

# SPECIAL REPORT

March 2009 — Issue 22

## Countering internet radicalisation in Southeast Asia

An RSIS–ASPI joint report



by Anthony Bergin, Sulastris Bte Osman, Carl Ungerer and Nur Azlin Mohamed Yasin

### Foreword

The internet is at the centre of modern life. It can facilitate understanding between people of different cultures and promote a sense of global community. At the same time, however, it can be a powerful tool for terrorists to promote extremist ideology and hatred.

The writings of terrorist groups are regularly posted on websites in our region. And extremists use various web forums and chat rooms to entice new recruits. Convicted terrorists have given evidence about the influence of the internet in their recruitment and communication strategies.

Although the internet has become an important tool for tactical operations such as bombings, psychological warfare and fundraising, the focus in this paper is on its use as a tool to radicalise potential supporters.

This study found that the internet has contributed to radicalisation, will probably grow in regional significance, and might become the dominant factor in radicalisation in the region. And it's not just passive websites that are important in this context: social networking sites of all kinds, such as blogs and forums, are evolving rapidly.

This paper discusses several policy approaches to counter the use of the internet for radicalisation in our region. These include blocking sites, creating counternarrative websites to promote tolerance, and intelligence-led methods to tackle the problem.

In preparing this report, the authors canvassed a range of views among officials in Australia and the region, as well as those of industry representatives and community stakeholders. The project was carried out jointly by the S. Rajaratnam School of International Studies and the Australian Strategic Policy Institute. We are grateful to the authors and all those, from both organisations, involved in the production of the report.

The report makes an important contribution to understanding how terrorist organisations use the internet in our region and provides clear pathways for policy development to counter online radicalisation at the national and regional levels.

Barry Desker  
Dean  
S. Rajaratnam School of International Studies

Peter Abigail  
Executive Director  
Australian Strategic Policy Institute

## Introduction

Since its inception, the internet has been an important medium for the dissemination of terrorist propaganda and materials. Leading al-Qaeda strategists have long demonstrated the importance of the internet as a tool of mass communication. More recently, the internet has become an important part of the radicalisation process by which some individuals move along the pathway from curiosity, to sympathy for extremist causes, to actual violence. Although there is a growing body of research on terrorists' use of the internet in Europe, the Middle East and North America<sup>1</sup>, less attention has been given to the role of the internet in online radicalisation in Southeast Asia and how it affects neighbouring countries, such as Australia.

As this report shows, terrorist groups in Southeast Asia are increasingly using the internet as a means to radicalise people, as well as to recruit and train supporters. The writings of terrorist leaders are regularly posted on popular websites. Bomb-making information is now freely available on some websites. Extremists use chat rooms and web forums to entice and to identify prospective members. Convicted terrorists in our region attest to the influence of the internet in their recruitment.

Moreover, the average age of terrorists appears to be declining, as is the age when young people are becoming radicalised. Teenagers are the greatest users of the internet and are therefore most likely to be influenced by it (Sageman 2008: 111). They've grown up with computers and they spend much time online. The trend of increased internet usage is expected to continue over the next decade.

The internet is an easily accessible operational platform, but it is also a complex set of systems, with many layers not known to the general public. That's why at the core of the

extremist message we find calls to operate as a decentralised network and encouragement for individuals to develop technical computer skills. It's no surprise that much of the focus of terrorist recruitment activity is on university and college campuses, where access to computers and skilled operators is highest.

The internet is used to reinforce religious and political messages, to increase commitment and to build online communities sharing similar perspectives. These messages can provide inspiration, ideological support, practical instructions, friends and a social support network that facilitates links with other cells.

But our knowledge of precisely how individuals become radicalised online remains limited. Of the few known case studies, the radicalisation process was the result of a variety of social and psychological factors (see Box 1). Clearly, there is not just one pathway along which radicalisation occurs.

Most extremist activity on the internet aims to communicate a narrative, to draw in support and to incite action. The operational aspect is certainly there, but it's much smaller than the communications and propaganda side. To put this bluntly: security agencies may detect the bomb manuals, but miss the process of radicalisation that produces the bombers.

Of course, we shouldn't neglect offline networks. As Marc Sageman notes:

... most online participants also have friends who share their views and desires but do not spend so much time on the internet. Terror networks consist of a mixture of online and offline elements, and their respective in-person and virtual discussions mutually influence each other. (Sageman 2008: 121)

The link between increasing extremist use of the internet and increasing extremism comes from the reality that terrorist activity

### Box 1: Internet radicalisation—recent case studies

The internet can make it easier for individuals nursing a sense of social alienation to search for an identity and a cause. This was the case for Singaporean Abdul Basheer, a law graduate who was lecturing at a local tertiary institution. Basheer was arrested by Singapore's Internal Security Department in February 2007 for attempting to join the Taliban in Afghanistan. He had turned to the internet for answers to his questions on religion and chanced upon radical explanations that resonated with his state of mind and his personality. He believed martyrdom and the promise of paradise would bring moral redemption within his family. His arrest came after the Internal Security Department investigated a small number of Singaporeans who had become attracted to radical and terrorist ideologies through the mass media, especially the internet.

In Australia, recent evidence given in the Victorian Supreme Court trial of Abdul Benbrika and others on terrorism-related offences shows how the dissemination of extremist material can contribute to radicalisation and violence. The court heard that the Benbrika group downloaded,

collated and distributed extremist material, including videos of hostage beheadings and documents entitled *The terrorist's handbook* and the *White resistance manual* that contained recipes for the manufacture of explosives. According to the evidence, there was widespread access to and discussion of these websites among the Muslim community. 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, for which such material provides extremely useful instruction.

Recent examples from Europe, including the cases of Younis Tsouli (a.k.a. 'irhabio07') and Ifran Rafa, show that the internet can be the main way some individuals become radicalised without external contact. Both men spent hundreds of hours downloading videos, posting email messages and chatting on web forums. As a result of those activities, and without any prior involvement with extremist groups, both Tsouli and Rafa concluded that they wanted to participate in a terrorist attack. They were joined by others online to create a 'virtual' terrorist cell. Both men were arrested by British authorities.

on the internet aims to culminate in either an attack on the ground or in a cyberattack. The internet provides all the pre-incident information for either scenario (Council of Europe 2007).

Most countries, including Australia, now face the problem of homegrown radicalisation. As police monitoring of physical spaces makes it harder for extremist groups to operate in the open, they're turning to cyberspace

(Sageman 2008: 110). And the internet offers a vast battleground where 'female fighters' are able to join the ranks at the front line, without restrictions (Mostarom 2009).

Understanding and countering online radicalisation must be one of the main pillars of the fight against regional terrorism. Therefore, this report recommends that national and regional plans be put in place to combat terrorists' use of the internet.

### Box 2: YouTube and auto-radicalisation

Recent research on how YouTube videos are posted and distributed highlights the potential radicalising influence of Web 2.0 applications that integrate information with social networking. A content analysis study conducted at the Dublin City University has traced the viewing activities of a small group of individuals who posted and discussed material concerning the conflict in Iraq. The results showed how individuals browsing generic websites could be integrated into a specific network. In one example, a young male who identified himself as an Irish rugby fan posted a comment citing his admiration for Islam and his wish to convert after viewing a martyrdom video. Within weeks of posting this message, he was targeted by several heavy users, with radical links, whose aim at a minimum was religious conversion. (See Conway and McInerney 2008.)

## Trends in terrorist use of the internet

In the future, we will see a number of trends in online radicalisation, as well as in the internet's role in terrorist operations.

Countermeasures should focus not only on the more passive (informational) websites, but on the chat rooms and interactive communication sites where people's relationships are being transformed. As Sageman has pointed out:

because of its apparent anonymity, people are more likely to self-disclose via computer mediated technology, which contributes to feelings of greater intimacy ... many people who have met on the internet have gone on to marry, including some

of the terrorists. The intensity of feelings developed online rival those that developed offline ... It is these forums, not the images of passive websites, which are crucial in the process of radicalisation. People change their minds through discussion with friends, not by simply reading impersonal stories. (Sageman 2008: 114–116)

The internet isn't likely to fully replace personal interaction in recruitment, which still involves social group dynamics. Virtual self-recruitment won't be common (Durodie and Ng 2008; Chatham House 2008).

Just as it's difficult to directly link watching violence on television to violent behaviour, it's also difficult to prove that surfing radical websites leads to radicalisation. Other factors have to be present in the psychology of the person, their immediate external environment and the larger society to prompt a series of radicalising deliberations that make them accept a revolutionary attitude and spur them to act against the status quo.

However, most experts now believe that internet-supported recruitment will grow in significance, even if recruitment solely via the internet continues to be the exception.

It's likely that there will be increased use of hidden internet architecture, such as file repositories and storage sites. This means terrorists are likely to increase their use of non-extremist forums and hidden parts of the web. These hidden layers remain unknown to the general public and are difficult for intelligence and law enforcement agencies to detect.

It's also likely that terrorist cells and groups will adopt greater vigilance against the activities of law enforcement agencies and develop more innovative information security measures. Terrorist groups will continue to exploit rapidly evolving technology, including convergent technologies like Voice over

Internet Protocol (VoIP) to communicate, disseminate and coordinate. However, they also know that the message must be relatively accessible to all, at least in the beginning.

The digital landscape will continue to evolve rapidly. Many young people already spend hours each week on social networking sites or blogs. Internet forums and chat rooms provide them with an instant group of friends. Sharing their aspirations makes them feel closer to one another, giving them a sense of belonging to a greater community. All this is likely to result in a larger recruitment pool of individuals who are well versed in internet communications.

The importance of online dissemination of extremist material can be expected to increase, particularly given the fast growing number of internet users in the region (see Table 1).

## The content of extremist websites in Southeast Asia

The phenomenon of online extremism first appeared in Southeast Asia in early 2000, particularly in the Bahasa Indonesia and Malay

language cyber-environment. These websites have shown a tendency to mimic the contents and features of their Arabic and Middle Eastern online counterparts. Although they aren't yet on par in operational coordination and tradecraft, they are catching up.

Many of the Bahasa Indonesia and Malay language websites have been used as online platforms to justify terrorist acts and propagate conspiracy theories. More recently, they have disseminated tradecraft materials, such as hacking, firearm and bomb-making manuals. One of the first appearances of a tradecraft manual was in August 2007 in the then new forum, *Jihad al-Firdaus*.<sup>2</sup> The forum had an entire section on electronic *jihad*, including several hacking manuals.

There have been at least two reported hacking incidents in the region. One of the targets was *Indonesia.faithfreedom.org*, a website that radical Islamists lambaste as degrading to Islam. The other was a *Friendster* account that belonged to a member of Faith Freedom Indonesia. While there's no evidence that the hackings were conducted by members of the *al-Firdaus* forum, that scenario is certainly plausible. The forum is no

Table 1: Southeast Asia—internet access statistics

Country	Internet users (2000)	Internet users (15 January 2008)	Growth (%) (based on 2000)
Australia	6,599,788	15,300,000	132%
Brunei	30,000	176,029	487%
Cambodia	n.a.	n.a.	n.a.
Indonesia	2,000,000	20,000,000	900%
Lao PDR	n.a.	n.a.	n.a.
Malaysia	3,700,000	14,904,000	303%
Myanmar	n.a.	n.a.	n.a.
Philippines	2,000,000	14,000,000	600%
Singapore	1,200,000	2,421,800	102%
Thailand	2,300,000	8,465,800	268%
Vietnam	200,000	18,226,701	9,013%

n.a. = data not available

Source: [www.Internetworldstats.com](http://www.Internetworldstats.com)

longer accessible, but other forums and blogs that have taken its place provide an array of similar hacking manuals.

More tradecraft materials followed with the emergence of *Forum Al-Tawbah* in February 2008. The forum is registered in Shah Alam, Selangor, Malaysia, and features strong Arabic influences and a high content of bomb-making and weaponry videos and manuals. The first sophisticated bomb-making manual and bomb-making video compilation were found on *Forum Al-Tawbah*. A detailed firearm manual was posted in April 2008 by the forum member who had posted the bomb manual.

The first tradecraft materials online met with enthusiastic support from forum participants and visitors. Although participants encouraged one another to put up more of such materials, the manuals are not known to have been put to use.

These materials clearly have a strong radicalising influence. Since the second quarter of 2008, forum participants have publicly declared their intentions to be

more proactive in armed violence. Many complained that the manuals were useless if they were not put into practice.

While there has been no serious attempt to plan or coordinate militant operations in these forums, some individuals have been asked to get in touch with others for Airsoft gun training and martial arts exercises. Such invitations are usually extended in the public forum area. Further details of the activities are always communicated through private messages or personal emails that are difficult to trace.

The Bahasa Indonesia and Malay language websites typically justify their radical and extremist ideologies and various acts of terror by propagating carefully selected Quranic verses, as well as academic articles and news reports. They glorify those they regard as holy fighters and turn subversive acts into examples of revolutionary victories, which are then used to further validate an ideology that seems sanctioned by God.

The websites upload articles, pictures and videos bearing messages that revolve around

**Table 2: Contents of Bahasa and Malay language radical and extremist websites, 2006 to 2009**

Time period	Content
Between 2006 and July 2007	<ul style="list-style-type: none"> <li>• Dissemination of al-Qaeda and Jemaah Islamiyah propaganda (videos, pictures, statements etc.)</li> <li>• Written articles on the theme of the victimised Muslim and the necessity to fight back</li> <li>• Celebration of <i>mujahidin</i> victories</li> <li>• Conspiracy theories</li> <li>• Anger directed at the West</li> <li>• Local grievances linked to the global jihad</li> <li>• Endorsements of highly selective Islamic doctrines</li> <li>• No tradecraft manuals</li> </ul>
August 2007	<ul style="list-style-type: none"> <li>• First posting of website hacking manual</li> </ul>
February 2008	<ul style="list-style-type: none"> <li>• First posting of bomb-making manual</li> <li>• First posting of bomb-making video compilation in Arabic</li> <li>• Emergence of a password-protected forum</li> </ul>
April 2008	<ul style="list-style-type: none"> <li>• First posting of a firearm manual</li> </ul>
Present	<ul style="list-style-type: none"> <li>• All the above</li> </ul>

the theme of a victimised global Muslim community that is under attack, urging the necessity to fight back.

The wars in Iraq and Afghanistan, as well as the Arab–Israeli conflict, are used as evidence of the aggressive encroachment of the West. The US and its allies are constantly painted as entities that will always bear enmity towards Islam. The websites uphold the inevitability of jihad as a *fardhu ain* (an individual obligation).

They blame everything from hikes in oil prices to global warming on the ongoing wars waged by the West in the Middle East, and on capitalism. By constantly showcasing how the West is hostile to Islam, the websites incite anger against the ‘other’. Jews and the US Government are seen as the ‘real’ masterminds behind the 9/11 attacks and the Bali bombings.

The Bahasa and Malay language websites include sites manned by radical and extremist groups, Islamic boarding schools (*pesantrens*), and groups of individuals who sympathise with and support the ideology of violent jihad.

### *Official websites manned by radical groups*

Some websites are run by groups, such as *Hizb-ut Tahrir Indonesia*, that adhere largely to a radical fundamentalist version of Islam. They strive for political change but don’t advocate the use of violence.

These websites contain materials that undermine the legitimacy of existing governments by declaring all laws, other than Islamic ones, to be invalid; propagate the implementation of the *syariah* (shari’a) and an Islamic caliphate for the betterment of the world; concoct conspiracy theories, especially around acts of terror; and promote mass rallies and seminars organised by radical groups.

### *Websites manned by extremist groups*

Some websites are run by groups that don’t discount the use of violence as a means to their political ends. All have their own military wings. Most have histories of being active in various conflict zones within the region, like the *Patani United Liberation Organisation* (PULO), which operates in southern Thailand.

These websites contain materials that emphasise the importance of protecting the religion at all costs, even sacrificing families and lives; propagate the urgency of establishing an independent state that implements the *syariah*; and portray the government in a malevolent way, using religious terms such as *kafir* (infidel) and *thogut* (evil).

### *Websites manned by pesantrens*

Some websites are manned by the Indonesian boarding schools. There are reportedly over 13,000 *pesantrens* throughout Indonesia, but only a few spread extremist ideologies. One of them is the *Al Mukmin Ngruki Pesantren*, which was founded by Abu Bakar Ba’asyir, a hardline cleric considered to be the spiritual leader of Jemaah Islamiyah. The *pesantren*’s alumni, a notable number of whom have been either suspected or convicted of terrorist activities, maintain a website that is largely used for networking.

### *Sympathetic websites*

Some websites are run by groups of individuals with no links to any radical or extremist groups. There are also cases of extant media groups aligning themselves with a particular radical or extremist group. They help produce and disseminate propaganda on the group’s behalf.

Such websites contain materials that promote the legitimacy and urgency of jihad; celebrate

acts of violence against the West; glorify militancy and terrorist groups; show no tolerance for and deny access to people who don't share similar beliefs; and disseminate bomb-making, firearm and hacking manuals.

## Numbers and online traffic

Bahasa Indonesia and Malay language websites with extremist messages are proliferating (see Table 3). Websites that are inactive or no longer accessible are constantly replaced with new ones, which often have more technologically advanced features.

Apart from the numerical increase, there's also a greater variety of websites. Blogs and personal social networking accounts provided more than half of the increase in 2008.

This shows that a growing number of individuals, encouraged by propaganda materials like the recently posted last will of Bali bomber Imam Samudra, are lending support to or sympathising with radical and extremist groups. The blogs and social networking accounts, as well as password-protected forums, help create a stable network among members of the Bahasa and Malay language online community.

Table 4 shows the country statistics of visitors to ten radical and extremist websites.

Unsurprisingly, the highest percentage of visitors to all ten sites comes from Indonesia.

## Bahasa Indonesia and Malay language forums

Forums are a relatively new development in the Bahasa and Malay language online environment, especially the password-protected ones. *Almuhajirun.com* hosted the first forum on its website in May 2007. This was soon followed by the password-protected forum, *Jihad al-Firdaus*, where the first hacking manuals were uncovered.

Password-protected forums make up one of the staples of Arabic language sites, and internet extremists operating in Bahasa Indonesia and Malay are increasingly adopting the concept. Restricting access to a virtual assembly means that only like-minded individuals are allowed into the site. Members can discuss issues as openly as they like without censorship, reprisal or the need for code words.

For example, entry into sensitive parts of the *Arrahmah.com* forum isn't permitted without prior registration. Entry is subject to approval from the forum administrator, who will ask questions about the person's gender, country of origin and beliefs, how they got to know

**Table 3: Numbers of Bahasa and Malay language radical and extremist websites**

Category	2007	2008
Websites manned by radical groups	2	11
Websites manned by extremist groups	1	4
Sympathetic websites	10	16
Forums	2	3
Sympathetic individual blogs and social networking accounts	–	82
Websites linked to pesantren	–	1
Websites inactive for at least 12 months	–	10
Websites that are currently down	–	8
<b>Total available websites</b>	<b>15</b>	<b>117</b>

Note: These websites are those detected and subsequently monitored by the authors in 2007 and 2008. There may be other sites not covered by this activity.

**Table 4: Nationalities of visitors to extremist websites**

<b>Hizbut-tahrir.or.id</b>		<b>Almuhajirun.com</b>	
Indonesia	92.6%	Indonesia	90.3%
South Korea	5.8%	Other countries	9.7%
Palestinian Territory	0.1%	<b>Kispa.org</b>	
Other countries	1.6%	Indonesia	100.0%
<b>Hidayatullah.com</b>		<b>Syabab.com</b>	
Indonesia	95.1%	Indonesia	63.0%
South Korea	2.8%	Japan	33.0%
Egypt	0.2%	Other countries	4.0%
Malaysia	0.2%	<b>Jamaahmuslimin.com</b>	
Singapore	0.1%	Indonesia	99.3%
<b>Infopalestina.com</b>		Other countries	0.7%
Indonesia	91.3%	<b>Muslimdaily.net</b>	
Philippines	0.4%	Indonesia	92.2%
Other countries	8.2%	Malaysia	3.3%
<b>Arrahmah.com</b>		Singapore	0.2%
Indonesia	88.5%	Other countries	4.3%
Iran	2.5%	<b>Media-islam.or.id</b>	
Australia	1.9%	Indonesia	95.6%
Malaysia	1.5%	Malaysia	1.1%
United States	1.4%	Other countries	3.3%

Information on online traffic was gathered at the start of December 2008 using alexa.com, an open source website that provides information on other websites. Alexa.com has provided snapshots of country visitors to various websites. However, small percentages are not reflected, and information from downed websites as well as from domains using internationally registered web hosts like *Multiply*, *Blogspot*, *Wordpress* and *Friendster* cannot be analysed.

about the forum, and why being a forum member is important to them. Registration requires satisfactory answers.

The forums usually have an exclusive section dedicated to discussing electronic jihad. There, forum members are encouraged to download from an assortment of pirated software like Microsoft Office, Adobe Photoshop and video converters. There are directions and advice on hacking into websites.

Few users critique the dominant radical discourse or offer an alternative point of view within these web forums. This creates an echo chamber in which members strengthen one another's view of the world.

## Blogs and individual social networking accounts

The Bahasa and Malay language websites reflect popular internet trends. Blogging and social networking using *Friendster* and *Multiply* have caught on across the spectrum of internet users. Southeast Asia seems more open to online social networking than the Middle East.

Using blog publishing tools and personal social networking accounts has a number of advantages over running a full website. They're less time-consuming to maintain and are free of establishment charges. They save the cost of getting an internet connection and personal computer (setting up and updating

blogs and social networking accounts can be done at cybercafes). Users are harder to identify: their real IP addresses are not compromised, as they're not required to fill in verifiable personal details.

Advances in the information revolution allow radical groups and their online media units to be in full command of the entire process of media production. This allows them to determine the 'three C's' in the communication of al-Qaeda-inspired extremist messages: *content*, *context* and *channel*.

## Communicating the brand

Southeast Asian militant groups recognise the importance of developing their internal media units to communicate with the public via the internet. Even media entities that are publicly visible, such as the *Ar Rahmah Media Network*, have been developing their online media wings.

Online media units can determine the *content* of their messages and report on what they want, without censorship. For radical groups lacking access to mainstream media, the internet allows the unhindered development of their message.

This was recognised by *Khattab Media Publication*, the self-proclaimed official media wing of the *Mujahidin Syura Council*, an extremist group that claims to operate in southern Thailand. Inspired by al-Qaeda, this group was reportedly in existence in 2004, but the official media wing was formed four years later in July 2008 as a blog on Google. The contents of the blog are mainly written in Malay.

*Khattab Media* translated a fatwa written by Palestinian intellectual Abdullah Azzam, the man behind the ideology of al-Qaeda, obliging Muslims to militarily defend their lands. The translation of Azzam's religious

opinion on Islamic law was then posted on the blog as the philosophical justification for adherents to take up arms in the name of Islam. Considering the controversial content of the message, its mass dissemination would have been highly unlikely without an online media wing.

The *Mujahidin Syura Council* used the *Khattab Media* blog to officially announce the start of a new military campaign, codenamed *Operation Tawbah* (Operation Repentance), that it hopes will come as a 'fresh shock to the un-Islamic regimes of Southeast Asia'. Declaring its intentions on the open internet environment allows its message of terror to be widely disseminated.

Online media units can determine the *context* of extremist messages by framing conflicts as part of a relentless war against Islam. *Arrahmah.com*, the online media wing of the *Ar Rahmah Media Network*, seeks to show how different conflicts on various global fronts are holy wars. In its news reports on places from the southern Philippines, Chechnya and Kashmir to Somalia, non-Muslims are all referred to as *kafir* (infidel), suicide bombings as 'martyrdom' bombings, and anyone who opposes the US, its allies and un-Islamic authorities as *mujahid* (holy warriors). *Arrahmah.com* glorifies militancy and those who fight in God's name. For example, the Bali bombers were made the website's top newsmakers and accorded exclusive pictures and interviews.

Online media units play a vital role in translating Arabic language and tradecraft materials into the local language, so regional groups don't miss out on current debates and resources. Arabic language websites contain the most relevant and influential extremist materials, and countless items can be traced back to them. Translated materials were once the staple of the Bahasa and Malay language extremist websites, but their online media

units are now increasingly producing their own materials to better resonate with the home audience.

A largely unregulated internet gives the online media units an important *channel* of mass communication. The continued visibility and relevance of convicted terrorists, such as the Bali bombers until their execution, are largely due to the efforts of sympathetic websites such as *Arrahmah.com*. Such websites helped to release the bombers' statements to the public, and published their letters and wills online.

### Online news agencies

Online media units are increasingly transforming themselves from information centres to online news agencies that function very much the same way as Reuters, Bloomberg or the Australian Associated Press.

The units report on group activities and provide up-to-the-minute news updates from various fronts across the globe, as well as current analyses on the Muslim world. They produce exclusive pictures, interviews and self-developed propaganda materials and offer newsfeed services direct from website to desktop. By emulating established media news outlets, they hope to narrow the credibility gap between themselves and the established news media, so that more people will tune into their radical Islamist version of world affairs.

In the past, these websites would occasionally try to establish their credentials by challenging the credibility of secular or mainstream media sources, cautioning Muslims that those sources were deceptive and misleading. Now the more sophisticated extremist websites in Southeast Asia try to look more like the mainstream media they disparage.

Hizb-ut Tahrir Indonesia's *Infokom HTI* often produces high-quality videos of HTI activities

and then uploads them onto YouTube. Many of the videos focus on the failings of the incumbent secular Indonesian Government and the need to implement *syariah* law and re-establish an Islamic caliphate. They are formatted and styled in the fashion of news aired on any major mainstream television network.

Some of these videos have tried to project a semblance of objective reporting. For example, in an *Infokom HTI* news report on an HTI protest in front of the US embassy in Jakarta, the HTI member doing the video voiceover deliberately distances himself from both the group and the group-led protest unfolding on screen, reporting on 'the actions of the HTI' as well as 'what the HTI regards as US interference in domestic Indonesian politics'. Referring to the group in the third person is part of an attempt to appear objective. Together with stylistic visual editing, polished animation and moving narratives, this adds to the impression of *Infokom HTI* as a credible source of news.

Many videos put out by *Infokom HTI* are tagged with the animated logo of a flying black flag inscribed with the *kalimah syahadah* (the Muslims' proclamation of faith), and use customised opening visuals and soundtrack. News produced by the media production house looks like it might have been part of any mainstream news broadcast.

The inclusion of English subtitles in an increasing number of videos produced by *Infokom HTI* ensures that members of Hizb-ut Tahrir movements outside Indonesia can follow local group developments. Conversely, Bahasa Indonesia subtitles in incoming propaganda materials from Hizb-ut Tahrir groups around the world allow local HTI members to understand them. This helps to fuel enthusiasm, as HTI members can feel that they belong to an even larger collective with a unified global purpose.

## Online promotion of mass gatherings

The most public manifestations of online extremist activities are openly organised mass meetings and rallies. The heavy online advertising of the 2007 International Caliphate Conference held by Hizb-ut Tahrir Indonesia in Jakarta shows the increasing importance of the internet in supporting real-world activities. Close to a hundred thousand people attended.

*Ar Rahmah Media Network's* September 2008 public engagement to promote the launch of the latest edition of its paper publication *Jihad Magz* also benefited from online promotion. Extremist religious figures, such as Abu Jibriel Abdul Rahman, a key leader of Jemaah Islamiyah, were called on to deliver expert opinions on the 9/11 attacks at a series of road shows. While it is not known how many attended, the event was described as a success by the *Ar Rahmah* group.

## Approaches to countering online radicalisation

To date, regional governments and national law enforcement agencies have done little to stop the rise of online radicalisation. Compared to territorial security or economic management, the possible threat from a handful of people radicalising themselves by spending long hours in front of computer screens hasn't been a priority. The many legal factors involved in attempts to regulate cyberspace have also been a political minefield for many regional governments.

While websites inciting violence are subject to criminal laws in some countries, there are often no specific regulations covering the internet. Some governments don't want to appear un-Islamic by coming down hard on Islamist groups, and some don't want to appear undemocratic by seeming to rein in freedom of expression in cyberspace.

In general terms, there are three broad policy approaches that governments could adopt:

- a hard strategy of *zero tolerance* (blocking sites, prosecuting site administrators, using internet filters)
- a softer strategy of *encouraging internet end users to directly challenge the extremist narrative* (including creating websites to promote tolerance)
- an intelligence-led strategy of *monitoring leading to targeting, investigation, disruption and arrest*.

These broad approaches can, and probably should, be pursued simultaneously. In most cases, regional countries should not adopt one approach to the absolute exclusion of the others. Also, while the focus here is on countering online radicalisation, the offline elements of terrorist networks are also important.

A range of stakeholder interests must be balanced in countermeasures to combat online radicalisation. Law enforcement and security (government); the internet industry, such as site administrators, domain hosts and internet service providers (ISPs); the community of online users; business (e-commerce); and the media all have an interest in access to information.

Each approach will have advantages and drawbacks in its security consequences, economic impacts (on public authorities, ISPs and consumers) and broader human rights implications (such as freedom of expression, access to information and privacy).

For example, hardline approaches using censorship and filtering might not be fully effective for technical and legal reasons, while softer approaches might be too slow to show real results and in the long run might not deter the extremists. Monitoring will be part of any sensible approach. However, it won't necessarily be easy to apprehend

### Box 3: Resources to counter radicalisation on the internet

Countering radicalisation on the internet requires technical, human and intellectual resources.

#### Technical infrastructure

The technical requirements are secure, unattributable, superfast (broadband and wireless) ICT systems, and the ability to access and view extremist sites (visibility of the environment is fundamental).

#### Human resources

People with analytical, linguistic and technical skills are essential. They will need adequate training and the support of experts.

#### Knowledge and intellectual capital

It's necessary to stay abreast of the latest trends and industry developments, and governments aren't normally at the forefront of internet-related trends. However, the means through which the extremist message has been communicated, via web pages, multimedia and bulletin boards, hasn't changed that much since 9/11.

those responsible for maintaining websites deemed illegal.

Of course, one option for regional states is to maintain current policies. The 'do nothing' option requires no new legislation and no boosting of law enforcement agencies' capacities and expertise. However, it would also put the region in a weaker position when it has to face the problem of online radicalisation and the growth of extremist websites in the future.

### Hard strategy—zero tolerance

A hard strategy would ban the hosting of extremist websites and the promotion or distribution of extremist material within the region. Countries would need to agree on common definitions of *extremist* (use of violence) and *material* (broadly, any form of media).

This approach would require adequate legislative mechanisms for agencies to prevent extremists publishing content that incites terrorism and to prosecute those who do. It would also require either a treaty or memorandum of understanding between nations. For example, a website could be hosted in one country but incite violence in another, while the extremists behind it plan operations in a third country. The transnational nature of the problem requires formal cooperation mechanisms.

Intelligence and law enforcement authorities are in a difficult position in the fight to contain online radicalisation. There's a lack of uniform legislation across jurisdictions, and limited capacity to cope with the volume of websites disseminating terrorist propaganda. And the internet operates extraterritorially. Its anonymity reduces the ability of law enforcement authorities to remove undesirable content and to investigate and prosecute those responsible for websites and their contents.

Currently, most regional countries can ask ISPs to take sites or material offline, as Indonesia has done with a recent Dutch film posted on YouTube. That's about the extent of most regional states' legal powers, although a notable successful prosecution in Indonesia involved [www.anshar.net](http://www.anshar.net) (see Box 4).

Some states could use legislation unrelated to terrorism, but legislative shortcomings might need to be overcome. The Hizbollah TV case in Australia highlighted some

#### Box 4: The case of anshar.net

After the second Bali bombings on 1 October 2005, police discovered that Noordin Top's associates had developed a website specifically to disseminate jihadist teachings from al-Qaeda sites. Several Indonesians were also contributors, including Aly Ghufron (alias Mukhlas), one of the masterminds of the 2002 Bali bombings. The site, [www.anshar.net](http://www.anshar.net), was subsequently shut down.

The investigation involved the cybercrime unit of the Indonesian police, the Yahoo administrator, the internet provider, and non-Indonesian investigators (the Australian Federal Police and the US Federal Bureau of Investigation).

One of the legal challenges was in determining the exact place where the law was broken. The police concluded that the cybercrime took place in central Java.

In several regional countries, digital evidence is not recognised in courts as legal evidence.

See <http://www.indonesiamatters.com/624/wwwansharnet-chatroom-jihad/>

of the issues involved. The Australian Communications and Media Authority (AMCA) investigated *Al-Manar*, a satellite subscription narrowcasting service, which broadcast terrorist material into Australia from Lebanon. Following ACMA's inquiries, an overseas-based satellite company confirmed that it had carried out a test transmission of the *Al-Manar* service. However, the company also confirmed that the test transmissions were terminated and that satellite facilities would not be provided to *Al-Manar*. ACMA

has proposed to amend the anti-terrorism standards to provide narrowcasters with greater certainty about which individuals and organisations are deemed to be terrorist entities.

There are also options to block foreign-based websites and sites hosted on foreign servers. At the moment, many Asia-Pacific states don't have adequate legislation to do this. Such a strategy would require states to develop an entire policy on addressing extremist content, as opposed to investigating it.

A zero tolerance approach might even hinder investigations, because it combines the objective of countering online radicalisation objective with the aim of frustrating terrorists' use of the internet for operational purposes. For example, some law enforcement agencies use 'honey pot' sites.

The internet is difficult to regulate, but there have been successes in curbing the distribution of other undesirable content, such as child pornography.<sup>3</sup> In most states it's a crime to participate in the exploitation of children by viewing, possessing or distributing such material. Laws to suppress the online distribution of child pornography are much tougher than those covering the publication and distribution of religious extremist material. And of course child abuse is very clearly definable, making the task easier.

While anti-paedophile internet actions might hold valuable lessons for the fight against extremism online, a policy of taking down extremist sites isn't necessarily a viable solution in the long run. No extremist site can be taken down for long: if a forum is closed by law enforcement authorities, it will more often than not spring up somewhere else very quickly. Instead of extremists working in known areas of the internet, where they can be relatively easily located, they could be driven into the far recesses of the web. And

deterrence doesn't always work against an ideological enemy.

One expert who has examined this issue closely has argued that the global nature of the internet makes common action to take down websites technically impossible and legally irrelevant in the absence of a binding international treaty and consensus on what material should be subject to censorship. However, even if those conditions were met and content hosted in a foreign jurisdiction were removed, there would be nothing to prevent the material remaining on other 'mirrored' host sites—allowing online

access to it from other foreign jurisdictions (Ryan 2007, chapter 2; see also Ali 2008).

A hardline censorship approach would be difficult, but that shouldn't stop governments making efforts to disrupt sites where necessary. For example, the United Kingdom has moved to a take-down policy, although it combines that policy with softer measures (see Box 5).

There's also the option of prosecuting individuals who establish, own, manage or fund extremist websites, those who distribute extremist material through them, and ISP or

### **Box 5: The United Kingdom's approach**

The British Government has a broad, evolving strategy for tackling terrorist use of the internet. The strategy is led by the Office for Security and Counter-Terrorism in the Home Office, with a wide range of domestic and international partners across government and in communities, industry and academia. The government aims to make the internet a more hostile environment for terrorists and violent extremists using it both operationally and for radicalisation and recruitment. The strategy seeks to disrupt terrorists' use of the internet, to reduce the availability of extremist material, and to promote positive voices online to challenge extremist messages.

The British approach is clear: the internet is not a no-go area for government, and the authorities want to see unlawful material removed from it. Should enforcement be required, section 3 of the *Terrorism Act 2006* allows for an ISP to be served with a notice asking for unlawful material to be removed or amended within

two working days. Failure to comply with a section 3 notice is not an offence, but the person served with the notice will not be able to use the statutory defence of non-endorsement contained in sections 1 and 2 of the *Terrorism Act* if a prosecution ensues under those sections.

So far, informal contact between the police and ISPs has been enough to have material hosted in the UK removed from the internet. The authorities have also worked with a number of providers of filtering and parental control software to have them voluntarily strengthen the protection their products provide against terrorism-related material.

The British approach acknowledges that disruptive measures and the removal of material or restriction of its availability must be used selectively, taking into account practicalities as well as the principles of freedom of expression. Encouraging communities and internet users to challenge extremism online is a crucial part of the solution, and one the UK is actively taking forward.

site administrators and moderators who host extremist content. However, ISP prosecutions could damage otherwise good working relationships with law enforcement bodies and other government agencies.

Countries in the region might also consider adopting laws against public provocations to commit terrorist offences through the internet. Relevant terrorism and cybercrime conventions originating from the Council of Europe would be a good place to start (see Box 6).

Governments could also introduce online filtering products, which have proved effective against internet-based paedophile activity. The argument for mandatory filters

is the same in principle as the argument for a film censorship system.

The Australian Government is currently conducting trials of internet filters. If the trials are successful, the government will introduce filters that will blacklist websites for (unspecified) unwanted content. Under the government's current plan, all Australians will be served a 'clean' internet feed—websites on a blacklist maintained by the communications watchdog will be blocked. A secondary filter to block material inappropriate for children will also be introduced. However, users will be able to opt out of this filtering system by lodging a request with their ISP.<sup>4</sup>

### Box 6: European legal approaches

The two Council of Europe (CoE) conventions that contribute to preventing terrorists' use of the internet are the Convention on the Prevention of Terrorism (2005) and the Convention on Cybercrime (2001). Both conventions are open to signature by non-member states.

The Convention on Cybercrime is the only international treaty dealing specifically with substantive and procedural criminal laws in the area of cyber-related crime, including the use of the internet for terrorist purposes, and which facilitates international cooperation in the investigation and prosecution of computer crimes. The convention opened for signature in November 2001 and entered into force on 1 July 2004. Of non CoE states, only the US has both signed and ratified the convention.

The convention requires states that sign and ratify to ensure that specific cybercrime offences are incorporated

into their domestic law, and to establish specific law enforcement powers to enable the investigation and prosecution of offences committed by means of a computer system. The convention also aims to establish a fast and effective regime of international cooperation for investigating and prosecuting cybercrime offences, and for gathering evidence in electronic form—including the expedited preservation, disclosure, search, seizure and real-time collection of data.

The CoE Convention on the Prevention of Terrorism also contains provisions that are relevant in the fight against terrorists' use of the internet. It aims to strengthen efforts to prevent terrorism by establishing as criminal offences acts such as public provocation to commit a terrorist offence, recruitment for terrorism, and training for terrorism. Complicity in the commission of these offences is also a crime (which has implications for anyone helping terrorists to create or maintain websites).

In October 2008, the Thailand Government also announced plans to set up an internet firewall to block and monitor inappropriate websites, including sites related to terrorism.

However, some experts argue that filtering is impractical, will slow internet connection speeds and will accidentally prevent access to a large number of legitimate websites (for example, the filters can't distinguish an individual posting on a web forum from the entire web forum, so user-generated sites could be blocked because of a suspect posting). For people who know how to use computers properly, filters aren't difficult to defeat. They might also increase the cost of internet access, and leave ISPs and governments legally liable if they fail. The wave of innovation produced by the open internet could be put at risk. And being heavy handed might play into the hands of potential terrorist recruiters (Ryan 2007, chapter 2).

### **Soft strategy—promoting a counter-narrative**

The soft strategy involves moderate Muslim communities drowning out more extreme voices to stop the slide towards greater online radicalisation. Without moderate voices to counter the extremist narrative, online participants (who take on the views of their friends over time) could be even more deeply radicalised (Sageman 2008: 160).

This kind of strategy requires community consultation, liaison and ownership, which need to be formalised in some type of joint working body. This is particularly the case where some members of vulnerable groups are alienated, and disassociation (one of the first steps of radicalisation) has begun.

As for measures to prevent the online exploitation of children, an appropriate awareness of 'what's out there' is important, especially as internet use proliferates. Cybersafety for young people is now a major

concern for regional governments, and schools are playing an important role in this context. Young people can be the subjects of cyberbullying; they can have their identities appropriated by others; photos or videos of them can be published online without their permission. Children can also visit inappropriate websites, and predators can use social networking sites to contact and 'groom' them.

Young people need to use the internet responsibly. Part of that message, to be reinforced by parents and schoolteachers, should be to alert students to the risks of websites that preach hatred and extremism. Teachers will need teaching materials that alert students to that risk.

In a potentially sensitive area like religious extremism, engaging the community will help to drive effective counteraction strategies. In tackling the online narrative that some young people in our region are using to groom themselves as militants, governments could fund moderate groups to develop and expand their internet presence and challenge online forums that promote extremist interpretations of Islam.

Johnny Ryan argues that *cultural intelligence* can be used to confront extremist narratives on militant Islamist websites (Ryan 2007, chapter 3). This involves information from government and government support to internet users through trusted enabling stakeholders across society.

Ryan makes a compelling case that internet users are no longer behaving as passive consumers of content, but are increasingly contributing to and creating their own content. The trend is to two-way, horizontal communication. The growth sector is in Web 2.0, or social networking technologies such as Bebo, MySpace, YouTube, Wikipedia, Flickr, and Facebook.

Daniel Kimmage (2008a) argues that the al-Qaeda media nexus is old hat: 'If Web 1.0 was about creating the snazziest official Web resources and Web 2.0 is about letting users run wild with self-created content and interactivity, Al Qaeda and its affiliates are stuck in 1.0'. The old internet world of extremist groups is one of direction: believe this and take these actions. Now the internet is much more about conversation, violent extremists are trying to keep up with the new media.

Kimmage notes that al-Qaeda statements are sometimes posted to social networking sites, but the reactions, ranging from praise to blanket condemnation, are a far cry from the invariably positive feedback al-Qaeda gets on moderated jihadist forums. Last year, a member of an Islamic jihad forum appealed for a 'Facebook invasion', describing it as a podium to reach millions of people. The member posted instructions on how to register and use Facebook and outlined the 'goals of the invasion' as 'reaching the vast base of Muslims who subscribe to Facebook' and 'participating and interacting with them'.<sup>5</sup>

Because individual internet users are now the designers and contributors of content on the internet, governments can no longer take the lead role in countering online calls to extremist violence. They lack the credibility and more often than not the technical wherewithal to do so (Ryan 2007, chapters 2 and 3).

Young Muslims in the region need to be able to engage with appealing web content that addresses their concerns and allows them to examine extremist narratives critically. Governments can offer incentives for such initiatives. The Islamic Religious Council of Singapore has come up with various websites to counter Islamist extremism online (see Box 7).

'Enabling' stakeholders should be trusted members of the relevant community who are able to work cooperatively with government in a two-way process.

Internet users can then determine for themselves whether to accept, debate or delete the extremist message when they encounter it on the internet. This approach empowers users to challenge or reconsider the call to violence in the chat rooms and web forums where governments find it difficult to reach.

By avoiding direct government involvement, this strategy avoids adding to the glamour of violence among those who prefer to reject statements from authority. And its open approach, based on dialogue, leaves the internet's social and economic potential undisturbed (Ryan 2007, chapter 3).

### **Intelligence-led strategy— monitoring, targeting, investigation, disruption and arrest**

In some ways, an intelligence-led strategy might complement an implementation plan for a zero tolerance approach. In this strategy, too, it will be important to draw up a plan that sets out clearly the objectives for countering the operational aspects of terrorists' internet use, as well as countermeasures against online radicalisation.

An intelligence-led strategy will involve more than monitoring to sample the themes of discussion on websites and forums. It will be necessary to engage online to obtain operational intelligence to aid targeting and arrests. Websites, chat rooms and forums frequented by extremists and sympathisers can yield intelligence dividends for law enforcement agencies.

Disruptive action could be undertaken, particularly against distributor sites and large web forums. There will be technical challenges here: encryption is already standard in some internet communications services, making data interception difficult. The growing number of public internet cafes supply anonymous internet access in cities, and people can use anonymous prepaid accounts to connect.

There are also possibilities for ‘cyber herding’—action to drive people towards a desired location within the electronic realm (Moon 2007).

From a law enforcement perspective, not all regional countries have robust legislation for this type of activity, and there could also be regulatory concerns about entrapment in counter-terrorism investigations. Therefore, there may be legal impediments preventing law enforcement services in some regional countries from participating in web forums under false identities. Because online extremism is a transnational matter, legislative arrangements would need to align to allow for prosecutions.

There could be problems, domestically and regionally, in expanding these types of

### Box 7: MUIS—countering extremism online

The Islamic Religious Council of Singapore, better known by its local acronym MUIS, is the country’s supreme Islamic authority and administers the affairs of the Muslim community. To check the proliferation of extremism on the internet, MUIS has taken to cyberspace to debunk radical and extremist strands of Islam and propagate a more balanced, harmonious and progressive viewpoint. MUIS and its proponents have set up interactive websites that promote discussions and answer people’s queries about Islam. The websites address all aspects of the religion, from day-to-day concerns (‘Can I eat at Subway?’) to significant events with global impact (‘What are the reasons behind the conflict in Gaza?’).

The <http://invoke.sg> and <http://iask.invoke.sg> websites feature articles, blog entries and street documentary videos that discuss faith and lifestyle matters from an Islamic perspective. Targeted at young adults, they host an online forum where uploaded questions on Islam are

personally answered by authoritative religious figures. The websites also feature an educational booklet co-produced by MUIS (*Questions & answers on jihad*). The booklet is a concise and comprehensive informational piece penned in response to general misconceptions about jihad—a concept exploited by terrorists to legitimise violence. Written by two prominent Singaporean Islamic scholars, the booklet is widely distributed to local schools and mosques.

The [www.radical.mosque.sg](http://www.radical.mosque.sg) website has been developed by MUIS in close collaboration with the same Islamic scholars, as well as the Religious Rehabilitation Group, a volunteer group made up of Islamic clerics, intellectuals and teachers who counsel detained Jemaah Islamiyah members. Beyond rectifying discordant perceptions of Islam and its practices, the website works to challenge the Jemaah Islamiyah organisation and its terrorist ideology by comparing and contrasting the group’s skewed concepts of holy war (*jihad*), migration (*hijrah*) and the Islamic state (*Darul Islam*) with the proper understanding of the terms.

operations if they were seen to develop into general ‘fishing expeditions’.

National agencies could also launch computer network attacks to prevent or disrupt the distribution of extremist material, or exploit computer networks to collect technical data related to a site or forum for operational use.

Legislation doesn’t always consider incitement to be a criminal offence, so for some states exploiting online forums is more an intelligence agency function than a law enforcement one.

A counterargument should be considered. If the internet is left largely undisturbed, terrorist organisations are more likely to regard it as a safe medium, making it more susceptible to effective monitoring. Attempts to infiltrate the internet might simply result in communications and other activity of concern becoming progressively more difficult to track.

It might also be argued that disrupting chat room activity doesn’t really address the much deeper social problems involved in radicalisation:

Ultimately, the Internet is a medium for communicating ideas that reflect society. If we want to see the content of the cyberworld changed, it is best achieved by addressing the issues in society at large—in the real world—that the Internet manifests. (see Durodie and Ng 2008)

## The way ahead

In addition to the three broad strategies to counter online extremism listed in the previous section, four specific measures would strengthen the ability of regional governments to counter online radicalisation at the national and regional levels.

## Recognise the trade-offs in countering online radicalisation

In crafting a comprehensive counter-radicalisation strategy, regional states first need to recognise that there may be trade-offs involved. If the primary focus is on disrupting operational activity, for example, that may have negative impacts on other measures, such as developing a counternarrative on the web.

In other words, in developing a strategy, it’s important for regional states to distinguish countermeasures for online radicalisation objectives from measures to counter the terrorist use of the internet for operational purposes.

Although the two are linked (the former being a prerequisite for the latter), their trajectories, manifestations and counteraction strategies can be markedly different. While some strategies might serve both purposes, others could undermine the subsidiary objective, whichever it is.

However, combining the two objectives when developing national and regional approaches could also have advantages for public diplomacy.

## Establish an interagency taskforce to develop a plan

Each regional government should establish an interagency taskforce to map out that government’s response to the problem. It will be essential to engage the security agencies, along with trusted community stakeholders from civil society.

The key stakeholders will be different in each country. They might include educators, religious leaders and community organisations. They should be trusted and credible, and they should be able to work cooperatively with the government.

It's also critical for governments to involve the internet industry, which has already had a great deal of experience working with government in areas such as the policing of paedophile activity. The government–industry interaction must be collaborative, so that public confidence is maintained.

The production of a national plan will help to outline both a prevention strategy and the means to counteract the terrorists' narratives. The plan will answer some very basic questions: who will do what, when, why and how, to make the strategy achievable?

Having a plan to develop countermeasures for online radicalisation will allow a clear understanding of what's being policed. This will help to assuage public concerns about basic human rights, such as freedom of expression and access to information.

The national plan will provide a clear framework for legislative amendments that might be needed. It will also provide a baseline for industry engagement, and give the telecommunications sector clear guidelines to help it police the content.

Such a plan will be an essential first step in developing a national strategy on preventive and pursuit mechanisms, especially in the legislative realm. If a national counter-terrorism strategy already exists, the plan for countering online radicalisation should complement that broader national framework.

### **Create national 'fusion' centres**

Governments need to consider innovative ways of working to maintain effectiveness in a threat environment that's increasingly 'flat'—interconnected, easily accessed and non-hierarchical.

Regional countries should consider the 'fusion' model for internet-driven

counter-radicalisation work. Fusion centres have traditionally been used for intelligence work. What's needed now is a fusion cell with a broader mandate.

Staff from different agencies working in the online space could be brought together under one roof, with shared databases and online tools, and secure communication channels back to their own agencies and systems. Developing intellectual capital, part of which is achieved when people get together to talk and share, should be considered a paramount objective.

Apart from problems involving jurisdictions and classifications, resource problems will need to be overcome to establish such a cell. Many agencies are already stretched to target online activity in their counter-terrorism operations, which require linguistic and data-capture resources and storage and preservation of evidence, along with resources for analysis and investigations.

There should be no general 'fishing expedition', which would divert scarce resources from other core tasks. Therefore, it will be crucial to undertake a national study of some kind to identify key areas, priorities, target groups and profiles, along with a policy on how intelligence will be gathered and targets investigated. It may be necessary to review legislative amendments to allow the prosecution of those involved in disseminating extremist material online.

Each regional government will need to drive the creation of a fusion centre with a very firm hand. They will need to answer some basic questions: Who 'owns' the centre? Who pays for it? Who should have access to the information? How much information should be shared with other countries for investigations? The last question is critical: terrorist networks are transnational.

## Develop a regional ‘Check the Web’ project

Pooling technical and linguistic resources to monitor extremism on the internet could benefit regional states significantly. Therefore, the region should adopt a version of Europol’s Check the Web Project, which is an online portal, staffed by a small number of agency members, that checks the web for online activity.

A similar information portal in our region would improve cooperation between states in monitoring and evaluating Islamist terrorist websites. States could use it to make their information accessible to each other, creating a database available within the broader region. They would have direct access to information on the work of other regional countries, and on the results.

The Multi-National Operations Support Team (MNOST) could be used for this purpose. MNOST is a hub of regional law enforcement officers working collaboratively in response to terrorist threats in the region. Located in Jakarta, MNOST includes police representatives from Thailand, the Philippines, Singapore, Indonesia and Australia. There’s potential to expand the membership of MNOST to include agencies from other ASEAN nations.

A regional Check the Web collaborative project would cross the divide between monitoring and preventing the online dissemination of extremist materials. Any transnational project will have to overcome challenges. Issues that will need to be worked through could include accreditation, matters for collaboration, participation numbers (restricting access to a limited number of people from each agency), release of data to third parties/countries, operational sensitivities, decisions between shutting down and monitoring websites, and legislative frameworks.

However, a regional Check the Web initiative under the auspices of MNOST would build on other regional initiatives, such as:

- the ASEAN Regional Forum Seminar on Cyber Terrorism—an annual counter-terrorism program attended by the ten ASEAN member states and other observing countries (including the US, Australia, India, China and the European Union) that discusses ideas on national policies covering cyberterrorism and misuse of the internet by terrorists
- the Jakarta Centre for Law Enforcement Cooperation—formed in 2004 with assistance from Australia as part of a regional effort to combat transnational crime
- the International Centre for Political Violence and Terrorism Research—based in Singapore and cooperating with various international government bodies and NGOs, with an informatics unit that studies online radical and extremist discourses and the groups and individuals behind them
- the Southeast Asia Regional Centre for Counterterrorism—established by the Malaysian Government with help from the US in 2002, with a focus on training, capacity-building and public awareness programs.

## Conclusion

For extremist groups in our region, the internet is an increasingly important tool for recruitment to violence. Using this international platform, they’re attempting to shape people’s ideas about whose ideology is right and who should win. Importantly, they aren’t attacking only the West, but are drawing on their narrative to attack the governance arrangements of regional states. Therefore, it’s up to those states to ensure that the purveyors of extremist ideology don’t prey upon future generations.

A growing number of young people are turning to the web for guidance in all aspects of their lives. Extremist groups without access to mainstream media place great value on having online media units to boost their reputations and recruit people via the internet.

Regional governments will need to monitor closely the increasing sophistication of cyberportals, such as web forums, and their ability to produce and disseminate extremist messages. They'll also need to develop comprehensive strategies to counter the rise of online radicalisation.

This report provides a basic menu of best practice options that regional governments can draw upon in establishing a comprehensive counter-radicalisation strategy.

National circumstances and domestic political considerations will influence the choice of policy responses, so a 'one size fits all' approach will not work. However, the problem of online radicalisation crosses national borders and will require a concerted international response.

## Endnotes

- 1 See, for example, Neumann (2008), National Coordinator for Counterterrorism (2007), Weimann (2006), Kimmage (2008), CHSGA (2008), Rogan (2006), Givner-Forbes and Shwery (2007), Ali (2008). Although there is a considerable literature on the internet and terrorism, there is almost no detailed consideration of countering online radicalisation. One notable exception is Ryan (2007).
- 2 The domain was registered under the name of Hapsoro Adiyanto, who belonged to *Media Qita*, a one-stop web design company based in Indonesia, and located in Surakarta, central Java.
- 3 Several countries in Asia are filtering internet pornography. See the Open Net Initiative at <http://www.opennet.net>.
- 4 For a discussion of the Australian Government's introduction of an internet filtering system, see <http://www.abc.net.au/rn/mediareport/stories/2008/2405376.htm>
- 5 See <http://www.abc.net.au/news/stories/2008/12/11/2444149.htm>

## References

- Ali S 2008. 'Fighting online extremism: tackling old challenges in the Internet Age', *RSIS Commentaries*, 2 July.
- Chatham House 2008. *Terrorism, radicalization and the internet*, report of a private roundtable, Chatham House, London, July.
- CHSGA (US Committee on Homeland Security and Government Affairs) 2008. *Violent extremism, the internet, and the homegrown terrorism threat*, CHSGA.
- Conway, M and McInerney, L 2008. 'Jihadi video and auto-radicalisation: evidence from an exploratory YouTube study' in EuroISI 2008 - First European Conference on Intelligent and Security Informatics, 3–5 December 2008, Esbjerg, Denmark.
- Council of Europe 2007. *Cyberterrorism: the use of the internet for terrorist purposes*, Council of Europe, January.
- Durodie B, Ng SC 2008. 'Is internet radicalization possible?', *RSIS Commentaries*, 21 November.
- Givner-Forbes R, Shwery C 2007. 'Mapping the electronic jihad: an outline of the virtual jihadi community', *RSIS Commentaries*, 25 April.
- Hassan MH 2008. 'Online "curriculum" of jihad: four broad themes', *RSIS Commentaries*, 28 May.
- Hoffman B 2006. 'The use of the internet by Islamic extremists', RAND testimony presented to the US House Permanent Select Committee on Intelligence, 4 May, Washington DC.
- Kimmage D 2008. *The al Qaeda media nexus: the virtual network behind the global message*, Radio Free Europe / Radio Liberty Report, March.
- Kimmage D 2008a. 'Fight terror with YouTube', *New York Times*, 26 June.
- Moon D 2007. *Cyber herding: exploiting Islamic extremists' use of the internet*, US Naval Post Graduate School, Monterey, California.
- Mostarom TR 2009. 'Al Qaeda's female jihadists: the islamist ideological view', *RSIS Commentaries*, 6 February.

National Coordinator for Counterterrorism 2007. *Jihadis and the internet*, Ministry of Justice, The Netherlands.

Neumann P 2008. *Joining al-Qaeda: jihadist recruitment in Europe*, Adelphi paper no. 399, International Institute for Strategic Studies, London, chapter 5.

Rogan H 2006. *Jihadism online*, FFI/RAPPORT, Norwegian Defence Research Establishment.

Ryan J 2007. *Countering militant islamist radicalisation on the internet*, Institute of European Affairs, Dublin.

Sageman M 2008. *Leaderless jihad*, University of Pennsylvania Press, Philadelphia.

Silber MD, Bhatt A, no date. 'Radicalization in the West: the homegrown threat', New York Police Department, available from: [http://www.nyc.gov/html/nypd/downloads/pdf/public\\_information/NYPD\\_Report-Radicalization\\_in\\_the\\_West.pdf](http://www.nyc.gov/html/nypd/downloads/pdf/public_information/NYPD_Report-Radicalization_in_the_West.pdf) [accessed 20 February 2009].

Weimann G 2006. *Terror on the internet: the new arena, the new challenges*, US Institute of Peace, Washington DC.

## About the Authors

**Dr Anthony Bergin** is Director of Research Programs, Australian Strategic Policy Institute.

**Sulastri Bte Osman** is a research analyst with the Civil and Internal Conflict Programme at the S. Rajaratnam School of International Studies, Nanyang Technological University.

**Dr Carl Ungerer** is Director of the National Security Project, Australian Strategic Policy Institute.

**Nur Azlin Mohamed Yasin** is a research analyst with the International Centre for Political Violence and Terrorism Research at the S. Rajaratnam School of International Studies, Nanyang Technological University.

## Acknowledgement

The authors thank Ms Leah Farrall, Research Scholar, Global Terrorism Research Centre, Monash University, for helpful comments on an earlier draft of this paper.

## About the Organisations

**RSIS** is a leading research and graduate teaching institution in strategic and international affairs in the Asia–Pacific region.

**ASPI** is a leading Australian think tank in the fields of strategic, defence and security affairs.

### Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

### About Special Reports

Generally written by ASPI experts, Special Reports are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations. In some instances, material of a more technical nature may appear in this series, where it adds to the understanding of the issue at hand. Special Reports reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

#### ASPI

Tel +61 2 6270 5100  
Fax + 61 2 6273 9566  
Email [enquiries@aspi.org.au](mailto:enquiries@aspi.org.au)  
Web [www.aspi.org.au](http://www.aspi.org.au)

© The Australian Strategic Policy Institute Limited 2009

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers.