XML Template (2007) [14.11.2007-1:45pm] [148-153]
{TANDF_REV}RIOC/RIOC_I_36_04/RIOC_A_274007.3d (RIOC) [Revised Proof]

TAKING ON THE RADICALS

DAVID LIVINGSTONE

TACKLING EXTREMISM ON THE WEB DEMANDS SOPHISTICATED CYBER TACTICS, NOT OLD-FASHIONED CENSORSHIP

In July 2007, in an important case at the Old Bailey, the UK's Central Criminal Court, five young British-Muslims were found guilty under the Terrorism Act 2000, with the key prosecution evidence being the discovery of large volumes of radical, Islamic-related material on their computer drives. The defendants all received sentences of between two and three years' imprisonment. The reason for the lack of detailed media attention was that there was no uncovered 'plot' to detonate bombs on public transport, or to make up poisons and infect populations of people, or to assassinate an iconic public figure. However, their guilt in respect of the 'commission, preparation or instigation of an act of terrorism' under the Terrorism Act 2000 seemed to be, at first glance, at odds with evidential presentation. According to the defence, it seemed that at no stage did the prosecution identify what that act of terrorism was supposed to have been, except that there was a case that the group would at some time in the future commit such an act.

However, the circumstances in which the five defendants found themselves in a jury trial at the Central Criminal Court give rise to questions on the nature of radicalisation in the modern, information-rich world, and whether society's current strategies in coping with radicalising groups and individuals are appropriate to this new era of global communications. The case calls into question whether there is an argument for some form of censorship of the Internet and other media to help slow the volume of individuals and groups, of whatever cause (environmentalism, human rights, animal rights, religion), from proceeding down a path of radicalisation.

One single defendant in the Old Bailey case had, significantly, 'turned back' from the path of radicalisation and was beginning to seek readjustment into mainstream society, but was found as guilty as the other four defendants who were not taking steps to redeem themselves, and was handed down an equally severe prison sentence. In a more perfect world, there is a case that this person should have been handled differently and, perhaps, more compassionately.

The substance of the defendants' crime, the court found, was the downloading of a large quantity of extremist material from open-source websites. Analysis of Internet chatroom conversations between group members also pointed to them being some way along a path of radicalisation, although the defence case made out that there was still some uncertainty between them on how they were going to

DOI: 10.1080/03064220701740608

pursue their idealistic conflict with liberal western democracy in some sort of act of 'jihad'.

The volume of material available on the Internet, and in any other media that plays a part in the radicalisation process, is vast. In the case of the Old Bailey defendants, such was the amount of discovered material, that, if printed, the pile of paper would have reached as high as Nelson's Column, whilst the amount of material under contention, which the prosecution thought to be extremist, would be only six inches high. The spectrum of material was equally as vast, with completely inoffensive material at one end and, at the other, depictions of some of the severest acts of barbarism. It also included a so-called 'manual on terror'. Much was made of this in the prosecution case and also in the limited media reporting. This publication was the *Military Guide to Terrorism in the 21st Century*, a manual produced by the Training and Doctrine Command of the United States Army. Its preamble states that it is 'a high level primer produced for the benefit of American servicemen and other citizens working overseas and explaining to them certain modus operandi of worldwide terrorist groups'.

It is an unclassified publication and was put on the world wide web by the American government, presumably not by accident, and therefore in the sure knowledge that it could not be useful to the ill disposed. As a key theme this leads to the conclusion that some material can support a charge of terrorism when held by one party, but can be a sensible precaution in anti-terrorism when held by another. This also applies to some leading 'counter-terrorist' websites in the western world which also show the same clips of barbaric acts, but this time to support the posted texts (which the site owners claim to be, therefore, acceptable images).

However, all five were convicted of possessing material for terrorist purposes, which seems to suggest there was a presumption at some stage that all or most of the five would have ultimately carried out an act of terrorism, as defined by law officers in the United Kingdom. In the judge's words, when passing down sentence, the group had become 'intoxicated'. If they had been poisoned, then who was the poisoner? Who was the root instigator of the (real or presumed) act of terrorism?

Aspects of this case point to a need for liberal democracies to develop more sophisticated techniques in managing the current phenomenon of core radicals, of whatever cause, who are increasingly using the Internet to engender societal discontent and to promote their messages. Hand in hand with this, there needs to be a fresh look at a new set of measures to prevent individuals and groups, of whatever persuasion, from progressing down paths of radicalisation. Management of the web-based peddling of radical and criminal creeds seems to be a useful

strategy to prevent people and groups from 'kicking off from the side of the pool' in the first instance.

There is a complicating factor when the global nature of the Internet is taken into account: although there is generally a common view of what terrorism is, there is no single international definition of terrorism. This is a fault line in developing a global response. Along with the relatively unpoliceable state of the world wide web, there will always be problems in limiting the amount and severity of material made available to those with a PC, a mouse and a network connection. National laws relating to freedom of speech will generally lead to inconsistencies in how agencies respond around the world. There is little current guidance, even in the UK, on when a curious individual browsing the web may go too far by collecting 'too much' or 'too horrible' material and then be identified de facto as an instigator of terrorism and dubbed a criminal.

In addition to material downloads, there is the parallel problem of the Internet chat room. Once individuals have met and found a shared narrative (and many will cycle through chat rooms until they do) there is a known phenomenon of 'risky shift', where the narrative of a group tends to propel its members on a path of radicalisation, whether ideological, religious, or just extreme football fanaticism as an example. Interaction between these people on the Internet, without face-to-face contact, makes individuals less inhibited and less cautious. This adds to the propelling effect as the agenda is taken forward. However, there is a counterbalancing benefit in that the behaviour and the rate at which a group will radicalise becomes more predictable. In the case of individuals on a similar agenda, through activism to terrorism, the tipping point at which extreme action is deemed essential by the subject is much less predictable – for example, David Copeland, the neo-Nazi nail bomber, and, most probably, Timothy McVeigh in his attack on the FBI building in Oklahoma City, who subscribed to a 'Revenge for Waco' agenda.

But who are the target individuals on whom society needs to focus a new strategy of intervention? It is tempting to define a target as any individual whose belief diverges from liberal democratic or mainstream idealism, but this approach would stand the risk of reducing the richness of society by pruning out some of the more colourful buds at the extremities of the twigs and branches. There can be no set international standards of acceptable behaviour, much as there is no international standard on a definition of terrorism. However, the radicalising subject tends always to seek to legitimise his thoughts and feelings through association with those of similar standpoints.

This legitimisation is generally a product of the agreement of a series of views inside a peer group, and that group must be able to discuss and agree its policy by interaction. In former times, group members would have met up.

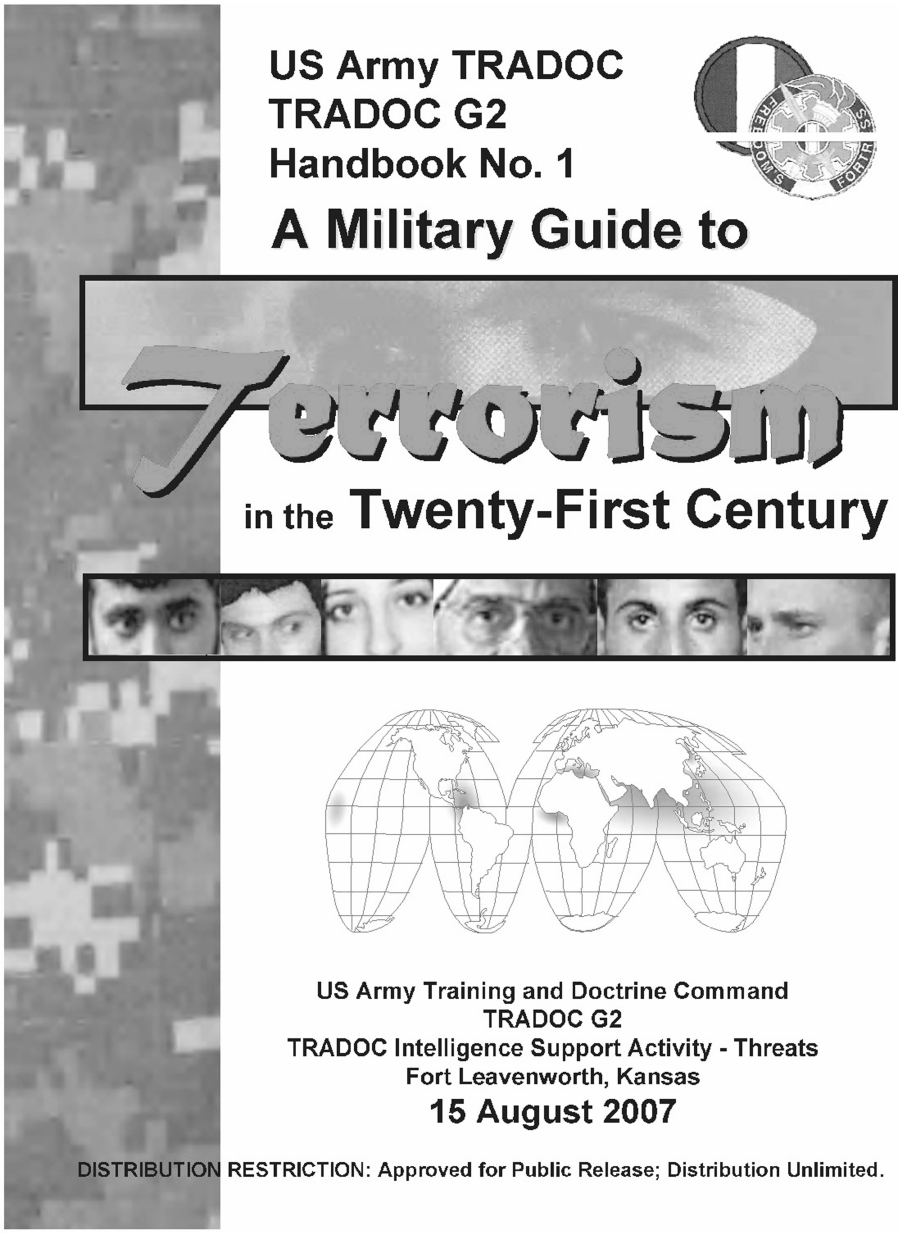
Early encounters could be reasonably hit and miss (meeting by coincidence or acting on knowledge imparted from third parties). The world wide web now creates the ability to travel in virtual terms to meet others, no matter how far apart the conversants are in the physical world, just by a few clicks of the mouse. It is difficult to characterise how these conversations are first struck up, and then developed, and the overall defence strategy against radicalisation on the Internet does need, therefore, to incorporate more than the on/off application of a legislative enforcement process. It demands the integration of societal and community-based interventions in the early stages of a person's or group's progress down a particular path. This journey is most often supported by material from the net.

In most cases, radical movements are quite unchallenged as they use the web to promote their views and policies. Thus a key instrument in the fight against radicalisation of individuals and communities should now be the development of a web-engagement strategy. The depiction and description of 'real world' events on the net provide ample 'evidence' to those who may be susceptible to supporting a notional cause. Success on this cyber-battleground, by making the growth medium of radicalisation less supportive, will logically lead to abatement in the progress of radicalisation across the board and will help stabilise relationships between governments and their peoples.

A key question is – has the ability of wider governance to apply societal intervention, to take the heat out of the radicalisation agenda, been able to match the pace at which activists have developed their media-based 'marketing skills'? Is there a case, in the first instance, for a global regime of increased censorship of the Internet and the media as a response to this phenomenon, to inhibit the politicisation of the masses around the world?

It is difficult to see how the politicisation of individuals and groups can be halted by censorship. Any attempts to legislate against the information sources which give rise to radical material will encounter the problem of the physical domain (in which governments exist) pitting itself against the virtual. Server space is highly mobile and web pages can be transferred to any IP address in an instant, while non-terrestrial television is being overtaken by the richness of trans-national satellite. The Great Firewall of China, currently a huge but (to the Chinese government) affordable cost, clearly will not be able to continue over time – partly because of the growing labour costs of the national cyber-police as the Chinese economy quickens, but chiefly because of the constant pressure of the information streams as they seek their IP targets. Modern means of communication are designed to be resilient and to link people, no matter what obstructions are put in their way.

It is for this reason that censorship of the web to deny the use of the medium to radical groups is, and will continue to be, unachievable. If sites are blocked or



Manual on terror?

taken down, then alternatives will be found, and the game of cat and mouse will continue. Liberal democracies must, therefore, accept that the information technology environment which they designed, and which they now use to great effect in driving improvements in the global economy, will also be used by people or groups to spread less acceptable doctrines, strategies, policies and plans – and that no amount of authoritarian censorship will have the desired effect.

The response to marginalised communities who use the net in their radicalisation campaigns, must not therefore be to try and block the communications structures, but to constantly identify the routes by which the radical messages are being directed towards their intended audiences. Cyber-strategies need to be drawn up on a relatively two-dimensional battleground, matching philosophy with counter-philosophy and message with counter-message, in a higher level of intellectual debate. Legislation may have a useful short-term effect (and the political class may feel that it would be useful to be seen to be doing something), but, in the longer term, restrictions on the liberty to associate may be felt by many people to be an intrusion on their rights. Lessons learnt from anti-terrrorist campaigns in the past, in the real world, would seem to indicate that inappropriate short-term measures, such as censorship, have long-term implications on the wider campaign for stability. ❑

David Livingstone *is an Associate Fellow on the International Security Programme, Chatham House*

This is an extract from a longer paper on radicalisation-intervention strategies for Chathan House