CHAPTER FIVE

Terrorist Use of the Internet and the Challenges of Governing Cyberspace

Maura Conway

In Dunn, Myriam, Victor Mauer, & Felisha Krishna-Hensel (Eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. London: Ashgate (2007): 95 – 127.

Introduction

Information is the lifeblood of the international system. World politics today transcends simple international relations, and much of the change has taken place as a result of the spread of information infrastructures. The rapid expansion and diffusion of new International Communications Technologies (ICTs), particularly evident in the growth of the internet, contribute to the set of phenomena collectively labelled 'globalisation' and cut across traditional temporal and spatial boundaries. Yet the central and causal role of communications in the transformation of our world still tends to be neglected or minimised by most International Relations (IR) scholars. As recently as 2003, the editors of *Millennium*, in the introduction to a special issue devoted to 'IR in the Digital Age', observed that 'Whereas other social sciences have begun to address aspects of this issue, IR as a discipline is once again playing catch-up.'[1]

The ongoing advances in ICTs are significantly impacting the ways in which states and societies relate to one another. The information revolution underlines several challenges to global governance, chief amongst which are the following:

- The creation of electronic platforms where new, or hitherto less powerful, actors have emerged and influenced policy agendas while bypassing established channels of participation
- The potential crisis of democratic accountability, legitimacy, and identity arising out of the empowerment of these
- The changing conception of how states define their interests, their power bases, and their security

- Mounting challenges to states' ability to govern and control the dissemination of information.[2]

Both global governance and the sub-set of issues that may be termed 'internet governance' are vast and complex issue areas. The difficulties of trying to 'legislate' at the global level – efforts that must encompass the economic, cultural, developmental, legal, and political concerns of diverse states and other stakeholders – are further complicated by the technological conundrums encountered in cyberspace. The unleashing of the so-called 'Global War on Terrorism' (GWOT) complicates things yet further.

Today, both sub-state and non-state actors are said to be harnessing – or preparing to harness – the power of the internet to harass and attack their foes. Clearly, international terrorism had already been a significant security issue prior to 11 September 2001 and the emergence of the internet in the decade before. Together, however, the events of 11 September 2001 and advancements in ICTs have added new dimensions to the problem. In newspapers and magazines, in film and on television, and in research and analysis, 'cyber-terrorism' has become a buzzword. Since the events of 11 September 2001, the question on everybody's lips appears to be 'is cyber-terrorism next?'.[3] It is generally agreed that the potential for a 'digital 9/11' in the near future is not great. This does not mean that IR scholars may continue to ignore the transformative powers of the internet. On the contrary, the internet came of age on 11 September 2001, as that was the day when the 'Digital Age' and the 'Age of Terror' converged.[4]

This chapter explores the difficulties of internet governance in the light of terrorists' increasing use of the medium. In particular, it details the clampdown on the burgeoning internet presence of extremist groups, undertaken by both state-based and sub-state actors, in the wake of the attacks of September 2001 in the US and of July 2005 in London. The ensuing governance challenges are many and varied, but include

- Debates over the role of various actors in the governance process, including national governments, hacktivists, and Internet Service Providers (ISPs)
- The appropriate legislative response to the terrorist internet presence
- The debate over free speech vs. limits on speech

The description and analysis of these challenges are at the centre of this chapter. First, however, it is worth considering what exactly is meant by the term 'internet governance'.

What is Meant by 'Internet Governance'?

The internet had unique governance structures during its development and early growth. It began life as a government project: in the late 1960s, the US government sponsored the establishment of the Defence Advanced Research Projects Agency (DARPA), which was charged with developing a resilient communication facility designed to survive a nuclear attack. By the 1980s, a wider community was using the facilities of this network, which had come to be referred to as the internet. In 1986, the Internet Engineering Task Force (IETF) was established to manage the further development of the internet through a cooperative, consensus-based decision-making process involving a wide variety of individuals. At this point, internet governance was relatively simple: 'There was no central government, no central planning, and no grand design.'[5] However, in 1994, the US National Science Foundation decided to involve the private sector by subcontracting the management of the Domain Name System (DNS) to Network Solutions Inc. (NSI). This angered many end users and resulted in a conflict, which was only resolved in 1998 with the establishment of a new organisation, the Internet Company for Assigned Names and Numbers (ICANN).[6]

Since the establishment of ICANN, the debate on internet governance has been characterised by the more direct involvement of national governments, mainly through

the UN framework and institutions. The first World Summit on the Information Society (WSIS), held in Geneva in December 2003, officially placed the question of internet governance on diplomatic agendas. The Declaration of Principles and Action Plan adopted at WSIS 2003 proposed a number of actions in the field of internet governance, including the establishment of a Working Group on Internet Governance (WGIG).[7] This became necessary because each of the terms 'internet' and 'governance' was the subject of controversy as, indeed, was the concept of 'internet governance' itself.

It was the second part of the concept (i.e. 'governance') that was the subject of particular controversy, especially during the WSIS. Misunderstandings stemmed from terminological confusion arising out of the use of the term 'governance' as a synonym for 'government'. When the term 'internet governance' was introduced in the WSIS process, many countries linked it to the concept of government. One of the consequences was the belief that internet governance issues should be addressed primarily at the inter-governmental level with only the limited participation of other actors. What were the main reasons for this terminological confusion? Gelbstein and Kurbalija argue that it is not necessarily obvious to many that the term 'governance' does not mean 'government'. They point out, for example, that the term 'good governance' has been used by the World Bank to promote the reform of states by introducing more transparency, reducing corruption, and increasing the efficiency of administration and that, in this context, the term 'governance' was directly related to core government functions.[8]

In his analysis of internet governance, Klein draws on Robert Dahl's seminal text *Democracy and Its Critics* (1989), in which Dahl identifies what he views as the

minimal conditions necessary for the establishment of an effective system of governance:

> The first is an *authority*. Governance requires a governor or a sovereign. An entity, be it an individual or a group, must make policy decisions that apply to the members of the polity. A second governance mechanism is *law*. Laws implement policy decisions. They might take the form of a tax, a license, or simply a binding rule. Third, there must be some mechanism for imposing *sanctions*. This allows for punishment of those who violate laws. Finally, governance requires the definition of *jurisdiction*. Jurisdiction defines the space over which the authority makes decisions and within which the laws apply and are enforced by the threat of sanctions. These four mechanisms make governance possible: the governing *authority* can make a policy decision that applies within its *jurisdiction*, embodying that decision in *law* and imposing *sanctions* on whomever disobeys [italics in original].[9]

Dahl's conception of governance is quite hierarchical, however, and closer to 'government' than perhaps many of those connected with the development of the internet – other than national governments – might find acceptable. Indeed, the WGIG has since published the following working definition of internet governance: 'Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.'[10] This does not mean that the four issues identified by Dahl – authority, law, sanctions, jurisdiction – are of no importance; they arise repeatedly in any discussion of the relationship between terrorist use of the internet and internet governance; what the WGIG definition does draw our attention to, however, is the legacy of the early years of the internet's development and the resultant importance of actors-other-than- states in the internet governance process.

Terrorism and the Internet: A Brief History

For a considerable time, the terrorism-internet relationship consisted largely of fears about the potential for so-called 'cyber-terrorism'. In 1998, Mark Pollitt defined cyber-terrorism as 'premeditated, politically motivated attack[s] against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents.'[11] On the basis of this definition, no act of cyber-terrorism has ever yet occurred; this has not mitigated against cyber-terrorism – conceived of as everything from sending pornographic e-mails to minors, posting offensive content on the internet, and defacing web pages, to using a computer to cause US$400 worth of damage, stealing credit card information, posting credit card numbers on the internet, and clandestinely redirecting internet traffic from one site to another[12] – receiving widespread coverage in newspapers, magazines, film, and television.

Cyber-threats became the object of increased attention from the US federal government in the 1990s. A particular concern was that enemies of the US, unable to defeat US forces on the conventional battlefield, would pursue alternative approaches to inflicting damage on the sole remaining superpower.[13] The events of 11 September 2001 were therefore doubly shocking for many US government officials: not only were the attacks appalling in themselves, but the conventional nature of the attacks was also completely unexpected. Far from reducing the fear of cyber attack however, for many the 11 September 2001 attacks only served to increase the credibility of the cyber-threat. In the weeks and months following 11 September 2001, in particular, the likelihood of a follow-up cyber-terror attack was widely referred to in the US press and was also taken up internationally (see Tables 1 and 2).

[table 1 here]

[table 2 here].

The one-sided nature of this analysis only became apparent to many when, in a little over four weeks in April and May 2004, the now-deceased Abu Musab al-Zarqawi, one-time leader of 'al-Qaida in Iraq', 'rocketed to worldwide fame, or infamy, by a deliberate combination of extreme violence and internet publicity'.[14] In early April 2004, Zarqawi posted online a 30-minute audio recording which explained who he was, why he was fighting, and details of the attacks for which he and his group were responsible. Zarqawi was interested in using the internet as a weapon, but not of the sort predicted by those hyping the threat of cyber-terrorism. Prior to the instigation of his internet-based PR campaign, each of Zarqawi's attacks had to kill large numbers of people in order to get noticed in the chaos and mounting daily death toll in Iraq. By going online, however, Zarqawi was able to both control the interpretation of his violent actions and achieve greater impact with smaller operations. By the end of April 2004, his group was regularly issuing communiqués via the internet. The first of these claimed responsibility for a suicide speedboat attack on Iraq's offshore oil export terminal in the Gulf which, although the operation failed, still shook oil markets because of Zarqawi's efforts at publicising the attack through the internet.

In May 2004, Zarqawi took things a step further and used the internet's force-multiplying power to the maximum effect when he was videotaped cutting off the head of a US hostage and had the footage posted online. The purpose of this video was to create images that would grab the attention of allies and enemies alike. In this respect, it was an undoubted success; Zarqawi risked very little in this undertaking, but accomplished 'as much if not more to undermine US plans as a bomb that killed 100 people in Najaf. And [at the same time] made himself a hero to jihadis across the

world.'[15] The free availability of this and other grisly 'snuff movies' on the internet led to a realisation that the most important aspect of the terrorism-internet relationship was not the much vaunted 'cyber-terrorism', but those more mundane and everyday terrorist uses of the internet, from information provision to recruitment, which have a history stretching back for many years before Zarqawi's appearance on the internet.

In 1998, it was reported that approximately half of the (then) 30 groups designated as 'Foreign Terrorist Organisations' under the US Antiterrorism and Effective Death Penalty Act of 1996 operated websites. Today, virtually every active militant group – there are approximately 70 operating worldwide – has an online presence, and many groups are the subjects of more than one site. A majority of the 42 groups that appear on the US State Department's 2006 list of Designated Foreign Terrorist Organizations have an established online presence. A number of these groups have already shown a clear understanding of the power of the global information network to publicise their position. The Lebanese Hizbollah has clearly demonstrated this ability, as have the Tamil Tigers, al-Qaida, and numerous other political violence movements that maintain a web presence.[16] Unsurprisingly, in the post-11 September 2001 world, the latter are subject to much increased scrutiny. The remainder of this chapter is concerned with describing and analysing the attempts at internet governance instigated by those with concerns about increasing extremist use of the internet for the purposes of, amongst other things, information dissemination and thence recruitment. Much of the following is therefore concerned with what is called 'content control': efforts on the part of stakeholders to regulate what sort of material is available on the internet, including the removal of 'objectionable' materials currently accessible and the erection of barriers to the uploading of such materials in the future.

Content Control Issues

Who is Responsible for Content Policy?

When it comes to terrorism, governments are generally held to be the main players in the area of content control, as it is they who prescribe what should be controlled and how. Some groups of individual users, such as hacktivists, are also keen to play their part, however, and indeed have had some success in disrupting the online presence of a number of terrorist organisations. In practical terms, of course, both legislated content control and private initiatives require the participation of private enterprises, particularly Internet Service Providers (ISPs) and search engine companies, and pressure has increasingly been brought to bear on such firms, both by nation-states and private groups and individuals, to regulate terrorism-related content. In addition, the availability of appropriate control technologies is also a matter for discussion.

Three Approaches to Content Policy

Content policy is generally approached from one of three standpoints: 1.) Human rights (freedom of expression and right to communicate), 2.) Government (legislated content control), 3.) Technology (tools for content control).

Freedom of expression and the right to seek, receive, and impart information is a fundamental human right, according to Article 19 of the UN's Universal Declaration of Human Rights (1948). On the other hand, the Declaration also recognises that freedom of expression is counter-balanced by the right of states to limit freedom of expression for the sake of morality, public order, and general welfare (Article 29). Thus, both the discussion and the implementation of Article 19 must be put in the context of establishing a proper balance between these two concerns. This ambiguous international

regime opens many possibilities for different interpretations of norms relating to speech, and ultimately for different implementations.

Content control is very much bound up with free-speech issues and concerns regarding restrictions on freedom of expression. Controls on internet-based speech are especially contentious in the US context, where the First Amendment guarantees broad freedom of expression, even the right to publish hate speech and similar material. [17] Achieving a proper balance between content control and freedom of expression has therefore proven to be a considerable challenge, and much of the recent internet governance debate, including court cases and legislation, has been concerned with finding this balance. Whereas the US Congress has inclined towards stricter content control, particularly in the wake of the events of 11 September 2001, the US Supreme Court has sought to uphold First Amendment protections. This commitment to freedom of expression is what largely shapes the US position in the international debate on internet governance. So while the US has signed on to the Cybercrime Convention, it is constitutionally barred from signing the Additional Protocol to this convention that deals with the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[18] In other words, while the Additional Protocol is now available to EU governments and other signatories, adding to other hate crimes statutes under which they may prosecute terrorist groups and their supporters who publish hate material online, the same legal options are not available to the US authorities.[19]

It is for this reason that many terrorist groups' sites are hosted in the US. For example, a Connecticut-based ISP was at one time providing co-location and virtual hosting services for a Hamas site in data centres located in Connecticut and Chicago.[20] While sites such as those maintained by Hamas have been subject to more intense

scrutiny following the events of September 2001, similar websites had already been the subject of debate in the US even before the events of 11 September 2001. In 1997, controversy erupted when it was revealed that the State University of New York (SUNY) at Binghamton was hosting the website of the Revolutionary Armed Forces of Colombia (FARC), and that a *Tupac Amaru* (MRTA) solidarity site was operating out of the University of California at San Diego (UCSD). SUNY officials promptly shut down the FARC site. In San Diego, officials decided in favour of free speech, and the *Tupac Amaru* site remained in operation on UCSD's servers for some years.[21] It is not illegal to host such a site, even if a group is designated a 'Foreign Terrorist Organisation' by the US Department of State, as long as a site is not seeking financial contributions nor providing financial support to the group. Other content is generally considered to be protected speech under the First Amendment of the US Constitution.

Constitutional guarantees notwithstanding, states are not technologically impotent when faced with political violence groups seeking to use the internet for information dissemination purposes. Rather, states have access to myriad technologies with which they can limit and constrain how dissidents are able to use the internet. The successful use of the internet for recruitment and other types of political action is based on the assumption that both users and audiences have access to the messages communicated via the internet. States can therefore constrain the effectiveness of these cyber-based strategies by limiting user and audience access to internet technologies, either by actively censoring internet content or by controlling the internet infrastructure, or by some combination of the two.[22] The common element for governmental filtering is generally an index of websites that citizens are blocked from accessing. If a website appears on this list, access will not be granted. Technically speaking, the filtering

typically utilises router-based IP blocking, proxy servers, and DNS redirection. Filtering of content is carried out in many countries: in addition to those countries, such as China, Saudi Arabia, and Singapore, which are usually associated with such practices, other countries increasingly practice censorship also.[23] For example, Australia has a filtering system for specific national pages, while the German state of North-Rhine-Westphalia requires ISPs to filter access to mainly, but not solely, neo-Nazi sites.[24]

Three Types of Content

Discussions about content also usually focus on three types. The first type consists of content where a global consensus regarding its control exists. Control of the dissemination of child pornography online is the area in which the greatest amount of consensus currently exists.[25] While incitement or organisation of terrorist acts are prohibited by international law (*ius cogens*) – that is, a general consensus about the need to remove this content from the Net has been established – disputes still arise. This is because there is no globally accepted definition of terrorism, which makes it difficult, not to say impossible, to come to any agreement as to what exactly might constitute terrorism-support in any given instance.

In terms of controls, the second type of content that is generally discussed is that which might be sensitive for particular countries, regions, or ethnic groups due to their particular religious and/or cultural values. There can be little doubt that globalized, high-volume, and more intensive communication challenges cultural and religious values held in differing regional, national, and local spaces. In fact, most internet court cases are concerned with this type of content. Germany has very developed jurisprudence in this area, with many court cases against those responsible for websites hosting Nazi materials. In the Yahoo! Case, a French court requested that Yahoo.com

(USA) prohibit French citizens from accessing parts of a website selling Nazi memorabilia. Most content control in Asia and the Middle East is officially justified as the protection of specific cultural values.[26] This usually includes blocking access to pornographic and gambling sites, but also those of a radical political nature.

This brings the discussion to the third type of content, which consists of politically and ideologically sensitive materials. In essence, this involves internet censorship. There is a dilemma here between the 'real' and 'cyber' worlds. Existing rules about speech, promulgated for application in the real world, *can* be implemented on the internet. This is probably best illustrated within the European context where, for example, the EU Council Framework Decision on Combating Racism and Xenophobia explicitly indicates 'what is illegal off-line is illegal on-line.'[27] However, one of the arguments put forward by those who believe that the internet requires specific legislation tailored to its specific characteristics is that quantity (i.e. intensity of communication, number of messages, etc.) makes a qualitative difference. In this view, the problem of hate and terrorism-related speech is not that no regulation against it has been enacted, but that the share and spread of the internet render cyber-based hate and terrorism different kinds of legal problems than their 'real world' equivalents. In particular, more individuals are exposed to this type of speech and it is difficult to enforce existing rules. Therefore, the difference that the internet brings is mainly related to problems of enforcement, not the rules themselves.[28]

The Contemporary Legislative Landscape

The legal vacuum in the field of content policy that characterised early internet use provided national governments with high levels of discretion in content control. National regulation in the field of content policy may provide better protection for

human rights and resolve the sometimes-ambiguous roles of ISPs, enforcement agencies, and other players, but such laws may also prove highly divisive. In recent years, many countries have for the first time introduced internet content policy legislation. Some of this legislation was introduced as a result of the boom in internet use and the perceived need to protect the interests of user-citizens; however, a large amount of content policy was also hastily promulgated in the wake of 11 September 2001 on the basis of perceived risks to national security. Civil libertarians and others point to the knee-jerk nature and dubious efficacy of some such policies.

The US Position

In the immediate aftermath of 11 September 2001, the FBI was involved in the official closure of hundreds – if not thousands – of US-based internet sites. For instance, several radical internet radio shows, including *IRA Radio, Al Lewis Live* and *Our Americas,* were pulled by an Indiana ISP in late September 2001 after the FBI contacted them and advised that their assets could be seized for promoting terrorism. The New York-based *IRA Radio* was accused of raising funds for the Real IRA. The site contained an archive of weekly radio programmes said to back the dissident Irish republicans.[29] The archive of political interviews from the programme *Al Lewis Live*, hosted by iconoclastic actor/activist Lewis,[30] drew some 15,000 hits a day. *Our Americas* was a Spanish-language programme about rebels in Latin America.[31] However, because these and many of the other sites that were closed didn't directly incite violence or raise money, they were not contravening US law and many were therefore up and running again relatively shortly after they had been shut down.

Of all the legislation promulgated in the wake of 11 September 2001, the most relevant in terms of internet governance is the Uniting and Strengthening America by

Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), which makes it illegal to advise or assist terrorists, such as via an internet site. The case of Babar Ahmad is an interesting one in this regard. Ahmad, a British citizen, was the publisher of two prominent jihadi websites, azzam.com and qoqaz.com, which were hosted in the US and through which he is accused of raising money for Islamic militants in Chechnya and elsewhere. The UK government has agreed to a US extradition request and Ahmad is to be tried in the US on charges relating to his use of the internet for terrorism-related purposes, which fall under the heading of 'conspiracy to provide material support to terrorists'. This includes not just the solicitation of financial support referred to above, but also, according to an affidavit filed in US District Court in Connecticut in 2004, urging all Muslims to 'use every means at their disposal to undertake military and physical training for jihad' and providing 'explicit instructions' about how to raise funds and funnel these to violent fundamentalist organizations through conduits such as Benevolence International Fund, a front organization operating as a charity.

Similar charges as those pending against Ahmad have been brought against other US residents. However, due to the high levels of speech protection in the US referred to earlier, at least two defendants have so far been tried and freed without charge on the basis of similar complaints: these are Sami Omas al-Hussayen, a Ph.D. candidate in computer science at the University of Idaho who established and maintained a radical website, and Sami Amin al-Arian, a professor at the University of South Florida who was tried on charges relating to, amongst other things, his utilization of the internet to publish and catalogue acts of violence committed by Palestinian Islamic Jihad. Babar Ahmad's trial will serve as yet another test of the new US anti-terrorism law that makes

it a crime to provide material support in the form of expert advice or assistance to terrorists, including IT support. Clearly, Ahmad's case will be one to watch in terms of its impact on terrorism-related internet-based speech in the US.[32]

The UK Position

The July 2005 London bombings provided the spur for the British government to act against terrorist websites operating out of the UK. In the immediate aftermath of the attacks, the then-home secretary, Charles Clarke, indicated in a parliamentary speech that he would be seeking to extend the state's powers 'to deal with those who foment terrorism, or seek to provoke others to commit terrorist acts'. In his speech, Clarke noted specifically that 'running websites or writing articles that are intended to foment or provoke terrorism' were activities that would fall within the ambit of these new powers.[33] His plans were endorsed by Britain's Association of Chief Police Officers, who in turn requested that new legislation be drawn up giving law enforcement agencies 'powers to attack identified websites'.[34] The UK Prevention of Terrorism Bill 2005 narrowly avoided defeat in Westminster in October 2005; opposition centered on two key measures: new police powers to detain suspects for up to 90 days without charges[35] and a proposed offense of 'encouragement or glorification of terrorism'. With regard to the 'glorification of terrorism', such a measure would clearly criminalize the establishment, maintenance, and hosting of many websites currently operational within the UK.

The major criticism, of course, is that the latter clause may serve to stifle legitimate political speech. Several other measures included in the bill that may also impact terrorist internet use in the UK, such as the outlawing of 'acts preparatory to terrorism' and the giving or receiving of 'terrorism training', went largely uncontested

in parliamentary debates.[36] In the event, the Blair government was defeated on the detention issue. However, the remainder of the bill's provisions went into force on receiving royal assent on 30 March when the bill became the Terrorism Act 2006.[37] What impact the new legislation will have on terrorism-related materials produced by or disseminated to UK citizens via the internet is unknown at the time of writing.

International Initiatives

At the international level, the main content control initiatives have been undertaken by European countries with strong legislation in the area of hate speech, with European regional institutions trying to impose those same rules in cyberspace. The key international legal instrument addressing the issue of content is the Council of Europe's Additional Protocol on the Cybercrime Convention. The protocol specifies various types of hate speech that should be prohibited on the internet, including racist and xenophobic materials, justification of genocide, and crimes against humanity.[38] The Organization for Security and Co-operation in Europe (OSCE) is active in this field also. In June 2003, the OSCE Meeting on Freedom of Media and the Internet adopted the Amsterdam Recommendations on Freedom of the Media and the Internet. The recommendations promote freedom of expression and attempt to reduce censorship on the internet. In June 2004, the OSCE organised a Conference on the Relationship between Racist, Xenophobic, and Anti-Semitic Propaganda on the Internet and Hate Crimes. The focus of this event was on the potential misuses of the internet and freedom of expression. These OSCE events provided a wide range of academic and policy views addressing these two aspects of content control, though no new rules were instituted as a result of these discussions.

The EU has also undertaken several initiatives in the context of content control, adopting the European Commission Recommendation against Racism via the Internet. On a more practical level, the EU also introduced the EU Safer Internet Action Plan, which resulted in the establishment of a European network of hotlines, known as Inhope, for reporting illegal content. At the present time, the major type of illegal content focused upon is child pornography and paedophilia.[39] However, there is nothing stopping national governments or EU bodies from instituting a similar reporting system for terrorism-related content. Shortly after 11 September 2001, for example, the British domestic Security Service (MI5) took the unprecedented step of posting an appeal for information about potential terrorists on dissident Arab websites. The message, in Arabic, was placed on sites that the authorities knew were accessed by extremists, including Islah.org, a Saudi Arabian opposition site, and Qoqaz.com, a Chechen site that advocated *jihad*. MI5 were hopeful of eliciting information from persons on the margins of extremist groups or communities who were sufficiently shocked by the events of 11 September 2001 to want to contact the agency. The agency had intended to post the message on a further 15 sites known to be accessed by radicals, but many of these were shut down by the FBI in the aftermath of the attacks.

The Role of Private Actors

Legislating for terrorism-related content on the internet is clearly the domain of governments. However, because of the nature of the internet, private companies and groups are never far from the frontlines. In this section, the focus is on actors-other-than-states and their contributions to the effort to eradicate terrorism-related materials from the internet. Two groups, in particular, are focused on here: internet search companies and hacktivists.

Geo-Location Software

One of the properties of the internet is said to be that it overcomes national borders and erodes the principle of sovereignty. In his famous 'Declaration of the Independence of Cyberspace' (1996), John Perry Barlow sent the following message to national governments: 'You are not welcome among us. You have no sovereignty where we gather. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders.'[40] Since Barlow's declaration, there have been many changes, both in terms of the development of the internet and in the wider world. In analyses of internet governance, one of the key arguments frequently advanced was that the decentralised nature of the internet made attempts at censorship redundant. Today, this is in many respects untrue: the internet includes many techniques and technologies that can provide effective control. Having said this, from a technology standpoint, control mechanisms can also be bypassed. In states with government-directed content control, technically-savvy users have found ways around such controls.

Today, it is still difficult to identify exactly who is behind any given computer screen, but it is fairly straightforward to identify through which Internet Service Provider (ISP) the internet was accessed. The latest national laws worldwide require ISPs to identify their users and, if requested, to provide necessary information about them to authorities. Numerous governments have also announced plans to more closely monitor those who access the internet in public places, particularly internet cafes. Increased surveillance of the latter is now taking place in Italy, India, Thailand, and a host of other countries; the explanation generally offered is 'national security'. Interestingly, the more the internet is anchored in geography, the less unique its

governance will be. For example, with the possibility to geographically locate internet users and transactions, the complex question of jurisdiction on the internet can be solved more easily through existing laws.

One technical solution is geo-location software, which filters access to particular internet content according to the national origin of users. The Yahoo! Case was important in this respect, since the group of experts involved indicated that in 90 per cent of cases, Yahoo! would be able to determine whether sections of one of its websites hosting Nazi memorabilia were being accessed from France. This technological assessment helped the court to come to a final decision. Geo-location software companies claim that they can currently identify the home country without mistake and the accessing city in about 85 per cent of cases, especially if it is a large city. Such software can therefore help internet content providers filter access according to nationality and thus avoid court cases in foreign jurisdictions.[41]

Content Control Through Search Engines

There are significant differences between the availability and the accessibility of online materials: the fact that particular web-based content is available on the internet does not mean that it can be easily accessed by large numbers of users. The bridge between the end user and web content is usually a search engine. Therefore, if a particular website cannot be found on Google, or another major search engine, its visibility is seriously diminished. It has been widely reported that one of the first instances of censorship through search engines was carried out by the Chinese authorities in conjunction with Google, Inc. If users entered prohibited words into Google, they would lose their IP connectivity for a few minutes. Also, on German and French versions of Google, it is not possible to search for and find websites with Nazi materials. This indicates a certain

level of self-censorship on the part of Google in order to avoid possible court cases. In terms of terrorist websites, many internet companies voluntarily purged sites perceived as terrorist in the wake of 11 September 2001. For example, Yahoo! pulled dozens of sites in the Jihad Web Ring, a coalition of 55 *jihad*-related sites, while Lycos Europe established a 20-person team to monitor its websites for illegal activity and to remove terrorism-related content.[42]

The transition from the hit economy to the link economy, in the late 1990s, meant that an organization's internet reputation no longer depended on its site design, but was rather a product of the organisation's showing in 'reputable' websites.[43] As Rogers points out, the 'chaos' of the internet may be viewed as a product of the lack of source authority in an information free-for-all. However, while search engines such as Google have to some extent resulted in 'a new form of basic Web epistemology' by providing an indication of the status of information according to measurable reputability dynamics as determined by the web,[44] this works less well in terms of searches for terrorist sites as opposed to sites containing more mainstream views. Let's take the example of the New People's Army (NPA), a group operating in the Philippines, which appears on the US State Department's list of Designated Foreign Terrorist Organisations. With some 25,000 pages with something to say about the NPA, all being listed by engines, returning sites with frequent NPA keywords, one might expect that search engines with link authority logics (such as Google) would return www.philippinerevolution.org at the top of the returns. This is not the case, however; instead of the NPA themselves being viewed by internet users as the most reliable source of information about their group, the US government is instead the most frequently consulted source of information about

the organisation, and the same is true of a number of the other groups that appear on the US list (see Table 3).

[table 3]

This brief discussion of search engines and their impact on internet governance illustrates two things. First, major search engines are wont to err on the side of caution when it comes to their operation in 'foreign' jurisdictions and tend to comply with applicable legislation in those states in order to avoid legal challenges. While such policies of compliance can be viewed as political in character and have thus come under fire, particularly from free-speech advocates, the second point is less contentious, as it relates more to search engine architecture than informed political or economic decisions made by internet companies: the basis on which the most popular search engine, Google, operates serves to obscure the websites of many terrorist groups. Clearly, this is unlikely to be a deterrent to persons intent on searching out these sites, but it does prevent the casual surfer from stumbling upon them by accident, thus reducing the audience for such sites.

Hackers and Hacktivists

The events of 11 September 2001 acted as the spur for many private groups and individuals to take to the internet in search of 'terrorist' websites to disrupt. Computer hackers were particularly well placed to engage in this sort of activity. In the immediate aftermath of the attacks, for example, a group calling itself 'The Dispatchers' proclaimed that they would destroy web servers and internet access in Afghanistan and also target nations that support terrorism. The group of 60 people, led by a 21-year-old security worker from Ohio, proceeded to deface hundreds of websites and launch Distributed Denial of Service (DoS) attacks[45] against targets ranging from the Iranian

Ministry of the Interior to the Presidential Palace of Afghanistan. Another group, known as Young Intelligent Hackers Against Terror (YIHAT), claimed in mid-October 2001 to be negotiating with one European and one Asian government to 'legalize' the group's hacking activities in those states. The group's founder, Kim Schmitz, claimed the group had breached the systems of two Arabic banks who had allegedly done business with Osama Bin Laden, although a bank spokesperson denied any penetration had occurred. The group, whose stated mission was to impede the flow of money to terrorists, issued a statement on its website requesting that corporations make their networks available to group members for the purpose of providing the 'electronic equivalent to terrorist training camps'. Later, their public website was taken offline, apparently in response to attacks from other hackers.[46]

Not all hacking groups were supportive of the so-called 'hacking war'. On 14 September 2001, the Chaos Computer Club, an organization of German hackers, called for an end to the protests and for all hackers to cease vigilante actions. A well-known group of computer enthusiasts, known as Cyber Angels, who promote responsible behaviour, also spoke out against the hacking war. They sponsored television advertisements in the US urging hackers to help gather information and intelligence on those who were participating in this hacktivism.[47] In any event, the predicted escalation in hack attacks[48] did not materialize. In the weeks following the attacks, web page defacements were well publicized, but the overall number and sophistication of these remained rather low. One possible reason for the non-escalation of attacks could be that many hackers – particularly those located in the US – were wary of being negatively associated with the events of 11 September 2001 and curbed their activities as a result.

It's never been all plain sailing for terrorist users of the internet, even prior to 11 September 2001. Their homepages have been subject to intermittent DoS and other hack attacks, and there have also been strikes against their ISPs that have resulted in more permanent difficulties. In 1997, for example, an e-mail bombing was conducted against the Institute for Global Communications (IGC),[49] a San Francisco-based ISP, hosting the web pages of the *Euskal Herria* or *Basque Country Journal*, a publication edited by supporters of the Basque group Homeland and Liberty (ETA). The attacks against IGC commenced following the assassination of a popular town councillor in northern Spain by ETA. The protesters wanted the site pulled from the internet. To accomplish this, they bombarded the IGC with thousands of fake e-mails routed through hundreds of different mail relays, spammed IGC staff and customer accounts, clogged their web page with bogus credit card orders, and threatened to employ the same tactics against other organizations using IGC services. IGC pulled the *Euskal Herria* site on 18 July 1997, but not before archiving a copy of the site enabling others to put up mirrors. Shortly thereafter, mirror sites appeared on half a dozen servers on three continents. Despite this, the protesters' e-mail campaign raised fears of a new era of censorship imposed by direct action from anonymous hacktivists. Furthermore, approximately one month after the IGC had pulled the controversial site off its servers, Scotland Yard's Anti-Terrorist Squad shut down Internet Freedom's UK website for hosting the journal. Scotland Yard claimed to be acting against terrorism.[50] The so-called 'cyber-war' that raged between Israelis and Palestinians and their supporters in 2000 was a mere nuisance in comparison with such targeted and sustained campaigns, although more recently, a more sustained targeting of pro-Palestinian and also jihadist websites has emerged.

Since 11 September 2001 a number of web-based organizations have been established to monitor terrorist websites. One of the most well-known of such sites is Internet Haganah,[51] self-described as 'an internet counterinsurgency'. Also prominent is the Washington, D.C.-based Search for International Terrorist Entities (SITE) Institute[52] that, like Internet Haganah, focuses on Muslim terror groups. Clients of SITE's fee-based intelligence service are said to include the FBI, the Office of Homeland Security, and various media organizations. But what are the goals of these private organizations? SITE is a for-profit concern, while Internet Haganah survives on donations and advertising revenue. SITE's co-founder and director, Rita Katz, has commented: 'It is actually to our benefit to have some of these terror sites up and running by US companies. If the servers are in the US, this is to our advantage when it comes to monitoring activities.'[53] Aaron Weisburd, who runs Internet Haganah out of his home in Southern Illinois, says his goal is to keep the extremists moving from address to address: 'The object isn't to silence them – the object is to keep them moving, keep them talking, force them to make mistakes, so we can gather as much information about them as we can, each step of the way.'[54] On the Haganah website, the mark of victory is a little blue graphic of an AK-47 assault rifle, each of which represents another terrorist website put out of commission (at least temporarily). Weisburd's *modus operandi* is to first research a site, he then makes a 'whois' inquiry. If there is evidence of extremism, he contacts the hosting company and urges the host to remove the site from its servers. If successful, Internet Haganah may purchase the domain name so the address can never be used again. Since its inception in 2003, Internet Haganah has taken credit for or claims to have assisted in the shutdown of more than 600 sites it alleges were linked to terrorism.

Information Gathering and Content Control

Thus far, the focus in this chapter has been on the control of content posted online by terrorists and their sympathisers and on the challenges faced by those wishing to regulate such speech. In terms of the terrorism-internet relationship, however, controlling content may include a lot more than simply trying to disrupt or close down extremist websites. One interesting approach is to explore the use of the internet by extremists for information-gathering purposes, and the responses of governments and other actors. Information-gathering is thought to be one of the main uses of the internet for extremists.

These information-gathering activities rely not on the operation of the extremists' own websites, but on the information contributed by others to 'the vast digital library' that is the internet.[55] There are two major issues to be addressed here. The first may be termed 'data mining' and refers to terrorists using the internet to collect and assemble information about specific targeting opportunities.[56] The second issue is 'information-sharing,' which refers to more general online information collection by terrorists.

Data Mining

In January 2003, US Defense Secretary Donald Rumsfeld warned in a directive sent to military units that too much unclassified, but potentially harmful material was appearing on Department of Defense (DoD) websites. Rumsfeld reminded military personnel that an al-Qaida training manual recovered in Afghanistan states: 'Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy.' He went on to say that 'at more than 700 gigabytes, the DoD web-based data makes a vast, readily available source of

information on DoD plans, programs and activities. One must conclude our enemies access DoD websites on a regular basis.'[57]

In addition to information provided by and about the armed forces, the free availability of information on the internet about the location and operation of nuclear reactors and related facilities was of particular concern to public officials post 11 September 2001. Roy Zimmerman, director of the Nuclear Regulatory Commission's (NRC) Office of Nuclear Security and Incident Response, said the 11 September 2001 attacks had highlighted the need to safeguard sensitive information. In the days immediately after the attacks, the NRC took their website off–line altogether. When it was restored weeks later, it had been purged of more than 1,000 sensitive documents. Initially, the agency decided to withhold documents if 'the release would provide clear and significant benefit to a terrorist in planning an attack.' Later, the NRC tightened the restriction, opting to exclude information 'that could be useful or could reasonably be useful to a terrorist'. According to Zimmerman, 'it is currently unlikely that the information on our website would provide significant advantage to assist a terrorist.'[58]

The measures taken by the NRC were not exceptional. According to a report produced by OMB Watch,[59] since 11 September 2001, thousands of documents and tremendous amounts of data have been removed from US government sites. The difficulty, however, is that much of the same information remains available on private-sector websites.[60] Patrick Tibbetts points to the Animated Software Company's website, which has off-topic documents containing the locations, status, security procedures, and other technical information concerning dozens of US nuclear reactors,[61] while the Virtual Nuclear Tourist site contains similar information. The latter site is particularly detailed on specific security measures that may be implemented at various nuclear

plants worldwide.[62] Many people view such information as a potential gold mine for terrorists.[63] Their fears appear well founded given the capture of al-Qaida computer expert Muhammad Naeem Noor Khan in Pakistan in July 2004, which yielded a computer filled with photographs and floor diagrams of buildings in the US that terrorists may have been planning to attack.[64] The Australian press has also reported that a man charged with terrorism offences there had used Australian government websites to get maps, data, and satellite images of potential targets.[65]

Terrorists can also use the internet to learn about anti-terrorism measures. Gabriel Weimann suggests that a simple strategy like conducting word searches of online newspapers and journals could allow a terrorist to study the means designed to counter attacks, or the vulnerabilities of these measures. Weimann provides the example of newspaper articles detailing attempts to slip contraband items through airport security. He mentions a report, which noted that at Cincinnati airport, contraband slipped through over fifty per cent of the time. 'A simple Internet search by terrorists would uncover this shortcoming, and offer the terrorists an embarkation point for their next operation.'[66] A number of authors have also lambasted reports on various online news sites which noted that US law enforcement agencies were tracing calls made overseas to Al Qaida cells using phone cards, cell phones, phone booths, or internet-based phone services. These authors were concerned that exposing the targeting techniques of law enforcement agencies would allow the terrorists to alter their operating procedures accordingly.[67]

Sharing Information

Policymakers, law enforcement agencies, and others are also concerned about the proliferation of 'how to' web pages devoted to explaining, for example, the technical intricacies of making homemade bombs. Many such devices may be constructed using

lethal combinations of otherwise innocuous materials; today, there are hundreds of freely available online manuals containing such information. As early as April 1997, the US Department of Justice had concluded that the availability of this information played a significant role in facilitating terrorist and other criminal acts:

> It is readily apparent from our cursory examination that anyone interested in manufacturing a bomb, dangerous weapon or weapon of mass destruction can easily obtain detailed instructions for fabricating and using such a device. Available sources include not only publications from the so called underground press but also manuals written for legitimate purposes, such as military, agricultural, industrial and engineering purposes. Such information is *also readily available to anyone with access to a home computer equipped with a modem* [italics mine].[68]

Jessica Stern provides details of one such manual, *Bacteriological Warfare: A Major Threat to North America* (1995), which is described on the internet as a book for helping readers survive a biological weapons attack and is subtitled 'What Your Family Can Do Before and After.' However, it also describes the reproduction and growth of biological agents and includes a chapter entitled 'Bacteria Likely To Be Used By the Terrorist.' The text is available for download, in various edited and condensed formats, from a number of sites,[69] while hard copies of the book are available for purchase over the internet from major online book sellers for as little as US$13. Its author is one Larry Wayne Harris, a microbiologist and former neo-Nazi who at one time purchased three vials of the bacterium that causes bubonic plague.[70]

More recently, an al-Qaida laptop found in Afghanistan had been used to visit the website of the French Anonymous Society (FAS) on several occasions. The FAS site publishes a two-volume *Sabotage Handbook* that contains sections on planning an assassination and anti-surveillance methods, amongst other resources.[71] Another manual, *The Mujahadeen Poisons Handbook* (1996), authored by Abdel-Aziz, is

available via the Hamas-Palestinian Information Center's Arabic-language website. The 'handbook' details in 23 pages how to prepare various homemade poisons, poisonous gases, and other deadly materials for use in terrorist attacks. A much larger manual, nicknamed *The Encyclopedia of Jihad* and prepared by al-Qaida, runs to thousands of pages; distributed via the internet, it offers detailed instructions on how to establish an underground organization and execute terror attacks.[72] Further, BBC News reported that at least one jihadist website had posted careful instructions on how to use mobile phones as detonators for explosives prior to the Madrid train bombings in 2004, the perpetrators of which subsequently employed this method of detonation (Corera 2004).

This kind of information is sought out not just by sophisticated terrorist organizations, but also by disaffected individuals prepared to use terrorist tactics to advance their idiosyncratic agendas. In 1999, for instance, right-wing extremist David Copeland planted nail bombs in three different areas of London: multiracial Brixton, the largely Bangladeshi community of Brick Lane, and the gay quarter in Soho. Over the course of three weeks, he killed three people and injured 139. At his trial, he revealed that he had learned his deadly techniques from the internet by downloading copies of *The Terrorist's Handbook* and *How to Make Bombs: Book Two.* Both titles are still easily accessible.[73] According to the US Bureau of Alcohol, Tobacco, and Firearms, federal agents investigating at least 30 bombings and four attempted bombings between 1985 and June 1996 recovered bomb-making literature that the suspects had obtained from the internet. None of these were terrorism-related, but many involved minors.[74]

Gabriel Weimann provides the example of a further deadly bomb attack, which occurred in Finland in 2002, and was also carried out by a minor. The brilliant chemistry student, who called himself RC, spent months discussing bomb-making

techniques with other enthusiasts on a Finnish website devoted to bombs and explosives. RC posted numerous queries on topics like manufacturing nerve gas at home. And he often traded information with the site's moderator, who used the screen name Einstein and whose postings carried a picture of his own face superimposed on Osama bin Laden's body, complete with turban and beard. Then RC exploded a bomb that killed seven people, including himself, in a crowded Finnish shopping mall. The site's sponsor, a computer magazine called *Mikrobitti*, immediately shut down the website used by RC, known as the Home Chemistry Forum. However, a backup copy, with postings by teenagers who used aliases like Ice Man and Lord of Fire, was immediately reposted, on a read-only basis.[75]

The Open Source Threat?

The threat posed by the easy availability of bomb-making and other 'dangerous information' is a source of heated debate. Patrick Tibbetts warns against underestimating the feasibility of such threats. He points out that captured al-Qaida materials include not only information compiled on 'home-grown explosives', but also indicate that this group is actively seeking out the data and technical expertise necessary to pursue chemical, biological, radiological, and nuclear (CBRN) weapons programs. According to Ken Katzman, a terrorism analyst for the Congressional Research Service, much of the material in these captured documents was probably downloaded from the internet.[76] As a result, many have called for laws restricting the publication of bomb-making instructions on the internet, while others have pointed out that this material is already easily accessible in bookstores and libraries.[77] In fact, much of this information has been available in print media since at least the late 1960s with the publication of William Powell's *The Anarchist Cookbook* and other, similar titles.

Jessica Stern has observed: 'In 1982, the year of the first widely reported incident of tampering with pharmaceuticals, the Tylenol case, only a few poisoning manuals were available, and they were relatively hard to find.'[78] This is doubtless true; they were hard to find, but they *were* available. As Stern herself concedes, currently, how-to manuals on producing chemical and biological agents are not just available on the internet, but are advertised in paramilitary journals sold in magazine shops all over the US.[79] According to a US government report, over 50 publications describing the fabrication of explosives and destructive devices are listed in the Library of Congress and are available to any member of the public, as well as being easily available commercially.[80]

Despite assertions to the contrary,[81] the infamous *Anarchist Cookbook* (1971) is not available online, although it is easily purchased from online retailers. According to Ken Shirriff, author of 'The Anarchist Cookbook FAQ,' there are various files available on the internet that rip off the name 'Anarchist Cookbook' and have somewhat similar content, but are not the real *Anarchist Cookbook*. There are other files that do contain parts of the content from the original *Anarchist Cookbook*, often mixed with other material, but the entire unedited publication is not available online. The original author, William Powell, had this to say in 2001: 'I conducted the research for the manuscript on my own, primarily at the New York City Public Library. Most of the contents were gleaned from Military and Special Forces Manuals.'[82] The anonymous authors of websites claiming to post the *Cookbook* and similar texts often include a disclaimer that the processes described should not be carried out. This is because many of the 'recipes' have a poor reputation for reliability and safety. One author points out that at least one

of the recipes for poison gas contained in *The Mujahadeen Poison Handbook* was nothing more than the standard procedure for making a stink bomb.[83]

In terms of obtaining information about the construction of CBRN weapons from the internet, it is generally agreed that much of this type of information is also flawed, while some is, in fact, pure imagination. Although some relatively accurate information on the construction of such weapons *is* available online, raw data on such a process is not particularly valuable. Putting together a terrorist operation requires elaborate planning, as demonstrated by the 11 September 2001 hijackers. Organizations with the structure and control over their members required for such planning might also be expected to have the resources for developing and distributing their own proprietary tactical materials. As, indeed, al-Qaida has done.[84] However, even when a terrorist outfit draws inspiration and data from materials published on the internet, these materials often duplicate other materials already available in other public fora. In addition, while on the surface, information about scientific processes may be more technical than information regarding terrorist tactics, the same analysis ultimately applies. Actually utilizing a formula for poison gas or a nuclear device, for example, requires not only the cultivation of a body of knowledge and professional judgment, but also the financial resources to build and maintain a physical plant for the manufacture and distribution of the weapon. Developing the expertise and the infrastructure to exploit the information gathered thus demands a significant investment of time and money. Individuals with sufficient skills and resources to exploit the information are unlikely to need the published formula to carry out their plans. Similarly, persons lacking such expertise cannot benefit from the information even when it is published on the internet or elsewhere. The upshot of this is that attempts to stop the flow of ‘harmful’ information

have no useful purpose and would, in any case, doubtless inspire what Peter Margulies has termed ‘an endless virtual fun-house of mirror sites.’[85]

Perhaps the most likely online ‘recipes’ to be of use to terrorists are those related to hacking tools and activities. Such information is also likely to be considerably more accurate than bomb-making information, for example; this is because the internet is both the domain and tool of hackers. In testimony before the US House Armed Services Committee in 2003, Purdue University professor and information assurance expert Eugene Spafford said that bulletin boards and discussion lists could teach hacking techniques to anyone: ‘We have perhaps a virtual worldwide training camp,’ he testified.[86] Terrorists have been known to exploit this resource. In 1998, Khalid Ibrahim, who identified himself as an Indian national, sought classified and unclassified US government software and information, as well as data from India's Bhabha Atomic Research Center, from hackers communicating via Internet Relay Chat (IRC). In conversations taken from IRC logs, Ibrahim claimed to be a member of Harkat-ul-Ansar,[87] a militant Kashmiri separatist group. Confirming Ibrahim's true identity was difficult; the most compelling evidence that he was acting on behalf of Harkat-ul-Ansar was a US$1,000 money order he sent to a teenage hacker in the US in an attempt to buy stolen military software. Although he used several anonymous Hotmail accounts to send his e-mails, Ibrahim always accessed the web from an internet service provider in New Delhi. He approached members of various cracking teams looking for sensitive information. In one transcript of an internet chat conversation between Ibrahim and crackers, Ibrahim threatens to have the youths killed if they reported him to the FBI. In the event, it appears that almost all of Ibrahim's efforts to buy information were rebuffed.[88]

Finally, it is important to keep in mind that removal of technical information from public websites is no guarantee of safeguarding it. In essence, this effort is akin to 'closing the barn door after the horse has bolted'. Intelligence and technical data obtained by terrorist operatives prior to 11 September 2001 can be archived, stored, and distributed surreptitiously irrespective of government or private attempts to squelch its presence on the internet in 2006. Indeed, these materials can be loaded onto offshore or other international web servers that cannot be affected by US legislation, rendering futile any attempt to halt their spread outside the reach of US law enforcement.[89] This point is made in a recent RAND report whose authors believe that the threat posed by open-source data is small. The 2004 report advises that federal officials should consider reopening public access to about three dozen websites withdrawn from the internet after the 11 September 2001 attacks because the sites pose little or no risk to US national security. Baker *et al* report that the overwhelming majority of federal websites that reveal information about airports, power plants, military bases, and other potential terrorist targets need not be censored because similar or better information is easily available elsewhere. RAND's National Defense Research Institute identified 629 internet-accessible federal databases that contain critical data about specific locations. The study, conducted between mid-2002 and mid-2003, found no federal sites that contained information a terrorist would need to launch an attack. It identified four databases where restricting access probably would enhance national security; none remain available to the public. These included two websites devoted to pipelines, one to nuclear reactors, and one to dams. The researchers recommended that officials evaluate 66 databases with some useful information, but they did not anticipate restrictions would be needed, because similar or better data could be easily obtained elsewhere.[90]

Conclusion: Where Do We Go From Here?

What is the future of the internet? It is generally agreed that it is difficult to predict outcomes for the internet because of the complicated relationships between secrecy and openness, security and insecurity, freedom and oppression, the public and the private, the individual and the community, etc. It is commonly agreed also that the potential for a 'digital 9/11' in the near future is not great. This does not mean that IR scholars may continue to ignore the transformative powers of the internet. On the contrary, as of 11 September 2001, the internet has come of age. Both terrorism and the internet are significant global phenomena, reflecting and shaping various aspects of world politics (sometimes separately but oftentimes in unison). Due to its global reach and rich multilingual context, the internet has the potential to influence in manifold ways many different types of political and social relations. Unlike the traditional mass media, the internet's open architecture has restricted efforts by governments to regulate internet activities, which, in turn, has provided Netizens with immense freedom and space to shape the internet in their own likeness: a patchwork of peoples, ideas, hierarchies, ideologies, images, etc.

In large part, internet users learn by doing. Once users figure out what the Net is good for – donating to charity, disseminating information, communicating securely, etc. – on their own terms, they quickly begin to develop new uses, and the volume and sophistication of traffic on the internet is increased. This, in turn, contributes to an unprecedented independence on the part of the users as information gatherers and producers. Included within this cohort are terrorists who are not limiting themselves to the traditional means of communication; they increasingly employ the new media to pursue their goals. The terrorists of today, like those of yesteryear, are keen to exploit

the traditional mass media while also recognizing the value of more direct communication channels. As has been pointed out, 'if what matters is openness in the marketplace of ideas […] then the Web delivers an equal opportunity soapbox' (Norris 2001, 172).

As far back as 1982, Alex Schmid and Janny De Graaf conceded that

> If terrorists want to send a message, they should be offered the opportunity to do so without them having to bomb and kill. Words are cheaper than lives. The public will not be instilled with terror if they see a terrorist speak; they are afraid if they see his victims and not himself […] If the terrorists believe that they have a case, they will be eager to present it to the public. Democratic societies should not be afraid of this.[91]

Not everybody is in agreement with this position, however. Over time, both state- and non-state actors have endeavoured to curb the availability of terrorism-related materials online with varying degrees of success. Authoritarian governments have met with some success in this regard by deploying technologies that constrain their citizens' ability to access certain sites. There are fewer options for restriction available to democratic governments, however, and although more restrictive legislation has recently been promulgated in a number of jurisdictions, it is not yet clear that it will be any more successful than previous attempts at controlling, for example, cyber-hate. In terms of terrorist websites, however, those private initiatives instituted by a range of sub-state actors in conjunction with ISPs have been much more successful. The activities of individual hacktivists, such as Aaron Weisburd of Internet Haganah, raise a number of important issues relating to limits on speech and who has the ability to institute these limits, however. These same limits and their efficacy are also central to the discussion on removing of information from the public internet, whether about bomb-making or computer hacking, that could be deemed of use to terrorists. The ability of private

political and economic actors to bypass the democratic process and to have materials they find politically objectionable erased from the internet is a matter for concern, as is the removal by government agencies of information that was previously publicly accessible online. Such endeavours may, in fact, cause us to think again about the matter of legislation, not just in terms of putting controls in place – perhaps, for example, outlawing the posting and dissemination of beheading videos – but also writing into law more robust protections for radical political speech.

Notes

[1] Eva Gross and Alvaro Mendéz, 'Editorial Note', *Millennium*, 32/3 (2003): iii.

[2] Gross and Méndez, 'Editorial Note'.

[3] Dorothy Denning, 'Is Cyber Terror Next?' in Craig Calhoun, Paul Price, and Ashley Timmer (eds), *Understanding September 11* (New York, 2001).

[4] James Der Derian, 'The Question of Information Technology in International Relations', *Millennium*, 32/3 (2003): 441-456.

[5] Eduardo Gelbstein and Jovan Kurbalija, *Internet Governance: Issues, Actors and Divides* (Geneva, 2005), p. 8.

[6] Hans Klein, 'ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy', *The Information Society*, 18/3 (2002): 201.

[7] See World Summit on the Information Society, *WSIS Plan of Action*, WSIS-03/GENEVA/DOC/5-E (Geneva, 2003), section 13b, <http://www.itu.int/wsis/docs/geneva/official/poa.html>, accessed 19 February 2007.

[8] Gelbstein and Kurbalija, p. 11.

[9] Klein, 'ICANN and Internet Governance': 194-195.

[10] Working Group on Internet Governance (WGIG), *Report of the Working Group on Internet Governance* (Château de Bossey, 2005), p. 4.

[11] Mark M. Pollitt, 'Cyberterrorism: Fact or Fancy?' *Computer Fraud and Security* (February 1998): 8-10, here 9.

[12] See Maura Conway, 'What is Cyberterrorism? The Story So Far', *Journal of Information Warfare*, 2/2 (2003): 34-35.

[13] Neal A. Pollard, 'Indications and Warning of Infrastructure Attack', in Lars Nicander and Magnus Ranstorp (eds), *Terrorism in the Information Age: New Frontiers?* (Stockholm, 2004), p. 43.

[14] Paul Eedle, 'Al Qaeda's Super-Weapon: The Internet', paper presented at the conference *Al-Qaeda 2.0: Transnational Terrorism After 9/11*, Washington, D.C., 1-2 December 2004.

[15] Ibid.

[16] For an exploration of Hizbollah's internet presence, see Maura Conway, 'Cybercortical Warfare: Hizbollah's Internet Strategy', in Sarah Oates, Diana Owen, and Rachel Gibson (eds), *The Internet and Politics: Citizens, Voters and Activists* (London, 2005), pp. 100-117; an analysis of the LTTE's websites is contained in Shyam Tekwani's 'The Tamil Diaspora, Tamil Militancy, and the Internet', in K.C. Ho, Randolph Kluver, and Kenneth C.C. Yang (eds), *Asia.Com: Asia Encounters the Internet* (London, 2003). A comparative analysis of a number of English-language terrorist websites is to be found in Maura Conway, 'Terrorist Web Sites: Their Contents, Functioning, and Effectiveness', in Philip Seib (ed.), *Media and Conflict in the Twenty-First Century* (New York, 2005), pp. 185-215.

[17] For a general introduction to the legal protection of speech in the US, UK, and elsewhere, see Eric Barendt's *Freedom of Speech* (Oxford, 1987).

[18] The full text of the Additional Protocol to the Convention on Cybercrime is accessible online at <http://conventions.coe.int/Treaty/EN/Treaties/Html/189.htm> (accessed 19 February 2007).

[19] Yaman Akdeniz, *Stocktaking on Efforts to Combat Racism on the Internet* (Geneva, 2006), pp. 10-11.

[20] Jay Lyman, 'Terrorist Web Site Hosted by US Firm', *NewsFactor Network*, 3 April 2002, <http://www.newsfactor.com/perl/story/17079.html>, accessed 19 February 2007.

[21] Robert Collier, 'Terrorists Get Web Sites Courtesy of US Universities', *San Francisco Chronicle*, 9 May 1997. The site hosted by UCSD was at <http://burn.ucsd.edu/~ats/mrta.htm>, but is no longer operational; however the official homepage of the MRTA (in Europe) may still be accessed at <http://www.voz-rebelde.de> (accessed 19 February 2007).

[22] W. Sean McLaughlin, 'The Use of the Internet for Political Action by Non-State Dissident Actors in the Middle East', *First Monday*, 8/11 (2003): 9.

[23] For an account of China's Internet content policy, see Charles Li's 'Internet Content Control in China', *International Journal of Communications Law and Policy*, 8 (Winter 2003/04); W. Sean McLoughlin discusses Saudi Arabia's approach in 'The Use of the Internet for Political Action', while Singapore's policy is discussed in Gary Rodan's 'The Internet and Political Control in Singapore', *Political Science Quarterly*, 113/1 (1998): 63-89.

[24] On the Australian position, see Carolyn Penfold, 'Nazis, Porn, and Politics: Asserting Control Over Internet Content', *JILT: The Journal of Information Law and Technology*, 2 (2001), while links to documents related to the German decision may be accessed via Robert W. Smith, 'Administrative Court in Düsseldorf Affirms Blocking Order in North Rhine-Westphalia', *Heise Online*, 15 June 2005, <http://www.heise.de/english/newsticker/news/60662>, accessed 19 February 2007.

[25] See Marie Eneman, 'The New Face of Child Pornography', in Mathias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (London, 2005), pp. 27-40; also Akdeniz, pp. 8-9.

[26] For a discussion of the situation in Asia see, for example, Ida M. Azmi, 'Content Regulation in Malaysia: Unleashing Missiles on Dangerous Web Sites', *JILT: Journal of Information Law and Technology*, 3 (2004), while the Middle East situation is explored in Gary E. Burkhart and Susan Older, *The Information Revolution in the Middle East and North Africa* (Santa Monica, 2003) and in Marcus Franda, *Launching Into Cyberspace: Internet Development and Politics in Five World Regions* (Boulder, 2002), chapter 3.

[27] Commission of the European Union, *Proposal for a Council Framework Decision on Combating Racism and Xenophobia* (Brussels, 2001), pp. 6 and 8.

[28] Gelbstein and Kurbalija, pp. 127-128; Akdeniz, pp. 3-4 and 11.

[29] Ian Cobain, 'FBI Closes Website Linked to Real IRA', *The Times* (London), 8 October 2001: 8.

[30] Janet Kornblum, 'Radical Radio Shows Forced from the Net', *USA Today*, 25 October 2001: 3D, <http://www.usatoday.com/tech/news/2001/10/16/ebrief.htm>, accessed 19 February 2007. Lewis was formerly Grandpa on the 1960s hit TV show 'The Munsters'!

[31] Al Lewis Live can still be heard on Pacifica Radio in the United States. The IRA Radio site was allowed back online in March 2002 at <http://www.iraradio.com>. However, it appears to have closed

down again some time after February 2003. Site archives are available via the Internet Archive. The other sites mentioned remain offline.

[32] Maura Conway, 'Terrorism and the Internet: New Media, New Threat?' *Parliamentary Affairs*, 59/2 (2006): 295-296.

[33] The full text of Clarke's remarks may be accessed online at <http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm050720/debtext/50720-04.htm> (accessed 19 February 2007).

[34] The APCO proposals are outlined in a press release available online at <http://www.acpo.police.uk/asp/news/PRDisplay.asp?PR_GUID={423FD3C2-2791-403A-B5D0-8FC6B5476B0B}> (accessed 19 February 2007).

[35] One of the main reasons suggested for the former was that suspects needed to be detained without charge for longer than 14 days because of the difficulty and complexity of decrypting computer hard drives, a suggestion which has been challenged by both the UK Intelligence Services Commissioner and the UK Interception of Communications Commissioner.

[36] Conway, 'Terrorism and the Internet'; see also Ian Cram, 'Regulating the Media: Some Neglected Freedom of Expression Issues in the United Kingdom's Counter-Terrorism Strategy', *Terrorism and Political Violence*, 18/2 (2006): 343-348.

[37] The full text of the Act may be viewed at the website of the UK's Office of Public Sector Information <http://www.opsi.gov.uk/acts/acts2006/20060011.htm> (accessed 19 February 2007). See, in particular, Part 1, Section 3, 'Application of ss. 1 and 2 to internet activity, etc'.

[38] See Akdeniz, pp. 18-24.

[39] Ibid., pp. 24-26.

[40] The full text of the Declaration is available online at <http://homes.eff.org/~barlow/Declaration-Final.html> (accessed 19 February 2007).

[41] Gelbstein and Kurbalija, p. 125.

[42] Stephanie Gruner and Gautam Naik, 'Extremist Sites Under Heightened Scrutiny', *The Wall Street Journal Online*, 8 October 2001; Julia Scheeres, 'Blacklisted Groups Visible on Web', *Wired News*, 19 October 2001.

[43] Robert Rogers, 'Operating Issue Networks on the Web', *Science as Culture*, 11/2 (2002): 191–214, here 205.

[44] Ibid.: 200.

[45] Distributed Denial of Service (DDoS) attacks are actions by distributed computers that prevent any part of another computer system from functioning in accordance with its intended purpose. DDoS attacks generally employ armies of 'zombie' machines taken over and controlled by a single master to overwhelm the resources of a target with floods of packets.

[46] Denning, 'Is Cyber Terror Next?' The site was located at <http://www.kill.net>.

[47] C. Hauss and A. Samuel, 'What's the Internet Got to Do With It? Online Responses to 9/11', paper presented at the American Political Science Association Annual (APSA) Annual Convention, Boston, 29 September - 1 August 2002; National Infrastructure Protection Center, *Cyber Protests Related to the War on Terrorism: The Current Threat* (Washington, D.C., 2001).

[48] Institute for Security Technology Studies (ISTS), *Cyber Attacks During the War on Terrorism: A Predictive Analysis* (Dartmouth College, 2001).

[49] Online at <http://www.igc.org/igc/gateway/index.html> (accessed 19 February 2007).

[50] Dorothy Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, 2001), pp. 239-288, here pp. 270-71. For more information on the e-mail bombing and IGC's response to it see the institute's website <http://www.igc.apc.org> (accessed 19 February 2007). See also the press release issued by Internet Freedom UK in response to the shutting of their operations by Scotland Yard at <http://www.fitug.de/debate/9709/msg00018.html> (accessed 19 February 2007). The group's website is located at <http://www.netfreedom.org/> (accessed 19 February 2007).

[51] In Hebrew, 'Haganah' means defence. Internet Haganah is online at <http://www.haganah.org.il/haganah/index.html> (accessed 19 February 2007).

[52] The SITE website is at <http://www.siteinstitute.org/> (accessed 19 February 2007).

[53] As quoted in John Lasker, 'Watchdogs Sniff Out Terror Sites', *Wired News*, 25 February 2005.

[54] Ibid.; see also Gary Bunt, *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments* (London, 2003), pp. 24 and 93.

[55] Gabriel Weimann, *WWW.terror.net: How Modern Terrorism Uses the Internet* (Washington, D.C., 2004), p. 6.

[56] Others exploring terrorist use of the Net have employed the term 'data mining' in a less expansive fashion to refer to the systematized analysis of large bodies of data using specialist computer software. For an introduction to the latter, see Mary De Rosa, *Data Mining and Data Analysis for Counterterrorism*. (Washington, D.C., 2004), <http://www.csis.org/tech/2004_counterterrorism.pdf>, accessed 22 March 2007.

[57] Declan McCullagh, 'Military Worried About Web Leaks', *CNET News*, 16 January 2003.

[58] Mike M. Ahlers, 'Blueprints for Terrorists?' *CNN.com*, 19 November 2004.

[59] Office of Management and Budget (OMB) Watch is a watchdog group based in Washington, D.C. Their home page is at <http://www.ombwatch.org> (accessed 19 February 2007).

[60] McCullagh; Gary D. Bass, and Sean Moulton, 'The Bush Administration's Secrecy Policy: A Call to Action to Protect Democratic Values', working paper (Washington, D.C., 2002).

[61] See <http://www.animatedsoftware.com/environm/no_nukes/nukelist1.htm> (accessed 19 February 2007).

[62] Patrick S. Tibbetts, 'Terrorist Use of the Internet and Related Information Technologies', unpublished paper (Fort Leavenworth, 2002), p. 15. The Nuclear Tourist website is at <http://www.nucleartourist.com/> (accessed 19 February 2007).

[63] See chapter six of Dan Verton's *Black Ice* (New York, 2003), which is entitled 'Web of Terror: What al-Qaeda Knows About the US'; it provides a wide-ranging, though somewhat breathless, survey of the potential dangers posed by Web-based information.

[64] David Jehl and Douglas Johnston., 'Reports That Led to Terror Alert Were Years Old, Officials Say', *New York Times*, 3 August 2004; Dan Verton and Lucas Mearian, 'Online Data a Gold Mine for Terrorists', *ComputerWorld*, 6 August 2004.

[65] Australian Broadcasting Corporation (ABC), 'NSW Considers Limits on Government Website', *ABC Online*, 28 April 2004.

[66] Gabriel Weimann, 'Terror on the Internet: The New Arena, the New Challenges', paper presented at the annual meeting of the International Studies Association (ISA), Montreal, Canada, 17 March 2004, p. 15. <http://archive.allacademic.com/publication/prol_index.php> (accessed 19 February 2007).

[67] Christopher Andrew, 'Counsel of War', *The Times* (T2 Supplement), 4 October 2001: 2-3; Timothy L. Thomas, 'Al Qaeda and the Internet: The Danger of '"Cyberplanning"', *Parameters*, Spring (2003): 114; Weimann, 'Terror on the Internet', p. 15.

[68] US Department of Justice, *Report On The Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Federal Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent With the First Amendment to the United States Constitution* (Washington, D.C., 1997), pp. 15-16.

[69] See, for example, <http://www.uhuh.com/reports/harris/book.htm> (accessed 19 February 2007).

[70] Jessica Stern, *The Ultimate Terrorists* (Cambridge, 1999), p. 51.

[71] Thomas, 'Al Qaeda and the Internet: 115; Weimann, *WWW.terror.net*, p. 9. The two-volume handbook is available for download from a number of Internet sites including <http://sabotage.org/handbook/> (accessed 19 February 2007).

[72] Weimann, *WWW.terror.net*, p. 9; see also Rodney A. Smolla, 'From Hit Man to Encyclopaedia of Jihad: How to Distinguish Freedom of Speech from Terrorist Training', *Loyola Entertainment Law Review*, 22/2 (2002).

[73] Weimann, *WWW.terror.net*, p. 10.

[74] Anti-Defamation League (ADL), 'Terrorist Activities on the Internet', *Terrorism Update* (Winter 1998).

[75] Weimann, 'Terror on the Internet': 15.

[76] Tibbetts, 'Terrorist Use of the Internet and Related Information Technologies', p. 17.

[77] ADL, 'Terrorist Activities on the Internet'.

[78] Stern, p. 50.

[79] Ibid., p. 51.

[80] US Department of Justice, *Report On The Availability of Bombmaking Information*, p. 5. The same report mentions that one Kansas bomber got his bomb instructions from the August 1993 *Reader's Digest* (pp. 6-7).

[81] See, for example, Weimann's *WWW.terror.net*, p. 9.

[82] Ken Shirriff, *Anarchist Cookbook FAQ* <http://www.righto.com/anarchy/>, accessed 19 February 2007.

[83] George Smith, 'The Recipe for Ricin, Part II: The Legend Flourishes', *National Security Notes*, 4 March 2004. See also George Smith, 'The Recipe for Ricin: Examining the Legend', *National Security Notes*, 20 February 2004.

[84] Portions of an Al Qaeda Training Manual are available via the Federation of American Scientists site at <http://www.fas.org/irp/world/para/manualpart1.html>, accessed 22 March 2007.

[85] Peter Margulies, 'The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment', *UCLA Journal of Law and Technology*, 8/2 (2004): 74-76.

[86] Eugene Spafford, *Testimony before the US House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities*, 24 July 2003, p. 31.

[87] Harkat-ul-Ansar is on the State Department's list of FTOs.

[88] Niall McKay, 'Do Terrorists Troll the Net?' *Wired*, 4 November 1998.

[89] Tibbetts, 'Terrorist Use of the Internet and Related Information Technologies', p. 17.

[90] John C. Baker et al., *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information* (Santa Monica, 2004); John C. Baker et al., 'America's Publicly Available Geospatial Information: Does It Pose a Homeland Security Risk?' *Rand Research Brief*, RB-9045-NGA (2004).

[91] Alex P. Schmid and Janny De Graaf, *Violence as Communication: Insurgent Terrorism and the Western News Media* (London, 1982), p. 170.

Bibliography

Ahlers, Mike M., 'Blueprints for Terrorists?' *CNN.com*, 19 November 2004, <http://www.cnn.com/2004/US/10/19/terror.nrc/>, accessed 19 February 2007.

Akdeniz, Yaman, *Stocktaking on Efforts to Combat Racism on the Internet*, E/CN.4/2006/WG.21/BP.1 (Geneva: UN Commission on Human Rights, 2006), <http://www.cyber-rights.org/reports/ya_un_paper_int_06.pdf>, accessed 19 February 2007.

Andrew, Christopher, 'Counsel of War', *The Times* (T2 Supplement), 4 October 2001.

Anti-Defamation League (ADL), 'Terrorist Activities on the Internet.' *Terrorism Update* (Winter 1998), <http://www.adl.org/Terror/focus/16_focus_a.asp>, accessed 19 February 2007.

Australian Broadcasting Corporation (ABC), 'NSW Considers Limits on Government Website', *ABC Online*, 28 April 2004.

Azmi, Ida M., 'Content Regulation in Malaysia: Unleashing Missiles on Dangerous Web Sites', *JILT: Journal of Information Law and Technology*, 3 (2004), <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/azmi/>, accessed 19 February 2007.

Baker, John C. et al., *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information* (Santa Monica: Rand, 2004), <http://www.rand.org/publications/MG/MG142/>, accessed 19 February 2007.

Baker, John C. et al., 'America's Publicly Available Geospatial Information: Does It Pose a Homeland Security Risk?' *Rand Research Brief* RB-9045-NGA (2004), <http://www.rand.org/publications/RB/RB9045/>, accessed 19 February 2007.

Barendt, Eric, *Freedom of Speech* (Oxford: Clarendon Press, 1987).

Bass, Gary D. and Sean Moulton, 'The Bush Administration's Secrecy Policy: A Call to Action to Protect Democratic Values', working paper (Washington, D.C.: OMB Watch, 2002), <http://www.ombwatch.org/rtk/secrecy.pdf>, accessed 19 February 2007.

Bunt, Gary, *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments* (London: Pluto Press, 2003).

Burkhart, Gary E. and Susan Older, *The Information Revolution in the Middle East and North Africa* (Santa Monica: Rand, 2003), <http://www.rand.org/publications/MR/MR1653/MR1653.pdf>, accessed 19 February 2007.

Cobain, Ian, 'FBI Closes Website Linked to Real IRA', *The Times* (London), 8 October 2001: 8.

Collier, Robert, 'Terrorists Get Web Sites Courtesy of US Universities', *San Francisco Chronicle*, 9 May 1997.

Commission of the European Union, *Proposal for a Council Framework Decision on Combating Racism and Xenophobia* (Brussels: European Commission, 2001), <http://europa.eu.int/eur-lex/en/com/pdf/2001/com2001_0664en01.pdf>, accessed 19 February 2007.

Conway, Maura, 'Terrorism and the Internet: New Media, New Threat?' *Parliamentary Affairs*, 59/2 (2006): 1-16.

Conway, Maura, 'Terrorist Web Sites: Their Contents, Functioning, and Effectiveness', in Philip Seib (ed.), *Media and Conflict in the Twenty-First Century* (New York: Palgrave, 2005), pp. 185-215.

Conway, Maura, 'Cybercortical Warfare: Hizbollah's Internet Strategy', in Sarah Oates, Diana Owen and Rachel Gibson (eds), *The Internet and Politics: Citizens, Voters and Activists* (London: Routledge, 2005), pp. 100-117.

Conway, Maura, 'What is Cyberterrorism? The Story So Far,' *Journal of Information Warfare*, 2/2 (2003): 33-42.

Corera, Gordon, 'A Web Wise Terror Network', *BBC News* (World Edition), 6 October 2004, <http://news.bbc.co.uk/2/hi/in_depth/3716908.stm>, accessed 19 February 2007.

Cram, Ian, 'Regulating the Media: Some Neglected Freedom of Expression Issues in the United Kingdom's Counter-Terrorism Strategy', *Terrorism and Political Violence*, 18/2 (2006): 335-355.

Dahl, Robert A., *Democracy and Its Critics* (New Haven, CT: Yale University Press, 1989).

Denning, Dorothy, 'Is Cyber Terror Next?' in Craig Calhoun, Paul Price, and Ashley Timmer (eds), *Understanding September 11* (New York: New Press, 2001), <http://www.ssrc.org/sept11/essays/denning.htm>, accessed 19 February 2007.

Denning, Dorothy, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: Rand, 2001), pp. 239-288,

<http://www.rand.org/publications/MR/MR1382/MR1382.ch8.pdf>, accessed 19 February 2007.

Der Derian, James, 'The Question of Information Technology in International Relations', *Millennium*, 32/3 (2003): 441-56.

De Rosa, Mary, Data Mining and Data Analysis for Counterterrorism (Washington DC: Center for Strategic and International Studies), <http://www.csis.org/tech/2004_counterterrorism.pdf>, accessed 22 March 2007.

Eedle, Paul, 'Al Qaeda's Super-Weapon: The Internet', paper presented at the conference *Al-Qaeda 2.0: Transnational Terrorism After 9/11*, New America Foundation, Washington, D.C., 1-2 December 2004, <http://www.outtherenews.com/modules.php?op=modload&name=News&file=article&sid=89&topic=7>, accessed 19 February 2007.

Eneman, Marie, 'The New Face of Child Pornography', in Mathias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (London: Glasshouse Press, 2005).

Franda, Marcus, *Launching Into Cyberspace: Internet Development and Politics in Five World Regions* (Boulder and London: Lynne Rienner, 2002).

Gelbstein, Eduardo and Jovan Kurbalija, *Internet Governance: Issues, Actors and Divides* (Geneva: DiploFoundation, 2005), <http://www.diplomacy.edu/isl/ig/>, accessed 19 February 2007.

Gross, Eva and Alvaro Mendéz, 'Editorial Note', *Millennium*, 32/3 (2003): iii.

Gruner, Stephanie and Gautam Naik, 'Extremist Sites Under Heightened Scrutiny', *The Wall Street Journal Online*, 8 October 2001, <http://zdnet.com.com/2100-1106-530855.html?legacy=zdnn>, accessed 19 February 2007.

Hauss, C. and Samuel, A., 'What's the Internet Got to Do With It? Online Responses to 9/11', paper presented at the American Political Science Association Annual (APSA) Annual Convention, Boston, 29 September - 1 August 2002.

Jehl, David and Douglas Johnston, 'Reports That Led to Terror Alert Were Years Old, Officials Say', *New York Times*, 3 August 2004.

Klein, Hans, 'ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy', *The Information Society*, 18/3 (2002): 193-207.

Kornblum, Janet, 'Radical Radio Shows Forced from the Net', *USA Today*, 25 October 2001.

Lasker, John, 'Watchdogs Sniff Out Terror Sites.' *Wired News*, 25 February 2005, <http://www.wired.com/news/privacy/0,1848,66708,00.html>, accessed 19 February 2007.

Li, Charles, 'Internet Content Control in China', *International Journal of Communications Law and Policy*, 8 (Winter 2003/04), <http://www.ijclp.org/8_2004/pdf/charlesli-paper-ijclp-neu.pdf>, accessed 19 February 2007.

Lyman, Jay, 'Terrorist Web Site Hosted by US Firm', *NewsFactor Network*, 3 April 2002, <http://www.newsfactor.com/perl/story/17079.html>, accessed 19 February 2007.

Margulies, Peter, 'The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment', *UCLA Journal of Law and Technology*, 8/2 (2004), <http://www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf>, accessed 19 February 2007.

McCullagh, Declan, 'Military Worried About Web Leaks', *CNET News*, 16 January 2003, <http://news.com.com/2100-1023-981057.html>, accessed 19 February 2007.

McKay, Niall, 'Do Terrorists Troll the Net?' *Wired*, 4 November 1998, <http://www.wired.com/news/politics/0,1283,15812,00.html>, accessed 19 February 2007.

McLaughlin, W. Sean, 'The Use of the Internet for Political Action by Non-State Dissident Actors in the Middle East', *First Monday*, 8/11 (2003), <http://www.firstmonday.org/issues/issue8_11/mclaughlin/index.html>, accessed 19 February 2007.

National Infrastructure Protection Center, *Cyber Protests Related to the War on Terrorism: The Current Threat* (Washington, D.C.: National Infrastructure Protection Center, 2001), <http://www.iwar.org.uk/cip/resources/nipc/cyberprotestupdate.htm>, accessed 19 February 2007.

Penfold, Carolyn, 'Nazis, Porn, and Politics: Asserting Control Over Internet Content', *JILT: The Journal of Information Law and Technology*, 2 (2001), <http://elj.warwick.ac.uk/jilt/01-2/penfold.html>, accessed 19 February 2007.

Pollard, Neal A., 'Indications and Warning of Infrastructure Attack', in Lars Nicander and Magnus Ranstorp (eds), *Terrorism in the Information Age: New Frontiers?* (Stockholm: National Defence College, 2004).

Pollitt, Mark M., 'Cyberterrorism: Fact or Fancy?' *Computer Fraud and Security*, (February 1998): 8-10.

Powell, William, *The Anarchist Cookbook* (Arkansas: Ozark PR LLC, 2003 [1971]).

Rodan, Garry, 'The Internet and Political Control in Singapore', *Political Science Quarterly*, 113/1 (1998): 63-89.

Rogers, Robert, 'Operating Issue Networks on the Web', *Science as Culture* 11/2 (2002): 191–214.

Scheeres, Julia, 'Blacklisted Groups Visible on Web', *Wired News*, 19 October 2001.

Schmid, Alex P. and Janny De Graaf, *Violence as Communication: Insurgent Terrorism and the Western News Media* (London: Sage, 1982).

Smith, George, 'The Recipe for Ricin: Examining the Legend', *National Security Notes*, 20 February 2004, <http://www.globalsecurity.org/org/nsn/nsn-040220.htm>, accessed 19 February 2007.

Smith, George, 'The Recipe for Ricin, Part II: The Legend Flourishes', *National Security Notes*, 4 March 2004, <http://www.globalsecurity.org/org/nsn/nsn-040304.htm>, accessed 19 February 2007.

Smith, Robert W., 'Administrative Court in Düsseldorf affirms blocking order in North Rhine-Westphalia', *Heise Online*, 15 June 2005, <http://www.heise.de/english/newsticker/news/60662>, accessed 19 February 2007.

Smolla, Rodney A., 'From Hit Man to Encyclopedia of Jihad: How to Distinguish Freedom of Speech from Terrorist Training', *Loyola Entertainment Law Review*, 22/2 (2002), <http://elr.lls.edu/issues/v22-issue2/smolla.pdf>, accessed 19 February 2007.

Spafford, Eugene, *Testimony before the US House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities*, 24 July

2003, <http://commdocs.house.gov/committees/security/has205260.000/has205260_0f.htm>, accessed 19 February 2007.

Stern, Jessica, *The Ultimate Terrorists* (Cambridge: Harvard University Press, 1999).

Tekwani, Shyam, 'The Tamil Diaspora, Tamil Militancy, and the Internet', in K.C. Ho, Randolph Kluver, and Kenneth C.C. Yang (eds), *Asia.Com: Asia Encounters the Internet* (London: Routledge, 2003).

Thomas, Timothy L., 'Al Qaeda and the Internet: The Danger of "Cyberplanning"', *Parameters,* (Spring 2003), <http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.htm>, accessed 19 February 2007.

Tibbetts, Patrick S., 'Terrorist Use of the Internet and Related Information Technologies', unpublished paper (Fort Leavenworth: United States Army Command and General Staff College, 2002), <http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=0&keyfieldvalue=ADA403802&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA403802.pdf>, accessed 19 February 2007.

US Department of Justice, *Report On The Availability of Bombmaking Information, the Extent to Which Its Dissemination Is Controlled by Federal Law, and the Extent to Which Such Dissemination May Be Subject to Regulation Consistent With the First Amendment to the United States Constitution* (Washington, D.C.: US Department of Justice, 1997), <http://cryptome.org/abi.htm>, accessed 19 February 2007.

Verton, Dan and Lucas Mearian, 'Online Data a Gold Mine for Terrorists', *ComputerWorld*, 6 August 2004, <http://www.computerworld.com/securitytopics/security/story/0,10801,95098,00.html>, accessed 19 February 2007.

Verton, Dan, *Black Ice: The Invisible Threat of Cyberterrorism* (New York: McGraw Hill, 2003).

Weimann, Gabriel, *WWW.terror.net: How Modern Terrorism Uses the Internet* (Washington, D.C.: United States Institute of Peace, 2004), <http://www.usip.org/pubs/specialreports/sr116.pdf>, accessed 19 February 2007.

Weimann, Gabriel, 'Terror on the Internet: The New Arena, the New Challenges', paper presented at the annual meeting of the International Studies Association (ISA), Montreal, Canada, 17 March 2004, <http://archive.allacademic.com/publication/prol_index.php>, accessed 19 February 2007.

Working Group on Internet Governance (WGIG), *Report of the Working Group on Internet Governance* (Château de Bossey: WSIS, 2005), <http://www.wgig.org/docs/WGIGREPORT.pdf>, accessed 19 February 2007.

World Summit on the Information Society (WSIS), *WSIS Plan of Action*, WSIS-03/GENEVA/DOC/5-E (Geneva: WSIS, 2003), <http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf>, accessed 19 February 2007.