REGULATING THE ‘DARK WEB’

HOW A TWO-FOLD APPROACH CAN TACKLE PEER-TO-PEER RADICALISATION

TIM STEVENS

The internet plays a contributory role in radicalisation, but is only one of a number of mechanisms currently deployed to win recruits to global jihad. Technical regulation of online content is difficult and may be counter-productive, driving forums deeper underground or alienating users. Tim Stevens argues that adopting a social approach that educates and empowers online communities could have more success.

In recent years, the role of the internet in the facilitation of terrorism and other forms of violent extremism has been the focus of academic and public scrutiny, as well as increasingly the subject of Western government policy and legislation. States have, with the advent of the internet as a near-ubiquitous and global communications medium, been presented with an unenviable dilemma: how best to prevent the use of the internet by terrorists whilst preserving the ideals of free speech and democracy? The paradoxical trade-off between security and democracy is at the heart of modern counter-terrorism, although many governments would prefer either to feign ignorance of this or to privilege security at the expense of human rights entirely, presumably hoping no one will notice.1

One of the issues of most concern to the UK government is the radicalisation of individuals, facilitated in part by their exposure to extremist multimedia on the internet. In the current security context, Islamist material is the principal focus of government efforts to intervene in this area, although it could equally apply to other forms of violent political expression such as neo-Nazism and animal liberation movements. The UK government’s counter-terrorism strategy (CONTEST) is explicitly aimed at Islamists and Muslim communities but, while remaining mindful of the specifics of the contemporary security situation, any strategy for dealing with terrorism and violent extremism – especially once legislated – should be applicable across the spectrum of political expression and activism. This is certainly true when governments address the issue of what is, and what is not, acceptable behaviour online, particularly when attempting to regulate individual pathways of radicalisation.2

Radicalisation and the Internet

Although – as with ‘terrorism’ – there is no universally agreed definition of ‘radicalisation’, most commentators and analysts describe it as the process (or processes) whereby individual(s) come to approve of, and ultimately participate in, the use of violence for political ends. CONTEST defines radicalisation as ‘the processes whereby certain experiences and events in a person’s life cause them to become radicalised, to the extent of turning to violence to resolve perceived grievances’.3 In the context of the jihad, grievances are generated and maintained at both local and global levels, and the internet plays a major communicative role in the propagation and dissemination of information and propaganda relating to the ummah and its perceived persecution by the West.4 Although there is little evidence that the internet is a major factor in, for example, the radicalisation and recruitment of foreign fighters in Iraq and Afghanistan5 – principally due to lack of internet access and resources in countries from which the majority of these individuals derive – the picture is very different in Europe, and in the context of so-called ‘home-grown’ terrorism.6 There is currently a dearth of primary data regarding the exact role of the internet in radicalisation in the UK and Europe although an informed consensus does exist as to the reality of the situation.

‘Terrorists use the Internet just like everybody else’, remarked then White House cybersecurity chief Richard Clarke in 2004,7 a truth reminding us that the reality of the situation.

© RUSSI JOURNAL APRIL 2009 VOL. 154 NO. 2 pp. 28–33

DOI: 10.1080/03071840902965587
terrorists, both actual and would-be, use the internet in ways dissimilar to ‘everybody else’. For example, the relative anonymity of the internet has lowered the threshold for engaging in risky behaviours relative to legal and social norms.

The internet normalises behaviours considered unacceptable or inappropriate in the real world

and this is perhaps one reason why the internet has proven to be fertile territory for those promoting or supporting terrorist causes.

In the context of radicalisation, there are three types of internet use that are especially problematic. First, the internet can be used to illustrate and reinforce extremist messages, particularly through the use of suggestive multimedia in the form of video and audio. Second, the internet facilitates an individual’s ability to find, join and integrate into wider virtual communities of interest. Third, the internet serves to normalise behaviours considered unacceptable or inappropriate in real-world environments, which allow extremist views to reverberate and be corroborated within online and interactive ‘echo chambers’ of self-reinforcing discourse.

Although there is some evidence that the internet serves as a form of ‘virtual sanctuary’ for individuals and groups denied freedom of movement, assembly and organisation in the physical world, it is important not to overstate the importance of the internet as a factor in radicalisation. It is undeniably critical to the development of mindsets and social groups amenable to violent words and actions but is by no means the sole vector through which radicalisation occurs. Although there appears to be a clear correlation between internet use and radicalisation, it is too early to define a causal relationship in the absence of detailed data collection and analysis.

It is still the case that most radicalisation is anchored in real-world social interaction and environments. The internet cannot yet replace the crucial human facilitation of individuals’ transitions to violence. The loci of face-to-face discussion and persuasion occur in a variety of milieus – mosques, educational establishments, community centres, family homes, prisons, workplaces – and involve a range of ‘gateway organisations’ and actors. These persons, described variously as ‘shape-shifters’, ‘mystery men’, ‘activists’ and ‘entrepreneurs’ are important human factors in radicalisation, to whom the internet is but an adjunct, albeit a powerful one.

Examples of ‘self-radicalisation’ or ‘auto-radicalisation’ through the internet are rare, although we cannot tell whether this will remain the case. The best-known example is that of Younes Tsouli, the self-styled “Terrorist 007”, whose online activities, in particular the distribution of Al-Qa’ida in Iraq (AQI) video propaganda, led to his 2005 arrest and subsequent conviction. Tsouli is thought to have conducted his activities entirely on the internet. Although connected to a number of jihadists internationally, he never met them in person.

It is too early to define a causal relationship between internet use and radicalisation

On the basis that internet activities are therefore only one factor in the radicalisation of individuals into violence, it seems unlikely that a purely internet-based approach to ‘online radicalisation’ will elicit satisfactory results. We might additionally characterise the issue as non-linear in that the feedback between the internet and its users is often unpredictable and not disposed to simple countermeasures. Nevertheless, many states have proposed or experimented with technical ‘solutions’ to what is, essentially, a social problem.

Technical ‘Solutions’

There are three main types of technical measure that could be used to deny access by users to internet content implicated in radicalisation.

First, undesirable websites and content can be removed from the servers of companies who host them, or those sites can be ‘de-registered’ through negotiation with registration services. In both cases, the material cannot then be accessed by users. In the UK, this can be achieved under the provisions of the Terrorism Act (2006), which allow for ‘notice and takedown’ of websites that fall foul of various items of terrorism legislation, although these have yet to be used. Takedowns have limited utility in that website administrators can merely move content to another jurisdiction. For example, the US is favoured by many purveyors of extremist material because the First Amendment to the Constitution allows for the freedom of speech outside the control of government.

Second, web searches can be manipulated to return negative results when looking for certain types of material. Several European states have attempted
REGULATING THE ‘DARK WEB’

Most radicalisation is anchored in real-world social interaction.

There are valid questions as to whether this form of filtering constitutes censorship; it is generally accepted, however, that this situation is the exception that proves the rule of free access to information over the internet. It is also questionable whether any but the most naïve of would-be terrorists use search engines to find appropriate material anyway, although it may provide an initial portal to the world of the jihadi internet.

Third, internet traffic can be filtered to restrict or block access to internet material. These systems usually operate either by monitoring for restricted keywords, or by preventing access to sites and content inventoried on ‘blacklists’. The most famous example of this is the ‘Great Firewall of China’, a sophisticated and extensive filtering regime maintained by the Chinese state to the detriment of political freedom and much-criticised by Western democracies. What is less well-known is that many of these selfsame democracies also filter internet traffic for a variety of purposes. One scheme is the partnership of the UK internet industry with the Internet Watch Foundation (IWF), which attempts to interdict child sexual abuse images on the internet. Ninety-five per cent of UK internet users are unknowingly subject to this system which, although supported by government, is led by the industry itself. Although the scheme has significantly reduced the volumes of this material hosted in the UK, most of it has simply been moved to locations abroad. Similar schemes operate in many countries, but the lack of truly international co-operation means that this material usually has no problem in finding a home, no matter how temporary. In addition, the blacklists the IWF maintains can be ‘reverse engineered’ to reveal details of their contents, thereby negate the point of producing them in the first place. From the point of view of accuracy, some of these techniques have a propensity to ‘overblock’, denying access to perfectly acceptable material either through the generation of ‘false positives’ or simply because it is on the same server or website as undesirable material. Some of the more sophisticated schemes are also expensive to implement, although this is unlikely to be of too much concern to governments: in Western countries, the end-costs are, somewhat ironically, likely to be borne by internet users themselves. Also, most of these measures can, sometimes with little technical ability, be circumvented; as such, they only represent a first – and low – obstacle to internet users.

A recent exhaustive study by the OpenNet Initiative determined that over forty countries currently deploy combinations of these techniques to various levels of extent and efficacy. Apart from the above problems associated with many of these techniques, there are other issues too. In the context of radicalisation, how effective are such methods likely to be?

The most serious political issue for government is the accusation of censorship, a charge that would be difficult to ignore. It has become common for politicians to link, in rhetorical terms at least, child sexual abuse material with extremist material, for example. The reasons for this are twofold. First, there is a perception that the IWF model can be transferred to the field of extremism, an erroneous assumption that has provided a smokescreen for a lack of other ideas. Second, it is an attempt – through the use of emotive language such as ‘grooming’ – to create a ‘terrorism’ taboo equivalent to that of child abuse. Neither reason has long-term validity, although lessons can be learned from the fight against online child abuse. There is little equivalency between approaches one can take to their ultimate resolution because terrorism occupies the political domain, whereas child abuse is judged in the moral domain. Any direct attempt to remove ‘terrorist’ material from users will be interpreted as censorship, particularly in those communities which will feel victimised by it, such as Muslim communities in the UK. In that sense, this may well fuel exactly the processes of radicalisation such measures are intended to combat.

The most significant practical issue may be that most technical measures may not actually successfully target the internet loci where radicalisation is mainly thought to occur. Filtering techniques are less useful when dealing with ‘dynamic’ content, such as forums, social networking sites, instant messaging, email, and environments like virtual worlds. Most of the debate and discussion so essential to forming and maintaining extremist worldviews happen in forums and chatrooms that are usually password-protected and often invitation-only. These forums are frequently infiltrated by intelligence officials, researchers and private investigators, a fact of which many forum users are all too aware. Even if this type of dynamic content were amenable to filtering, it is unlikely that a lot of extremist interaction would be caught on these well-known forums. In September 2008, three renowned jihadi forums, Al-Ekhlaas, Al-Firdaws and Al-Boraq, suddenly went offline, for reasons unknown. Forum members sought alternative outlets, with exhortations to ‘invade Facebook’, for example, a popular social networking site unlikely to be closed by intelligence or legal measures. One forum member wrote, ‘with the closure of all our sites, you have left us with no choice but to physically join the caravan of Jihad’. It is too early to know to what extent forum members have reverted to more mainstream options – either on- or offline – but it is clear that the jihadi movement will not be stopped by removing forums from the internet, whoever is responsible. Of more concern to intelligence agencies, who viewed the major jihadi forums as a conveniently corralled source of information, is the operation of extremists in the so-called ‘dark web’.

A purely internet-based approach to ‘online radicalisation’ is unlikely to elicit satisfactory results.

The dark web is the part of the web containing websites and file locations...
that are not indexed by conventional search engines and are therefore hard to find. This may be because there are no hypertext links to their content, because registration is required to access them, or because their content is dynamically generated from, for example, back-end databases. Extremists can use the attributes of this type of material to ‘hide’ from search engines and monitoring, and often use a series of ‘redirects’, links that must be followed by invited users to reach certain sites and files. The surface web with which we are all familiar is but a tiny subset of the entire web, possibly as little as 2 to 3 per cent, with the rest effectively hidden from the majority who use tools such as Google to locate content. If it is not indexed by search engines, it will not be possible to, for example, tweak search results to hide it. If its location is not known, filtering with reference to blocklists will not work, as it will not make onto these lists in the first place. For the same reason, if agencies cannot locate content, they cannot attempt to remove it. Google’s own Chief Executive Officer estimated in 2005 that it would be 300 years before all the world’s information is indexable,21 a timescale of near irrelevance to the world’s security agencies and governments. Although initiatives such as the Dark Web project at the University of Arizona have used sophisticated data mining techniques and network analysis to enumerate and identify dynamic and transient content of the types described,22 there is as yet little ability to interdict the vast amount of terrorism-related content ‘out there’, let alone systematically identify those who produce it and engage with it.

**UK Political Discourse**

In one sense, it is understandable that states continue to seek technical solutions to the issue of the internet and radicalisation. There is a perception that the internet is the problem in this arena and, therefore, that it is the internet that requires treatment. As we have seen, this is a misreading of the situation, yet one that has been reproduced in political discourse.

In January 2008, Home Secretary Jacqui Smith announced that the internet was ‘not a no-go area for government’ and that ‘where there is illegal material on the net, I want it removed’.23 She was correct to assert that cyberspace will indeed be the subject of government regulation. In most countries it already is, and cyberspace no longer resembles the ‘Wild West’ frontier lands of cyber-utopians of the past. Smith cited the relative success of removing child sexual abuse imagery from the internet in the UK, but this material has not disappeared from the internet, it is merely hosted elsewhere. This material may be difficult for the average user to access but is still available for those with the technical nous and sufficient intent to do so. As the inventor of British Telecom’s Cleanfeed system – which aims to block access to child sexual abuse content – Mike Galvin admitted, the system ‘won’t stop the hardened paedophile’.24 The belief that network level filtering techniques can be used to prevent access was previously voiced by, for example, Home Office Minister Vernon Coaker. In 2006, he stated in a Parliamentary written answer that, ‘[r]ecently, it has become technically feasible for ISPs [internet service providers] to block home users’ access to websites irrespective of where in the world they are hosted’,25 a statement that is factually incorrect as well as misleading. Perhaps articulating remnant institutional willingness to pursue such methods, Secretary of State Andy Burnham was quoted on The Guardian website at the end of 2008 as saying, ‘There is content that should just not be available to be viewed. That is my view. Absolutely categorical.26

Discussions with UK civil servants have indicated strongly that there is currently little enthusiasm for such techniques within Whitehall or from the Home Secretary herself.27 Even the above statements could be interpreted as attempts to cajole the internet industry into forms of self-regulation that would see them responsible for material deemed inappropriate by government. Self-regulation of content can be construed as self-censorship, of course, which hints further at the problematic crux of the security/democracy puzzle. The Home Secretary has withdrawn from promoting the utility of technical interdiction of material, a positive development which was interpreted in some sections of the media as a lack of action in this field.28

It is true that the UK government is increasingly reluctant – notwithstanding the public utterances of some of its members – to support or enforce technical regulatory regimes on the internet industry. Instead, they have been looking for ways to address the problem through non-technical measures, but have found this a difficult path to tread for lack of perceived positive outcomes relative to the growing radicalisation of British Muslims. Despite the provisions of the Terrorism Act (2006) allowing for the takedown of websites, these have not been deployed on even a single occasion. Government has not been so reluctant to intervene on other issues though, with gang culture videos, online glorification of knife crime, ‘pro-anorexia’ sites and ‘pro-suicide’ sites all coming under scrutiny from government, and effecting action from sites such as YouTube in removing this material from their servers. In the US, Senator Joe Lieberman conducted a very public campaign against Google that resulted in YouTube – Google’s subsidiary – capitulating by removing dozens of insurgent videos from its site.29 In Australia, a proposed network filtering system has been massively opposed by politicians and public alike30 and, in Sweden, legislation for a national internet monitoring scheme resulted in so many complaints that it crashed government servers.31

**Conclusion**

Political backlash, a potential uptick in radicalisation, expense, inaccuracy, and generally limited utility: it is little wonder...
that the UK government has moved away from embracing full-scale technical measures as the primary solution to the role of the internet in radicalisation. Instead, it is exploring ways in which the social factors relating to internet use can be positively addressed. This is actually more in line with mainstream PREVENT concepts, problematic as they are. It may be that the recent panic over the internet and radicalisation largely fades away. Although the internet in many of its guises is very different from traditional media, there are enough similarities to suggest that the problems associated with the internet have historical analogues with television, radio, telephony and the printing press. All social technologies present problems of this type, and all have been the subject of regulation, as well as public concern. All continue to challenge the capacity and will of governments to regulate human behaviour.

Where the internet does differ is in its volume and velocity, its interactivity and transnationality. It is also a highly dynamic evolving environment. It is therefore crucial that countermeasures to perceived misuse of this technology are flexible and adaptable, and social policy has more capacity for this than relatively crude technological regimes. Approaches to undesirable internet use should focus more on prosecuting the producers, rather than the consumers, of extremist material. It should attempt to empower rather than disenfranchise internet users and communities. The promotion of positive messages to counter the negative of violent, inciteful and hateful propaganda is partly responsible for the creation of cross-departmental bodies like the Research, Information and Communications Unit (RICU) but more attention should be given to bottom-up, community-led initiatives, rather than centralised, hierarchical narrative propagation. Perhaps of most long-term promise is a review of current educational emphasis on media literacy, particularly of critical literacy in online environments. Teaching of critical literacy, although an integral part of the National Curriculum, is patchy and unevenly distributed, and a renewed commitment to its importance might help young people to more successfully parse, analyse and interpret the complexities of cyberspace in which they increasingly spend their time.

Suggested investment in these fields is unlikely to win friends amongst hardliners, nor satisfy the political desires of some policymakers. It will also not completely eradicate the role of the internet in extremism – the desire to voice and inflict violence will always be integral to the human experience. What a social approach to the internet is more likely to achieve is an institutional understanding of its social nature, and a gradual erosion of the bulwarks of extremism: ignorance, isolation, and paranoia.

* With the closure of all our sites, you have left us with no choice but to physically join the caravan of Jihad*

© RUSI JOURNAL APRIL 2009


16 Vernon Coaker, written answer on pornography and the internet, Commons Hansard Parliamentary Debates, 16 June 2008, Column 684W.


20 Quoted in Awan and Al-Lami, op cit.


25 Coaker, op cit.


