Title

A critical analysis of the role of the internet in the preparation and planning of acts of terrorism

Abstract

The purpose of this paper is to offer a critical assessment of the way in which the internet and online material features as part of the process individuals embark on to plan acts of terrorism. The paper begins by evaluating concepts used to describe the role of the internet in the context of terrorism and political violence before analysing a single case study in detail in order to explore particular nuances that emerge which shed light on the relationship between perpetrator on the one and hand and online content and behaviour on the other. The case study, in turn, is developed into a conceptual appraisal of terrorist use of the internet. The paper concludes by exploring the important distinction between the 'theoretical' application of online learning as set out in terrorist propaganda and the hurdles that individuals face in practice.

Key words

Terrorist propaganda, terrorist use of the internet, IED assembly, attack preparation, *Inspire* magazine

Contact

Dr Donald Holbrook
CSTPV, School of IR, University of St Andrews
Library Park, The Scores, St Andrews, Fife, KY16 9AX
E: bdp4@st-andrews.ac.uk, Tel +44 (0) 1334 462935

Biography

Donald Holbrook is Senior Research Fellow at the School of International Relations, University of St Andrews. Research interests include terrorism, international security and the study of ideology. Recent publications include the monograph *The Al-Qaeda Doctrine: The Framing and Evolution of the Leadership's Public Discourse* (Bloomsbury, 2014).

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

1. Unpicking 'terrorist use of the internet' and 'cyberterrorism'

The development of modern terrorism is often seen through the prism of technological innovation. Inventions such as the automated printing press helped to shape the emergence of anti-State terrorism in the late 19th Century. Terrorists have exploited the spread of commercial aviation and tailored attacks to maximise publicity through satellite television broadcasts and 24-hour news coverage. Some technological innovations thus present new attack opportunities whilst others provide new ways of maximising publicity and impact of attack through improvements in communication technology. The spread of the World Wide Web presents a form of technological innovation that may combine both these factors: the ability to communicate is greatly enhanced whilst virtual arenas provide new opportunities for inflicting damage.

Terrorists or terrorist sympathisers, it is argued, can exploit the internet for communicative purposes, using email, social networks, financial transaction channels, blog-sites, web repositories and other online entities for their own specific purposes. The web is also seen as presenting a realm in its own right, a parallel universe where terrorists can do harm by directing their attacks online. The former can be described as 'terrorist use of the internet' whilst the latter phenomenon is commonly referred to as 'cyberterrorism' (see e.g. Conway, 2002).

The former, according to Weimann (2004, 2006), sees terrorists using the internet for a variety of purposes such as communication, data mining, fundraising, publicity, recruitment, networking and training. Noting the extent of "overlap" in wording between conceptualisations of terrorist use of the internet, Conway (2005: 3) offered something of a consensus typology. Terrorists, she argued, use the internet for "information provision, financing, networking, recruitment, and information gathering". Terrorists, therefore, can use the internet just like everyone else: to communicate and exchange ideas, media and money.

The latter concept, 'cyberterrorism' involves individuals using online means to cause harm and inflict damage in pursuit of a particular ideological agenda. Denning (2001: 241) wrote in an early paper on the topic that "cyberterrorism […] refers to the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes

to collide". Common components of conventional terrorism typologies, therefore, feature in descriptions of the "cyber terror threat", whereby computer-based means are used to coerce governments and intimidate populations (Archer, 2014).

Beneath the apparent clarity and distinction of these broad descriptions, however, lurks a deeper sense of conceptual ambiguity. Many references to 'terrorist use of the internet', for example, seem inherently problematic since some of the activities incorporated within that categorisation include actors and activities that in themselves hardly seem 'terroristic'. If an individual gathers information about terrorism, that hardly makes him a terrorist. The actor-focused 'terrorist' distinction is here complicated by the fact that some of the activities cited as part of 'terrorist use of the internet' above become themselves part of that definition. The UK Terrorism Act 2006, for example, proscribes the dissemination of "terrorist publications" even if the disseminator is merely "reckless" as to whether such dissemination encourages or assists in the planning of a terrorist act (2006: section 2). An individual may be convicted under this act even if he or she is not a 'terrorist' in any conventional sense of the term. This concerns, what Ramsay (2013: 182) has defined as "a condition of 'violent radicalism", a "certain sort of engagement with 'radical' discourses about violence" that are distinct from any notions of 'violent radicalisation' implying processes leading towards actual participation in acts of violence. Indeed, the "online violent radical milieu may actually generate its own *positive* reasons for non-engagement", he argues (Ibid: 186). The neat typologies described above also obscure the true heterogeneity of the problem at hand. As Ramsay (2013: 7-8) notes:

> *it is fully recognized by researchers working in this area that the types of internet use from which this threat is supposed to emerge are by and large 'its more prosaic properties' from a technical point of view; that the terrorists using the internet are ordinary people who use the internet "like the rest of us", and that the dangers arising from their use of it are heterogeneous. And yet there seems to be an irresistible urge, nonetheless, to constitute "terrorist use of the internet" as a single research field in which terrorism comes to be talked about, even if only as a conceptual short hand, as a sort of unified essence which somehow inhabits cyberspace and, further, as if the internet represented a unique sphere for terrorist action,*

rather than one of many modern technologies all of which make it easier to do certain things.

There are problems with 'cyberterrorism' too. As Conway (2002) observed in an early paper on the topic, one problem concerns lack of solid examples of cyber-terrorism that allow us to move beyond speculation and hypotheses. Cyber-terrorism would imply some sort of cyber-attack that would qualify as terrorist attack. Rosenfield (2009: 77) divided cyber-attacks into two parts: (1) attacks targeting data, including website vandalism and distributed denial-of-service (DDoS) attacks; and (2) attacks targeting control systems that direct usage of physical infrastructure (Archer, 2104). The former, under which the vast majority of cyber-attacks fall, would hardly qualify as terrorism and attacks under the latter category might stretch conventional understanding of terrorism and the way in which the concept is commonly applied.

A fundamental and underlying problem with both sets of typologies, moreover, concerns lack of empirical clarity. There appears, at times, to be a tendency to start at the wrong end, so to speak. To hypothesise about ways in which terrorists *could* use the internet that are analogues to ways in which non-terrorists (including 'hacktivists') are using the internet already and to focus on the vast volumes of user-generated content, terrorist propaganda and other such types of content that are *available* online rather than focusing on tracing actual cases of individuals involved in terrorism and ways in which they have used the internet and interacted with media content.

1.1 *Methodology*

This paper, therefore, departs from such macro-perspectives in the first instance by scrutinising the detail of a single case of (planned) terrorism within the UK by analysing court documents setting out the case and the way in which the defendants used the internet to plan an act of terrorism.

The court papers are public documents that set out the case for the prosecution in a concluded trial of two individuals who were convicted of the terrorist-related offences with which they were charged. Whilst the data is open-source and even though the case was discussed openly in the media at the time, this paper will not use the subjects' names in order to protect their identity. The specific background and identity

of the subjects, moreover, is beyond the scope of the paper. The purpose is to dissect the role the internet played in a concluded case of terrorist attack preparation in order to add empirical clarity to questions concerning the interplay between terrorism and the internet.

The case study is based on the analysis of four documents produced by the Crown Prosecution Service: (a) a provisional opening note setting out all the circumstances of the case, background, unfolding events and details from police examination; (b) an opening note for sentencing, setting the case in the context of similar terrorist-related cases; (c) a sequence of events schedule identifying markers on a timeline for significant events, including online and offline behaviours and; (d) the closing speech summarising the prosecution's case against the subjects and reiterating evidence.

The next section dissects relevant details of the case to prepare the analysis. Based on our example the third section offers some thoughts on where this case leaves us in terms of understanding the interaction between—in this case—'would be' terrorists and the internet. The purpose is not to offer concrete generalisations but to highlight nuances and particulars relevant to this relationship that are presented by our case study with the aim of informing the debate on computer-aided terrorism.

2. The role of the internet in a case of a planned domestic terrorism within the UK

This section sets out the details of a case involving two individuals who were convicted for engaging in preparation of an act (or acts) of terrorism within the UK. The purpose is to highlight the role the internet played in order to build up the conceptual case in the section that follows. The analysis is based on court documents concerning the case but the focus will be on those aspects relevant to our enquiry alone. The subjects are anonymised and circumstantial details are left out since they lie beyond the scope of the current study.

Both individuals received extensive prison sentences for planning to carry out a terrorist attack and possessing material useful in the commission of such an act. One defendant, 'Subject A', pleaded guilty just before the trial commenced whilst his

associate, 'Subject B', was convicted by a jury in court. Most of the court material, therefore, concerns Subject B, whilst also describing the activities of Subject A that are relevant to the case.

2.1 Particulars of the case

The prosecution alleges that both subjects became "radicalised" primarily via material available on the internet over a 10 month period leading up to their arrest. At the end of that period police were called to an address frequented by Subject B for reasons unrelated to terrorism but gleaned, from their initial investigations into that matter, the full extent of the activities in which both subjects were involved.

Counter-terrorism police searched properties and vehicles belonging to the subjects and studied computers and mobile phones found in those locations. In one of the properties frequented by both subjects, police found pots and pans with remnants of bleach and peroxide-based products that had been heated and mixed in an apparent attempt to make ingredients for an improvised explosive device (IED), according to forensic experts. Searching this property, police found quantities of chemicals and apparent bomb-making components, including peroxide products, bleach and citric acid, laboratory equipment, firelighters, batteries, a string of lights and a list of items to be procured, including an alarm clock. Police also found a radio frequency detector, commonly referred to as a 'bug detector', which can be purchased online in the UK. Such devices are described by one online distributor as enabling 'the operator to quickly establish what kind of signal [has been detected] whilst carrying out a counter-surveillance sweep' (Spycatcheronline.co.uk, 2014).

A desktop computer was also found at the address which offered insights into the subjects' internet activities prior to arrest. Subject A had been active on Facebook and on the online chat programme Paltalk using, for the latter, the username 'Mujahid Al-Britani'. The computer contained images glorifying terrorist figures such as Usama bin Ladin and internet searches pertaining to the procurement of household chemicals and laboratory tools, including from the Ebay online marketplace. Six Facebook accounts had been registered on the desktop computer, although four had already been closed by Facebook for terms of use violations (Regina v *anonymous, date withheld* (1)).

Police also searched two vehicles that were used by both subjects. In the first car, police found quantities of CDs with ideological content, including Islamist extremist material described in more detail below. Further CDs with ideological material were found in the second car, along with a hard-copy of a book titled 'The Commanders of the Muslim Army' and a laptop computer. Police also found a portable Satellite Navigation system which had archived trips made over the past few months. Detectives analysed the readout of this archive which showed a series of unexplained journeys to known Jewish areas, Jewish community centres and a synagogue in an area to which the subjects otherwise had no links. Forensic experts studied the laptop that was found in the car and found evidence of internet searches pertaining to these same locations. These repeated trips, the prosecution alleged, amounted to "hostile reconnaissance" in preparation of attack against Jewish targets (Regina v *anonymous, date withheld* (2)). Subject B admitted, during questioning, to participating in these activities and to spending significant amounts of time with Subject A parked outside synagogues watching worshippers coming and going. The latter reportedly expressed his vehement hatred for Jews during these trips, remarking on one occasion: 'we must kill them all' (Regina v *anonymous, date withheld* (1)).

The laptop that was found in one of the vehicles also formed part of the investigation. Whilst forensic experts found evidence suggesting the subjects had tried to destroy evidence and erase internet search histories permanently, other more obvious signs were left that appeared to hint at the subjects' mindset. The first clue was offered by the background wallpaper, which displayed a high-quality image of the black 'jihadi' banner commonly associated with Islamist militants. The desktop itself contained links to two documents that ultimately formed part of the prosecution's case against the defendants since they were judged to constitute 'proscribed' material. These were the sixth edition of the English-language *Inspire* magazine by Al-Qaeda in the Arabian Peninsula and a document titled 'Class Notes from the Security and Intelligence Course' (Ibid). The copy of *Inspire* was secured via a contact on Facebook whilst the Class Notes appeared to have been downloaded directly from jihadi websites.

Overall, the nature of the media material to which the subjects were exposed and the nature of topics in which they appear to have been interested can be divided into two broad categories: (1) operational and 'actionable' guidelines concerning bomb-making, counter-surveillance and other such 'tactical' concerns and (2) ideological

material setting out the broader ideational framework and justificatory context. The next subsections look at each set of themes in more detail.

2.2 Operational and 'actionable' guidelines

Inspire issue 6 had been acquired a few days prior to arrest and forensic experts managed to establish that it had been opened and viewed on numerous subsequent occasions. This edition of the extremist magazine covers a range of topics and eulogises Usama bin Ladin, who was killed shortly prior to publication. Detectives were primarily interested in an article under the section 'Open Source Jihad' called 'Making acetone peroxide'. The introduction to Open Source Jihad (in all editions of *Inspire*) presents the section as a "resource manual for those who loathe the tyrants; includes bomb making techniques, security measures, guerrilla tactics, weapons training and all other jihad related activities" (Al-Malahem, 2011: 36). The article on 'Making acetone peroxide', in turn, details how to assemble peroxide-based chemical mixtures that can be used in a home-made IED and lists the ingredients needed and where they can be found. The process described in *Inspire* 6 appeared to correspond to the subjects' efforts to acquire the correct ingredients and extract the substances needed from bleach and other products in order to make the explosive component of their improvised devise.

Some of the other apparent bomb-making components appeared to correspond with guidelines offered in the first issue of *Inspire* in an article titled 'Make a bomb in the kitchen of your Mom'. The article began by asking: "can I make an effective bomb that causes damage to the enemy from ingredients available in any kitchen of the world? The answer is yes". The article offered a detailed step-by-step guide for making a simple pipe bomb, ignited with a modified set of fairy lights and an alarm clock. As well as providing these technical details, however, the article offered stark ideological justifications for urging European and American Muslims to refrain from traveling to areas of conflict in favour of assembling IEDs and targeting Jews and Christians directly "inside the West" (Al-Malahem, 2010: 33).

Several clues, particularly the string of lights, the "shopping list" for other relevant items such as an alarm clock, and the stockpile of chemicals and flammables led detectives to believe that a copy of this magazine may have been used as well. Furthermore, computer forensic experts found electronic traces of the software

'asraralmujahideen2.0', a file-erasing programme advertised in *Inspire* 1, which had apparently been used successfully to wipe some of the files and folders from the computer.

Prior to these downloads, however, the subjects sought to secure bomb-making guidelines on the web via a large torrent download from a site called 'BT Junkie', a BitTorrent repository. The torrent file was called titled 'Massive Chemistry and Explosives Book Collection' and a folder with the same name was created on the subjects' laptop shortly after the downloading was commenced. This torrent file contained a huge number of publications in various formats that all provided detailed guidelines on bomb making and assembly of home-made IEDs. These publications were originally produced by a number of different organisations, from terrorist entities to academic bodies, commercial organisations and government agencies. Topics ranged from bomb making recipes and guidelines to efforts of concealment and assembly of devices, as well as different tactics of sabotage and the wider scientific context. Titles included well-known publications such as the 'Anarchist Cookbook' and the 'Mujahideen Explosives Handbook'. The torrent file also included material from government agencies, such as the 'List of Explosives Materials' publication from the US Bureau of Alcohol, Tobacco, Firearms and Explosives. Another publication contained within this torrent file was a booklet titled 'Car Bomb Recognition Guide' (Regina v *anonymous, date withheld* (3)). The publication, according to its author (Scott, 1996), was "prepared for law enforcement officers, military officers, and counterterrorist specialists to assist in the recognition and identification of improvised explosive devices and booby traps emplaced in and around automobiles".

The subjects appeared to be having some difficulties in applying the knowledge gleaned from these documents, or perhaps were unwilling to digest such large quantities of content. Whatever the reason, analysis of their internet searches from this period reveal that they sought further guidance from the internet by searching for some basic queries that appeared to be part of their bomb-making process. These included entries for "potassium chlorate and how to make it from bleach", "where can I buy potassium chlorate" and "how to make potassium chlorate", which led the subjects to web pages by explosives enthusiasts, rather than terrorist propagandists. (Regina v *anonymous, date withheld* (1) and (3)). One such site which the subjects appeared to frequent was the YouTube channel for 'NurdRage'. This channel was dedicated to

compiling and providing videos showing how to conduct various different 'science experiments', including procedures relevant to bomb making. In the 'about' section, the proprietors described 'NurdRage' (2013) as a "channel run by science nerds for science nerds. We demonstrate science experiments for all levels, from kitchen chemistry to advanced synthesis".

The document 'Class Notes from the Security and Intelligence Course' was downloaded about a week prior to arrest and was opened multiple times according to forensic experts. This document is an abridged translation of a publication in Arabic which probably borrowed initially from Pakistani intelligence manuals. 'Class Notes' is presented as an aid to the jihadi fighters in their efforts to evade capture from the authorities, detect and counter surveillance and manage interrogations if captured. In the event of capture in Western countries, the authors of the publication advise jihadists to remain silent and ignore questions. Since the interviewers in these countries need to respect human rights, the authors note, there is little they can do if the interviewee simply refuses to answer (Bin Adam, 2011). Tellingly, once arrested, Subject A displayed some of these 'counter-interrogation' techniques, for example by staring fixedly on one point of the interview room, whilst ignoring all of the questions (Regina v *anonymous, date withheld* (1); (Regina v *anonymous, date withheld* (2)).

Although it cannot be stated with any certainty, it is possible that the document impacted on other elements of the subjects' behaviour during this period. For instance, 'Class Notes', urges fighters to look out for recording devices and 'bugs' to see if they are being monitored, which might correspond with the 'bug detector' found at the property as noted above. The document does also emphasise the importance of hostile reconnaissance, although whether this impacted on the subjects' decision to scope predominant Jewish residential areas is unclear, particularly in light of the fact that the subjects appeared to have embarked on the latter months prior to downloading 'Class Notes' (ibid).

The subjects, therefore, used the internet extensively in their attempt to procure operational guidelines in order to, apparently, put together an IED, scope potential targets and ensure operational security. The review above reveals that these guidelines came from multiple sources, including amateurs and enthusiasts who post material online and government agencies whose publications, perhaps after they have ostensibly expired, become available via torrents and websites. Some of the content in the latter

category focuses on countermeasures, rather than device assembly, suggesting such *counter-terrorist* techniques form part of the overall repertoire of operational manuals and guidelines available online. Despite this availability of detailed, and supposedly straightforward bomb-making guidelines, the subjects did not appear to be particularly successful in their attempts to apply the literature to practice. The internet searches appear to suggest they were struggling to overcome some of the basic hurdles in this process. Furthermore, although forensic and explosives experts judged the chemical residue found at the main property to be evidence of an attempted explosive device, this residue was over three weeks old when the properties were searched, whilst the subjects' research and experimenting continued, suggesting the assembly process was not going very well (Regina v *anonymous, date withheld* (1)).

2.3 Ideological content

Subject B revealed in interviews that he and his associate had both consumed Islamist ideological content, including extreme material in the weeks and months prior to arrest (Regina v *anonymous, date withheld* (1)).

Much of the material was downloaded from the internet or secured via online social networks such as Facebook. A copy of the *Inspire* magazine, as noted above, was secured via a contact on Facebook and the subjects used their Facebook profiles to share and access links to Islamist propaganda material, including Al-Qaeda Central and Al-Qaeda in Iraq publications hosted on YouTube. There was also evidence that extremist Islamist ideological material had been streamed online directly, often from YouTube, and some of the links to this content had been bookmarked on the subjects' web browsers. The subjects also carried out several internet searches concerning many of the topics covered in the ideological material which they accessed. During an extensive session two weeks prior to arrest, for example, the subjects searched the web for entries relating to past terrorist incidents and their perpetrators, such as the two British suicide bombers responsible for an attack on a bar in Tel Aviv in April 2003 and entries relating to the Taliban and Somalian *mujahideen*. Other searches during this period concerned religious topics, including 'martyrdom' and 'green birds', which are supposed to carry the souls of martyrs in heaven (Regina v *anonymous, date withheld* (3)).

On the laptop computer that was found in one of the vehicles police also found a large quantity of Islamist beheading and execution videos. This collection, it was established, came from a large torrent download of over 70 such videos which was still being processed at the time of arrest. According to statements made by Subject B, both individuals had watch at least some of these videos in the weeks prior to arrest (Regina v *anonymous, date withheld* (1)).

Most of the more substantive ideological content uncovered as part of this investigation, however, appears to have been stored on copied CDs, rather than being secured from the internet. As noted above, police found stacks and wallets with copied CDs with audio and PDF files of ideological content. The subjects appeared to have listened to this material even whilst driving, judging by the fact that a CD with Abdullah Faisal lectures was found still inserted in the CD player of one of the cars. Faisal is a firebrand Islamist cleric who was imprisoned in the UK in 2003 for soliciting murder and has since been deported. His material has reportedly influenced a number of individuals convicted on terrorism charges (Attewill, 2007; Hoffman, 2009). The Faisal CD belonging to the subjects in this case included lectures such as 'Them versus us,' which emphasises the supremacy of Islam over other faiths and the importance of enmity towards non-believers, and 'Requirements of Jihad', which lists psychological and physical conditions that need to be in place for a believer to embrace militancy, celebrating Usama bin Ladin's example as a beacon to follow. Material from Australian cleric Feiz Mohammed, as well as more moderate content from Ahmed Deedat, also featured on some of the recovered CDs (Regina v *anonymous, date withheld* (4)).

The most notable item from this collection was a CD labelled 'The True Creed'. This appeared to be a rather sophisticated and comprehensive compilation of some of the most prominent and extreme English language Islamist jihadi publications. These included translated statements by Ayman Al-Zawahiri and Usama bin Ladin, content from the Al-Qaeda affiliate organisations and lectures by Anwar Al-Awlaki, a hugely popular radical cleric who was killed in Yemen by a US drone strike in 2011. A copy of '39 Ways to Serve and Participate in Jihad' by Muhammad bin Ahmad as-Salim, translated for At-Tibyan Publications by Tarek Mehanna, also featured on the CD and this publication formed part of the prosecution's case against the defendants, with reference of the less serious charge of possessing terrorism-related articles (Cole, 2012). As the prosecutor noted, '39 Ways', which lists various ways in which believers

should prepare for, support and join jihad, has cropped up in a number of other terrorism investigations in the UK to date (Regina v *anonymous, date withheld* (1)). Whilst much, if not all, of the material contained on the CD is readily available online, it is interesting to note that the subjects themselves appeared to have acquired the disk from associates, since there was no evidence that either of them had located, downloaded or assembled this material themselves. Furthermore, it should be noted that although the content on 'The True Creed' all focused on broadly similar themes, the material did not come from a single source online or offline. In other words, someone will have actively identified and assembled the titles for this particular CD.

Finally, the prosecution emphasised another publication as being indicative of the mind-set of the defendants. This was a PDF file contained within a folder titled 'Possible Strategies' that was created on the desktop of the laptop computer found in one of the vehicles. The title of this document was 'Abu Mu'sab al-Suri: Profile of a Jihadist Leader'. The document described how a principal Al-Qaeda strategist called Abu Musa'ab Al-Suri sought to plan the "future jihadist war" after 9/11 with an emphasis on "the jihad of individual terrorism", urging European-based recruits to "begin the jihad at home" since "the entire globe has become the theatre of war". The prosecution argued that this was "a very important document in this case as the contents declare the very nature of terrorism alleged against the two defendants" (Regina v *anonymous, date withheld* (1)). The couple had found and accessed a document describing a strategic treatise that prescribed precisely the sort of terrorist violence that they were seeking to carry out and this document had been kept in a special folder on the desktop, suggesting it was of some value to the subjects. What is revealing, however, is the fact that this document, 'Abu Mu'sab al-Suri: Profile of a jihadist Leader', was not published or distributed by terrorist groups but by an academic. This is a transcript of a lecture given by Dr Brynjar Lia at King's College in London in April 2006. Here, Lia describes the core facets of Al-Suri's strategic doctrine in a short 5-page summary of the strategist's major viewpoints on grassroots jihad (Lia, 2006). It is clear, therefore that—at least in this case—'would-be' terrorists seek cues on ideological arguments from a range of sources beyond the most obvious original repositories of such content.

2.4 Some observations

Although the subjects in this case were unsuccessful in their efforts to assemble an IED and carry out a terrorist attack, it seems probable that they at least had the desire, and perhaps eventually the capacity, to carry out such an attack and there appears to be ample proof, as the jury found, that the defendants were preparing to carry out an act of terrorism. Much of this preparation relied on material gleaned from the internet, although, at least in practical terms, this seemed to create substantial operational hurdles that they were yet to overcome at the time of arrest.

Although the internet was important, however, it seems like some or much of the more substantive ideological content may have been secured through other means, even if it might have been downloaded off the internet by someone at some point.

In terms of engagement with media content overall, it appears that two patterns emerge. Firstly, there was selectivity in terms of substantive ideological content. There were no 'bulk downloads' of ideological publications, even though these are readily available online. The subjects chose such material more carefully, it seems, either via their own internet searches or through accessing material that others had compiled and put on CDs. Secondly, less substantive ideological content, such as the beheading and assassination videos, and the collections of operational manuals were downloaded in bulk, rather than selected individually. Internet searches, in turn, are used to 'fill in the gap' of knowledge, both as regards operational questions and ideological concepts.

What also emerged from this case is that these operational guidelines in particular, but also—in the case of the academic presentation on Abu Musab Al-Suri—some of the ideological content, were secured from sources that were completely unrelated to terrorist groups or websites affiliated with or sympathetic towards terrorist organisations or ideologies. This raises questions about Weimann's (2006: 5) focus on websites 'serving terrorists and their supporters', when many websites that provide material that 'terrorists' certainly appear to find useful are very much part of the 'open', legitimate and mainstream part of the web with no links to terrorism.

These observations, it should be stressed, are based on this one case alone and the argument is not being made here that these themes and findings are universally applicable. Indeed, such tendencies to generalise about 'terrorism and the internet' and 'cyberterrorism' as they play out for individuals on the ground appear to be a fundamental weakness of much of the literature on the topic. With these caveats in mind, however, the next section explores what we can, nonetheless, extrapolate from

the case examined about some of the ways in which individuals preparing acts of terrorist can approach the internet and how online content in this respect can be conceptualised.

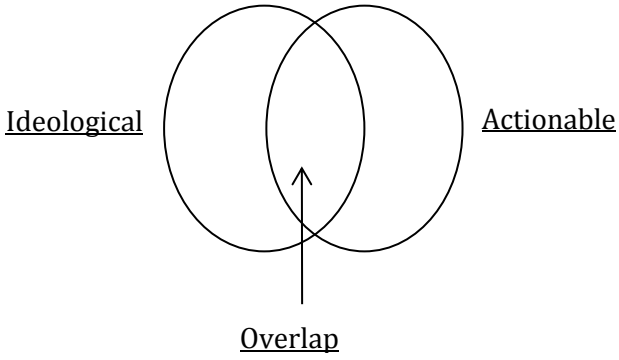
3. Lessons: exploring conceptual implications

Our case study revealed nothing in terms of cyberterrorism but offers several examples of how terrorists might use the internet to aid or inform their activities. Two interrelated categories appear to emerge: (1) using internet tools for data dissemination, networking and overcoming practical challenges; and (2) securing specific types of media material through online means.

The former set of activities could be described as online *facilitation* methods consisting of, in this case, interacting with apparently like-minded individuals on Facebook and Paltalk, using internet search engines to seek answers to specific technical questions, using online marketplaces, and gaining access to data via streaming websites or torrent downloads.

The latter manifestation of these online activities consists of compiling a particular corpus of *content*. This was divided above into: (a) ideological material and (b) 'actionable' material. Ideological content consists of material conveying religious or political sentiments and attitudes whilst 'actionable' material concerns particular aspects of problem-solving, such as IED assembly. Whilst these rather crude categories might offer initial ways in which to organise content, the preceding discussion offered plenty of examples where there is a considerable amount of overlap between the two. These distinctions, therefore, might be more accurately displayed on a Venn diagram (see figure 1).

Figure 1: Conceptualising online content



Here, according to the diagram individual publications could be described as (i) purely ideological, (ii) purely implementable or 'actionable', or (iii) somewhere in between. From our case study above, religio-political sermons and publications would be in the first category and dedicated technical guidelines, such as the 'NurdRage' material, would be in the latter. Several titles, moreover, would be in between where the two categories overlap. The 'Mujahideen Explosives Handbook' and the 'General Guidelines' referred to above, for example, are *primarily* actionable guidelines that are still framed in deeply ideological ways. The *Inspire* publications, meanwhile, consist mostly of ideological and propagandistic content whilst dedicating a small section to purely technical and practical matters such as bomb-making.

The ideological material covered in the case study contained items from a variety of different sources with a discourse that ranged from moderate to extreme (see further on grading ideological content in Holbrook and Taylor, 2014; Holbrook, Ramsay and Taylor, 2013).

Whilst large quantities 'actionable' material relevant to bomb-making and bomb-detection can clearly be accessed via torrent downloads online, moreover, these too appear to have been originally authored by a range of different actors and organisations. These included: terrorist actors, explosives enthusiasts, government agencies and the academic-scientific community.

The subjects in this case, therefore, appeared to have applied online tools and accessed and used online material in order to plan what could be described as a relatively 'typical' act of home-grown terrorism. At the same time, however, the analysis reveals particular nuances and paradoxes that may not be generalisable but yet point to difficulties and hurdles that the subjects appeared to struggle to overcome, perhaps partly because they were so reliant on the internet to move things forward. The concluding section explores some of these issues in more detail.

4. Conclusions

The introduction to the aforementioned *Inspire* (Al-Malahem, 2010: 33) article 'Make a bomb in the kitchen of your mom' rationalised the publication of such detailed IED guidelines on the following basis:

> *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 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 and then use this explosive device properly.*

Whilst these sentiments may describe the aspirations of the subjects in the case described above, their ultimate failure to produce anything tangible suggests that the process is not all that simple or straightforward. Indeed, the same introduction in *Inspire* seeks to present failed would-be terrorists Faisal Shahzad and Umar Farouk Abdulmutallab as ultimately successful because they managed to attract media attention and put pressure on politicians. The process of engagement, therefore, is presented as ultimately more important than the outcome.

For the subjects in our case study this process of engagement appears to have begun approximately four months prior to arrest with a series of 'hostile reconnaissance' missions to Jewish communities and centres of worship. This period appears to have been followed by attempts to procure and mix chemical substances in order to create a crude explosive device. The subjects began experimenting with flammables and chemicals approximately three weeks prior to arrest, seeking further information online from bomb-making manuals and internet searches after these initial attempts appear to have failed. Ideological content, in turn, was acquired and consumed prior to this initial preparatory phase and continued feature up until the time of arrest. 'Counter-surveillance' also appears to have been a preoccupation during, at least, the latter half of this period. It is unclear when the 'bug detector' was purchased, but other items concerning file deletion and the 'Class Notes' document described above were secured in the week prior to arrest. On the surface, perhaps, the case could thus be described as a typical example of 'home-grown' terrorists using the internet to plan and prepare a terrorist attack.

Yet a number of details to emerge from this case study reveal how far the subjects were removed from the *Inspire* ideal type of sophisticated 'self-starters' who wreak havoc in their local areas, thus contributing to the global *jihad.*

The subjects clearly struggled with their IED assembly despite repeated attempts and extensive research. Furthermore, despite being preoccupied with 'counter-surveillance', they left some very overt and obvious clues as to their mindset and activities. The laptop contained helpful links to extremist material such as the sixth edition of the *Inspire* magazine on the desktop which was adorned with a black 'jihadi' flag. Despite efforts to delete internet search histories, therefore, a cursory glance at the computer would have raised suspicions concerning the motives of the owner. The fact that one of the subjects used the username 'Mujahid Al-Britani' on Paltalk hardly suggests that anonymity or covert action was always the primary objective. Whilst the subjects tried to delete their internet search histories, moreover, they left the cache on their satellite navigation untouched which allowed the police and prosecution to recreate their 'hostile reconnaissance' with considerable detail. Police were even alerted to this fact in the initial interviews where Subject B sought to score points against his associate.

Applying the 'theory' of internet and computer aided terrorism as articulated in jihadist publications such as *Inspire* and 'Class Notes from the Security and Intelligence Course' to practice, therefore, is far from straightforward. What else can we glean from this case in terms of the role of online content? There are three main observations:

1. Huge repositories of bomb-making material and other 'actionable' content from a range of sources are available online that can be secured as bulk downloads. Dedicated amateur and enthusiast forums then offer opportunities to address specific technical questions in more detail, whilst significant hurdles remain in terms of applying this knowledge in practice.
2. Quantities of substantive ideological content featured as well, but these publications appear to have been chosen more selectively. Whilst some of the material was secured from the internet, large corpora of ideological compilations were found on copied CDs. 'Offline' content, therefore, still features. This material was primarily in English even though some of the content had originally been published in Arabic before being translated and edited by English-language

publishing networks such as At-Tibyan. Less substantive content, that could be described as ideological, such as beheading videos, was secured in bulk via torrent downloads.

3. Internet searches appear to be used to fill remaining gaps in knowledge when other sources of information are unavailable. These relate both to technical issues concerning bomb-making and dense theological issues such as martyrdom and ascent to heaven. It is notable too in this case that the subjects sought information about other existing cases of Islamist-inspired terrorism and the subjects behind them, such as the 2003 Tel Aviv bombers.

Our case study illustrates how easy it appears to be for individuals attracted to notions of violent extremism to use online methods of facilitation and approach online content in order to embark on some of the initial steps towards planning and participating in terrorism. At the same time, however, the case highlights the difficulties of progressing beyond this exploratory and experimental phase, especially in terms of overcoming technical hurdles when relying on the internet. The subjects appeared to have dangerous intentions but lacked the sophistication and resolve to see them through. They appeared attracted to notions of 'jihadi' glory which are presented in ideological material distributed both online and offline and appeared keen to display overt signs of these loyalties and sentiments in sharp contrast with the 'tactical' advice they consumed. Whilst they focused on ideological content throughout the period in question it appears underlying prejudices such as anti-Semitism had been present for some time. Computers and the internet were central to this case and formed an important part of the investigation but presented significant challenges in terms of 'real world' applicability which greatly diminished the threat that these activities initially seemed to pose.

Reference list

Al-Malahem (2010) *Inspire* Issue 1 (summer), published by Al-Malahem Media of Al-Qaeda in the Arabian Peninsula.

Al-Malahem (2011) *Inspire* Issue 6 (summer), published by Al-Malahem Media of Al-Qaeda in the Arabian Peninsula.

Archer, E. M. (2014) 'Crossing the Rubicon: Understanding Cyber Terrorism in the European Context', *The European Legacy: Toward New Paradigms* (19:5, pp. 606-621, DOI: 10.1080/10848770.2014.943495).

Attewill, F. (2007) 'Race hate preacher Faisal deported', in *The Guardian* (25 May), <http://www.theguardian.com/uk/2007/may/25/terrorism.race> [as of October 2014].

Bin Adam, A. A. (alias) (2011) 'Class Notes from the Security and Intelligence Course', Global Islamic Media Front.

Cole, D. (2012) '39 ways to limit free speech', in *The New York Review of Books* (19 April) <http://www.nybooks.com/blogs/nyrblog/2012/apr/19/39-ways-limit-free-speech/> [as of October 2014].

Conway, M. (2002) 'Reality Bytes: Cyberterrorism and Terrorist "Use" of the Internet', *First Monday* (7:11, November) <http://firstmonday.org/ojs/index.php/fm/article/view/1001/922> [as of December 2014].

Conway, M. (2005) 'Terrorist "Use" of the Internet and Fighting Back', conference paper delivered September 2005 at the Oxford Internet Institute, Oxford University.

Denning, D. E. (2001) 'Activism, Hacktivism, and Cyberterrorism: The internet as a Tool for Influencing Foreign Policy' in John Arquilla and David Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239-288), Santa Monica: RAND Corporation.

Hoffman, B. (2009) 'Radicalization and Subversion: Al Qaeda and the 7 July 2005 Bombings and the 2006 Airline Bombing Plot' in *Studies in Conflict and Terrorism* (32:12, pp. 1100-1116), DOI 10.1080/10576100903319896

Holbrook, D. & Taylor, M. (2014) 'Developing Grading Processes for Ideological Content' in *Journal of Policing, Intelligence and Counter Terrorism* (9:1, pp. 32-47).

Holbrook, D., Ramsay, G., & Taylor, M. (2013) "Terroristic Content" - Towards a Grading Scale', in *Terrorism and Political Violence* (vol. 25, pp. 202–223).

Lia, B. (2006) 'Abu Musab Al Suri: Profile of a Jihadist Leader', conference paper delivered at a conference titled 'The Changing Faces of Jihadism', King's College London (27-28 April).

NurdRage (2013) YouTube account <http://www.youtube.com/user/NurdRage> [as of August 2013]

Ramsay, G. (2013) *Jihadi Culture on the World Wide Web*, New York: Bloomsbury.

Regina v *anonymous, date withheld* (1). Opening Note for Sentence, Crown Prosecution Service.

Regina v *anonymous, date withheld* (2). Provisional Opening Note, Crown Prosecution Service.

Regina v *anonymous, date withheld* (3). 'Sequence of Events Schedule', Crown Prosecution Service.

Regina v *anonymous, date withheld* (4) Closing Speech, Crown Prosecution Service.

Rosenfield, D. (2009) 'Rethinking Cyber War', *Critical Review* (vol. 21).

Scott, L. (1996) *Car Bomb Recognition Guide: How They're Made, How to Detect Them*, Boulder: Paladin Press.

Spycatcheronline.co.uk (2014) 'Bug Detector', <http://www.spycatcheronline.co.uk/bug-detector-pr7000.html> [accessed November 2014].

Terrorism Act (2006) <http://www.legislation.gov.uk/ukpga/2006/11/contents> [accessed November 2014].

Weimann, G. (2004) 'www.terror.net: How Modern Terrorism Uses the Internet', *Special Report,* Washington, DC: United States Institute of Peace <http://www.usip.org/sites/default/files/sr116.pdf> [accessed December 2014].

Weimann, G. (2006) *Terror on the Internet: The New Arena, The New Challenges*. Washington DC: United States Institute for Peace Press.