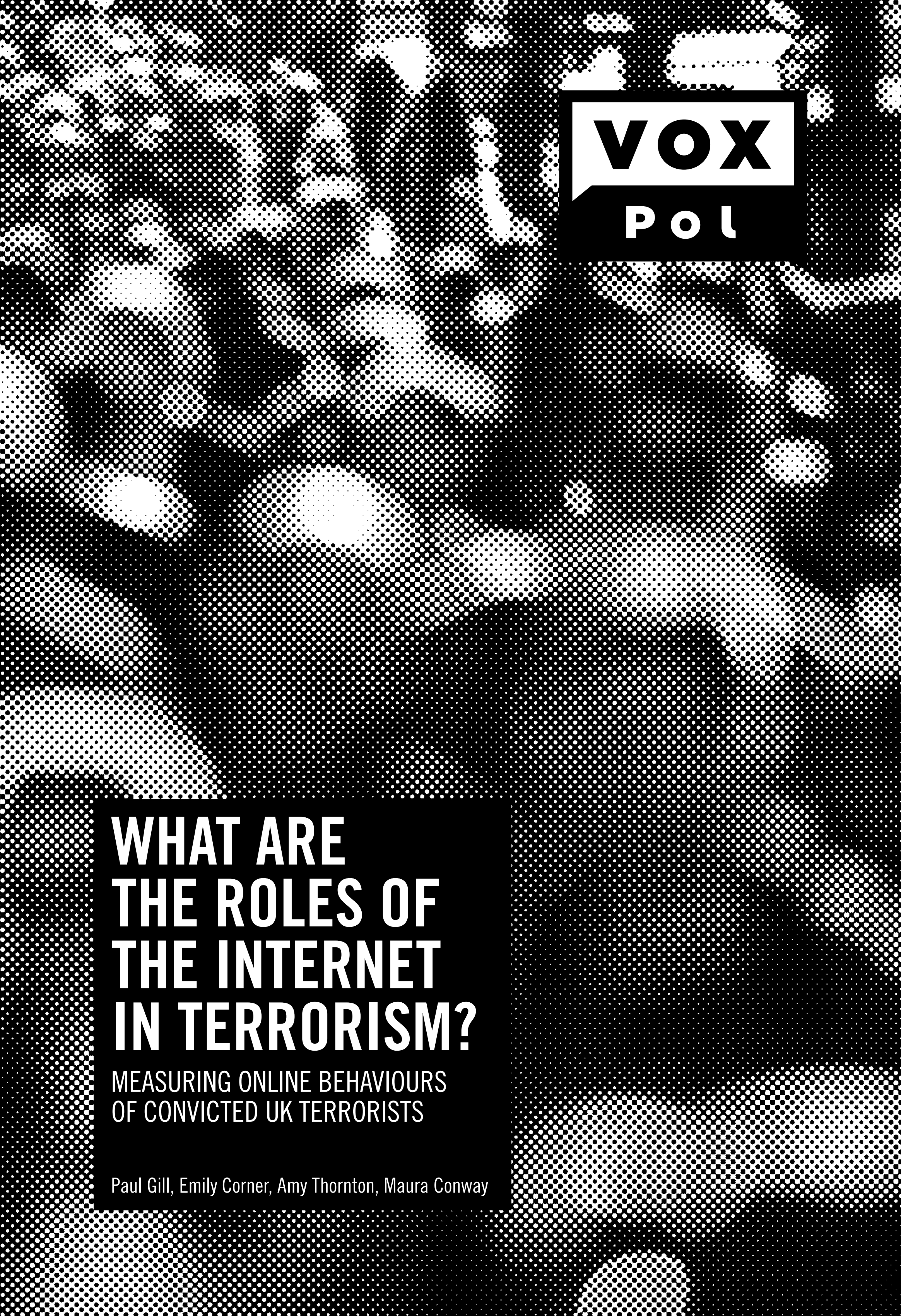


VOX Pol

WHAT ARE THE ROLES OF THE INTERNET IN TERRORISM?

MEASURING ONLINE BEHAVIOURS OF CONVICTED UK TERRORISTS

Paul Gill, Emily Corner, Amy Thornton, Maura Conway

WHAT ARE THE ROLES OF THE INTERNET IN TERRORISM?

MEASURING ONLINE BEHAVIOURS OF CONVICTED UK TERRORISTS

Paul Gill, Emily Corner, Amy Thornton
University College London

Maura Conway
Dublin City University

About the authors

Dr Paul Gill is a lecturer in Security and Crime Science at University College London. Previous to joining UCL, Dr. Gill was a postdoctoral research fellow at the International Center for the Study of Terrorism at Pennsylvania State University. Dr Gill has previously managed projects funded by the Office for Naval Research and the Department of Homeland Security. Dr Gill is the author of Lone-Actor Terrorists: A Behavioural Analysis (Routledge 2015).

Dr Emily Corner is a research assistant and doctoral student at University College London. She has conducted research for Defence Science and Technology Laboratory, the Department of Homeland Security, Manchester Metropolitan Police, and European funded research projects VOX-Pol and PRIME. She also conducts research for the Fixated Threat Assessment Centre, investigating fixated individuals who approach or pose a threat to prominent individuals.

Dr Amy Thornton is a research associate at the What Works Centre for Crime Reduction in the Department of Security and Crime Science, University College London. Focusing on the emergence of radicalising settings in different contexts, Dr Thornton has conducted interviews with former far-right and Islamist extremists, and de-radicalisation professionals in the UK, USA and Canada, allowing her to explore best practices in de-radicalisation and counter-radicalisation programmes in these countries.

Dr Maura Conway is a senior lecturer in international security in the School of Law and Government at Dublin City University and the Coordinator of VOX-Pol.

Acknowledgements

The authors are extremely grateful to the speakers and participants of the associated VOX-Pol workshop, held in Berlin in December 2014, and to all those who provided comments on a draft of this report.

ISBN: 978-1-873769-49-2

Like all other VOX-Pol publications, this report can be downloaded free of charge from the VOX-Pol website: www.voxpol.eu

Designed and typeset by Soapbox, www.soapbox.co.uk

TABLE OF CONTENTS

INTRODUCTION

Pundits, the media and the general citizenry have a tendency to reach for mono-causal explanations of terrorist behaviour and/or motivation. Typical master narratives posit the strength of single causes like mental illness, ideological attractors, and grievances. In recent years, ‘online radicalisation’ has been added to this list. When evidence emerges that an individual engaged in online behaviour associated to his/her ideology, the immediate consensus is that the Internet caused the action (as opposed to the intended action causing the individual to have recourse to the Internet). The truth however is “typically more complicated. Neither [online] radicalisation nor grievances alone are typically sufficient to cause an individual to engage in terrorism” (Borum, 2013:105). The question remains whether this complexity is actually illustrated within the academic literature or not. Is it a case of academics also offering simplistic mono-causal explanations, or is it a case of rigorous scientific evidence failing to be communicated to the masses?

EXISTING LITERATURE

A quick search of the relevant academic literature on online radicalisation on Google Scholar largely supports the former. We examined the first 200 abstracts based on a search of "online radicalisation OR online radicalization". In particular we were interested in (a) whether/if any data informed the analysis and (b) whether there were continuing 'truisms' within the literature regarding the process of online radicalisation or the means to counter it which remained empirically unverified. Below we document a number of recurring problems.

One of the key problems is an abundance of conceptual problems. A wide-range of virtual behaviours is subsumed into the category of online radicalisation. A simple search of news articles from March 2015 shows that a range of behaviours from accessing information on overseas events via the Internet, to accessing extremist content and propaganda, to detailing attack plans in a blog post, have all been considered as online radicalisation. Academic efforts have tried to categorise these different forms of behaviour. Neumann (2013), for example, delineates instrumental uses (e.g. logistics and reconnaissance, fund raising, provision of training manuals and videos, using the Internet as a weapon) from communicative uses (e.g. publicising the cause, generating political support and recruitment). However, there has been no study to date that attempts to to quantify the regularity of these behaviours. Instead the field occasionally relies upon single in-depth case studies or simple anecdotal illustrations (see Appendix 1).

> *The other key problem is that of data. Even for a field as bereft of empiricism as terrorism studies, the striking lack of data is surprising. Of the 200 abstracts analysed, only 6.5% utilised any form of data. Primary data was utilised in just 2% of the studies, but this mostly focused on extremist forums and social media and, therefore, largely captured radicalised individuals (and not*

> *necessarily individuals prepared to conduct terrorism). There was also a distinct lack of psychological (1%) or criminological (0%) inquiry into online radicalisation in this sample. This is striking because psychological paradigms may help explain the process through which people become engaged/radicalised in a virtual space and how it differs from a real-world space. Instead, the literature assumes virtual space is a good substitute for physical interactions, but fails to tell us why and in what contexts in particular.*

The lack of criminological inquiry is also striking since it has fairly well developed paradigms for the study of online crimes and how they are committed (e.g. cyber enabled vs. cyber dependent) (McGuire and Dowling, 2013a; McGuire and Dowling, 2013b). There is also a tendency to treat all terrorists in an aggregated way, expecting that what applies to one type (e.g. an al-Qaeda inspired individual) may also apply to a second type (e.g. a right-wing inspired individual) despite the grievances, ideological underpinnings and radicalising settings looking very different. Finally, the 200 abstracts regularly made unempirical (and sometimes unverifiable) claims. For example, Sageman (2008) outlines that "during the past two or three years… face-to-face radicalisation has been replaced by online radicalisation". Omotoyinbo (2009) similarly outlines that "it has been initially identified that radicalisation is basically having two versions which are online and offline". Neumann (2013) comments on countering online radicalisation, and argues that "approaches aimed at restricting freedom of speech and removing content from the Internet are not only the least desirable, they are also the least effective". It is assumptions like these that we put to the test in this report.

Typically, the truth behind these assumptions is far more complex. However, in the absence of data, we cannot begin to try and unpack this complexity in a scientifically rigorous way. Here we seek to unpack the degrees to which the Internet is used across a large sample of terrorist offenders; whether some attributes of the offender make it more likely he/she will make use of the Internet; measure the degrees to which different behaviours are occurring online; and outline which of these behaviours are on the increase and whether they can be linked to an uptake in terrorism offenders in general, thus providing one of the first empirical treatments of online radicalisation.

Perhaps the stand-out empirical study of online radicalisation is that of von Behr et al. (2013). They examined primary data of 15 radicalised individuals, nine of whom were convicted under UK terrorism legislation. The study made use of interviews (with police and the individuals themselves), trial records and computer registries.[1] They came to the following empirically-informed conclusions:

1. The Internet affords more prospects for radicalisation. For all 15 cases, the Internet was a "key source of information, communication and of propaganda for their extremist beliefs".

2. The Internet provides a "greater opportunity than offline interactions to confirm existing beliefs".

3. The Internet does not necessarily accelerate the process of radicalisation.

4. The Internet is "not a substitute for in-person meetings but, rather, complements in-person communication".

5. The Internet does not necessarily increase the opportunities for self-radicalisation; interactions, be they physical or virtual, are still crucial for radicalisation.[2]

In terms of measuring the degree to which a large sample of terrorists engaged in online activities, Gill et al.'s (2014) study was perhaps the first. In a sample of 119 lone actor terrorists, they found that 35% of the sample virtually interacted with a wider network of political activists and that 46% learned aspects of their attack method through virtual sources. They also found that al-Qaeda inspired lone actors (65%) were significantly more likely to learn through virtual sources

[1] Computer registries essentially log all activities conducted on a computer.

[2] See the full report at www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

than their right-wing inspired (37%) or single-issue inspired (19%) counterparts. They also found that isolated dyads were significantly more likely to interact with co-ideologues online than those who committed their attacks alone. These latter results emerged from two inferential comparative analyses across ideologies and actor type. Using a range of inferential statistical techniques, Gill and Corner (2015) took this disaggregated comparative approach further and specifically compared the behaviours and traits of a sample of lone-actor terrorists who either (a) learned online or (b) interacted with co-ideologues online, with a sample of lone-actor terrorists who did neither. Their study came to seven main conclusions:

1. The growth of the Internet did not correlate with a rise in lone-actor terrorist activity year-on-year from 1990 to 2011.

2. There is a growing trend amongst lone-actors to make use of the Internet. In other words, whilst the Internet has not caused a growth in numbers of lone actor terrorists, it has altered their means of radicalisation and attack learning. The Internet, therefore, acts as a substitute for other factors such as intelligence gathering and attack planning, not necessarily a force enabler.

3. Younger offenders were significantly more likely to engage in both virtual learning and virtual interaction than older offenders.

4. The non-US based offenders were significantly more likely to learn through virtual sources.

5. Offenders who interacted virtually with co-ideologues were significantly less likely to successfully carry out a violent attack.

6. Offenders who made use of online tools to prepare for an attack were significantly less likely to kill or injure (despite being significantly more likely to plot an attack against indiscriminate soft targets).

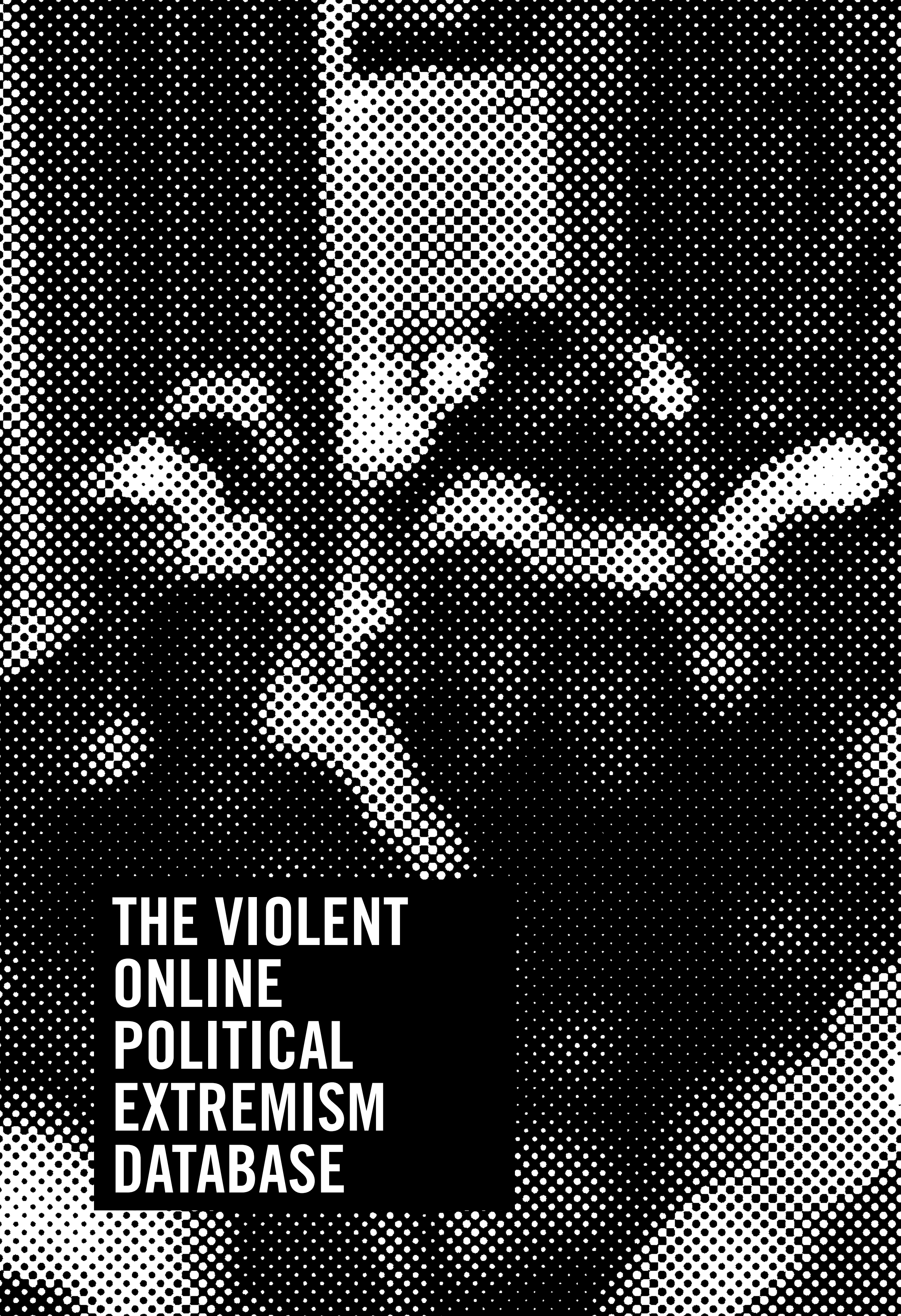
7. There was a significant positive correlation between those who virtually interacted with co-ideologues and who interacted with co-ideologues face-to-face. Radicalisation (at least for lone actors)

> is not a dichotomy of either offline or online, but rather a dichotomy of interaction with others versus no interaction with others.

The Gill and Corner (2015) and von Behr et al. (2013) studies stand apart from rest of the literature for their empirical focus on terrorist offenders. Despite the disparity in their sample size, data and method, they are largely in agreement about the role of the Internet in radicalisation particularly in three key facets. First, the Internet has not led to a rise in terrorism. Second, off-line interactions often go hand-in-hand with those online. Third, the Internet facilitates radicalisation, but does not accelerate it.

Gill and Corner (2015) also outlined a series of illustrative examples that highlighted the different forms of online learning undertaken and interaction engaged in by lone actors. Forms of virtual interactions included (a) reinforcing of prior beliefs; (b) seeking legitimisation for future actions; (c) disseminating propaganda and providing material support for others; (d) attack signalling; and (e) attempting to recruit others. Forms of virtual learning included (a) accessing ideological content; (b) opting for violence; (c) choosing a target; (d) preparing an attack; and (e) overcoming hurdles.

This study builds upon the Rand and Gill and Corner studies by quantifying the degree to which these behaviours occurred and by outlining the behavioural correlates of such activity. It seeks to further improve our empirical understanding of online radicalisation. It is focused upon finding out (a) whether those who interact virtually with like-minded activists, or learn online, display markedly different experiences (e.g. radicalisation, event preparation, attack outcomes) than those who do not; (b) whether the online space is an enabler for radicalisation or a substitute for previous locations in which radicalisation occurred; and (c) how the Internet has helped individuals overcome some of the hurdles involved in undertaking a terrorist attack. In some ways, this study is seeking to explain whether the previous findings by Gill and Corner (2015) regarding online activities are generalisable to the terrorist sample as a whole, or whether they are specific to lone-actors. But it also forges ahead in new domains of interest.



THE VIOLENT ONLINE POLITICAL EXTREMISM DATABASE

ANYONE FAMILIAR WITH the terrorism studies field will not be surprised by the lack of data-driven analyses noted above. Reviews of the literature have long since noted the paucity in data (Schmid and Jongman, 1988; Silke, 2001, 2004). Improvements are occurring, but tend to focus upon terrorist events as opposed to the terrorists who conduct them (Silke, 2013). The growth in empirical examinations of terrorist events is largely due to the provision of the Global Terrorism Database by the START consortium[3] and to the fact that terrorist events are much easier to observe, operationalise and code compared to the myriad factors that may be of interest in the coding of an individual and his/her motivation. This is not to say that the coding of individual terrorists is an impossible task, it is just comparatively more time-consuming and complex. The past decade has seen a small number of studies that utilised this approach provide remarkable insight into the cadres of Irish Republican groups (Horgan and Morrison, 2011; Gill and Horgan, 2013), ETA (Reinares, 2004), right-wing groups (Gruenewald et al., 2013) and al-Qaeda (Sageman, 2004), as well as lone-actor terrorists (Gill et al., 2014, Gill, 2015).

The data utilised in this report builds upon these types of data collection processes and analyses. Our remit was to create a comprehensive database of individuals reportedly radicalised via the Internet and conduct a series of quantitative and qualitative analyses of this data. In order to maximise the potential utility of this endeavour and its scientific rigour, a number of potential hurdles needed to be surmounted. First (and arguably most significantly), much of the terrorism studies literature suffers from a simple methodological problem: empirical studies on terrorism regularly sample on the dependent variable. Put simply, this process involves selecting cases only on the basis of a certain criteria being met, and only making using of these cases as evidence for the criteria. For example, Pape's (2005) study of suicide terrorism selects states that experienced suicide terrorism and then analyses what they shared in common

[3] See www.start.umd.edu for full details of the START consortium and www.start.umd.edu/gtd/search/Results.aspx?region= for the Global Terrorism Database.

(i.e. democratic structures, foreign occupation, etc.). He neglects to look at states that also share these characteristics but did not experience suicide terrorism. This has profound implications for the strength and generalisability of his findings (see Ashworth et al., 2008 for a full examination of Pape's sampling problems). If the present study were to simply consider only individuals reported to have been radicalised via the Internet, we would be unable to look at the correlates of terrorists' decisions to use the Internet as the data would not include those cases that neglected to use the Internet. In other words, we would be unable to falsify the claims we make or test hypotheses based on the arguments of the wider literature.
The decision was therefore made to build a database of terrorist actors and code for a number of Internet-related activities whether they were present or not. This meant we could capture a continuum of Internet-inspired actors from the fully uninspired to the fully inspired, and plot many positions along the way.

This decision had implications for how far we should spread our scope geographically and ideologically. Deciding to widen our net in terms of including the non-virtually radicalised necessitated tightening the net in other areas to allow for the sort of empirically rich data-crawl needed. The decisions taken here were a mixture of practical and conceptual ones. In order to build a dataset of terrorist actors, the first step is to build an actor dictionary (simply, a list of individuals to be coded). We needed our actor dictionary to be sufficiently large to allow for inferential statistical methods to be applied. However, it was decided that the actor dictionary must be limited to a single country in order to minimise the bias that might arise in the open-source reporting and availability of data cross-nationally. In other words, (online) radicalisation might be reported in very different ways in different countries such that the differences identified may just be the vagaries of culturally distinct reporting methods. To minimise bias, a single country with sufficient terrorism cases was deemed the most appropriate approach. Access to open sources is, of course, also key to the building of such a database; thus the availability of English language texts were also deemed crucial. This left us with two countries, the United Kingdom and the United States. We chose the

United Kingdom for a number of reasons: (a) prior research by Gill and Corner (2015) that showed higher levels of online behaviours in the UK sample vs. the US sample of lone actor terrorists; (b) availability of terrorism actor dictionaries; (c) spread of ideologically inspired actors; (d) location of the researchers; and (e) source of research funding. It was later decided to omit Irish Republican actors from the data collection activities as their online activities were rarely, if ever, mentioned in open source reporting. Their inclusion would, therefore, make the data analyses biased to an unacceptable extent as each field would be entered as a 'No', thus dramatically undercounting the likely representation of online behaviours by Irish Republicans.

The list of actors to be coded was identified through a number of sources. The most significant was the Simcox et al. (2011) study that lists all al-Qaeda inspired individuals convicted in the United Kingdom. For the purposes of this study, the list was updated through to the end of 2014. Further (largely extreme right-wing) names were also sourced through tailored search strings developed and applied to the LexisNexis "All English News" option. More individuals were also identified through START's Global Terrorism Database. Lone-actors were identified through previous studies (Gill et al., 2014). It was then decided to limit the population to post-1990 events because a large portion of our data was sourced from the LexisNexis[4] archive, which remains relatively limited pre-1990. Finally, we limited our scope to those who were either convicted in the UK or died in the commissioning of a terrorist act in the UK; British fighters in Syria and elsewhere were therefore omitted.

In total 227 offenders fit the specified geographical, temporal and operational criteria. Once the actor dictionary was compiled, the codebook was developed. 136 separate data points were coded for each actor. The variables included in the codebook span socio-demographic information (e.g. age, gender, occupation, family characteristics, relationship status, occupation, employment); network behaviours (e.g. number of co-offenders, training location);

[4] LexisNexis currently provides an electronic online archive from more than 20,000 global news sources.

event-specific behaviours (e.g. attack method(s), target(s)); and post-event behaviours and experiences (e.g. claim(s) of responsibility, arrest/conviction details). Data were collected on demographic and background characteristics and radicalisation-linked behaviours by examining and coding information contained in open-source news reports, sworn affidavits and, when possible, publically available first-hand accounts. The vast majority of data was culled from press reports via tailored LexisNexis searches. Additional information was gleaned from online public record depositories (e.g. documentcloud.org), terrorist biographies and relevant scholarly articles.

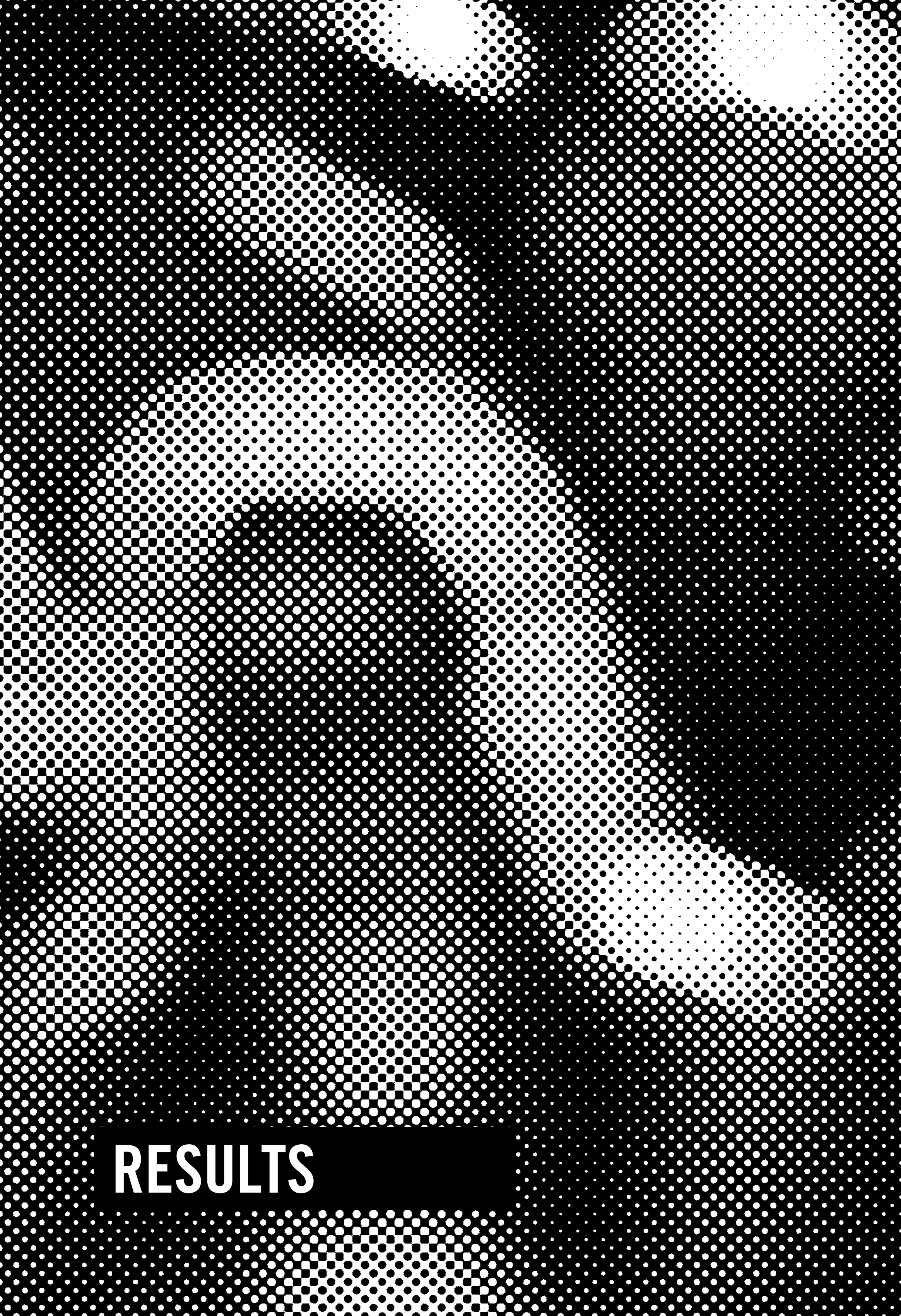
We also coded for attributes and behaviours commonly associated with online radicalisation. These questions were developed in two stages. The first stage developed from previous research conducted by the researchers on lone-actor terrorists (Gill et al., 2014; Gill and Corner, 2015). The Gill et al. (2014) study simply asked two questions related to online behaviour: Did the individual learn from virtual sources? Did the individual interact with co-ideologues online? The Gill and Corner (2015) study unpicked these two questions further and outlined a series of illustrative examples to show that the types of learning and interaction differed from case to case. These more disaggregated behaviours were coded for in this study. The second stage involved an iterative coding process with new questions developed as the data was collected and reviewed.

Two coders were tasked with coding the data on each terrorist offender. In cases where coders could not agree on the correct assignment of particular variables, differences were resolved based on an examination of the original sources that the coders relied upon to make their assessments. Such decisions factored in the comparative reliability and quality of the sources (e.g. reports that cover trial proceedings versus reports issued in the immediate aftermath of an event) and the sources cited in the report.

It is important to emphasise some limitations inherent in the sources used in this study. First, the sample only includes information on individuals who planned or conducted attacks reported in the media. It is possible incidents could be missed altogether because they either (a) led to convictions, but did not register any national media interest but may have been reported in local news sources not covered in the LexisNexis archives or (b) were intercepted or disrupted by security forces without a conviction being made. Second, as the level of detail reported varied significantly across incidents, data collection was limited to what could reasonably be collected for each terrorist offender. Third, it is often difficult to distinguish between missing data and variables that should be coded as a 'no'. Given the nature of newspaper and open-source reporting, it is unrealistic to expect each biographically oriented story to contain lengthy passages that list each variable or behaviour the offender did not engage in (e.g. the offender was *not* a substance abuser, a former convict, recently exposed to new media). For the statistical analyses that follow, where possible, we do report or distinguish between missing data and 'no' answers, but it should be kept in mind that the likely result is that 'no' answers are substantially undercounted in the analysis. Each variable in the analysis is treated dichotomously (e.g. the response is either a 'yes', or not enough information to suggest a 'yes'). There is precedent for this in previous research on attempted assassinations of public figures, fatal school shootings, and targeted violence affecting higher education institutions (Fein and Vossekuil, 1999; Vossekuil et al., 2002) as well as the terrorism offender datasets outlined at the outset of this sub-section. Unless otherwise stated, each of the figures reported below are of the whole sample (n=227). Finally, the fact that 'online radicalisation' is seen as a moral hazard means that the level of available granular behavioural data is far higher than for some other types of issues that could be equally important (such as family upbringing or other factors associated with exposure to extremist narratives). However, this granularity does not go so far as to consistently outline the website(s) relied upon, exact information gathered online, or frequency of Internet activity, for example.

Despite these limitations, open source accounts can provide rich data. This has been demonstrated in other studies focusing upon the socio-demographic characteristics, operational behaviours and developmental pathways of members of formal terrorist organisations and lone-actor terrorists (Gill and Horgan, 2014; Gill et al., 2014).

Reporting (and hence data availability) also tends to be richer when terrorism incidents are relatively rare and can therefore add great insight into terrorist offenders in the UK considering it remains a relatively low base-rate phenomenon.



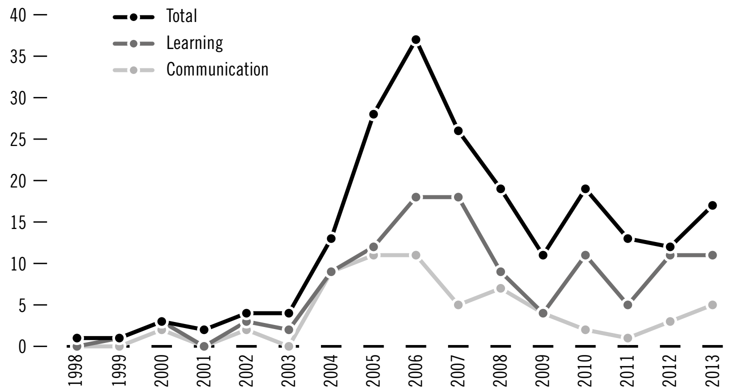
RESULTS

BASIC DESCRIPTIVE FINDINGS

The offenders captured in this database were largely male (96%). They ranged in age from 16 to 58 with a median age of 27, a mode of 22 and a mean of 28. One third were unemployed, a further one third worked in the service or administrative workforce and 14% were students. 22% had some form of university education. One half of the convictions related to a planned attack whilst the other half related to facilitative behaviours (e.g. financing, distributing propaganda). Only 14% of the convictions related to a completed attack.

The results suggest that key signals of intent to act, such as seeking legitimisation from epistemic authority figures (legitimisation) and announcing the intent to act (AttackSignal), rarely co-occur (e.g. they are on opposite ends of the two-dimensional space). As demonstrated within the matrix, commonly occurring behaviours such as passive consumption of websites (Websites) and extremists texts (Texts) are in the middle. To the bottom-right of this cluster are behaviours directly related to attacks and include behaviours related to attack preparation, target choice, overcoming difficulties in preparing the attack (Hurdles) and signalling intent (AttackSignal). On the direct-opposite side to these clusters (i.e. the top left) lie behaviours related to terrorist facilitation (rather than action) and include behaviours like disseminating propaganda (Dissemination), provision of material support and actively engaging with other co-ideologues in chatrooms and forums. These two clusters may distinguish violent online radicals from the wider population of non-violent online radicals.

Figure 1: Number of terrorism offenders per year



> *Turning to actors' virtual activities, in 61% of cases there was evidence of online activity related to their ultimate attack or conviction. The results indicate there is a substitution effect at play to some degree: greater Internet usage within the UK does not correspond with a surge in terrorist activity (see Figure 1), instead the number of arrests (black line) closely correspond to the onset of new and greater legislative powers in the UK What we can identify is the Internet shaping some of the pre-attack behaviours like online communication (lighter grey line), which is particularly the case from 2012 onwards with regards to online learning (darker grey line).*

As mentioned previously, we then disaggregated the content of this activity and these behaviours are rank ordered by popularity below.

Just over half (54%) of all actors used the Internet to learn about some aspect of their intended terrorist activity. From 2012 onwards, the figure is 76%.

Extremist media was found or downloaded and subsequently reported upon in the open-source domain for 44% of actors. In half of these cases (21%), the content was reported to be videos with smaller figures reported for lectures (7%) and photographs (6%). The content itself ranges broadly and includes videos of 9/11 and attacks on coalition forces; beheadings and executions; crimes

32%

A third of all actors prepared for their attacks using online resources

against Muslims in Chechnya, Afghanistan and Iraq; news footage of bombings; interviews with and speeches by Anwar al-Awlaki, Osama bin Laden, Abu Hamza and other radical preachers; pro-jihad rallies; bomb-making instruction videos and terrorist training videos.

A third (32%) prepared for their attacks using online resources. These included bomb-making instruction videos; poison manuals; *Inspire* magazine; surveillance advice; an assassination guidebook; torture techniques; suicide vest production; body disposal; plans for the London Underground, Buckingham Palace and other prestigious landmarks; MP voting records and terrorist training method manuals.

At least 30% accessed extremist ideological content online. In many cases, there was arguably too much material for any one individual to consume and understand thoroughly. One actor had 17,779 computer files of ideological material, 1,152 of which contained extremist content. This may be typical for those individuals that download materials in large volumes via BitTorrent.[5]

Just under a third (29%) of actors communicated with others virtually, half of whom did so via email (15%). Smaller figures were said to communicate with others via online discussion forums (8%) and chat rooms (9%). Some of these interactions circled around the legitimacy of targets. In one case, the interactions involved discussion of the comparative legitimacy of targeting civilians as opposed to civil servants or the police. In other cases, the interactions involved discussion of the intricacies of carrying out an attack. For example, one case involved a detailed discussion around the making of Hexamethylene Triperoxide Diamine (HMTD)[6] and how to develop the correct concentration of hydrogen peroxide.

Fifteen per cent of actors disseminated propaganda online. Some of these individuals set up specific websites for this purpose.

[5] A protocol that allows for transferring large amounts of data via peer-to-peer file sharing.

[6] A highly explosive organic compound.

For example, the administrators of the Aryan Strike Force website are included in the actor dataset. Others attempted to publish manuals concerning firearms and explosives on the Internet in order to incite others.

Evidence suggests that 14% of the offenders opted to engage in violence after witnessing something online. In one case, an individual read a letter on an extremist website about an Iraqi woman who said she had been repeatedly raped by her captors at Baghdad's Abu Ghraib; prison, he relayed that this made him firm-up his plans to take "positive action" in response.

One in ten of the sample used online resources to help overcome a hurdle they faced in the physical planning of an attack.

A small minority of individuals (9%) sought to recruit others online.

Whilst we outline above that a third of the sample prepared for some aspect of their attacks online, 9% specifically chose their target after online research. The analysis undertaken by police on one Islamist-inspired plot showed the plotters had used the Internet to research the English Defence League, their activists, and the locations of its leader for up to a month prior to the day they plotted to bomb an EDL rally.

Some (6%) provided material support to others online, for example by asking others to donate money to their cause or by selling *The Anarchist Cookbook* online.

A very few (5%) sought legitimisation for future actions from epistemic authority figures online; others did this indirectly by searching for fatwas and other legitimating texts. One individual conducted the following Google searches: "three places were [*sic*] you can kill someone in Islam", "three place [*sic*] were [*sic*] you can kill someone in Islam in punishment".

Five per cent also signalled online their plans to engage in attacks prior to the attack itself.

As mentioned in the data section, the degree to which actors utilised Internet sources was difficult to determine due to data unavailability. In the vast majority of cases it was only possible to identify whether the Internet was used or not. Isolated cases do provide some insight, but this is variable and not generalisable. One actor only began researching bomb-making techniques weeks before engaging in his attack whilst others reportedly spent months on Internet research, with one actor spending a reported six hours a day watching extremist footage and videos.

In most plots we see a great deal of the above outlined activities occurring. In the following sections, we outline these overlaps both qualitatively (through a brief overview of major terrorist plots) and quantitatively (through the use of a multi-dimensional scaling technique called Smallest Space Analysis).

QUALITATIVE ANALYSIS: BEHAVIOUR CLUSTERING

The purpose of this section is to outline a number of brief illustrative examples of serious terrorist plots/attacks in the UK The intention of these illustrations is to (a) provide greater context to the descriptive statistical results outlined above; (b) illustrate the strategic and/or tactical utility of turning to the Internet; (c) highlight that despite each case being alluded to as examples of 'online radicalisation', the actual co-occurring behaviours differ widely from case to case; and (d) provide the basis from which a quantitative analysis of behavioural clustering can be conducted.

The first illustration is that of David Copeland. His nail bombing campaign occurred between 17 and 30 April, 1999. In total, three bombs targeted minority communities across London. The bombings occurred over three successive weekends, killed three (including a pregnant woman), and injured a further 129. Two years previously, Copeland had tried to carry out an attack using a bomb 'recipe' from *The Terrorist's Handbook*, a manual that he downloaded from the Internet in April 1997. He purchased ammonium nitrate and the required detonators; he also managed to steal a large canister of nitric acid. However, the manual failed to provide an exhaustive list of all of the necessary explosive compounds, and Copeland found it "too complex" to manufacture and procure the missing chemical compounds by himself. Frustrated, Copeland temporarily gave up. In June 1998 he downloaded a second manual, *How to Make Bombs Part 2*. At first he tried to build a fertiliser bomb; he purchased liquid ammonium from a local medical supply shop and ordered rocket fuses, but again he failed to manufacture a fully functioning device. Copeland then sought to build smaller devices and again used the second manual to learn how to make a pipe bomb. Twelve years later, Anders Breivik faced similar problems while attempting to manufacture a series of car bombs. Breivik initially planned to build four IEDs. He began work on 3 May. On 5 May, Breivik ground aspirin tablets with a mortar and pestle and later with a dumbbell. On 6 May, Breivik began synthesising acetylsalicylic acid from the powdered aspirin. This proved problematic because the instructions he followed in the bomb-making manual he downloaded did not work. According to Breivik himself, he "began to somewhat panic...and began to lose heart" (Breivik, 2011: 1455). This delayed him for three days until a YouTube video provided a viable alternative solution that he tested successfully on 9 May 2011. Rather than downscaling the nature and complexity of his IED as Copeland did, Breivik had recourse to YouTube and a solution to his problem. The Copeland example offers two key insights with regard to the role of the Internet. First, his political socialisation occurred face-to-face within the British National Party but his attack planning was facilitated by his online activities. The two main aspects of radicalisation, ideological affinity and violent preparation were therefore compartmentalised into physical and virtual domains. Second, Copeland's difficulties were overcome by Breivik quite easily twelve years later, highlighting the ever-changing nature of aspects of virtual learning as new technologies develop and increase the capacity of malevolently intentioned actors.

In March 2004, Operation Crevice disrupted the Fertiliser Bomb Plot. This plot involved several conspirators buying 600kg of ammonium nitrate with the intent of developing a large IED that would target either a shopping market or the National Grid. The disruption was seen as the British Intelligence Services' first major success against a domestic al-Qaeda inspired terrorist plot. The five convicted plotters used Internet chat rooms on pornographic websites to communicate with each other about the plot and also emailed associates discussing how to manufacture detonators. The plotters also downloaded fertiliser bomb instruction manuals and purchased clothing and camping equipment online for training camps in Pakistan. Much of this activity occurred in an Internet café. Again, the openly available information about this case points to the fact that the Internet helped build capacity for the attack and not necessarily the willingness to conduct the attack in the first place. In other words, the Internet fostered internal cohesion, security, networks (both facilitative and action-oriented) and instruction. All of these activities are possible in the physical world, but the Internet perhaps provided greater security and easier access to these materials and people.

The 7 July 2005 London transit suicide bombers wanted to make use of the Internet to spread their message. They created a farewell video regarding the impending attack and wanted to produce a website to disseminate propaganda and other radicalising materials. They too downloaded information about explosives and how to manufacture bombs, watched videos of radical preachers and of violent crimes against Muslims in Chechnya, Afghanistan and Iraq. The failed suicide bomb attacks that followed two weeks later had far fewer press reports about their online activity, which is at odds with the reporting of other plots and attacks in which court testimony was heavily reported upon. The case was made in court, however, that the 21 July plotters watched bomb-making videos online, downloaded Bin Laden's speeches, and read online about crimes committed against Muslims in Iraq. These two cases differ from Copeland and Operation Crevice because there is clear evidence of the Internet's role across the arc of the terrorist plot – from attaining an ideological cause, deciding to act, and planning the attack to post-attack propaganda dissemination – these cases demonstrate that the Internet enabled every aspect of the plot but was not the sole contributor.

In August 2006, British intelligence disrupted a plot to detonate liquid explosives upon seven transatlantic flights. There is very little to distinguish this plot from the two in July 2005 in terms of their online behaviours. The plotters sent coded shared online messages and made efforts to make a documentary to be posted on YouTube about injustices against Muslims in the Middle East alongside their last will and testament videos. They utilised an Internet café to research flight timetables on the BAA Heathrow website, researched how to make explosive devices using soft drink bottles, found bomb-making recipes online and researched potential suppliers of hydrogen peroxide.

In June 2007, two individuals conducted coordinated car bomb attacks in London and a follow-up attack at Glasgow International Airport in which they drove their Jeep Cherokee loaded with propane canisters into the terminal doors. The perpetrators utilised jihadi forums and chat rooms and other more popular websites like YouTube that hosted extremist material. Using Internet message services, they logged hours of communications and later saved emails chronicling their plans to commit an attack in their drafts folders for family members to access them. They also utilised Skype to talk about bomb-making amongst themselves. On other websites, they researched bomb-making techniques, including how to set off a bomb with a mobile phone and later bought some components online. They also regularly posted on blogs and websites that promoted violence against the West, and downloaded speeches by Bin Laden alongside 15,000 files of ideologically inflammatory materials. The pattern set in motion during the July 2005 plots at this stage appears to become the norm, the Internet playing a facilitative or enabling role at many parts of the attack preparation and conduct stages. Each of these behaviours can occur offline, however, so again these are depicted as cyber-enabled behaviours rather than cyber-dependent.

On 14 May, 2010, student Roshonara Choudhry stabbed Stephen Timms, a Labour Party Member of Parliament, causing him serious bodily injury. Investigators established that Choudhry began downloading Anwar al-Awlaki's videos and sermons in the autumn and winter of 2009. She began spending an abundance of time in her bedroom; her parents believed she was studying, but in reality she was downloading extremist material, including more than 100 hours of al-Awlaki's sermons. It was supposedly during this time that Choudhry decided to engage in a violent attack. During her police interview, Choudhry responded to a question concerning the transition from immersing herself in religion to committing violence by stating: "Because as Muslims we're all brothers and sisters and we should all look out for each other and we shouldn't sit back and do nothing while others suffer. We shouldn't allow the people who oppress us to get away with it and to think that they can do whatever they want to us and we're just gonna' [*sic*] lie down and take it". Choudhry referred to a specific YouTube video of Sheikh Abdullah Azzam that made her understand "even women are supposed to fight" and that she had an obligation to turn toward violence. According to the police interviews, Choudhry had this realisation at some point in April and soon after began her preparations for the attack.

As part of her preparations, Choudhry devised a list of Members of Parliament who voted for the 2003 invasion of Iraq. She researched the backgrounds of London-based Members of Parliament using the website 'They Work For You', which includes information on voting records. She appears to have concentrated her research on Labour ministers Jim Fitzpatrick, Margaret Hodge, Nick Raynsford and Stephen Timms. Detectives later declared that Timms was her "sole and easiest target". The decision to attack Timms, Choudhry's local Member of Parliament, was made three to four weeks prior to the attack itself. Her online research showed that Timms regularly voted with his political party, which held power at that time. Choudhry later told detectives that, "he just voted strongly for everything, as though he had no mercy. As though he felt no doubts that what he was doing was right even though it was such an arrogant thing to do and I just felt like if he could treat the Iraqi people so mercilessly, then why should I show him any mercy?" The Choudhry case appears to buck the trend of the previous illustrations and may be a result of her (a) being a lone actor (in a far greater Internet-dependent world than Copeland operated within 10 years prior); (b) adopting an extremist ideology in the absence of co-ideologues in the physical world, most likely because of her gender; and (c) choosing a primitive attack type. Whereas the balance in the other cases tipped towards attack facilitation, this is the first illustration where ideological attainment appears to be far more dependent upon virtual behaviours.

In June 2013, Ian Forman's plot to firebomb a number of mosques in the Liverpool area was disrupted. Forman had previously communicated his desire to "blow them up" in a series of YouTube posts.

He had also conducted some online surveillance of his targets, downloading pictures of Mosques in his home town and, following months of Internet research, drawing-up a shopping list of bomb components. Where the Forman plot differs from the other two lone actor cases is that (a) he chose a far more complex attack type than Choudhry's, necessitating greater online learning, and (b) the greater powers of the Internet allowed for more sophisticated surveillance techniques to be used in the attack planning compared to Copeland in 1999 whose attack planning was riddled with basic errors (see Gill, 2015 for a full analysis of Copeland's decision-making).

> *These cases are very different in terms of ideological underpinnings, attack types chosen, and network structure (ranging from lone actors to big cells). However, they share a number of commonalities. The use of the Internet was largely for instrumental purposes whether it be pre-attack (e.g. surveillance, learning, practice, communication) or post-attack (e.g. disseminating propaganda). In criminological terms, these activities were cyber-enabled rather than cyber-dependent. There is little-to-no evidence to suggest the Internet was the sole explanation that got actors to the point of deciding to engage in a violent act. Instead, it was just one factor amongst many that helped crystallise motivation, intent and capability at the same time and place. Evidence further suggests that many went online not to have their beliefs changed but rather reinforced. In the aftermath of Ian Davison's trial (in which his son was also convicted on other offences) for developing ricin, police sources noted that Davison's "views developed over time. After going online he accessed websites and started to look at places where those kinds of views were shared with other people". This further confirms the "echo chamber" hypothesis put forward in the von Behr et al. (2013) study mentioned earlier. The above cases are just illustrations, however. In the next section, we seek to quantitatively test whether certain behaviours are more closely correlated within our wider sample of plotters.*

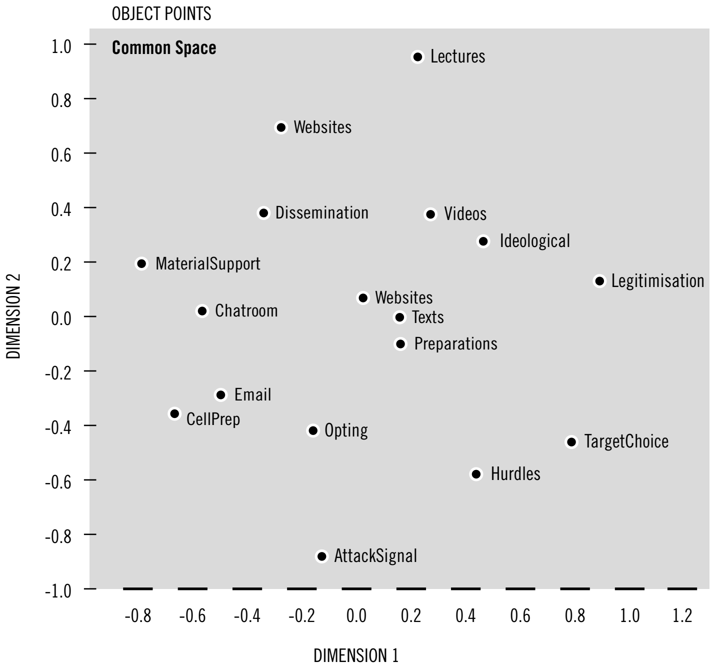
QUANTITATIVE ANALYSIS: BEHAVIOUR CLUSTERING

The above illustrations are problematic in terms of generalisable validity and reliability, so the decision was taken to look at quantitative correlations between the various online behaviours that we described in the results for above. Pearson correlations show a high degree of positive correlation across the various online behaviours. However, these results are entirely dyadic and there may be intervening variables causing these associations. Such concerns may therefore warrant the use of multi-dimensional scaling (MDS) techniques, which uncover distinctive clusters of variables by providing geometric representations of the level of association between variables. In other words, MDS outputs represent a matrix wherein variables that regularly co-occur are plotted closer together in a Euclidean space. The utility of such a representation is that the variable configuration is based upon variables' relationships with each other rather than their relationships with pre-determined dimensions (Davis, 2009:508).

One form of MDS, Smallest Space Analysis (SSA), has been used to examine a wide spectrum of offences including sexual assault (Alison and Stein, 2001; House, 1997; Canter et al., 1998), homicide (Godwin, 2000; Salfati and Canter, 1999), arson (Canter and Fritzon, 1998), stalking, (Canter and Ioannou, 2004) and terrorism events involving hostage taking (Fritzon et al., 2001). SSA is "based upon the assumption that the underlying structure of complex systems is most readily appreciated if the relationship between each and every other variable is examined, but that such examination is much clearer if the relationships are represented visually not only in terms of numbers" (Canter et al., 2004:308).

The analysis below depicts an SSA output based on the online behaviours quantified earlier. The Jaccard co-efficient, which represents the level of association between two variables, was calculated for each pair-wise set of variables. The closer two variables appear within the matrix, the higher their co-occurrence across observations.

Figure 2: Smallest space analysis of 17 online behaviors



The results suggest that key signals of intent to act, such as seeking legitimisation from epistemic authority figures (legitimisation) and announcing the intent to act (AttackSignal), rarely co-occur (i.e. they are on opposite ends of the two-dimensional space). A cluster of behaviours on the right-side indicates that in many cases offenders both opted (Opting) to engage in violence and prepared for their attacks (Preparation) in virtual spaces and that much of this was aided by online ideological content (Ideological), such as videos, lectures and texts. On the other hand, the left-hand cluster indicates a different set of behaviours linked to the passive consumption of static websites that are more closely aligned with the provision of material support and target choices.

INFERENTIAL FINDINGS

In order to compare those actors who engaged in online activities with those who did not, we followed the procedures in Gruenewald et al. (2013). We first conducted a series of bivariate tests such as chi-square analyses and, where appropriate, Fisher's exact tests. The significant differences between these sub-sets are explained below. A series of odds-ratios were then calculated.

First, we examined the differences between those who learned online and those who did not. We found:

1. Extreme right-wing offenders were 3.39 times more likely to learn online than al-Qaeda inspired individuals. A regression analysis indicates that this disparity was largely accounted for through the use of extremist websites and the downloading of extremist images. There was no significant difference in terms of their propensity to utilise videos, lectures, extremist texts or other media. A second regression analysis indicated that the sole difference in terms of the instrumentality of the learning was in attack preparation. Extreme right-wing offenders were 4.19 times more likely to utilise online learning for attack preparation. There was no significant difference in terms of opting for violence, target choice, or overcoming hurdles.

2. Those who plotted to attack a government target (as opposed to the civilian population) were 4.50 times more likely to learn online. Indeed 83% of those who plotted to attack a government target displayed traits of online learning. This significant finding holds when offenders convicted of facilitative activities were omitted. Of all those who actually plotted an attack, those who targeted the government were 3.58 times more likely to have learned online.

3. Of those who plotted an actual attack, those who targeted the military were significantly less likely to have learned online.

4. Those who used/plotted to use an Improvised Explosive Device (IED) were 3.34 times more likely to have learned online. Those

who utilised an IED in an actual attack were 4.57 times more likely to have learned online. This is a reflection of the relative ease of availability of bomb-making manuals and YouTube videos that provide helpful demonstrations.

5. Those who used more primitive attack types like arson or unarmed assaults were significantly less likely to have learned online. Similarly, those who plotted an attack at a non-government location were significantly less likely to have learned online.

6. Those who were members of a cell were significantly less likely to have learned online than lone actors. This may be a reflection that within a cell there is likely to be a pooling of human, social, technical and financial capital, the absence of which leads individuals to go online to learn how to conduct attacks. The corresponding finding that lone actors who tried to recruit others (and failed) were five times more likely to have learned online also lends credence to this interpretation.

7. The evidence suggests that online learning was also significantly more likely to be accompanied by face-to-face interactions with non-violent co-ideologues. Those who learned online were 4.39 times more likely to have experienced non-virtual network activity and 3.17 times more likely to have experienced non-virtual place interaction. Of those who plotted an attack, the individuals who attended training camps were also significantly more likely to have learned online. This finding confirms the earlier research of von Behr et al. (2013) and Gill and Corner (2015).

Second, we examined the differences between those who communicated online and those that did not. We found:

1. Extreme right-wing offenders were 2.41 times more likely to have communicated online with co-ideologues than al-Qaeda inspired individuals. This may be a function of the differing circumstances these ideological movements experience in the UK The UK's extreme-right movement tending to be located online (Thornton,

7.4%
of those who plotted against the military communicated online with co-ideologues

2015) and extreme right-wing terrorist activity more likely to be conducted by lone actors in the UK (Gill, 2015). A regression analysis indicated that this disparity was largely accounted for by extreme-right wing offenders' greater propensity to use extremist online forums. There was no difference in terms of email or chat room usage. The latter forms of communication were more likely to be used for communication with (a) non-violent radicals and (b) non-radicals. There was no difference in terms of extreme-right wing actors' propensity to communicate online with other cell members or other terrorists. A final predictor of this disparity was extreme-right offenders' greater likelihood of having used the Internet to disseminate propaganda compared to al-Qaeda inspired individuals. There was no significant difference in terms of reinforcing prior beliefs, seeking legitimisation for future actions, disseminating propaganda, providing material support to others, or attack signalling.

2. Those who targeted the military were significantly less likely to have communicated online. Only 7.4% of those who plotted against the military communicated online with co-ideologues.

3. Those who targeted property were twice as likely to communicate online than those who did not.

4. Those who plotted to use an IED were 1.78 times more likely to have communicated online.

5. The evidence also suggests that communicating with co-ideologues online was significantly more likely to have been accompanied by face-to-face interactions with non-violent co-ideologues. Those who communicated online were 3.89 times more likely to have experienced non-virtual network activity and 3.17 times more likely to have experienced non-virtual place interaction. Of those who plotted an attack, the individuals who attended training camps were also significantly more likely to have communicated online. This finding confirms the earlier research of von Behr et al. (2013) and Gill and Corner (2015).

DISCUSSION AND CONCLUSION

COLLECTIVELY THE BASIC descriptive results, illustrative case studies, multi-dimensional scaling techniques, and inferential statistical methods provide much insight and instruction for the study of radicalisation as a whole and not just online radicalisation. The results also largely confirm the results found in von Behr et al. (2013) and Gill and Corner (2015). The Internet has not led to a rise in terrorism. It is largely a facilitative tool; radicalisation is enabled by the Internet rather than being dependent upon it. These three studies have now covered these questions with a number of different methodological approaches and samples and have arrived at largely the same conclusions.

The results provide further confirmation of the need for disaggregated approaches to understanding terrorists. Traditionally, academic studies have focused upon aggregate understandings of terrorists or the 'radicalised'. However this aggregate understanding hides the complexities that may differ across ideologies, across roles and across networked structures. Treating all terrorists in such a manner differs from criminological approaches that tend to split the outcome variable (Monahan, 2012) across crime types, or offender types (e.g. violent versus non-violent). This study illustrated the value to be gained from such distinctions and we regularly uncovered behavioural differences online in terms of target type, ideological motivations and attack types.

> *The study also draws attention to the alleged dichotomy of online versus offline radicalisation. There is no easy offline versus online radicalisation dichotomy to be drawn. It is a false dichotomy. Plotters regularly engage in activities in both domains. Often their behaviours are compartmentalised across these two domains. For example, plotters may engage in face-to-face interaction regarding the ideological legitimacy of their actions whilst engaging in virtual communication regarding the technical specificity of bomb-making. Threat management procedures would do well to understand the individuals' breadth of interactions rather than relying upon a dichotomous understanding of offline versus online, which represent two extremes of a spectrum that regularly provide prototypical examples in reality.*

As previously mentioned, emerging research argues that rather than analysing the 'terrorist' on an aggregate level, it might be more instructive to disaggregate our conception of the 'terrorist' into discrete groups (e.g. foreign fighters versus homegrown fighters, bomb-makers versus bomb-planters, group-actors versus lone actors) (LaFree, 2013). Our results suggest that any of those disaggregated approaches should not dichotomise whether radicalisation occurred online or offline. The reality is that in the vast majority of cases it is both. The multi-dimensional scaling also shows that online behaviours can take a multiplicity of forms. We found significant differences across targeting strategies, ideologies and network forms and actors' propensity to engage in online learning and communication. However, the question remains whether these differences were caused by the needs inherent in such activities or whether access to particular online materials sparked these changes in behaviour. In other words, we are left with a chicken and egg situation: did the decision to target military forces necessitate the need to go online and develop capacity or did access to materials promoting the need to target military forces direct potential offenders toward that end?

The types of analyses conducted in this study are unable to answer these questions with great confidence, however, because the granularity of the data does not allow for sequential analyses to be undertaken. Only through engaging with hard drives of convicted terrorists can such research be undertaken. In saying that, the narrative that the needs of a plot drive online search behaviour seems to make more intuitive sense given the findings herein. Selection of some harder targets led to online learning. Technically more difficult attacks like IEDs led to more online searching compared to primitive attack types. Lone-actors needed to learn more online because they lacked the pooling of human talent typically found in an attack cell. Extreme-right wing offenders were more likely than violent Jihadists in the UK to learn and communicate online, which may be due to the structural unavailability of co-offenders in their vicinity and being more likely to be lone-actors. Finally, as illustrated throughout, rare were the cases of everything being conducted online. Face-to-face interactions were still key to the process for the vast majority of actors even if they were aware of, and made use of, the bounty of ideological and training material available online. Radicalisation should therefore be framed as cyber-enabled rather than cyber-dependent whilst also underlining that enabling factors differ from case to case depending upon need (e.g. who to attack, what tactic to use) and circumstance (e.g. availability of co-offenders, expertise, ideology).

REFERENCES

Alison, L., Snook, B., and Stein, K. (2001). "Unobtrusive Measurement: Using Police Information for Forensic Research", *Qualitative Research* 1, 241–254.

Ashworth, S., Clinton, J. D., Meirowitz, A., and Ramsay, K. W. (2008). "Design, Inference, and the Strategic Logic of Suicide Terrorism", *American Political Science Review*, *102*(02), 269–273.

Borum, R. (2013). "Informing Lone-Offender Investigations", *Criminology and Public Policy*, *12*(1), 103–112.

Canter, D., and Fritzon, K. (1998). "Differentiating Arsonists: A Model of Firesetting Actions and Characteristics", *Legal and Criminological Psychology* 3, 73–96.

Canter, D. M., and Ioannou, M. (2004). "A Multivariate Model of Stalking Behaviours", *Behaviormetrika* 31, 113–130.

Canter, D., Hughes, D., and Kirby, S. (1998). "Paedophilia: Pathology, Criminality, or Both? The Development of a Multivariate Model of Offence Behavior in Child Sexual Abuse", *The Journal of Forensic Psychiatry* 9, 532–555.

Canter, D., Alison, L. J., Alison. E., and Wentink, N. (2004). "The Organized/Disorganized Typology of Serial Murder: Myth or Model?", *Psychology, Public Policy and Law 10*(3), 293–320.

Davis, M. R. (2009). In Defence of Multidimensional Scaling for the Analysis of Sexual Offence Behaviour: Cautionary Notes Regarding Analysis and Interpretation. *Psychology, Crime and Law*, *15*(6), 507–515.

Fein, R. A., and Vossekuil, B. (1999). "Assassination in the United States: An Operational Study of Recent Assassins, Attackers, and Near-lethal Approachers", *Journal of Forensic Sciences*, *44*(2), 321–333.

Fritzon, K., Canter, D., and Wilton, Z. (2001). “The Application of an Action System Model to Destructive Behaviour: The Examples of Arson and Terrorism”, *Behavioral Sciences and the Law* 19, 657–690.

Gill, P., and Horgan, J. (2013). “Who Were the Volunteers? The Shifting Sociological and Operational Profile of 1240 Provisional Irish Republican Army Members”, *Terrorism and Political Violence, 25*(3), 435–456.

Gill, P., Horgan, J., and Deckert, P. (2014). “Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists,” *Journal of Forensic Sciences, 59*(2), 425–435.

Gill, P. (2015). *Lone-Actor Terrorists: A Behavioural Analysis.* London: Routledge.

Gill, P. and Corner, E. (2015). “Lone-Actor Terrorist Use of the Internet and Behavioural Correlates”, in *Terrorism Online: Politics, Law, Technology and Unconventional Violence*, L. Jarvis, S. Macdonald and T. Chen (eds.). London: Routledge.

Godwin, G. M. (2000). *Hunting Serial Predators: A Multivariate Classification Approach to Profiling Violent Behavior*. Florida: CRC Press.

Gruenewald, J., Chermak, S., and Freilich, J. D. (2013a) “Distinguishing ‘Loner’ Attacks from Other Domestic Extremist Violence”, *Criminology and Public Policy, 12*(1), 65–91.

Horgan, J., and Morrison, J. F. (2011). “Here to Stay? The Rising Threat of Violent Dissident Republicanism in Northern Ireland,” *Terrorism and Political Violence, 23*(4), 642–669.

House, J. C. (1997). “Towards a Practical Application of Offender Profiling: The RNC’s Criminal Suspect Prioritization System”. In J.L. Jackson and D. A. Bekerian (Eds.), *Offender Profiling: Theory, Research and Practice* (pp.177–190). Chichester: Wiley.

LaFree, G. (2013). “Lone-Offender Terrorists”. *Criminology and Public Policy, 12*(1), 59–62.

Monahan, J. (2012). “The Individual Risk Assessment of Terrorism”, *Psychology, Public Policy, and Law, 18*(2), 167.

Neumann, P. (2013). “Options and Strategies for Countering Online Radicalization in the United States”, *Studies in Conflict and Terrorism, 36*(6), 431–459.

Omotoyinbo, F. R. (2014). “Online Radicalisation: The Net or the Netizen?”, *Social Technologies*, (01), 51–61.

Reinares, F. (2004). “Who are the Terrorists? Analyzing Changes in Sociological Profile Among Members of ETA”, *Studies in Conflict and Terrorism, 27*(6), 465–488.

Sageman, M. (2008). “The Next Generation of Terror”, *Foreign Policy, 165*, 36–42.

Sageman, M. (2004). *Understanding Terror Networks*. Pittsburgh: University of Pennsylvania Press.

Salfati, C., and Canter, D. (1999). “Differentiating Stranger Murders: Profiling Offender Characteristics from Behavioral Styles”, *Behavioral Sciences and the Law* 17: 391–406.

Schmidt, A. P., and Jongman, A. I. (1988). *Political Terrorism: A Research Guide to Concepts, Theories, Databases and Literature.* North Holland Publishing Company: Amsterdam and New Brunswick.

Silke, A. (2001). “The Devil You Know: Continuing Problems with Research on Terrorism”, *Terrorism and Political Violence, 13*(4), 1–14.

Silke, A. (2004). “The Road Less Travelled: Recent Trends in Terrorism Research”. In A. Silke (ed.), *Research on Terrorism: Trends, Achievements and Failures*, 186–213. London: Routledge.

Silke, A. (2013). “Research on Terrorism: A Review of the Impact of 9/11 and the Global War on Terrorism”. In Adam Dolnik (ed.), *Conducting Terrorism Field Research: A Guide.* London: Routledge.

von Behr, I., Reding, A., Edwards, C., and Gribbon, L. (2013). *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Retrieved from www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

Vossekuil, B., Fein, R. A., Reddy, M., Borum, R., and Modzeleski, W. (2002). *The Final Report and Findings of the Safe School Initiative*. Washington, DC: US Secret Service and Department of Education.

APPENDIX 1 – 200 RESOURCES REFERENCING 'ONLINE RADICALISATION'

Abigail, P., and Desker, B. (2009). Countering Internet Radicalisation in Southeast Asia. Barton: Australian Strategic Policy Institute.

Agarwal, S., and Sureka, A. (2014). A Focused Crawler For Mining Hate and Extremism Promoting Videos on YouTube. In *Proceedings of the 25th ACM conference on Hypertext and social media* (pp. 294–296). ACM.

Akbar, A. A. (2013). Policing 'Radicalization'. *Ohio State Public Law Working Paper*, (210).

Akhgar, B., and Arabnia, H. R. (Eds.). (2013). *Emerging Trends in ICT Security*. Waltham, MA: Elsevier.

Alexander, D. C. (2010). Offline and Online Radicalization and Recruitment of Extremists and Terrorists. *Journal of Homeland Security*, September.

Alexander, D. C. (2010). The Radicalization of Extremists/Terrorists-Why It Affects You. *Security*, *47*(7), 42–43.

Alexander, D. C. (2011). Al Qaeda and al Qaeda in the Arabian Peninsula: Inspired, Homegrown Terrorism in the United States. *Journal of Applied Security Research*, *6*(4), 467–482.

Alhadlaq, A. (2013). Radicalization and Rehabilitation in Saudia Arabia. http://repository.nauss.edu.sa/handle/123456789/59687

Almagor, R. C. (2014). People Do Not Just Snap: Watching the Electronic Trails of Potential Murderers. *J Civil Legal Sci*, *3*(113), 2169–0170.

Alqahtani, Y. (2013). *Saudi Counter-Terrorism Strategy: Identifying and Applying Lessons Learned.* Carlisle Barracks, PA: US Army war College.

Aly, A. (2012). An Audience-Focused Approach to Examining Religious Extremism Online. *Australian Journal of Communication, 39*(1), 1.

Aly, A., Weimann-Saks, D., and Weimann, G. (2014). Making 'Noise' Online: An Analysis of the Say No to Terror Online Campaign. *Perspectives on Terrorism, 8*(5).

Ampofo, L. P. (2011). *Terrorism 3.0: Understanding Perceptions of Technology, Terrorism and Counter-Terrorism in Spain* (Doctoral dissertation, University of London).

Andre, V. (2014). The Janus Face of New Media Propaganda: The Case of Patani Neojihadist YouTube Warfare and Its Islamophobic Effect on Cyber-Actors. *Islam and Christian–Muslim Relations, 25*(3), 335–356.

Anzalone, C. (2012). The Evolution of an American Jihadi: The Case of Omar Hammami. *CTC Sentinel, 5*(6).

Archetti, C. Terrorism, Counterterrorism and the New Media: Explaining Radicalization in the Digital Age. *Perspectives on Terrorism* 9(1) www.terrorismanalysts.com/pt/index.php/pot/article/view/401/html

Argomaniz, J. (2015). European Union Responses to Terrorist Use of the Internet. *Cooperation and Conflict, 50*(2), 250–268.

Ariely, G. A. (2014). Adaptive Responses to Cyberterrorism. In T.Chen, L. Jarvis and S. Macdonald (eds) *Cyberterrorism: Understanding, Assessment and Response* (pp. 175–195). Springer New York.

Arunachalam, R., and Sarkar, S. (2013). The New Eye of Government: Citizen Sentiment Analysis in Social Media. In *Sixth International Joint Conference on Natural Language Processing* (p. 23).

Asghar, M. Z., Ahmad, S., Marwat, A., and Kundi, F. M (2015). Sentiment Analysis on Youtube: A Brief Survey. http://brisjast.com/wp-content/uploads/2014/12/Jan-124-2015.pdf/

Ashour, O. (2011). Online De-Radicalization? Countering Violent Extremist Narratives: Message, Messenger and Media Strategy. *Perspectives on Terrorism, 4*(6).

Awan, A. N. (2012). Jihadi Ideology in the New-Media Environment. In Deol, J. and Kazmi, Z. (eds.) *Contextualising Jihadi Thought*. London: C. Hurst and Co.

Bachmann, V., Bialasiewicz, L., Sidaway, J. D., Feldman, M., Holgersen, S., Malm, A. and Simonsen, K. (2012). Bloodlands: Critical Geographical Responses to the 22 July 2011 Events in Norway. *Environment and Planning D: Society and Space*, *30*(2), 191–206.

Ball, L., and Craven, M. (2013). Automated Counter-Terrorism. In 2013 European Intelligence and Security Informatics Conference: IEEE. pp.216.

Bates, R. A., and Mooney, M. (2014). Psychological Operations and Terrorism: The Digital Domain. *The Journal of Public and Professional Sociology*, *6*(1), 2.

Bates, R., and Mooney, M. (2014). Distance Learning and Jihad: The Dark Side of the Force. *Online Journal of Distance Learning Administration*, *17*(3).

Bergin, A. (2009). *Contest Two and Counter Extremism: Lessons for Australia*. Australian Strategic Policy Institute.

Bergin, A., and Ungerer, C. (2010). *Homeward Bound: Australia's New Counter-Terrorism White Paper*. Australian Strategic Policy Institute.

Bermingham, A., Conway, M., McInerney, L., O'Hare, N., and Smeaton, A. F. (2009, July). Combining social network analysis and sentiment analysis to explore the potential for online radicalisation. In *Social Network Analysis and Mining, 2009. ASONAM'09. International Conference on Advances in* (pp. 231–236). IEEE.

Betz, D. J. (2012). Cyberspace and Insurgency. *Routledge Handbook of Insurgency and Counterinsurgency*. London: Routledge.

Bizina, M., Northfield, V. T., and Gray, D. H. (2014). Radicalization of Youth as a Growing Concern for Counter-Terrorism Policy. *Global Security Studies*, *5*(1).

Blanquart, G., and Cook, D. M. (2013). Twitter Influence and Cumulative Perceptions of Extremist Support: A Case Study of Geert Wilders. Proceedings of the 4th Australian Counter Terrorism Conference, Edith Cowan University, Perth, Western Australia.

Bloom, M. (2013). In Defense of Honor: Women and Terrorist Recruitment on the Internet. *Journal of Postcolonial Studies, 4*(1), 150–195.

Borum, R. (2011). Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security, 4*(4), 2.

Boucek, C. (2008). The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia. *CTC Sentinel, 1*(9).

Bowman-Grieve, L., and Conway, M. (2012). Exploring the Form and Function of Dissident Irish Republican Online Discourses. *Media, War and Conflict, 5*(1), 71–85.

Bowman, E. K. (2012, May). Persistent ISR: the Social Network Analysis Connection. In *SPIE Defense, Security, and Sensing* (pp. 83891F-83891F). International Society for Optics and Photonics.

Brandon, J., and Vidino, L. (2012). European Experiences in Counterradicalization. West Point: *Combating Terrorism Center at West Point.*

Breslin, J. (2010). Focused Concept Detection and Polarity Measurement of Web Video Using Social Context. http://journal.webscience.org/378/

Briggs, R., and Feve, S. (2013). *Review of Programs to Counter Narratives of Violent Extremism.* London: Institute of Strategic Dialogue.

Brown, I. (2010). Internet Self-Regulation and Fundamental Rights. *Index on Censorship, 1.*

Brown, I. (2011). Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, *19*(2), 95–109.

Browne, D., and Silke, A. (2011). 'The Impact of the Media on Terrorism and Counter-Terrorism". *The Psychology of Counter-Terrorism (London: Routledge, 2011)*, 89–110.

Cantwell, D. M. (2008). *Force of No Choice: The Role of the Military in Interagency Operations*. Army Command and General Staff Coll Fort Leavenworth KS School of Advanced Military Studies.

Carvalho, C. (2014). 'Okhti' Online. Spanish Muslim Women engaging online Jihad–a Facebook case study. *Online-Heidelberg Journal of Religions on the Internet*, *6*.

Chalothorn, T., and Ellman, J. (2012). Sentiment Analysis Of Web Forums: Comparison Between SentiWordNet And SentiStrength. The 4th International Conference on Computer Technology and Development (ICCTD 2012). 24–25 November 2012.

Chalothorn, T., and Ellman, J. (2013). Affect Analysis of Radical Contents on Web Forums Using SentiWordNet. *International Journal of Innovation Management and Technology*, *4*(1), 122–124.

Chalothorn, T., and Ellman, J. (2012). Using SentiWordNet and Sentiment Analysis for Detecting Radical Content on Web Forums. Proceedings of the 6th Conference on Software, Knowledge, Information Management and Applications.

Chen, T. M., Jarvis, L., and MacDonald, S. (2014) *Cyberterrorism: Understanding, Assessment and Response*. Springer New York.

Cheong, P. H. (2014). New Media and Terrorism. In M.Eid (ed.) *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia*, 184.

Choudhury, S., and Breslin, J. G. (2010). User Sentiment Detection: a YouTube Use Sase. 21st National Conference on Artificial Intelligence and Cognitive Science.

Coar, K. R. (2013). Islamist Radicalization in the United States and the Influence of Western Jihadist Ideologues. http://sdsu-dspace.calstate.edu/handle/10211.10/4763

Cole, J. (2012). Radicalisation in Virtual Worlds: Second Life Through the Eyes of an Avatar. *Journal of Policing, Intelligence and Counter Terrorism*, *7*(1), 66–79.

Conway, M. (2012). From al-Zarqawi to al-Awlaki: The Emergence and Development of an Online Radical Milieu. *CTX: Combating Terrorism Exchange*, *2*(4), 12–22.

Conway, M. (2012). Introduction: Terrorism and Contemporary Mediascapes: Reanimating Research on Media and Terrorism. *Critical Studies on Terrorism*, *5*(3), 445–453.

Conway, M. (2014). From "Cyberterrorism" to "Online Radicalism". In M.Eid (ed.) *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia*, 198.

Conway, M., and McInerney, L. (2008). Jihadi Video and Auto-Radicalisation: Evidence from an Exploratory YouTube Study. In *Intelligence and Security Informatics* (pp. 108–118). Springer Berlin Heidelberg.

Conway, M., and McInerney, L. (2012). What's Love Got To Do With It? Framing 'JihadJane'in the US press. *Media, War and Conflict*, *5*(1), 6–21.

Cook, D. M. (2010). The Use Of Governance To Identify Cyber Threats Through Social Media. In *International Cyber Resilience Conference* (p. 31).

Cook, D. M. (2014). Birds of a Feather Deceive Together: The Chicanery of Multiplied Metadata. *Journal of Information Warfare*, *13*(4), 85–96.

Corb, A. (2014). Online Hate and Cyber-Bigotry. In Hall, N., Corb, A., Giannasi, P., and Grieve, J. (eds.) *Routledge International Handbook on Hate Crime*, (Routledge International Handbooks) London: Routledge p.306.

Corb, A., and Grozelle, R. (2014). A New Kind of Terror: Radicalizing Youth in Canada. *Journal Exit-Deutschland: Zeitschrift für Deradikalisierung und demokratische Kultur*, *1*, 32–58.

Correa, D., and Sureka, A. (2013). Solutions to Detect and Analyze Online Radicalization: A Survey. *arXiv preprint arXiv:1301.4916*.

Damanuri, A. (2014). Muslim Diaspora dalam Isu Identitas, Gender, dan Terorisme. *ISLAMICA: Jurnal Studi Keislaman*, *6*(2), 232–251.

Domina, T. B. K. (2012). Domestic Extremism in Europe.Athena Institute: http://athenainstitute.eu/pdf/EUR_MAP_STUDY_ENG_closed.pdf

Doyle, J. (2012). New Media and Democratisation. *Irish Studies in International Affairs*, *23*(1), 1–4.

Earnhardt, R. L. (2014). Al-Qaeda's Media Strategy: Internet Self-Radicalization and Counter-Radicalization Policies. *Digital America*, *4*(3).

Edwards, C., and Gribbon, L. (2013). Pathways to Violent Extremism in the Digital Era. *The RUSI Journal*, *158*(5), 40–47.

Eid, M. (2013). The New Era of Media and Terrorism. *Studies in Conflict and Terrorism*, *36*(7), 609–615.

Forcese, C., and Roach, K. (2015). Terrorist Babble and the Limits of Law: Assessing a Prospective Canadian Terrorism Glorification Offence. *TSAS Working Paper Series No. 15–02.* http://library.tsas.ca/media/TSASWP15-02_Forcese-Roach.pdf

Forest, J. J. (2012). Perception Challenges Faced by Al-Qaeda on the Battlefield of Influence Warfare. *Perspectives on Terrorism*, *6*(1).

Forest, J. J. Influence Warfare and Modern Terrorism. *Georgetown Journal of International Affairs*, *10*(1), 18.

Frenett, R., and Smith, M. L. R. (2012). IRA 2.0: Continuing the Long War – Analyzing the Factors Behind anti-GFA Violence. *Terrorism and Political Violence*, *24*(3), 375–395.

Geeraerts, S. B. (2012). Digital Radicalization of Youth. *Social cosmos, 3*(1), 25–32.

Gliwa, B., Koźlak, J., Zygmunt, A., and Cetnarowicz, K. (2012). Models of Social Groups in Blogosphere Based on Information About Comment Addressees and Sentiments. In *Social Informatics* (pp. 475–488). Springer Berlin Heidelberg.

Graham, C. (2013). Terrorism.com: Classifying Online Islamic Radicalism as a Cyber Crime. *Small Wars Journal.* http://smallwarsjournal.com/printpdf/14767

Groen, J., and Kranenberg, A. (2010). *Women Warriors for Allah: an Islamist Network in the Netherlands.* Pittsburgh: University of Pennsylvania Press.

Gunaratna, R. (2012). Terrorist Rehabilitation: An Introduction to Concepts and Practices. *Pakistan Journal of Criminology 4*(1): 143–157.

Gunaratna, R., and Haynal, C. (2013). Current and Emerging Threats of Homegrown Terrorism: The Case of the Boston Bombings. *Perspectives on Terrorism, 7*(3).

Halverson, J. R., and Way, A. K. (2012). The Curious Case of Colleen LaRose: Social Margins, New Media, and Online Radicalization. *Media, War and Conflict, 5*(2), 139–153.

Hammer, H., Bratterud, A., and Fagernes, S. (2014). Crawling JavaScript Websites Using WebKit–with Application to Analysis of Hate Speech in Online Discussions. *Norsk informatikkonferanse (NIK), 2013.*

Hannah, G., Clutterbuck, L., and Rubin, J. (2008). Radicalization or Rehabilitation. Rand Europe: www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR571.pdf

Harris, L. (2013). An 'Alternative Sense of Reality? The Case of Anders Breivik and the Threat of Right Wing Terrorism in Europe. In Monaghan, R., Ramirez, J. M., and Walters, T.K.

(eds.) *Radicalization, Terrorism, and Conflict*, 47. Cambridge: Cambridge Scholars Publishing.

Hassan, M. H., and Mohamed, Z. (2012). Research Note: Inside an Indonesian Online Library for Radical Materials. *Perspectives on Terrorism*, *6*(6).

Heinke, D. H., and Hunter, R. (2011). Radicalization of Islamist Terrorists in the Western World. *FBI Law Enforcement Bulletin*, *80*(9), 25–31.

Holtmann, P. (2011). Virtual Jihad: A Real Danger. In R. Lohlker (ed.) *New Approaches to the Analysis of Jihadism: Online and Offline.*

Hoskins, A., and O'Loughlin, B. (2009). Media and the Myth of Radicalization. *Media, War and Conflict*, *2*(2), 107–110.

Hoskins, A., and O'Loughlin, B. (2009). Pre-Mediating Guilt: Radicalisation and Mediality in British News. *Critical Studies on Terrorism*, *2*(1), 81–93.

Hutchinson, C. H. (2012). *Enhancing the Stability and Security of Iraq through the Monitoring of Former Detainee Recidivist Insurgent Activity*. Naval War Coll Newport R1 Joint Military Operations Dept.

Ilyas, M. (2014). Women Affiliated with Muslims Against Crusaders and Women4Shariah. *Journal of Muslims in Europe*, *3*(1), 49–65.

International Association of Chiefs of Police, and United States of America. (2014). Online Radicalization to Violent Extremism. www.theiacp.org/portals/0/pdfs/RadicalizationtoViolentExtremismAwarenessBrief.pdf

Iribarnegaray, D. (2010). Considering Relations between Islam and the West in Three "Discrepant Experiences": From Invasion to Retribution. *Journal of Alternative Perspectives in the Social Sciences*, *2*(2), 472–494.

Jayasanka, R. A. S. C., Madhushani, M. D. T., Marcus, E. R., Aberathne, I. A. A. U., and Premaratne, S. C. (2014). Sentiment Analysis for Social Media. http://dl.lib.mrt.ac.lk/handle/123/9807

Kamal, B. (2011). *Application of Sentimental Analysis in Adaptive User Interfaces* (Doctoral dissertation, BRAC University).

Kassam, R., and Sutton, R. (2012). Online Radicalisation: A Case Study. *Student Rights.*

Kenney, M. Organizational Learning and Islamic Militancy. www.ncjrs.gov/pdffiles1/nij/229887.pdf

Knox, E. G. (2014). The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists. *Hastings Law Journal, 66*(1).

Kumar, L. T., and Campbell, J. R. (2000). Global Governance: the Case of Money Laundering and Terrorist Financing. *Forum on Public Policy: A Journal of the Oxford Round,* 1.

Lakhani, S. (2013). *Radicalisation as a Moral Career* (Doctoral dissertation, School of Social Sciences, Cardiff University).

Lehr, P., and Ramsay, G. (2014). Responding to Terrorism and Ideologies of Hate. In Wolf, S.O., Casaca, P., Flanagan, A.J. and Rodrigues, C. (eds.) *The Merits of Regional Cooperation* (pp. 11–21). Springer International Publishing.

Lieberman, J., & Collins, S. (2008). Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat. *United States Senate Committee on Homeland Security and Governmental Affairs, 11.*

Mahmood, S. (2012, November). Online Social Networks: The Overt and Covert Communication Channels for Terrorists and Beyond. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for* (pp. 574–579). IEEE.

Malcher, A. (2013). Narratives: Pathways to Domestic Radicalisation and Martyrdom.Netherlands: GRIN Verlag.

Matusitz, J. A. (2013). *Terrorism and Communication: A Critical Introduction.* Los Angeles: Sage.

McCoy, J., and Knight, W. A. (2015). Homegrown Terrorism in Canada: Local Patterns, Global Trends. *Studies in Conflict & Terrorism, 38*(4), 253–274.

McFarlane, B. (2010). Online Violent Radicalisation (OVeR): Challenges facing Law Enforcement Agencies and Policy Stakeholders. In *ARC Linkage Project on Radicalisation–Conference 2010.*

Mealer, M. J. (2012). *Internet Radicalization: Actual Threat or Phantom Menace?* (Doctoral dissertation, Monterey, California. Naval Postgraduate School).

Metzger, T. (2013). Caught Between" Deradicalization" and" Disengagement:" Clarifying Terms in the Discourse of Terrorism. *Student Pulse, 5*(11).

Michelsen, N. (2009). Addressing the schizophrenia of global Jihad. *Critical Studies on Terrorism, 2*(3), 453–471.

Mock, J. (2014). Winning Hearts and Minds? The Role of the Internet in Shaping Attitudes Toward Terrorism. *The Role of the Internet in Shaping Attitudes Toward Terrorism* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2431065

Moore, K. S. (Ed.). (2013). Police Chief, Volume 80, Issue 2, February 2013. www.ncjrs.gov/App/Publications/abstract.aspx?ID=264577

Mozes, T., and Weimann, G. (2010). The e-Marketing Strategy of Hamas. *Studies in Conflict and Terrorism, 33*(3), 211–225.

Mukhopadhyay, A. R. (2011). The EU-India Strategic Partnership: Exploring the Security Paradigm. *Perspectives for a European Security Strategy Towards Asia: Views from Asia, Europe and the US,* (18), 189.

Munezero, M., Montero, C. S., Kakkonen, T., Sutinen, E., Mozgovoy, M., and Klyuev, V. (2014). Automatic Detection of Antisocial Behaviour in Texts. *Special Issue: Advances in Semantic Information Retrieval, 38,* 3–10.

Munir, M., Ali, S. R., Muhammad, N., Shah, M., and Abdullah, I. (2012). Terrorism: An Evaluation of Students' Awareness and Attitude at Kust, Khyber Pakhtunkhwa. *Pakistan Journal of Criminology*, 125.

Murray, A. D. (2011). Internet Regulation. In D. Levi-Faur (ed.) *Handbook on the Politics of Regulation.* London: Edward Elgar Publishing.

Neumann, P. (2012). *Countering Online Radicalization in America.* Washington D.C.: Bipartisan Policy Center.

Neumann, P. R. (2013). Options and Strategies for Countering Online Radicalization in the United States. *Studies in Conflict and Terrorism*, *36*(6), 431–459.

Nouri, L., and Whiting, A. (2014). In Baker-Beall, C., Heath-Kelly, C. and Jarvis, L. (eds.) Prevent and the Internet. *Counter-Radicalisation: Critical Perspectives.* London: Routledge.

O'Callaghan, D., Greene, D., Conway, M., Carthy, J., and Cunningham, P. (2013). An analysis of interactions within and between extreme right communities in social media. In M. Atzmueller, A. Chin, D. Helic, and A. Hotho, (eds.), *Ubiquitous Social Media Analysis*, (pp.88–107). Springer Berlin Heidelberg.

O'Callaghan, D., Greene, D., Conway, M., Carthy, J., and Cunningham, P. (2015). Down the (White) Rabbit Hole The Extreme Right and Online Recommender Systems. *Social Science Computer Review*, forthcoming.

Omotoyinbo, F. R. (2014). Online Radicalisation: the Net or the Netizen? *Social Technologies*, (01), 51–61.

Pantucci, R. (2008). Al-Qaeda 2.0. *Survival: Global Politics and Strategy* 50(6): 183–192.

Pantucci, R. (2010). A Contest to Democracy? How the UK has Responded to the Current Terrorist Threat. *Democratization*, *17*(2), 251–271.

Pauwels, L., and Schils, N. (2014). Differential Online Exposure to Extremist Content and Political Violence: Testing the Relative Strength of Social Learning and Competing Perspectives. *Terrorism and Political Violence*, (ahead-of-print), 1–29.

Perešin, A. (2014). Al-Qaeda Online Radicalization and the Creation of Children Terrorists. *Medijska istraživanja, 20*(1), 85–101.

Peters, R. A. (2014). Network Nazis: New Social Media and the German Extreme Right. *MedieKultur*, 1–23.

Petersen, R. R., and Wiil, U. K. (2013). CrimeFighter Investigator: Criminal Network Sense-Making. In Subrahmanian, V.S. (ed.) *Handbook of Computational Approaches to Counterterrorism* (pp. 323–359). Springer New York.

Petz, G., Karpowicz, M., Fürschuß, H., Auinger, A., Stříteský, V., and Holzinger, A. (2013). Opinion Mining on the Web 2.0– Characteristics of User Generated Content and their Impacts. In *Human-Computer Interaction and Knowledge Discovery in Complex, Unstructured, Big Data* (pp. 35–46). Springer Berlin Heidelberg.

Quayle, E., and Taylor, M. (2011). Social Networking as a Nexus for engagement and Exploitation of Young People. *Information Security Technical Report*, *16*(2), 44–50.

Rabiah, A., and Zahari, Y. (2012). A Dynamic Cyber Terrorism Framework. *International Journal of Computer Science and Informtion Security*, *10*, 149–158.

Ramsay, G. (2009). Relocating the Virtual War. *Defence Against Terrorism Review*, *2*(1), 31–50.

Ramsay, G. (2012). Online Arguments against Al-Qaeda: An Exploratory Analysis. *Perspectives on Terrorism, 6*(1).

Ravndal, J. A. (2013). Anders Behring Breivik's Use of the Internet and Social Media. *Journal Exit-Deutschland: Zeitschrift für Deradikalisierung und demokratische Kultur*, *2*, 172–185.

Reynolds, T. (2012). Ethical and Legal Issues Surrounding Academic Research into Online Radicalisation: a UK Experience. *Critical Studies on Terrorism, 5*(3), 499–513.

Richardson, D. L. (2011). *Al Qaida and Yemen-Is Our Current Policy Good Enough?* Army War Coll Carlisle Barracks PA Center for Strategic Leadership.

Richardson, M. W. (2012). *Al-Shabaab's American Recruits: A Comparitive Analysis of Two Radicalization Pathways* (Doctoral dissertation, University of Texas at El Paso).

Ryan, J. (2010). The Internet, the Perpetual Beta, and the State: The Long View of the New Medium. *Studies in Conflict and Terrorism, 33*(8), 673–681.

Saddiq, M. A. (2010). Whither e-jihad: evaluating the threat of internet radicalisation. RSIS Commentaries, 083/10, http://dr.ntu.edu.sg/handle/10220/6646

Sageman, M. (2008). A Strategy for Fighting International Islamist terrorists. *The ANNALS of the American Academy of Political and Social Science, 618*(1), 223–231.

Sageman, M. (2008). The Next Generation of Terror. *Foreign Policy, 165*, 36–42.

Saifudeen, O. A. (2014). *The Cyber Extremism Orbital Pathways Model.* RSIS Working Paper No. 283.

Saltman, E. (2014). Cyber Jihad: The Role of the Internet in Islamist Radicalisation. *Policy, 2012*, 2010.

Sampson, K. J. (2009). *Winning the Battle of Ideas Through Individual Resiliency: a Multi-Dimensional Approach for Countering Radicalization in the Homeland* (Doctoral dissertation, Monterey, California. Naval Postgraduate School).

Saskia Bayerl, P., Jacobs, G., Denef, S., van den Berg, R. J., Kaptein, N., Birdi, K., and Vonas, G. (2013). The Role of Macro Context for the Link Between Technological and Organizational Change. *Journal of Organizational Change Management, 26*(5), 793–810.

Schmid, A. P. (2013). Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review. *ICCT Research Paper, 97.*

Schmidle, R. E. (2010). Positioning Theory and Terrorist Networks. *Journal for the Theory of Social Behaviour, 40*(1), 65–78.

Seib, P., and Janbek, D. M. (2010). *Global Terrorism and New Media: The Post-Al Qaeda Generation.* London: Routledge.

Shah, N. (2009). *Global Village, Global Marketplace, Global War on Terror* (Doctoral dissertation, University of Toronto).

Shams, M., Saffar, M., Shakery, A., and Faili, H. (2012). Applying sentiment and social network analysis in user modeling. In *Computational Linguistics and Intelligent Text Processing* (pp. 526–539). Springer Berlin Heidelberg.

Shetret, L. (2011). Use of the Internet for Counter-Terrorist Purposes. *Center on Global Counterterrorism Cooperation (Feb 2011)* http://globalcenter.org/wp-content/uploads/2011/02/LS_policy-brief_119.pdf.

Shresthova, S. (2013). Between Storytelling and Surveillance. http://dmlhub.net/wp-content/uploads/files/Shresthova-Between%20Storytelling%20and%20Surveillance-Working%20Paper%20Report-Sept11-2013.pdf

Silber, M., and Frey, A. (2013). Detect, Disrupt, and Detain: Local Law Enforcement's Critical Roles in Combating Homegrown Extremism and the Evolving Terrorist Threat. *Fordham Urb. LJ, 41*, 127.

Simons, J. J. (2012). *Ten Years Later: Insights on al-Qaeda's Past and Future through Captured Records: A Conference Report.* National Defense Univ Fort McNair DC Inst for National Strategic Studies.

Singh, B. Youth Self-Radicalisation: Lessons from the Singapore Narrative. *Youth and Terrorism, A Selection of Writings*, 87.

Spaaij, R., & Hamm, M. S. (2015). Key Issues and Research Agendas in Lone Wolf Terrorism. *Studies in Conflict & Terrorism, 38*(3), 167–178.

Spalek, B., and Davies, L. (2012). Mentoring in Relation to Violent Extremism: A Study of Role, Purpose, and Outcomes. *Studies in Conflict and Terrorism, 35*(5), 354–368.

Staniforth, A. (2014). *Preventing Terrorism and Violent Extremism.* Oxford: Oxford University Press.

Stevens, T. (2009). Regulating the 'Dark Web': How a Two-Fold Approach can Tackle Peer-to-Peer Radicalisation. *The RUSI Journal, 154*(2), 28–33.

Stevens, T., and Neumann, P. R. (2009). *Countering Online Radicalisation: A Strategy for Action.* King's College London: International Centre for the Study of Radicalisation and Political Violence.

Sureka, A. (2012). 140 characters of @hate and #protest. https://repository.iiitd.edu.in/jspui/handle/123456789/28

Sureka, A., and Agarwal, S. (2014, September). Learning to Classify Hate and Extremism Promoting Tweets. In *Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint* (pp. 320–320). IEEE.

Sureka, A., Kumaraguru, P., Goyal, A., and Chhabra, S. (2010). Mining YouTube to discover extremist videos, users and hidden communities. In *Information retrieval technology* (pp. 13–24). Springer Berlin Heidelberg.

Swift, C. (2012). Arc of Convergence: AQAP, Ansar al-Sharia and the Struggle for Yemen. *CTC Sentinel, 5*(6), 1–6.

Tabatabaei, F. (2013). Investigating Radicalized Individual Profiles Through Fuzzy Cognitive Maps. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2465350

Tabatabaei, F., Nasserzadeh, S. M. R., Yates, S., Akhgar, B., Lockley, E., and Fortune, D. (2013). From Local to Global: Community-Based Policing and National Security. *Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies*, 85.

Thelwall, M., Kousha, K., Weller, K., and Puschmann, C. (2012). Assessing the Impact of Online Academic Videos. *Social information research. Bradford: Emerald Group Publishing Limited*, 195–213.

Thomas, M. S. J. L. C. (2014). *Cyberterrorism.* New York: Springer.

Thomas, T. L. (2009). *Countering Internet Extremism.* Foreign Military Studies Office (Army) Fort Leavenworth KS.

Tley, G. (2014). No Apologies for Cross-Posting: European Trans-Media Space and the Digital Circuitries of Racism. *Crossings: Journal of Migration and Culture, 5*(1), 41–55.

Torok, R. (2011). The Online Institution: Psychiatric Power as an explanatory model for the normalisation of radicalisation and terrorism. In *Intelligence and Security Informatics Conference (EISIC), 2011 European* (pp. 78–85). IEEE.

Torok, R. (2013). Developing an Explanatory Model for the Process of Online Radicalisation and Terrorism. *Security Informatics, 2*(1), 1–10.

Vergani, M. (2014). Neo-Jihadist Prosumers and Al Qaeda Single Narrative: The Case Study of Giuliano Delnevo. *Studies in Conflict and Terrorism, 37*(7), 604–617.

Vergani, M. (2014). Neojihadism and Muslim–Christian Relations in the Mindanao Resistance Movement: A Study of Facebook Digital Narratives. *Islam and Christian–Muslim Relations, 25*(3), 357–372.

Vergani, M., and Zuev, D. (2014). Neojihadist Visual Politics: Comparing YouTube Videos of North Caucasus and Uyghur Militants. *Asian Studies Review*, (ahead-of-print), 1–22.

Vidino, L. (2011). *Radicalization, linkage, and diversity: Current trends in terrorism in Europe*. Rand National Defense Research Inst Santa Monica CA.

von Behr, I., Reding, A., Edwards, C., and Gribbon, L. (2013) *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Retrieved from www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

Wadhwa, P., and Bhatia, M. P. S. (2013, February). Tracking On-Line Radicalization Using Investigative Data Mining. In *Communications (NCC), 2013 National Conference on* (pp. 1–5). IEEE.

Wadhwa, P., and Bhatia, M. P. S. (2014). Discovering Hidden Networks in On-line Social Networks. *International Journal of Intelligent Systems and Applications (IJISA)*, *6*(5), 44.

Wadhwa, P., Bhatia, M. P. S., Biju, I., and Naumann, I. (2014). Classification of Radical Messages in Twitter Using Security Associations. In Issac, B., and Israr, N. (eds.) *Case studies in secure computing: Achievements and Trends*, 273–294. London: Auerbach Publications.

Wawer, A. (2010). Monitoring Social Attitudes Using Rectitude Gains. In Daras, P. and Ibarra, O.M. (eds.) *User Centric Media* (pp. 349–354). Springer Berlin Heidelberg.

Weimann, G. (2014). New Terrorism and New Media. London: *Wilson Center Common Labs.*

Weimann, G., and Von Knop, K. (2008). Applying the Notion of Noise to Countering Online Terrorism. *Studies in Conflict and Terrorism*, *31*(10), 883–902.

Wiil, U. K. (2014). Criminal Network Investigation. *Security Informatics*, *3*(1), 1.

Williams, P. (2012). Violent Extremism. *Policing Terrorism*, 136.

Wilner, A. S., and Dubouloz, C. J. (2010). Homegrown Terrorism and Transformative Learning: an Interdisciplinary Approach to Understanding Radicalization. *Global Change, Peace and Security*, *22*(1), 33–51.

Woodring, D. (2014). *21st Century Radicalization: The Role of the Internet User and Nonuser in Terrorist Outcomes*. Thesis: University of Arkansas.

Woodward, J. D. (2006). Radicalization. Rand: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA456289

Yannakogeorgos, P. A. (2014). Rethinking the Threat of Cyberterrorism. In T. Chen, L. Jarvis and S. Macdonald (eds) *Cyberterrorism: Understanding, Assessment and Response* (pp. 43–62). Springer New York.

Yasin, N. A. M. (2011). Online Indonesian Islamist Extremism: a Gold Mine of Information. RSIS Working Paper www.rsis.edu.sg/rsis-publication/rsis/1616-online-indonesian-islamist-ext/#.VbV3Ouu_v8E

Yasin, N. A. M. (2012). Social Media and Terrorism in Indonesia: Enhancing or Diluting its Appeal?. www.rsis.edu.sg/rsis-publication/icpvtr/1713-social-media-and-terrorism-in/#.VbV3Heu_v8E

Yates, S. (2013). National Security Today and in the Future. *Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies*, 269.

Yeap, S. Y., and Park, J. (2010). Countering Internet Radicalisation: a Holistic Approach. http://dr.ntu.edu.sg/handle/10220/6657

Yunos, Z., Ahmad, R., Ali, S. M., and Shamsuddin, S. (2012). Illicit Activities and Terrorism in Cyberspace: an Exploratory Study in the Southeast Asian Region. In *Intelligence and Security Informatics* (pp. 27–35). Springer Berlin Heidelberg.

Zevnik, A. (2012). Women Suicide Bombers: Narratives of Violence by VG Julie Rajan. *Critical Studies on Terrorism*, *5*(3), 518–520.

The VOX-Pol Network of Excellence (NoE) is a European Union Framework Programme 7 (FP7)-funded academic research network focused on researching the prevalence, contours, functions, and impacts of Violent Online Political Extremism and responses to it.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312827

Email info@voxpol.eu
Twitter @VOX_Pol
www.voxpol.eu