisation on emerging ICT development opportunities.	DIRECT ACTION	
Environmental	Logistically/geographically convenient; Instant access; Affords anonymity; Relatively little effort for great gain.	COMMUNICATIONS	
Legislative	Non-jurisdictional; Unable to be policed effectively; By-pass localised legislative requirements.	INTELLIGENCE	

## References:

- AFP. 2010. *Al-Awlaki urges American killings* [Online]. aljazeera. Available: <http://english.aljazeera.net/news/middleeast/2010/11/2010118204835107675.html> [Accessed 23/01/2011 2011].
- AQAP. 2010a. Inspire Magazine. [Accessed 23/01/2011].
- AQAP. 2010b. Operation Hemorrhage. *Inspire Magazine* [Online]. [Accessed 22/11/2010].
- BERGIN, A., BTE OSAM, S., UNGERER, C. & AZLIN MOHAMED YASIN, N. 2009a. Countering internet radicalisation in Southeast Asia. *Australian Strategic Policy Institute - Special Report*.
- BERGIN, A., BTE OSMAN, S., UNGERER, C. & YASIN, N. A. M. 2009b. Countering internet radicalisation in Southeast Asia. . Australian Strategic Policy Institute.
- BRASHER, B. E. 2004. *Give Me That Online Religion*, New Brunswick, Rutgers University Press.
- CLUTTERBUCK, L. 2010. An overview of violent jihad in the UK: radicalisation and the state response. *In: RANSTORP, M. (ed.) Understanding violent radicalisation: terrorist and jihadist movements in Europe*. New York: Routledge.
- CROWN PROSECUTION SERVICE. 2010. *CPS: Violent Extremism and Related Criminal Offences* [Online]. London: Crown Prosecution Service. Available: [http://www.cps.gov.uk/publications/prosecution/violent\\_extremism.html](http://www.cps.gov.uk/publications/prosecution/violent_extremism.html) [Accessed 20/02/2011 2010].
- DODD, V. 2010. Roshonara Choudhry: Police interview extracts. *The Guardian*, 16/12/2010.
- FACEBOOK. 2011. *Press Room - Statistics* [Online]. Available: <http://www.facebook.com/press/info.php?statistics> [Accessed 16/01/2011].
- IBRHIM, Y. 2010. The Ultimate Mowing Machine. *Inspire Magazine* [Online]. [Accessed 25/11/2010].
- JUNIOR MEMBER. 2011. *Inspire Magazine for Jihadis by Al-Qaeda* [Online]. OzPolitic. Available: <http://www.ozpolitic.com/forum/YaBB.pl?num=1295569322> [Accessed 13/02/2011 2011].
- KING, M. & TAYLOR, D. M. 2011. The Radicalization of Homegrown Jihadists: A Review of Theoretical Models and Social Psychological Evidence. *Terrorism and Political Violence*, 23, 602-622.
- LEE, E. & LEETS, L. 2002. Persuasive storytelling by hate groups online: Examining its effects on adolescents. *American Behavioral Scientist*, 45, 927-957.
- LENHART, A., MADDEN, M., SMITH, A., PURCELL, K., ZICKUHR, K. & RAINIE, L. 2011. Teens, Kindness and Cruelty on Social Network Sites: How American teens navigate the new world of "digital citizenship". Washington: Pew Research Center's Internet & American Life Project.
- LENNINGS, C. J., AMON, K. L., BRUMMERT, H. & LENNINGS, N. J. 2010. Grooming for Terror: The Internet and Young People. *Psychiatry Psychology and Law*, 17, 424-437.
- LEUPRECHT, C., HATALEY, T., MOSKALENKO, S. & MCCAULEY, C. 2009. Winning the Battle but Losing the War? Narrative and Counter-Narratives Strategy. *Perspectives On Terrorism*, 3.
- LÖVHEIM, M. 2004. Young People, Religious Identity and the Internet. *In: DAWSON, L. L. & DOUGLAS, E. C. (eds.) Religion Online: Finding Faith on the Internet*. New York: Routledge
- MANDEL, D. R. 2010. Radicalization: What does it mean? *In: PICK, T. M., SPECKHARD, A. & JACUCH, B. (eds.) Home-grown terrorism: Understanding and addressing the root causes of radicalisation among groups with an immigrant heritage in Europe*. Amsterdam: IOS Press - NATO Science for Peace and Security Series E: Human and Social Dynamics.
- MCFARLANE, B. 2010. *The role online communications play in facilitating terrorism*. Masters of Arts (Criminal Intelligence), Charles Sturt University.
- MITCHELL, K. J., FINKELHOR, D., JONES, L. M. & WOLAK, J. 2010. Growth and change in undercover online child exploitation investigations, 2000–2006. *Policing and Society*, 20, 416-431.
- MOGHADDAM, F. M. 2005. The Staircase to Terrorism: A Psychological Exploration. *American Psychologist*, 60, 161-169.
- MONASH RADICALISATION PROJECT. 2011. *Understanding Radicalisation, De-radicalisation and Counter-radicalisation from an Australian Perspective* [Online]. Monash Univeristy. Available: <http://www.arts.monash.edu.au/radicalisation/about-the-project/what-is-radicalisation.php> [Accessed 23/10/2011 2011].

- MOSES, A. 2011. Alarm sounded over Dr Google's diagnosis. *The Age*, 10/02/2011.
- MOSKALENKO, S. & MCCAULEY, C. 2009. Measuring Political Mobilization: The Distinction Between Activism and Radicalism. *Terrorism and Political Violence*, 21, 239-260.
- PANTUCCI, R. 2011. Operation Neath: Is Somalia's al-Shabaab Movement Active in Australia? *Terrorism Monitor*, 9, 5-6.
- RADDATZ, M. & WONG, K. 2010. Al-Awlaki Urges Muslims to Kill Americans in New Video. *AQBC World News* [Online]. Available: <http://abcnews.go.com/WN/radical-muslim-cleric-anwar-al-awlaki-urges-killing/story?id=12089807> [Accessed 13/02/2011].
- RICHARDS, A. 2011. The problem with 'radicalization': the remit of the 'Prevent' and the need to refocus on terrorism in the UK. *International Affairs*, 87, 143-152.
- SAGEMAN, M. 2008. *Leaderless Jihad: Terror Networks in the Twenty-First Century*, Philadelphia, University of Pennsylvania.
- SILBER, M. D. & BHATT, A. 2007. *Radicalization in the West: The Homegrown Threat*. New York: New York City Police Department.
- STEVENS, T. & NEUMANN, D. P. R. 2009. *Countering Online Radicalisation: A Strategy for Action*. Available: <http://www.icsr.info/news/attachments/1236768445ICSROnlineRadicalisationReport.pdf> [Accessed 10/11/2010].
- THE AQ CHEF. 2010. *Inspire Magazine*. [Accessed 26/01/2011].
- THE MESSAGE 2012. The Sheikh Google Phenomenon. *The Message: islam*.
- UNKNOWN AUTHOR. 2010. *The Explosives Course* [Online]. Dar-ul-Jabhah Publication. Available: <http://ansar1.info/showthread.php?t=29965> [Accessed 15/01/2011].
- WEIMANN, G. 2004. Special Report: [www.terror.net](http://www.terror.net) How Modern Terrorism Uses The Internet Washington DC: UNITED STATES INSTITUTE OF PEACE.
- WEIMANN, G. 2006. *Terror on the Internet: The New Arena, the New Challengers*, Washinton DC, United States Institute of Peace Press.
- WILTON PARK. *Tackling online jihad: Understanding the issues and how to respond?* , 2011 Wilton Park, United Kingdom. Wilton Park.