ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

STRATEGIC POLICY FORUM 13 July 2009

Countering online radicalisation in Australia

This ASPI Strategic Policy Forum examines approaches to countering online radicalisation in Australia. Forum contributors participated in an ASPI outreach dialogue on the topic of internet radicalisation that was held in Perth, Western Australia, in May 2009.

The internet as a platform for radicalisation

Dr Anthony Bergin is ASPI's Director of Research Programs

Increasingly, extremists are using the internet to communicate, spread information and network. Although only a few individuals have been convinced to carry out terrorist operations simply by reading material online, this is changing. The internet is playing a significant conveyor-belt role in the transition of people from curiosity to seeking a cause to violence. As law enforcement agencies monitor the physical spaces, making it harder for extremist groups to operate in the open, some of these groups are turning to cyberspace.

The recent sentencing of Abdul Benbrika and others in Melbourne on terrorism-related offences showed how central the internet was to both the recruitment and radicalisation of individuals. According to the evidence, there was widespread access to and discussion of extremist websites among the group. In sentencing Benbrika to twelve years in prison, Justice Bongiorno noted that, although the possession of such material might not be a criminal offence, it takes on a more sinister complexion when used by charismatic leaders to encourage or engage in acts of terrorism. That said, most radicalisation still requires some 'real-world' face-to-face contact.

The internet reinforces political messages and builds online communities sharing similar perspectives. These messages provide inspiration, practical instructions and a support network that facilitates links with other cells. The anonymity of the internet has lowered the threshold for those wanting to engage in risky behaviour. There are, however, real legal problems confronting authorities where a website is hosted in one state and incites violence in another, while the extremists behind it plan operations from a third country.

There are at least three broad approaches to dealing with this very complex problem. First, a strategy of zero tolerance (blocking sites, prosecuting site administrators, using internet filters); second, encouraging internet end users to directly challenge the extremist narrative; and finally, intelligence-led strategies of monitoring leading to targeting, investigation, disruption and arrest. Each approach will have advantages and drawbacks in its security consequences, economic impacts and human rights implications.*

To date, Australian authorities have done little to tackle online radicalisation. The Rudd government's clear election commitment as part of its *Cyber-safety plan* was, however, to favour the introduction of Internet Service Provider (ISP)-level filtering, which has proved effective in blocking the content of internet websites, predominantly comprising images of the sexual abuse of children. The argument for mandatory filters is the same in principle as the argument for a film censorship system.

The government hopes to introduce mandatory ISP-level content filtering that would automatically block 'refused classification' material matched against a web page blacklist that is managed by the Australian Communications and Media Authority. Refused-classification material includes images of child sexual abuse, detailed instruction in crime, violence or drug use and material that advocates terrorist activity. Optus is participating in a broadband filtering trial being undertaken by the federal government. It is the eighth internet service provider to participate in the scheme. The government wants ISPs to conduct live tests to gauge the impact of content filtering on networks, and determine whether it would vastly slow down internet speeds.

Most Western governments prefer to monitor sites and extreme chat rooms to get a window into extremist groups' operations and thinking rather than trying to censor the internet. Many technical experts argue that a hardline censorship approach is not only expensive, but doesn't really work: eliminating one site often results in another site popping up. Closing down an extremist chat room might simply mean the online traffic goes to other sites.

Monitoring provides very useful information for policing and intelligence agencies, although it can raise civil liberties issues as well. Some extremist groups, of course, know they are being monitored. They might adopt measures such as coded messages to hide their online activities and stay below the radar screen of law enforcement.

Apart from monitoring, there may be occasions when Australian authorities might wish to take action against a particular site to show it's on the offensive or selectively prosecute those producing extremist websites (rather than the consumers).

Australian authorities should encourage internet end users to directly challenge the extremist narrative by providing incentives to create websites and online forums that promote tolerance.

Encouraging parents and teachers to alert students to the risks of websites that preach extremism is also important. This issue can be raised in the general context of cyber-safety education.

* These approaches are outlined within a Southeast Asian context in a joint ASPI and Rajaratnam School of International Studies (RSIS) report by Anthony Bergin, Sulastri Bte Osman, Carl Ungerer and Nur Azlin Mohammed Yasin, *Countering Internet Radicalisation in Southeast Asia*, March 2009.

Legal and policy issues in combating online radicalisation

Mr Michael Crowley is Senior Lecturer in Law, School of Law and Justice, Edith Cowan University, and Barrister of the Supreme Courts of Western Australia, New South Wales and the Australian Capital Territory and of the High Court of Australia

Any policy aimed at combating internet-based radicalisation by legislation is doomed to fail due to the nature of the internet and human ingenuity. Sometimes a legal solution is not the best or only solution to a policy issue. Blocking access to radical websites raises the spectre of 'political control', while monitoring the same websites to identify users is technically difficult unless the authorities have a target. A global approach would directly impinge upon traditional rights and freedoms, not to mention privacy laws. A worst-case scenario may reflect George Orwell's *1984* or resemble controls and restrictions in single party and totalitarian regimes. Nevertheless, when a government blocks websites and monitors access without reasonable suspicion of criminal activity it is threatening the foundations of our democracy in achieving the aims of the website promoters.

The reality is that 'war on terror' laws already exist in Australia that threaten democratic rights and freedoms. Breaches of these laws can result in a criminal conviction. To date there has been limited protest and these not-so-new 'war on terror' laws have had mixed results. Their potential for misuse was demonstrated in the cases concerning Dr Mohammed Haneef and medical student, Izhar ul-Haque.

Therefore, enacting any new legislation to 'block' or combat internet radicalisation should be approached with grave caution especially as Australia does not have a Bill of Rights. However, having a strong Constitution or Bill of Rights does not prevent bad laws. For example, although the United States has enacted *The Violent Radicalization and Homegrown Terrorism Prevention Act* of 2007 (S.1959/H.R.1955), criticisms include the focus on ideology rather than criminal behaviour. The ideological focus threatens Constitutional protections, jeopardises internet use as a free speech zone and erodes civil liberties.

Instead, a return to first principles is needed in combating criminal behaviour even if such behaviour is linked to internet-based radicalisation. More appropriately, we require effective gathering of evidence by police forces rather than focusing on enhanced powers via new laws. Banning websites and instituting widespread internet monitoring to combat internet-based radicalisation, while politically advantageous, would reap few real benefits.

In Australia, any legal attack on internet-based radicalisation to combat terrorism would invoke our 'terror laws'. These laws define 'terrorist activities' widely and encompass political dissent. They also provide significant powers for accessing computer networks and negating claims of privilege or privacy over information databases. In 2005 the laws were extended to include organisations that advocate the doing of a terrorist act. 'Terror laws' were used recently in convicting Abdul Benbrika and others in Melbourne. These convictions were significant because they demonstrated the prosecutorial advantage gained from allowing free, uninhibited internet access combined with traditional forensic police work. According to the judge, Abdul Benbrika's conviction was facilitated by acts of the accused in accessing and circulating materials from internet websites that would be commonly described as 'extremist'. In the end the accused were likely to have been convicted, not for their access of radical or extreme internet websites per se, but for adverse inferences that could be drawn from such access when combined with other 'acts'. Those same persons encouraged each other to engage in acts of violent jihad during meetings in urban and remote locations, supposedly for bonding and training purposes. They also stole a vehicle to raise money for their jihad. Abdul Benbrika was also convicted of possessing a 'thing' connected with a terrorist act, the 'thing' being a compact disc containing jihad material.

These prosecutions did not seem to need access to or co-operation with authorities or internet providers in other countries. Furthermore, the Australian Federal Police already engages in significant bilateral law enforcement cooperation. The issue there is whether or not this cooperation results in any beneficial intelligence flow-on to local police forces who may 'suspect' certain targets but lack enough evidence to raise a 'reasonable suspicion' to justify the use of search and listening device warrants. More use could also be made of criminal laws that aid surreptitious evidence collection. For example, controlled operations legislation commonly associated with drug and organised crimes syndicates offer a medium- to long-term approach to identifying home-grown terrorist operations.

Prohibition has generally proved to be ineffective. The recent prominence of the 'WikiLeaks' website illustrates problems governments have with prohibition and the internet. We have enough laws for counter-radicalisation operations. What we lack is imagination to counter the internet messages that foster radicalisation. Any claim for new laws based on assertions like 'if you have done nothing wrong you have nothing to fear' lulls citizens into a false sense of security.

Industry role in counter-radicalisation

Mr Richard Bone is President of the WA Internet Association, board member of the national Internet Industry Association and board member of the WA ICT Industry Collaboration Centre. He is also the director of three Internet-related software companies including Managing Director of Elk Software Group.

The internet industry is multi-faceted. In particular there are two main types of participants—Internet Service Providers (ISPs) and hosts.

ISPs provide a conduit that connects consumers to hosts and to each other. Their goal is to deliver an internet connection at the lowest possible cost with highest possible speed. The focus of an ISP is often highly technical, making use of routing and caching technologies to improve customer experience and reduce costs. With regard to radicalisation content, an ISP is often not aware of the content being delivered to subscribers and may not even be able to view it as a result of it being encrypted. An ISP will lose money on customers that: require support frequently, draw data volumes at a level that is near to their 'cap', and are in new areas where the ISP has made capital expenditure on equipment that does not yet return enough income to justify the cost. ISPs make money from established customers that operate well within their limits and do not draw on support resources. It is a business of averages and long-term relationships.

Hosts are internet industry participants that provide content for users to consume. Examples are Google and Yahoo. Their income is often derived from advertising. The trend in host service is 'Web 2.0' which is a buzz-word for consumer-generated content. With regard to radicalisation, a host may provide a Web 2.0 facility for consumers to start a 'thread' and then for others to join and share ideas on the thread.

The regulatory framework in Australia provides 'safe harbour' for ISPs but not for hosts. For this reason, much content is hosted off-shore and the majority of hosting contracts prohibit any content that is likely to result in liability or additional costs for hosts. At present the safe harbour legislation is being tested in the case iiNet vs AFACT.

Given the above nature of the industry participants, the internet Industry is relatively risk averse and will avoid radicalisation content because it has the potential to result in liability to the ISP/host and/or result in increased support costs.

A difficulty in engaging ISPs and hosts in the fight against radicalisation is the issue of jurisdictional boundaries. The difficulty arises where the hosted content may be legal in the country in which it is hosted but not legal in Australia. If the content is encrypted then the ISP will have no way of determining what the content is and little ability to determine whether access to it breaks any laws, in particular given that ISPs do not have a mandated regulatory role. It is arguably more valuable and productive for ISPs to work with Australian law enforcement agencies to help track and identify individuals involved in radicalisation rather than attempting to block such content.

The internet industry is generally opposed to ISP-level filtering because:

1. It is not an effective way to block or stop the content that it is designed to prevent.
2. Filters can be bypassed. This would be particularly relevant in radicalisation networks where the participants form a relationship with each other which could involve sharing of techniques to bypass filters.
3. The introduction of (arguably ineffective) filters will increase the costs to ISPs and impede their ability to provide superior performance. This will ultimately lead to higher costs and lower performance for consumers.
4. Legislative change is far too slow to be effective. For example, the time to introduce filtering legislation, or revisions to such legislation is months or years whereas technology to bypass and/or avoid filters would occur in days or even hours.
5. The introduction of filtering legislation would be an impediment to investment and innovation in the Australian internet industry. It is already the case that the lack of safe harbour legislation for hosts within Australia drives Australian content to be hosted offshore. If filtering is introduced this will worsen.

The Australian internet industry is largely supportive of the need for the internet to be used for ‘good’ rather than ‘evil’ and as a result is very prepared to cooperate with law enforcement in any way possible.

Of note is a recent move by Facebook to remove a group called ‘I Hate Muslims in Oz’ because it contained an explicit statement of hate which is a violation of the terms of service of Facebook. This group was created by consumers and only came to the attention of Facebook as a result of user complaints. Ultimately the group did little harm and certainly did not play any significant role in radicalisation but its removal highlights the risk-averse nature of Facebook in both terms of service as well as tolerance for such content.

In forming counter-radicalisation policy it should be remembered that the internet provides a tool to help humans communicate better and more easily. It is a facility that underpins a human activity system. As part of a human activity system, the internet evolves often very rapidly to trends driven by human behaviour. The internet is resistant to impediment—where changes are introduced they are often quickly circumvented.

From an industry perspective, the best way to fight radicalisation is to use human law enforcement, equipped with state-of-the-art technology, assisted by the Australian internet industry.

Online radicalisation and the Muslim Diaspora

Dr Anne Aly is a Research Fellow with the Faculty of Business and Law, Edith Cowan University

In 2005 and 2006 I conducted research into how Australian Muslims were responding to the discourse on terrorism in the Australian popular media. Even then, it was increasingly evident that Australian Muslims were turning to the internet to access information about the United States-led interventions in Afghanistan and Iraq, and engaging heavily in propaganda and conspiracy theories—readily accessible to large audiences through the internet. It is not until recently, however, that attention has focused on the role of the internet in the process of radicalising individuals and groups in support of violent action. As Anthony Bergin has rightly pointed out, the internet is increasingly becoming a platform for radicalisation.

In part this is due to the ubiquity of the internet. Many adolescents have integrated the internet as part of their daily existence and to a much higher intensity than many adults. According to a senior executive at Microsoft, this represents a discontinuous change in how adolescents behave. They view the internet as essential, with many adolescents being what the industry refers to as AORTAs - always online and real time available. For Muslim adolescents in Australia, the internet has become one of the primary sources of religious information. Several forums attract large numbers of Australian Muslims in discussion of topics as diverse as whether or not Islam sanctions the giving and receiving of Christmas gifts to whether or not Weapons of Mass Destruction can be used in armed Jihad.

The appeal of the internet for terrorists lies in its capacity not only to tap into existing audiences but to create new audiences within social spaces where users can interact across the divide of time and space. The immediacy of the internet and its reach provide terrorists with a platform to promote propaganda to a mass audience of potential sympathisers and recruits. In the contemporary terrorist environment in which psychological warfare plays an integral part, having a presence on the internet is almost as critical to the terrorists as tactical capability. The internet has become a one-stop shop for terrorists: a communicative space where they can identify, inform, influence and indoctrinate.

Questions remain about the terrorist audience: questions that relate to the role of audience agency and the role of the internet in the process of radicalisation.

Attempts by sociologists, psychologists and social scientists to explain why some individuals are more vulnerable to the militant propaganda of terrorist organisations such as al-Qaeda have concluded that it is impossible to psychologically profile a terrorist. There are, however, identifiable factors that characterise the contemporary context of Muslims and needs, including needs relating to the use of the internet and other media. These are:

1. Transnationalism and the emergence of a Muslim diaspora.
2. The development of a shared identity among Muslims around the globe grounded in victimhood and validated by the concept of the 'ummah'—a brotherhood that transcends boundaries of nationhood, ethnicity or race.
3. A widely-held perception among Muslims in the diaspora that the Western media is a complicit actor in a conspiracy to undermine Islam and subsequent disengagement with the Western media as a source of news and information.
4. The presence or perceived presence of a personal and communal crisis. This crisis is framed in terms of an ideological battle for the survival of Islam and expressed in terms of a war (violent jihad) between Islam and the West.

Technical solutions and legislative or policy options tend to target the producers of internet content and the focus of attention on content. However, the Hydra-like quality of internet terrorism means that cutting off one head will only grow more in its place. An approach which focuses on the terrorists' internet audience would address the reasons why certain people become attracted to the internet as a source of inspiration. Such an approach should focus on equipping internet audiences, particularly adolescents, with the skills and capability to identify and critically analyse terrorist propaganda on the internet. This may be done as part of a broader campaign of educating our youth about the internet and safety.

It is also important to recognise that the internet, though influential, does not fully determine consequences of radicalisation. The role of personal interaction with opinion leaders and influential people in the radicalisation process should also be taken into account in developing an understanding of how online interaction contributes to radicalisation.

As more and more people embrace the online environment, education that develops the skills to be discerning and judicious of online content will become more critical. The internet is not merely a virtual world where individuals interact on a virtual level: it is a social reality and, to the user, these interactions are real. Education would help to re-establish the boundaries between virtuality and reality.

Upholding the principle of free speech

Mr David Cake is Secretary of Electronic Frontiers Australia

Electronic Frontiers Australia is a membership-based lobby group focused on civil liberties in the online world, and as such it should come as no surprise that a group focused on free speech concerns would argue that free speech concerns should strongly inform any strategy for countering online radicalisation. We believe, however, that this is true not only because of the importance of free speech as a democratic principle, but also because a relatively open approach that respects the right to free speech is by far the most effective and practical basis for a strategy to effectively counter radicalisation.

We can roughly divide radical communities' online speech into two broad divisions. There is speech that is primarily ideological, arguing a position (political, religious, or social) without planning a specific action. And then there is speech that is operational, speech that involves planning radical action, be it legal or illegal.

One argument against a strategy based on suppressing radical speech is that ultimately very little that can be done that will effectively prevent an organised and technically savvy group from communicating covertly among themselves.

There are a range of technologies that can be used to conceal the content of a discussion, and even that the discussion is going on. There are also a number of practical techniques in use by groups on the internet including privacy activists and a range of malicious actors. There are anonymising routers like The Onion Router (TOR), a wide variety of encryption techniques, and steganography programs to conceal messages in innocent appearing content. Covert child abuse material rings, for example, now use the technique of trading encrypted, password-protected, and relatively innocuously named files via peer-to-peer networks, and covertly sharing only the password and file name via other channels.

Censoring internet activity is only effective for groups who lack the technical understanding to circumvent it. When a group is already radicalised to the point of planning illegal and covert activities, technologically-based methods will need to be supplemented by other means, such as infiltration (which can be hampered when attempts to restrict political speech drives such groups further underground).

So, for radical speech that is operational and illegal in nature, suppression via legislative or technological methods is likely to fail. We must rely on infiltration and other human intelligence methods.

Restricting free speech that is ideological in nature hampers both law enforcement, monitoring, and the important work of providing an alternate message. Radical speech must be countered by arguments for more tolerant and democratic points of view. Suppression of radical online speech might slow down or inconvenience outreach from radical online groups, but it hampers debate, and also isolates those already flirting with radical viewpoints from opposing arguments.

For operational issues that are discussing a legal expression of radical views, such as demonstrations and protests, the more open such discussions are, the more practical it is for law enforcement agencies to monitor these events and plan an appropriate response. Such discussions should not be suppressed, but monitored.

So in all cases, a strategy of countering online radicalisation that relies on attempts to directly suppress radical speech is likely to hamper effective response and appropriate counter-measures, and accomplish little.

To counter the threats posed by online radicalisation, we need to focus both on countering the possible operational efforts of already radical groups and on countering their efforts to promote radicalisation. Countering the operational efforts of already radical groups is helped little by suppression of their online activity, and law enforcement monitoring and infiltration is hampered.

To counter the efforts of radical groups to achieve outreach and recruitment, we need to present effective arguments for tolerance and more moderate viewpoints. And of course arguments in favour of a democratic and tolerant viewpoint are strengthened by demonstrating those principles. Countering online radicalisation is a challenging issue, but it seems clear that retaining our own free speech principles is the foundation of a strong and effective strategy.

Concluding remarks

Mr Raspal Khosa is an ASPI Research Fellow and Outreach Program Manager

The internet is a powerful tool for extremists to radicalise vulnerable individuals and potentially recruit them to violence. The subterranean character and cross-jurisdictional nature of the online environment is challenging for national authorities attempting to counter the insidious threat of radicalisation. Indeed, as Michael Crowley argues, any attempts by government to block radical websites through legislative means may be counter-productive and ultimately corrosive of democracy.

Instead, we require laws that enable intelligent policing to prosecute criminal activity where it exists. For example, law enforcement officers may have to adopt assumed identities to engage people online in order to gather evidence. However, this will require Australia-wide legislative support to indemnify officials from accusations of criminality, racial vilification and incitement. Here we must also consider the problem of entrapment.

For any counter-radicalisation strategy to be successful we require a strong partnership between government and the internet industry. Richard Bone contends that it is more advantageous for authorities to work with internet service providers—who are generally risk averse—to investigate and disrupt radical networks, rather than impose onerous legislative measures such as mandatory filtering of online content that may have the effect of stifling an industry which operates on narrow margins.

Anne Aly's piece focuses on the radicalisation of Muslim diaspora communities in the Western world. The internet, however, is an arena where a multiplicity of extremist groups ranging from white supremacists to radical environmentalists, seek to indoctrinate at-risk and often young audiences. Anne suggests one solution to this challenge is to empower internet users through education so they can deconstruct messages and question the validity of extremist propaganda.

We must also develop an alternative narrative to that espoused by organisations with a propensity for violence. Here authorities may need to take a back seat and allow appropriate community groups to present a contrapuntal discourse. Nevertheless, government can enable the process by providing grants to establish and support hosted sites.

In the United Kingdom the government funds the *Radical Middle Way* website (www.radicalmiddleway.co.uk) that promotes an understanding of mainstream Islam among young British Muslims. Another strategy to combat radicalism is an online advice line (www.elhatef.com) for Muslims on questions of faith which are answered by respected centrist Islamic scholars from Egypt's al-Azhar University. In addition to these initiatives counter-narratives from trusted community stakeholders may also be required on marginal websites in order to challenge extremist messages.

David Cake maintains that counter-radicalisation strategies should be predicated on respecting the principle of free speech, and in doing so we uphold our tolerant democratic values. In any case, he argues tech-savvy radical groups can circumvent attempts at suppression through a range of existing methodologies and will find other pathways with which to operate. Simply relying on technological solutions is a reactive strategy that will always place authorities on the back foot.

An unfettered approach to the internet demonstrates that we value freedom of information. It also offers a very real intelligence dividend to law enforcement agencies. For instance, so-called ‘honey pot’ sites may be monitored by authorities to obtain intelligence on extremists. To ensure the efficacy of this approach we should make available more resources to improve the cultural and linguistic skills of operatives conducting surveillance and otherwise engaged in counter-measures to online radicalisation.