Terrorism and Internet governance: core issues

Maura Conway

Global governance is a vast and complex issue area in itself, and the subset of issues that may be termed "Internet governance" are equally so. 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 complicates things yet further. Today, both substate and non-state actors are said to be harnessing—or preparing to harness—the power of the Internet to harass and attack their foes. 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 and advances in information and communication technologies have added new dimensions to the problem. In newspapers and magazines, in film and on television, and in research and analysis, "cyberterrorism" has become a buzzword. Since the events of 11 September 2001, the question on everybody's lips appears to be "is cyberterrorism next?" It is generally agreed that the potential for a "digital 9/11" in the near future is not great. This does not mean, however, that scholars of international relations may continue to ignore the transformative power 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 substate actors in the wake of the attacks of September 2001 in the United States and of July 2005 in the United Kingdom. The challenges of governance 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; and
- the debate over free speech versus 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".

Maura Conway is a lecturer in the School of Law and Government at Dublin City University, Ireland. Her principal research interests are in the area of terrorism and the Internet, including academic and media discourses on cyberterrorism, and the functioning and effectiveness of terrorist web sites. An extended version of this article, "Terrorism, the Internet, and International Relations: the Governance Conundrum", is to be published in M. Dunn, V. Mauer and F. Krishna-Hensel (eds), forthcoming 2007, *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace,* London, Ashgate.

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 United States government sponsored the establishment of the Defence Advanced Research Projects Agency, 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 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. This angered many end-users and resulted in a dispute, which was only resolved in 1998 with the establishment of a new international organization, the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit public-private partnership dedicated to preserving the operational stability of the Internet via broad representation of global Internet communities through bottom-up, consensus-based processes.

Since the establishment of ICANN, however, the debate on Internet governance has been characterized by the more direct involvement of national governments, mainly through the United Nations 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 the Plan of Action 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).[1] This became necessary because both "Internet" and "governance" were the subject of controversy, as was the concept of "Internet governance" itself.

"Governance" was the subject of particular controversy, especially during the WSIS. Misunderstandings stemmed from terminological confusion. 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 intergovernmental level with only limited participation from 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.[2]

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].[3] Dahl's conception of governance is 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."[4] 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 resulting 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-Qaeda in Iraq, "rocketed to worldwide fame, or infamy, by a deliberate combination of extreme violence and Internet publicity".[5] In early April 2004, al-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 this Internet-based public relations campaign, each of al-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, al-Zarqawi was able both to control the interpretation of his violent actions and achieve greater impact with smaller operations.

In May 2004, al-Zarqawi took things a step further and used the Internet's force-multiplying power to maximum effect when he was filmed cutting off the head of a US hostage and had the footage posted online.[6] 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; al-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."[7] The free availability of this and other grisly "snuff movies" on the Internet led to a realization that the most important aspect of the terrorism–Internet relationship was not the much discussed cyberterrorism, 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 al-Zarqawi's appearance.

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 publicize their position: Lebanese Hizbollah has clearly demonstrated this ability, as have the Tamil Tigers and Al-Qaeda. Unsurprisingly, in the post-11 September 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, among other things, information dissemination and thence recruitment: much 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.

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 they 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 organizations. In practical terms, of course, both legislated content control and private initiatives require the participation of private enterprises, particularly Internet service providers 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 considered.

Three approaches to content policy

Content policy is generally approached from one of three standpoints: human rights (freedom of expression and right to communicate), government (legislated content control) and 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 United Nations Universal Declaration of Human Rights (1948). On the other hand, the declaration also recognizes that freedom of expression is counterbalanced 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 diverging implementation.

Content control is very much bound up with free speech 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 toward stricter content control, particularly in the wake 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 United States has signed up to the Cybercrime Convention, it is constitutionally barred from signing the Additional Protocol to the convention, which deals with the criminalization of acts of a racist and xenophobic nature committed through computer systems.[8] In other words, while the Additional Protocol is now available to European Union (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 US authorities.

It is for this reason that many terrorist groups' sites are hosted in the United States. For example, a Connecticut-based ISP was at one time providing colocation 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 11 September 2001, similar web sites had already been the subject of debate beforehand. In 1997, controversy erupted when it was revealed that the State University of New York (SUNY) at Binghamton was hosting the web site of the Revolutionary Armed Forces of Colombia (FARC), and that a Túpac Amaru Revolutionary Movement solidarity site was operating out of the University of California, San Diego (UCSD). SUNY officials promptly shut down the FARC site. In San Diego, officials decided in favour of free speech, and the Túpac Amaru site remained in operation on UCSD's servers for some years.

States have access to myriad technologies with which they can limit and constrain how dissidents are able to use the Internet.

Constitutional guarantees notwithstanding, states are not technologically impotent when faced with political violence groups seeking to use the Internet to disseminate information. 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 web sites that citizens are blocked from accessing. If a web site appears on this list, access will not be granted. Technically speaking, the filtering typically utilizes router-based Internet Protocol (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 practise censorship too. For example, Australia has a filtering system for specific national pages, while the German state of North Rhine-Westphalia requires ISPs to filter access mainly, but not solely, to 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 organization of terrorist acts are prohibited by international law (*jus cogens*)—that is, a general consensus about the need to remove this content from the Internet 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 support for terrorism in any given instance.

In terms of controls, the second type of content generally under discussion is that which might be sensitive for particular countries, regions or ethnic groups due to their particular religious or cultural values. There can be little doubt that globalized, high-volume and more intensive communication challenges cultural and religious values. In fact, most Internet court cases are concerned with this type of content. Germany has highly developed jurisprudence in this area, having tried many cases against those responsible for web sites hosting Nazi materials. In France, a court requested that Yahoo.com (USA) prohibit French citizens from accessing parts of a web site selling Nazi memorabilia. And 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 leaves the third type of content that is often discussed, 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 may be summed up by the observation that what is illegal offline is illegal online.[9] 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. According to 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 relates mainly to problems of enforcing the rules, rather than the rules themselves.

The contemporary legislative landscape

The legal vacuum in the field of content policy that characterized early Internet use provided national governments with high levels of discretion in content control. National regulation 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 after 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 the events of 11 September, the Federal Bureau of Investigation (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.[10] However, because these and many of the other sites that were closed did not directly incite violence or raise money, they were not contravening US law and many were up and running again relatively shortly after they had been shut down.

Of all the legislation promulgated in the wake of 11 September, the most relevant in terms of Internet governance is the USA PATRIOT Act of 2001, which makes it illegal to advise or assist terrorists, including via an Internet site.[11] The case of Babar Ahmad is an interesting one in this regard. Ahmad, a British citizen, was the publisher of two prominent *jihadi* web sites, azzam.com and qoqaz.net, which were hosted in the United States 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 United States 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".[12] This includes not just the solicitation of financial support referred to above, but also, according to an affidavit filed in the 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.[13]

Similar charges to those pending against Ahmad have been brought against other US residents. However, due to the high levels of speech protection in the United States, 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 PhD candidate in computer science at the University of Idaho who established and maintained a radical web site, and Sami Amin al-Arian, a professor at the University of South Florida who was tried on charges relating to, among 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 USA PATRIOT Act. Clearly, Ahmad's case will be one to watch in terms of its impact on terrorism-related Internet-based speech in the United States.

The UK position

The July 2005 London bombings provided the spur for the British government to act against terrorist web sites operating out of the United Kingdom. In the immediate aftermath of the attacks, the then Home Secretary (Interior Minister) 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".[14] 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.[15] The prevention of terrorism bill 2005 narrowly avoided defeat in Westminster in October 2005; opposition centred on two key measures: new police powers to detain suspects for up to 90 days without charge and a proposed offence 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 web sites currently operational within the United Kingdom.

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 upon terrorist Internet use in the United Kingdom, 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 government was defeated on the issue of detention. However, the remainder of the bill's provisions went into force and became the Terrorism Act 2006.[16] 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 that already have strong legislation in the area of hate speech, and by 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 to 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 conference on The Freedom of the 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 organized a meeting 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 of these two aspects of content control, though no new rules were instituted as a result of these discussions.

The key international legal instrument addressing the issue of content is the Council of Europe's Additional Protocol to the Cybercrime Convention.

On a more practical level, in May 2007 EU ambassadors agreed that the European Police Office's (Europol) newly established high-security online portal known as *Check the Web* will need to be further strengthened to combat terrorism. The web site allows the 27 EU states to pool data on Islamist propaganda and Internet chatter and provides details on the experts monitoring the web in EU countries.

Check the Web is accessible only to law enforcement and experts, but the EU Safer Internet Action Plan has resulted in the establishment of a European network of hotlines, known as Inhope, for the reporting of illegal content by the general public. 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 frontline. 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: Internet search companies and hacktivists.

Geolocation software

In analyses of Internet governance, one of the key arguments frequently advanced was that the decentralized 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.

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 the Internet was accessed. Worldwide, the latest national legislation requires ISPs to identify their users and, if requested, to provide necessary information about them to authorities. Numerous governments have also announced plans to monitor more closely those who access the Internet in public places, particularly Internet cafés. Increased surveillance of the latter is now taking place in India, Italy, Thailand and a host of other countries; the explanation generally offered is "national security". The more the Internet is anchored in space, 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 geolocation software, which identifies the location of a computer and filters access to particular Internet content according to the national origin of the computer. The Yahoo! case was important in this respect, since the group of experts involved indicated that in 90% of cases, Yahoo! would be able to determine whether sections of one of its web sites hosting Nazi memorabilia were being accessed from France. This technological assessment helped the court to come to a final decision. Geolocation software companies claim that they can currently identify the home country without error and the accessing city in about 85% 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 web site 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 web sites 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 web sites, many Internet companies voluntarily purged sites perceived as terrorist after 11 September 2001. For example, Yahoo! pulled dozens of sites in the Jihad Webring, a coalition of 55 *jihad*-related

sites, while Lycos Europe established a 20-person team to monitor its web sites for illegal activity and to remove terrorism-related content. 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 11 September 2001 acted as the spur for many private groups and individuals to take to the Internet in search of "terrorist" web sites 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 it would destroy web servers and Internet access in Afghanistan and also target nations that support terrorism. The group proceeded to deface hundreds of web sites and launch Distributed Denial of Service (DDoS) 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 terrorist attacks of 11 September and curbed their activities.

It has never been all plain sailing for terrorist users of the Internet, even prior to September 2001. Home pages have been subject to intermittent DDoS 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 Fatherland and Liberty (ETA). The attacks against IGC began after ETA's assassination of a popular town councillor in northern Spain. The protesters wanted the site pulled from the Internet and IGC eventually removed it from its servers, but not before archiving a copy of the site, enabling others to put up mirrors: 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 September 2001 a number of more formal web-based organizations have been established to monitor terrorist web sites. One of the most well-known of such sites is Internet Haganah, self-described as "an Internet counterinsurgency". Also prominent is the Washington, DC-based Search for International Terrorist Entities (SITE), which, like Internet Haganah, focuses on Islamist 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 engaged in the collection (and sale) of open source intelligence—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."[17] 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".[18] Weisburd's *modus operandi* is first to research a site, then make 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?

While the potential of a "digital 9/11" is not great in the near future, the Internet has come of age since 2001. Both terrorism and the Internet are significant global phenomena, reflecting and shaping various aspects of world politics. 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 means that efforts by governments to regulate Internet activities are restricted, and this has provided users with immense freedom and space to shape the Internet in their own likeness. Included within this cohort are terrorists who increasingly employ 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.[19]

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 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 recently more restrictive legislation has 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 web sites and their removal, private initiatives instituted by a range of substate actors in conjunction with ISPs have been much more successful. But the activities of individual hacktivists raise a number of important issues relating to limits on speech and who can and should institute these limits. 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 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. See WSIS Plan of Action, World Summit on the Information Society, Geneva, 12 December 2003, document WSIS-03/GENEVA/DOC/5-E, at <www.itu.int/wsis/docs/geneva/official/poa.html>, paragraph 13b.
2. Eduardo Gelbstein and Jovan Kurbalija, 2005, *Internet Governance: Issues, Actors and Divides,* Geneva, DiploFoundation and Global Knowledge Partnership, at <www.diplomacy.edu/isl/ig>, pp. 10–12.
3. Hans Klein, 2002, "ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy", *The Information Society,* vol. 18, no. 3, pp. 194–195.
4. *Report from the Working Group on Internet Governance,* document WSIS-II/PC-3/DOC/5-E, 3 August 2005, paragraph 10.
5. Paul Eedle, "Al Qaeda's Super-Weapon: The Internet", paper presented at the conference "Al-Qaeda 2.0: Transnational Terrorism After 9/11", Washington, DC, 1–2 December 2004.

6. The video is entitled "Abu Musab al-Zarqawi Shown Slaughtering an American", and Central Intelligence Agency officials have since stated that it assesses with "high probability" that it is al-Zarqawi that carried out the beheading ("Jamaat al-Tawhid wa'l-Jihad / Unity and Jihad Group", *Global Security.org,* at <www.globalsecurity.org/military/world/para/zarqawi.htm>, and "'Zarqawi' beheaded US man in Iraq", *BBC News,* 13 May 2004, at <news.bbc.co.uk/2/hi/middle_east/3712421.stm>).
7. Eedle, op. cit.
8. Additional Protocol to the Convention on Cybercrime, signed at Strasbourg, 28 January 2003, at <conventions.coe.int/Treaty/EN/Treaties/Html/189.htm>.
9. Proposal for a Council Framework Decision on Combating Racism and Xenophobia, Official Journal of the European Communities 2002/C 75/E17, 26 March 2002.
10. 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 <www.iraradio.com>. However, it appears to have closed down again some time after February 2003. The other sites mentioned remain offline.
11. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).
12. *United States of America* v. *Babar Ahmad and Azzam Publications,* Indictment, United States District Court, District of Connecticut, at <www.usdoj.gov/usao/ct/Documents/AHMAD%20indictment.pdf>.
13. "British Man Arrested on Several Terrorism-related Charges", Press Release, United States Attorney's Office District of Connecticut, 6 August 2004, at <www.usdoj.gov/usao/ct/Press2004/20040806.html>.
14. Charles Clarke, in House of Commons Debates, *Hansard,* vol. 436, 20 July 2005, Column 1255.
15. Ibid.
16. The full text of the Act may be viewed at the web site of the UK's Office of Public Sector Information <www.opsi.gov.uk/acts/acts2006/20060011.htm>. See in particular Part 1, Section 3, "Application of ss. 1 and 2 to Internet activity, etc".
17. Quoted in John Lasker, "Watchdogs Sniff Out Terror Sites", *Wired News,* 25 February 2005.
18. Ibid.; see also Gary Bunt, 2003, *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments,* London, Pluto Press, pp. 24 and 93.
19. Alex P. Schmid and Janny De Graaf, 1982, *Violence as Communication: Insurgent Terrorism and the Western News Media,* London, Sage, p. 170.