



الطالقة او  
مرة (148)  
المستربا  
رهن وجوده  
لان يصوب  
بالتعامل مع  
تم الذي يبرع  
بنود يثرون  
ون اصواتهم  
حسبون جند  
س كل نسء  
بالتسناه

وصول النجال بقيادة الجزيرة الفضائية ان خصصت حلقة كاملة من



BY ROY ECCLESTON AND PAUL DALEY

# THE DARK

**The internet's ability to leap borders, thwart censorship and preserve anonymity is making it a crucial tool in recruiting jihadists. Discontented western Muslim youth, even in Australia, are ripe for the message of hate of the cyber imams.**

**I**T'S A FORMIDABLE blockade: 5000 armed police and troops, 5km of security fencing, closed-circuit TV surveillance and back-up muscle including army helicopters and water cannon. But when Sydney plays host next month to some of the world's top terror targets, there'll be another level of security few will see.

In a world where Islamic fundamentalists use 21st-century technology to further medieval ambitions, keeping out the bad guys has become much more complicated than throwing up a giant wall.

Protecting George W. Bush, Vladimir Putin, Hu Jintao, John Howard and the other 21 leaders gathering for APEC also requires massive computers tapped into the internet, trawling chat rooms and sites spawned by 9/11 and fuelled by the Iraq war.

When terrorists hit London, Madrid, Washington and New York, the internet featured every time. So for Sydney, the hunt is on for the slightest hint that an operation is under way.

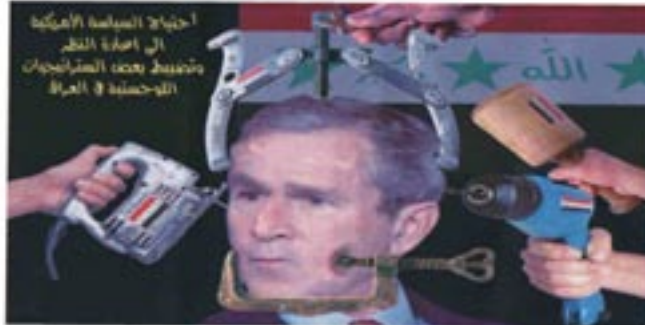
Australian Federal Police are "walking the beat" on the internet with British and US agents around the clock, setting up false web-sites and working closely with the Defence Sig-

nals Directorate to monitor communications. Deep inside the Canberra HQ of the Australian Security Intelligence Organisation, a compact team of specialists spends part of each day and night scanning the web.

Their work is not random: they are tracking the internet footprints of Australia's radical jihadi suspects. Every day, say Australian and international intelligence sources, suspected terrorists in Australia log onto computers at home and in internet cafes, to make new friends and affirm twisted beliefs, both with locals and others thousands of kilometres away.



**EXTRAORDINARY RENDITIONS**  
The world of jihadi websites includes how to make a roadside bomb, below left



وجه الرئيس جورج بوش تداء الى المجتمع الدولي "المساعدة العراقيين" في العملية السياسية. مخترقا لعمرة الاوس. بان ياختفهم مقاومة الاحتلال الامريكى. وبيان من يظنون ذلك "البسوا جميعا ن مهمة القوات الامريكية في ار في هذا البلد. وزاد "انا لن اهدى القذافي يستدفع قوته



**They'll take a fatwa saying it's OK for women to blow themselves up and marry that to videos //**

ABRAHAM COOPER SIMON WIESENTHAL CENTER

# WEB

Nothing much in the lives of 20 or so hardcore Australian-based jihadi terror plotters goes unnoticed. Unnoticed, that is, by ASIO and the AFP. And those who are not watched may well be if they use the internet to communicate with others of like mind.

Welcome to the world of cyber jihad, a fast-morphing conflict that pits tech-savvy terrorists against police and intelligence agencies who struggle to keep up. The net has been dubbed the new Afghanistan for recruiting young Muslims to terrorism, and it's available in anyone's home.

Using Google groups, you can find yourself chatting about jihad (holy war). Elsewhere you'll find Islamist games like "Night of Capturing Bush" or on YouTube see videos of roadside bombs blowing up Americans in Iraq. The aim is to inspire, and then provide the virtual imams who give the religious

guidance that perverts Islam but leads to radicalisation and jihad.

"THE INTERNET IS the new front in the fight," says Nick O'Brien, a former Scotland Yard counter-terrorism expert, now an associate professor at Charles Sturt University. "Any terrorist group in Australia will use the internet, even if it's for self-radicalisation or looking up religious justifications for doing stuff."

Hacking into government or business websites is not the problem. "Terrorists like to see blood, and bringing down a banking system is inconvenient but it doesn't kill people," says a former intelligence official. "Recruiting is the big thing. It's relatively easy to hide on the internet. In Australia, there's been some effort at internet recruiting - there have certainly been some connections made."

The main inspiration, even though it's not

directing attacks, remains al Qaeda. O'Brien's research shows the terror group generates more hits on Google than McDonald's and Coca-Cola. "It's probably the best known brand in the world."

And it stays there by constant advertising, thanks to the internet.

The US-based Simon Wiesenthal Center, which recently released its annual review of terror and hate websites, blogs and chat rooms found the number has now hit around 7000 - with terror outnumbering hate.

"There is a profound level of commitment among terrorists," says Rabbi Abraham Cooper, who has watched these websites increase from one - *stormfront.org* - at the time of the Oklahoma City bombing in 1995 to the huge number today.

"We're seeing a migration to new technologies. Whatever the cutting edge is, whatever

you might least expect, you'll see it. We saw a US department of transport site hacked to park information by a terrorist group. Then they might piggyback a Hamas website. Sometimes it could be on Yahoo club.

"They'll take something from al-Jazeera, a fatwa saying it's OK for women to blow themselves up to kill Jews, for example, and then marry that stuff to videos, sometimes to animation, with music - very high-quality stuff. You even have websites that give you the top 10 attacks on coalition troops."

It's the perfect storm, says Cooper, with highly motivated people who believe they're doing the right thing. "Borders are not relevant. That makes it very, very difficult for intelligence and law enforcement."

**A**TTORNEY-GENERAL Philip Ruddock admits the volume of information is an enormous challenge. "But one ought not assume that because of the enormity of the task, people could assume their activities would go unnoticed or investigated," he warns.

While the vast majority of Australia's 400,000 Muslims have a reputation for tolerance, there have been several cases where the internet featured in charges of Islamist-inspired terrorism. Architect Faheem Khalid Lodhi, convicted of plotting attacks on Australia's power grid, had allegedly used the net to find bomb-making material. One case still before the courts involves more than 20 men charged with terrorism offences after the 2005 Operation Pendennis raids in Melbourne and Sydney.

Is there any evidence that Australians have been recruited to terrorism using the internet?

Ruddock says there are allegations yet to be tested. "I would simply say, I suspect that the evidence that will be led will demonstrate that the people who are involved in the proceedings have a very high degree of internet and computer skills and utilised them extensively."

London-based journalist Abdel Bari Atwan, editor-in-chief of the newspaper *Al-Quds al-Arabi*, says the Howard government's decision to join the invasion of Iraq remains an incentive for internet jihadists to target Australia.

"Joining the American war in Iraq caused huge damage to Australia's image in the Muslim world," says Atwan, author of *The Secret History of al-Qaeda*, who will be a guest at the Brisbane Writers' Festival next month. "Your defence minister, I think, said, 'we went there for oil', so this does not help at all." Atwan's book details how the internet has boosted enormously terrorists' ability to recruit and fight.

Could Australia's actions in Iraq be used to inspire terrorism here? "Definitely," says Atwan. "These kind of stupid policies, stupid comments, will influence the small radical groups in Australia, in some way or another.

**CAPTION HEAD**  
Suicide bomber  
Reem Saleh  
Raiyshi appeared  
on a Hamas video



They will say, 'we came to this country because it's a good example of co-existence and peace, and tolerance. Now ... we can see a government that is 15,000 miles away from Iraq that is sending troops to kill our people there.'

"That is really damaging. Your government has done a lot of damage to your interests in that part of the world."

**T**RACKING SUSPECTED terrorists is simple enough, say security sources. An Australian already under surveillance signs into a chat room under a false name and posts a pro-jihad message; a sympathiser in Belgium responds. Within minutes, 15 others - from the US, Britain, France, Germany, New Zealand and Australia - have responded. "It's always like bees to a honey pot," says a European intelligence source. "It's truly frightening to watch this online ... because you know each one of these is a potential ... bomb-carrier."

Al Qaeda is the generic brand-name for violent radical Islam, but would-be jihadists are not operating under instructions from terror head office. "The most frightening and perplexing thing about al Qaeda is that it does not have to recruit anyone," said an Australian security source. "They recruit themselves."

Intelligence groups call this "auto-radicalisation", and the internet plays an integral part. "So ... there is no recruitment. Just enlistment," the Australian source said. "So how do you attack the problem at its source? It's not like

**These kind of stupid policies, stupid comments, will influence the small radical groups ...**

**ABDEL BARI ATWAN AUTHOR**

shooting missiles at al Qaeda training camps in Afghanistan."

In a recent report, New York police analysed the activities of recent terror plotters, including a large group of alleged jihadists in Australia foiled by Operation Pendennis.

"While the threat from overseas remains, terrorist attacks or thwarted plots against cities in Europe, Australia and Canada since 2001 fit a different paradigm," their report said. "Rather than being directed from al Qaeda abroad, these plots have been conceptualised and planned by 'unremarkable' local residents/citizens who sought to attack their country of residence, utilising al Qaeda as their inspiration and reference point."

The authors, Mitchell Silber and Arvin Bhatt, identified four stages in the radicalisation of home-grown terrorists: pre-radicalisation; self-identification; indoctrination and "jihadisation".

"In the self-identification phase, the internet provides the wandering mind of the conflicted

10101010101010101010  
01010101010101010101  
10101010101010101010  
01010101010101010101  
10101010101010101010  
01010101010101010101  
10101010101010101010  
01010101010101010101  
10101010101010101010  
01010101010101010101  
10101010101010101010  
01010101010101010101  
10101010101010101010  
01010101010101010101  
10101010101010101010



# INNOVATIVE MEDIA EXPOSURE



#### **BUSH WHACKED**

Wannabe jihadists  
can even play  
internet games  
tracking down  
George W. Bush



young Muslim or potential convert with direct access to unfiltered radical and extremist ideology. It also serves as an anonymous virtual meeting place – where virtual groups of like-minded and conflicted individuals can meet, form virtual relationships and discuss and share the jihadi-salafi agenda,” Silber and Bhatt found.

“In the jihadisation phase, when the individual commits to jihad, the internet serves as an enabler – providing broad access to an array of information targets, their vulnerabilities and the design of weapons.”

Commander Kevin Zuccato, director the AFP's Australian High Tech Crime Centre, says the internet poses an enormous challenge, given the volume of material and foreign websites. But there are computer tools for translating web pages, and navigating the data labyrinth.

“In the same way we patrol the streets, we have to be ... patrolling the internet,” says Zuccato. “We need to be participating in chat rooms; we need to be reading what's coming through on blogs on particular websites; we need to be in there developing our own personas interacting with individuals; we need to be far more connected in our international response. And we need to ensure the information is moved very quickly.

“Before, we may have had time on our side. The internet doesn't provide us that luxury, so we need to develop the relationships internationally that will allow us to move quickly [as

TRAVELVISION MEDIA IS A UNIQUE MARKETING COMPANY LEAD BY TRAVEL BROADCASTER AND MEDIA STRATEGIST DEREK TAYLOR GENERATING HIGH VALUE, INNOVATIVE MEDIA EXPOSURE FOR OUR CLIENTS FOR 25 YEARS.



*travel*vision  
media network

[www.travelvisionmedia.com](http://www.travelvisionmedia.com)

CONTACT DEREK TAYLOR 0425 264 747  
derek@travelvisionmedia.com

soon as] we get a piece of information.” But realising what a message means can be tricky, because emails are likely to be coded.

How well-prepared Australian police and security agencies are is an unknown. Government funding has been boosted, but the mix of language and computer skills needed to track terrorists can be extremely hard to find. And the AFP, despite devoting resources to Zuccato's centre, looked out of its depth on some technology issues when interviewing Indian doctor Mohamed Haneef last month over suspected links to the Glasgow bombings.

Haneef, whose chat room conversations with his brother in India were selectively used to justify suspicions about him, had to explain the internet phone service Skype to his interrogators. While the case illustrated the danger of jumping to conclusions from internet conversations, it also demonstrated the scale of the task when 31,000-odd pages of computer documents needed to be analysed quickly.

Several groups such as *siteinstitute.org*, *haganah.org.il* and the Wiesenthal Centre track terrorist-linked websites. Rabbi Cooper says he hasn't seen much evidence of involvement by Australian-based operators.

But Professor Hsinchun Chen, a computer scientist at the University of Arizona, says that doesn't stop Australians logging in to other global sites set up anonymously. Chen, who trawls the “dark web”, says increasingly the target audience for the terrorists is not radical men in Pakistan or the Middle East, but Muslims in western countries who may have shown no sign of radicalism.

## When they get on the web, there are – I won't call them virtual imams – but opinion leaders //

**HSINCHUN CHEN** COMPUTER SCIENTIST

“Many of the young men when they come in, they feel their religion has been persecuted and their voice is not being heard ... but mostly they are puzzled and angry,” Chen says. “But when they get onto the web there are – I won't call them virtual imams – but opinion leaders on websites, and forums and chat rooms.

“And they stay there on purpose, to give guidance, to tell them it's OK to engage in jihad, it's OK to kill civilians. And over time, their minds become infected with those radical ideas, so they change.”

It's like MySpace for terrorists, he says. People begin to bond. Mostly they're not religious fanatics, and many are well-educated. Disconcertingly, he says, most live in the West,

and may not even speak Arabic.

Clinton Fernandes, a senior lecturer in strategic studies at the Australian Defence Force Academy and a former Army intelligence officer, says auto-radicalisation begins with a sense of loneliness and alienation from mainstream society. On the internet, such people can fall victim to perverted versions of Islam.

“Australian Muslim community leaders are correct in saying that Muslim radicals aren't reflecting Islam's teachings,” he says. “Just as you wouldn't try to understand violent revolutionaries by reading Karl Marx ... you shouldn't try to understand Muslim radicals by reading the Koran.

“In fact, radicals aren't theologians, and they don't respect community leaders. They practise a do-it-yourself version of the little that they do read. This is akin to youngsters who don't buy a whole music album, but cherry-pick the songs they do like and download only those.

“Radical internet forums are in a sense an internal discussion among Muslims, and Australian Muslims should be encouraged to participate in these discussions where they can challenge the cherry-picked version of Islam that gets bandied about.”

This argument is also pushed by Cooper and Chen, who say the extremism has to be countered by more moderate Muslim voices. The Wiesenthal Centre is opening its own website, *askmusa.org*, next month to try to counter anti-Jewish propaganda.

“We need to learn a lesson from al Qaeda,” says Cooper. “If they're making an effort to

reach out to the young, educated elite, we'd better be doing the same thing”

Australia, though, will try to censor the web. In proposed new laws, Ruddock wants to ban material he says incites terrorism, in books, DVDs or on the web.

This won't work, says Chen. The web, after all, was designed to operate after a nuclear war. Any attempt to shut down terrorist websites is like “trying to fight fire with oil. You cannot. They move quickly from one website to another, all free of charge. They're hiding in the dark, it's the dark web”.

Yet author Atwan says many young Muslims will ignore moderate voices unless the root causes of their anger are also tackled. The Arab-Israeli conflict, the Arab dictatorships and the Iraq war all fuel the sense of injustice. The videos of attacks on US forces serve as “inspiration” that real blows can be struck.

But the internet isn't the cause of the trouble, he says, it's just a tool for angry Muslims to air their grievances and try to inspire others. And only a few fish need to be caught in this vast electronic sea.

“You don't need to radicalise a million Muslims, just a few thousand,” says Atwan. “And the internet is doing that.”

**The Secret History of al-Qa'ida** is published by Abacus, \$27.95. Abdel Bari Atwan is a guest of the Brisbane Writers' Festival from September 13-16, and will give a public talk in Sydney at the UNSW on Monday September 17.



**CONNECTIONS**  
Mobiles on sale in Pakistan display the 9/11 attack and Osama bin Laden

