The meeting with ‘A5’, one of nine convicted terrorists identified for this study, took place in an unassuming hotel in the north of England. The interview lasted nearly three hours. Sitting between his two mentors, A5 quietly began to describe his family history, his aggressive father, and the far-right friendships and rivalries online that he considered were key drivers in his radicalisation to violent extremist. A5 was able to live two separate lives – offline and online. Offline he ‘behaved normally’ with his friends and family. Online, however, his views grew increasingly extreme as he became more involved in right-wing chat forums and helped others out with creating and distributing right-wing extremist material.

The Internet is now part of almost every priority national-security investigation conducted by the UK security and intelligence agencies and police. Terrorists and extremists use it for a myriad of purposes: from disseminating propaganda and information, to fundraising and operational planning. For reasons of security and safety, accessibility and anonymity, terrorists and extremists have shifted many of their activities from public spaces (such as mosques, in the case of Islamist extremist groups) to private residences, personal computers and tablets.

According to the director-general of the Office for Security and Counter-Terrorism in the Home Office, ‘violent radicalisation in mosques or other religious institutions comprises no more than 1% or 2% of the total cases of radicalisation’. The process of radicalisation is becoming increasingly covert, posing problems for the security and intelligence agencies and UK law enforcement. The shift online in terrorists’ modus operandi largely reflects society’s expanding digital footprint, where everyday activities move seamlessly between online and offline domains. Understanding how those online and offline activities, domains and influences interact has become an urgent concern for terrorism analysts and policy-makers struggling to understand how the next generation of terrorists will be radicalised. Too often the public hears of individuals ‘radicalised online’ with little or no evidence of how such ‘radicalisation’ occurred. Details of cases made public are rarely discussed in a manner that helps the public to understand the topic. This article provides an overview of the phenomenon and explores some of the key issues associated with the use of the Internet in the process of radicalisation.

This article is based on a substantial study conducted by the authors in 2012 while at the RAND Europe, which will be published later this autumn. The article describes the study, highlights five of the fifteen cases used to demonstrate the role played by the Internet in the process of radicalisation, and highlights some key themes and issues that emerged from that research. It does not aim to provide a comprehensive analysis of the literature – that is included in the study; however, it is worth touching on some of the key issues and definitional terms.

Current Understanding of Internet Radicalisation

Some online terrorist activities, such as material procurement and operational planning, are well understood by governments and security agencies. They are either offences which can be prosecuted under UK legislation or those to which governments have implemented strategies in response. However, the Internet’s role in the process of radicalisation remains difficult to define and poses a challenge for governments. The public evidence base is contradictory and the academic field divided on the subject of online
Some recent studies have emphasised the Internet’s significance and its effect on the individual, while others have concluded that the Internet ‘does not appear to play a significant role in Al Qa’ida influenced radicalisation’.

Academic research has, to date, analysed online content and its messages and intent, rather than exploring how individuals use the Internet in the process of radicalisation – how a person comes to support terrorism or forms of extremism leading to terrorism. This is no surprise – access to terrorists and extremists is challenging, and interviewing them more so. It is the principal reason why so many academic studies rely on secondary sources. Primary data is exceptionally hard to come by. It follows that because of this paucity of data, the collective understanding of an issue as complex as the role of the Internet in the process of radicalisation is extremely limited. As a result, many academics and researchers have resorted to solely studying terrorist material they have found on the Internet – often assuming a link between extremist material online and its influence on the individual reading or watching it. They suggest a degree of causality between what is online and the influence on the person reading it, none of which can be proven. Often, it is left to the reader to connect the dots.

That said, the research on online content has provided policy-makers and practitioners with valuable insights into terrorist and extremist narratives, marketing strategies, beliefs and organisation. This approach, however, has largely failed to explore and analyse the impact this content has had on the individual – the consumer of the information. To put it another way, past and present research efforts have focused on the ‘supply’ side of terrorist and extremist material rather than the demand side – the individuals consuming and interacting with this online material. Very little is known about how individuals experience this content and, aside from a handful of cases, what impact it has on them.

Research has focused on the ‘supply’ side of terrorist material

This partial understanding of the problem has unintended (and avoidable) consequences. As governments (and to a lesser extent the private sector) have tackled the supply side, so have they created a range of tools to help them, such as software to filter out illegal online content and remove websites from public view. This approach and the tools that support it have raised serious concerns among civil-society groups, which accuse governments and private businesses of infringing on rights of free expression, undermining the right to privacy, and taking an indiscriminate and disproportionate approach to the issue.

Conducting the Research

The RAND study outlines the research methodology in full. For reasons of space, this section briefly describes the process of obtaining primary data, as this is often the greatest challenge to researchers. A review of media reporting and other grey literature identified convictions of individuals for terrorist offences under UK Terrorist legislation (henceforth TACT) in the timeframe 2001–12, in which use of the Internet appeared to be an element of the offences. The Association of Chief Police Officers (ACPO) and the Office for Security and Counter-Terrorism were approached and briefed on the aims of the research project. An interview protocol and ethical framework were agreed with them before interviews were conducted.

Following this, senior investigative officers (SIOs) from police forces across
the UK were identified and asked to support the research team. A similar approach was taken with government intervention providers, who work with vulnerable individuals at risk of being drawn into terrorism. ACPO also suggested examples from its own records of cases which involved use of the Internet in terrorist activities or where radicalisation through the Internet was deemed to be an element of the case. Police forces also provided access to cases of individuals who had not been prosecuted but were deemed to be vulnerable to the influence of extremists. These individuals were engaged under the auspices of the Channel programme. Data was obtained through interviews, evidence presented in court and the computer registries of individuals convicted under terrorism legislation.

Cases of Internet Radicalisation

In 2012, a research team (including the authors) examined nine TACT offender cases, five individuals identified as being vulnerable to extremism and one individual who had disengaged from international terrorism. The cases were selected in partnership with police because the Internet was judged to have been instrumental in the radicalisation of those involved. The aim of the research was to understand the role of the Internet in the process of radicalisation. Due to space constraints, five of the fifteen cases are outlined below as examples, with the specific findings from the research.

'A1' was born in Pakistan and came to the north of England aged three. Corroborated accounts at his trial suggest that his family life was unstable and that his father was absent during his formative years. He spoke English, basic Arabic and Urdu, and communicated radical Islamist extremist messages online in all three languages. Prior to his arrest for terrorism offences, trial proceedings indicate that he had a criminal record that included a range of offences, such as shoplifting and grievous bodily harm. On this basis, the police judge that he was well connected to local crime and drugs networks. A1 spent time in a number of prisons. Some prisons have been identified as possible hubs of radicalisation; however, it is not clear and there is no evidence to suggest whether A1 was radicalised while in prison. A1's computer registry (data on his computer activity) indicates that he was digitally literate and used the Internet on a daily basis. In 2010, he met a female on a Muslim dating site. After dating for a few months, they married. Accounts from his trial suggest that A1 was conservative in terms of his religious outlook but dressed in a Western style. However, less than five months later his behaviour changed and he grew a beard (which he had also done in prison) and began to dress in a more traditional style. By early 2011, A1 was accessing bomb-making websites and downloading videos of beheadings. In mid-2011, A1 purchased bomb-making material, including quantities of hydrogen peroxide and other ingredients.

According to police witness statements taken from associates, 'A2' was an outgoing woman living in the north of England. Trial documents suggest that her life was 'chaotic' and that A2 felt a sense of failure following two divorces. Police accounts suggest that her socially conservative father persuaded her to find a Muslim husband. After a short online relationship with A1, the two married. Soon after they moved in together, A2 began to dress in a traditional way and became more insular, reducing her work with clients of other ethnicities at her husband's behest. Her computer registry shows that she sold her Sex and the City DVDs on eBay, which witness statements suggest she did to gain her husband's favour.

'A3' grew up in Saudi Arabia with a Salafist religious education. At the time – the early 1990s – the Internet was less widespread, and information was passed around circles of friends and acquaintances. In 1994, A3 decided to travel to Bosnia, as other friends had. His radicalisation was, he argues, inevitable:

After everything you've seen, you don't want to go back to normal life – you feel so detached at that moment from social life, especially if you have a near-death experience. People seem to be having frivolous conversations; they don't have aspirations beyond their own daily life.

You start thinking of yourself as elite, a vanguard, and you look for other people like you.

A3 was identified as a good speaker and became a recruiter and fundraiser. Once he left Saudi Arabia, A3 was active for twelve years (including a period in the UK translating books on an extremist website) before he disengaged from all terrorist activities.

'A4' converted to Islam on the first anniversary of 7/7 at a prominent Birmingham mosque. Trial documents suggest that A4 was a drug user and had used heroin in the past. He was on methadone at the time of his arrest. A4 was described in witness statements as a loner; he had dropped out of school and spent a short time in a flat with his then-girlfriend before the relationship broke up. He lived in a hostel and had been homeless for a period of time. With support from the local council he was allocated a flat in a quiet area of a UK city. Trial documents suggest that in the months leading up to his arrest, he had a number of friends with whom he shared information about what he was doing and thinking. A4 has been described as having a compulsive personality and had a previous criminal conviction. He was arrested after a tip-off from a member of the local community. When police searched his flat they found both explosives and a suicide vest.

'A5' is a white male. He was a teenager when his parents split up and after a short period of time he moved in with his father. His father was racist and a member of a right-wing group. Interview evidence indicates that A5's father regularly threatened him for listening to rap music and watching television programmes that included ethnic minorities in prominent roles: if he was caught, his father would remove the television. His father threatened that he would 'hang him if he was found sleeping with [a] black woman'. After a few months of living with his father, A5 became increasingly curious as to what his father was involved in and, unbeknown to his father, visited some extreme right-wing websites.

A5 said he had used the Internet for 'as long as I can remember', and
as he became increasingly involved in an extreme right-wing group he began to engage in debates online and support group members online, communicating with them via Skype and MSN Messenger. He claimed not to have a Facebook account, although a lot of his non-extremist friends did. A5 suggested that his personal relationship with his father offline was a factor in his radicalisation and online behaviour: A5 acknowledged that his father began to open up when he told him what he was doing online and they began to have a more ‘friendly relationship’ as a result. A5’s online activity lasted for a year and a half. According to the computer registry, his activity was heavy for the first six months of this period, then A5 became less interested and started to meet up and spend more time with his previous friends. He was arrested at his mother’s house and charged with a number of offences, including inciting racial violence.

Based on the fifteen cases analysed, and highlighted by the five cases outlined above, this study identifies a series of themes: the rise of the ‘home-grown’ terrorist; the status of Google and Facebook as the tools of choice; the growing role of virtual communities in radicalisation; and indicators of online radicalisation.

The Rise of the ‘Home-Grown’ Terrorist

One trend that has emerged from the cases reviewed here is the fact that the radicalisation of individuals is becoming increasingly covert, as extremists have moved their activities from public spaces to private homes and spaces. The same can be said for most of the case-study participants’ online activities. Only four of the cases reviewed revealed the use of computers to access extremist content online in public libraries and college computer rooms. The majority of the cases reviewed used the Internet at home and nowhere else, for fear ‘of being caught online’ (Figure 1). A5, for example, always used the computer in his own room or his mother’s living room. He never used the Internet in school or Internet cafés, as he was worried about being ‘seen’ online.

For older individuals in the study such as A3, his experience of using Internet cafés in Pakistan and in the UK reflects the time period in the late 1990s when personal computers remained relatively expensive and use of the Internet at home was still new. It also reflects the changing dynamics of extremists who, at least when A3 was active, operated in a group, rather than as individuals networked through information and communication technologies. By contrast, A4 used a number of computers, including his personal desktop, mobile phone, his father’s computer and his college computer to access extremist content online. A4’s use of a wide range of computers reflects his personal circumstances. He did not have Internet access at his council flat, and relied on his father’s and a college computer to download material which he copied onto a USB stick.

Google and Facebook as the Tools of Choice

A1 had five Facebook accounts over time: each time an account was closed down by Facebook due to inappropriate content, A1 simply opened a new account, changing his username by only one numeric digit from that of the closed account. A1 used Facebook to engage
with other extremists online and used the Internet to download extremist material via BitTorrent. A1 had a high level of digital literacy and had purchased wi-fi hacking software, e-mail encryption and evidence-elimination software packages. Evidence from trial suggests that he had also invested in an anti-bugging device. By contrast, A2 did not seem to use the Internet as much as A1, but was clearly active: shopping at Tesco online, selling goods on eBay and browsing extremist material. A2 also searched for potential targets for an attack: targets that were logged on the TomTom device found in their car (Figure 2).

For A3, the Internet was one of a plethora of tools used to support his radicalising activity. As a former radicaliser, A3 made clear in the interview for this study the benefits of the Internet over other instruments. Before the spread of the Internet he would have to spend time going from cafés to Chicken Cottage restaurants (a halal fast-food chain), selling his ideas. The Internet provided him with a ready-made audience. He had gone, in his words, from retail to wholesale. While before using the Internet he might have been able to influence only one or two people through his proselytising, now he was able to speak to several hundred. Extremist groups that were local and whose membership was based on word of mouth now spread out across the country and region. However, A3 believes that the Internet is just another medium of communication, the effect will be dependent on the individual: what they are after; how far along the journey they are; and how much information they require to take the next step and use violence.

The Internet provided a ready-made audience

A3 suggests that in some cases the creation of online media – YouTube videos and Internet radio – has replaced the need for such interaction: ‘A person who is being radicalised will believe, as they watch Al-Awlaki, that he is talking directly to them’. As A3 explains: ‘A picture is worth a thousand words, a video is worth a thousand pictures’. The posting of videos was made possible only with the introduction of broadband. Until then, there was ‘always an imitation, that you had to put things on VHS … the idea of uploading large files was not a possibility … [I] didn’t think it would go to the point of using the internet for videos’.

A4 used Google to find and locate relevant material. Figure 3 shows the quantity of material A4 was looking at online over a period of months. The information was taken from the computer registry at his local college and his personal computer. The graphic shows what he looked at and when, broken down into four themes: explosions and instructional material on the practicalities of making a suicide bomb; other extremist content; religious content; and information on where suicide bombings had taken place.

A4 did not take part in online chat rooms or fora. He did not have a Facebook account. A4 did not reach out to people online and his online searches suggest that he developed his own target and approach. The Internet allowed him to find relevant material for building an improvised explosive device and for planning his attack. A4 was fascinated by suicide bombing (see Figure 3), converting to Islam on the first anniversary of the 7/7 bombings and searching for one of the 7/7 attackers several times before moving on to other extremist material. The inspiration for his planned attack did not come online but may have been from the US television series Sleeper Cell, which his brother had bought for him as a present. Aside from providing a resource for making his own improvised explosive device, material on the Internet reinforced A4’s own thinking and ideas, which he had discussed with friends.

A5, in contrast, was highly active on a web forum. The Internet gave A5 access to a lot of information, which he used to clarify points raised in fora, and then to support or challenge others online. According to A5, his online activities made him feel part of a group and important. He became a committee member and was approached numerous times to assist other members (for example, by helping to create images and leaflets), as illustrated in Figure 4.

There are numerous reasons why the individuals in the fifteen case studies used the Internet, but it is worth exploring why they decided against using any other form of communication or media. As some of the individuals in the case studies suggest, the Internet has been around since they were born, and just as most of society uses it every day, so it was used as the primary resource for obtaining information and, increasingly, for communicating between people, as seen by looking at A2’s search terms, taken from her computer registry.

The conversations that A1 and A2 had in their home are not known, but one
can see what they each downloaded from their computers and laptops. In the past, much of the material would have been passed between members of a group but now vast quantities of material can be saved to a single disk. Quantity is an important measure in an investigation. The police regularly cross-reference material seized in terrorism investigations with a centrally held list of extremist material. For example, a comparison between two cases included in the wider study shows that A6 had thirty-seven entries on the police list, while A10 had 229 entries. However, the question remains as to whether the individuals in question actually read all of the material or only some of it. The same material frequently appears and reappears in investigations. How individuals engage with such material and its influence on their attitudes and behaviour is a gap in the academic research.

Virtual Communities as a Growing Feature of Radicalisation

The argument that the Internet is an ‘echo chamber’ for extremist views appears frequently in academic reports and media commentary. The US Senate Homeland Security and Governmental Affairs Committee notes that the Internet has ‘become a virtual “echo chamber” – acting as a radicalisation accelerator’.10

Some of the interviewees, like A3 and A5, did suggest that the Internet acted as an echo chamber where they created, experienced and navigated online spaces that reinforced their world view. In the case of A1 and A2, the Internet was used to search for specific material, including bomb-making instructions, suggesting that while the Internet was used to view religious material (including information relating to martyrdom), much of the material viewed online was instructional and reinforced existing views. A2 did change her behaviour offline and no longer watched Coronation Street and EastEnders, preferring instead to read extremist material on her computer.

For A3, who like A6 spent much of his time online radicalising others, the Internet appears to have been simply another platform from which to broadcast – a platform, moreover, where there were competing views on offer. Their view was that the echo-chamber effect depends on the individual consumer in question: what the individual is seeking and how far along the journey he or she is. Interestingly, A3 did not think that the Internet accelerated the process of radicalisation. Instead, A3 suggested that each individual’s radicalisation journey is different and that, while the Internet might make information easier to find, ultimately the effect on the individual and their subsequent decision to take action will be a personal one.

In the cases of A4 and A5 the Internet was a tool with which they grew up and which was used for a range of purposes including social engagement with like-minded individuals. The computer-registry evidence does not show that they focused their attention solely on extremist material. Instead, it shows them searching for a myriad of information, including instructions on suicide bombing and clothes on eBay, and buying food at the supermarket.

Indicators of Online Radicalisation

The research explored whether any of the individuals in the case studies changed their use of the Internet and, if so, whether they experienced tipping points. This involved assessing longitudinal Internet usage patterns, whether TACT offenders consistently searched issues to elicit further information, and whether they stopped at any time or switched off and, if so, the reasons for this. Until they were arrested, A1 and A2 used the Internet on a regular basis, and at no point stopped looking at extremist material or switched off the computer. From their online activities alone, one can see a snowball effect, as A1 and A2 found what they were looking for, moved on to the next topic and so on (Figure 5). Their two computers were central to their activities, including playing an important role in their making of an improvised explosive device.

A3 suggested that those who are part of a network or are more aware of operational security issues may stop using the Internet prior to acting. This may include travelling overseas for specific training or in preparation for the event. What made A4 go online on a November day and search for 7/7 bombers remains unclear, but it was the beginning of a sustained period of Internet usage that culminated in his building a rudimentary suicide vest in his flat. A4 did stop using the Internet for short periods of time due to limited access, waning interest or because he was playing war games on another computer elsewhere.

A5 used the Internet more intensively over the first six months of the year and a half in which he was involved in extremist activities online.
After a while, he stuck with the forum and its members ‘for the sake of sticking with it’. He still enjoyed being part of a group, although he was doing more with friends offline, which could also have contributed to his lack of activity online. It is possible to view A5’s activities over a period of years. There were clear peaks in activity, particularly after a specific event, when he would post more material online about what had happened.

The British Government’s Response
The British government has been at the forefront of tackling terrorist use of the Internet. Since July 2006, when the UK made public its strategy to counter international terrorism (CONTEST), the Internet has been identified as a domain ‘where many types of radical views are strongly promoted’. The growth of the Internet, with its ability to connect people, to allow them to pass ideas between them and then to pass those ideas on to others, has had a significant impact on the accessibility and flow of radical ideas. In March 2009, the government published a revised version of CONTEST, which set out a more sophisticated approach to counter-terrorism online. The document acknowledged that ‘the internet presents significant challenges for CONTEST in general and Prevent in particular’.

This new approach included working with filtering companies, disrupting use of the Internet for extremist messaging and increasing use of the Internet for promoting alternative views. Part of the government’s response was furthering the development of specialist units to counter the threat of terrorism from online sources and material. In 2010, the Counter Terrorism Internet Referral Unit (CTIRU) was launched within ACPO. This unit removes or modifies unlawful Internet content, identifies the individuals responsible for posting such material, and supports the police counter-terrorism network in investigating and prosecuting terrorist or radicalising activity online.

CTIRU acts as a co-ordination point for UK police counter-terrorism Internet ‘take-down’ activity. The unit develops and shares new technologies to assess and process Internet content, and to improve the effectiveness of the police response to unlawful material. Between July and September 2012, there were 341 referrals in total, with 232 (68 per cent) from the general public via the Directgov website. The most frequently referred sites were Facebook, Twitter and Blogger and/or Blogspot. There were 105 removals (31 per cent) during this same period.

Internet service providers (ISPs) have also taken the initiative, changing their own terms of use, and some have introduced ways of identifying content which might breach legal guidelines. For example, YouTube has introduced a ‘promoting terrorism’ referral flag for videos deemed to be of a terrorist nature, while AOL has increased the visibility of the Metropolitan Police Anti-Terrorist Hotline by ensuring that it is presented when specific search requests are entered. Interview evidence suggests that the police and security and intelligence agencies have developed expertise through their increasing experience of cases which have involved the Internet. A key finding of this research is the importance of communications data to terrorism investigations. It is fair to say that without communications data many of the investigations could not have taken place.

Without communications data many of the investigations could not have taken place

Conclusion
As the interview with A5 came to an end, and as the police officer began to make arrangements to take him home, one of his mentors asked for help: ‘We’re kidding ourselves if we know what most of these kids are doing online – it’s a parallel world that’s hidden from most of us – our ignorance is preventing us from helping them’. This sense of powerlessness was echoed by police officers and practitioners alike. The Internet offers terrorists and extremists the capability to communicate, connect and collaborate in ways that are increasingly difficult to monitor. Only in the last few years has there been any serious attempt to examine how the Internet influences the process of radicalisation.

© RUSI JOURNAL OCTOBER/NOVEMBER 2013
The majority of policy documents and academic literature focus on online content and its potential influence on vulnerable individuals, rather than exploring how individuals use the Internet in the process of radicalisation. The reason for this is relatively straightforward. Access to terrorists (those convicted under UK terrorism legislation) or extremists (as identified by the police and multi-agency partners) is extremely difficult. Access to primary data remains a significant challenge. However, it is possible, as this research demonstrates. The core argument of this study is that governments and the academic community have focused on the content (of the Internet and radicalisation), rather than a person’s individual experience online. This needs to change. A more sophisticated approach will have a greater influence on the threat in the long term and will ensure that the government’s response remains focused, proportionate and, most importantly, has real impact.

Charlie Edwards is Director of National Security and Resilience Studies at RUSI. He is a former Deputy Director of Strategy and Planning in the Office for Security and Counter-Terrorism, Home Office.

Luke Gribbon is a Research Fellow in National Security and Resilience Studies at RUSI.


Notes

1 Each case analysed was given an alphabetic number (TACT Offenders A1-10, Channel Cases B1-B5).

2 Terrorism is defined in the Terrorism Act 2000 as an action that endangers or causes serious violence to a person or property; or seriously interferes or disrupts an electronic system. The use of threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious or ideological cause. Extremism is defined by the British government as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs.


4 The concept of radicalisation is open to interpretation – see, for instance, Peter R Neumann, ‘The Trouble with Radicalization’, International Affairs (Vol. 89, No. 4, July 2013), pp. 873–93. This study uses the British government definition and the one understood by UK policy-makers and practitioners. Radicalisation is therefore defined as ‘the process by which people come to support terrorism and violent extremism and, in some cases, then join terrorist groups’; UK Home Office, CONTEST: The United Kingdom’s Strategy for Countering Terrorism, Cm 8123 (London: The Stationery Office, July 2011).


8 Channel is a multi-agency approach to protecting people at risk of radicalisation. Channel uses existing collaboration between local authorities, statutory partners (such as the education and health sectors, social services, children’s and youth services, and offender management services) the police and the local community to identify individuals at risk of being drawn into terrorism; assess the nature and extent of that risk; and develop the most appropriate support plan for the individuals concerned.

9 House of Commons Home Affairs Committee, ‘Roots of Violent Radicalisation’.


13 Authors’ interview with CTIRU, September 2012.