

# Terrorism & Internet Governance: Core Issues

*Maura Conway*

School of Law & Government  
Dublin City University  
Glasnevin  
Dublin 9  
Ireland

[Maura.conway@dcu.ie](mailto:Maura.conway@dcu.ie)

---

## **Introduction**

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 (hereafter ‘9/11’) and the emergence of the internet in the decade before. Together, however, the events of 9/11 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 9/11, the question on everybody’s lips appears to be ‘is cyber-terrorism next?’ 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.

This paper 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 9/11 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 paper. 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. 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).

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).<sup>1</sup> 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.<sup>2</sup>

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: authority, law, sanctions, and jurisdiction. ‘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].<sup>3</sup> 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.'<sup>4</sup> This does not mean that the four issues identified by Dahl 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**

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'.<sup>5</sup> 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. 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.

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.'<sup>6</sup> 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 discussed '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.

Today, virtually every active militant group has an online presence, and many groups are the subjects of more than one site. 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. Unsurprisingly, in the post-9/11 world, the latter are subject to much increased scrutiny. The remainder of this paper 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. 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. 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 9/11, 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.<sup>7</sup> 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.

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. While sites such as those maintained by Hamas have been subject to more intense scrutiny following the events of 9/11, similar websites had already been the subject of debate in the US even before the events of 9/11. 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.

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. 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. 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.

### *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. 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. 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.'<sup>8</sup> 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.

## **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 9/11 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 9/11, 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.<sup>9</sup> 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 9/11, the most relevant in terms of internet governance is the USA PATRIOT Act of 2001, 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 front organizations operating as charities.

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.

### *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.<sup>10</sup> 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 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. 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.<sup>11</sup> 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. 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. However, there is nothing stopping national governments or EU bodies from instituting a similar reporting system for terrorism-related content.

### **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 hackers.

### *Geo-Location Software*

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.

#### *Content Control By 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. On German and French versions of Google, it is not possible to search for and find websites with Nazi materials, for example. 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 9/11. 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. Basically, 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. However, such policies of compliance can be viewed as political in character and have thus come under fire, particularly from free-speech advocates.

#### *Hackers and Hacktivists*

The events of 9/11 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 proceeded to deface hundreds of websites and launch Distributed Denial of Service (DoS) attacks against targets ranging from the Iranian Ministry of the Interior to the Presidential Palace of Afghanistan. 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. 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 were wary of being negatively associated with the events of 9/11 and curbed their activities as a result.

It's never been all plain sailing for terrorist users of the internet, even prior to 9/11. 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), 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 and IGC eventually removed it from their servers, 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.

Since 9/11 a number of more formal web-based organizations have been established to monitor terrorist websites. One of the most well-known of such sites is Internet Haganah, self-described as 'an internet counterinsurgency'. Also prominent is the Washington, D.C.-based Search for International Terrorist Entities (SITE) Institute 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.'<sup>12</sup> Aaron Weisburd, who runs Internet Haganah, 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.'<sup>13</sup> 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.

## **Conclusion: Where Do We Go From Here?**

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 9/11, 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. 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 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.<sup>14</sup>

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 raise a number of important issues relating to limits on speech and who has the ability to institute these limits, however. The capacity 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. 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.

## **Endnotes**

---

<sup>1</sup> 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.

<sup>2</sup> Gelbstein, Eduardo and Jovan Kurbalija, *Internet Governance: Issues, Actors and Divides* (Geneva: DiploFoundation, 2005), p. 11, <<http://www.diplomacy.edu/isl/ig/>>, accessed 25 May 2007.

<sup>3</sup> Klein, Hans, 'ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy', *The Information Society*, 18/3 (2002): 194-195.

<sup>4</sup> Working Group on Internet Governance (WGIG), *Report of the Working Group on Internet Governance* (Château de Bossey, 2005), p. 4.

<sup>5</sup> 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.

<sup>6</sup> Ibid.

<sup>7</sup> 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 25 May 2007).

<sup>8</sup> Commission of the European Union, *Proposal for a Council Framework Decision on Combating Racism and Xenophobia* (Brussels, 2001), pp. 6 and 8.

<sup>9</sup> 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.

<sup>10</sup> 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 25 May 2007).

<sup>11</sup> 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 25 May 2007). See, in particular, Part 1, Section 3, 'Application of ss. 1 and 2 to internet activity, etc'.

<sup>12</sup> As quoted in John Lasker, 'Watchdogs Sniff Out Terror Sites', *Wired News*, 25 February 2005.

<sup>13</sup> Ibid.; see also Gary Bunt, *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments* (London: Pluto Press, 2003), pp. 24 and 93.

<sup>14</sup> Alex P. Schmid and Janny De Graaf, *Violence as Communication: Insurgent Terrorism and the Western News Media* (London: Sage, 1982), p. 170.