15 Responding to cyberterror

A failure to firewall freedoms?

Rajash Rawal

Summary

While campaining for office of President of the United States in 2008, Barack Obama described a 'net attack' as being as serious and grave a problem as any potential nuclear or biological threat. Obama's concerns echo long-standing criticisms of the Internet and its capacity, such as its openness and the lack of a regulatory power. Governments have readily highlighted that terrorists have been quick to utilise the potential that the cyberworld has to offer them to deliver their messages, communicate with each other and retain their anonymity. As a result, efforts to curb and contain have often trampled over human rights, privacy and civil liberties. This chapter examines the developments by looking at the actual threats of cyberterrorism and what threats are posed by the use of the Internet by terrorists. This chapter analyses the trends in government measures to attempt to control hyperspace, question the nature of these measures and present how these measures threaten E-Democracy while at the same time highlighting the need for legitimate E-Identity mechanisms to be created.

Introduction

Barack Obama described a 'net attack' as being as serious and grave a problem as any potential nuclear or biological threat when running for office of President of the United States in 2008. He suggested that the 'War on Terror' had to become more diverse in its range of action in order to cope with the diverse threats being presented by the modern terrorist. Obama followed up on his words by launching a full cybersecurity review soon after being sworn into office in an attempt to shore up his nation's efforts in this area.[1]

Obama's concerns echo long-standing criticisms of the Internet and its capacity (i.e. its openness and the lack of a regulatory power).[2] Governments have readily highlighted that terrorists have been quick to utilise the potential that the cyberworld has to offer them in delivering their messages, communicating with each other and retaining their anonymity.[3] Scott and Street[4] further argue that the Internet has presented the opportunity for groups to plot in secret and 'bypass' nation-state mechanisms.

This chapter examines the developments by looking at what the actual threats of cyberterrorism are and what threats are posed by the use of the Internet by terrorists.

It analyses the trends in government measures to attempt to control hyperspace, questions the nature of these measures and presents how these measures threaten E-Democracy while at the same time highlighting the need for legitimate E-Identity mechanisms to be created. Finally, the chapter endeavours to present a conclusion as to whether (or not) cyberterrorism is a real and actual threat to modern society.

Background

As suggested above, governments and media alike have been very keen to present the threats of cyberterrorism and the use of the Internet by terrorists as being very grave and real.[5] Indeed, the lack of a regulatory power for the Internet has been a topic of much discussion for some time now.[6] Due to this lack of a regulatory power, government is on the back foot and can merely react; it is unable to act proactively.[7] The scenario of doom and gloom is only alleviated by the somewhat strange hope, given the ideas stated above, that the terrorists will be stopped. However, there are potent questions that need to be asked at this juncture such as: What evidence is there of any cyberterrorist attacks? Is it really true that little can be done to limit the terrorists who use the Internet?

These are questions which this chapter endeavours to answer in more detail. However, it is interesting to note at this point that a strange anomaly occurs when trying to look for examples of cyberterrorist attacks. Matai[8] suggests that the power outages across northeast North America, which affected cities such as New York, Detroit and Toronto in August 2003, were caused by the MSIBlast worm, which created a digital traffic jam. This, in turn, overloaded North American power stations and led to the collapse of electric power on a scale never before seen. The UK, Sweden, Denmark, Italy and Switzerland suffered power outages around this time too. The US government investigations suggested that while the outage was rare, no foul play was suspected. This is rather strange considering we are warned of the threats of a cyberterrorist attack, yet when one allegedly takes place, it is dismissed as an unfortunate accident. A reason for this is perhaps that such an attack taking place successfully would further undermine the notion of national security, which is held so dearly by governments around the world. Moreover, it would challenge the argument to move to E-Government systems as surely these large databases would be lucrative targets for the cyberterrorist. That said, we remain perfectly happy to raise the profile of potential attacks. One example is a report of a US Congressional panel which warned the outgoing Bush Administration in November 2008 that 'China was "stealing" vast amounts of sensitive information from US computer networks'.[9] A further example is Kyrgyzstan's recent suffering of a Distributed Denial of Service (DDoS) attack which paralysed the nation's Internet capabilities. The attack was officially blamed on Russia playing out Kyrgyzstan's potential as a victim, but spectators suggest there may have been domestic foul play.[10]

However, as governments seek to clamp down on the threat cyberterrorism poses, there are differences presented by the use of the Internet by terrorists which affect our basic freedoms more. It is these differences which this chapter examines.

Cyberterrorism v. terrorist 'use' of the Internet

Defining traditional terrorism is a very difficult task and cyberterrorism is no different. Cyberterrorism, a term first coined by Barry Collin[11] in the 1980s, is a wide-reaching concept which has no one, universally accepted definition. Crudely put, it is considered that cyberterrorism consist of acts of terror which take place in cyberspace; it is worth noting that it is not the same as cybercrime, as it must have strong terrorist elements. Terrorist attacks must seek to instil terror and fear; additionally they must have a political motivation, whereas cybercrime does not. Painter[12] adds the notion of 'cyberactivism' to the fray, which can be easily confused with cyberterrorism by the authorities and is one which limits our civil freedoms. The May Day riots of 2000 and the anti-globalisation protests of 2001 were all partially organised online, with web sites being created to inform activists of their legal rights and give phone numbers of sympathetic lawyers.

However, Denning contests that 'Cyberterrorism exists only in theory'[13] while cybercrime and cyberactivism are real. The following definition can be posited:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against property or persons, or at least cause enough harm to generate fear.[14]

This definition implies a very involved element in contrast to the concept of cyber-terrorism. Potential examples of cyberterror include spreading viruses, spamming (a 23-year-old was jailed in the UK for 'anarchic behaviour' after spreading abusive spam emails threatening to fire-bomb the headquarters of his county's trading standards office and petrol-bomb his local police office[15]), digital jamming and hacking (the Israelis and Palestinians were engaged in a cyberwar between 1999 and 2002, where each party attacked the other's Web resources[16]). Aggressive campaigns fought out on the Internet, or so called 'NGO-swarms',[17] have also been identified by the American military think tank RAND as potential forms of cyberterrorism. Additionally, in the aftermath of the riots that swept French cities in the autumn of 2005, French authorities jailed two bloggers for inciting violence.[18] It is questionable as to whether the latter can be considered to be an act of cyberterror or terrorist use of the Internet, as is illustrated later in this chapter. The authorities will often confuse protest and terror, allowing them to classify protest as terror to meet their own political needs.

However, it can be argued that the standard definition of cyberterrorism as quoted above is not one to which the wider public would adhere. They view cyberterrorism as the use of the Internet by terrorist groups to propagate their message. This view is further endorsed by the popular media,[19] which, as 'conduits for symbolism',[20] have become enmeshed in the symbolic war against terror, where fear becomes the main element.

'In newspapers and magazines, in film and on television, "cyberterrorism" is the zeitgeist.'[21] Moreover, Lanzone[22] adds a special new 'war on terror' element to cyber-terrorism, which he phrases as 'cyberjihad'. In addition to this, Weimann[23] identifies that terrorism on the Internet is a very dynamic phenomenon. However, what exactly does this involve? What is cyberterrorism and how do terrorists use the Internet?

Why terrorists use the Internet

Considering Webster's assertion that ICTs have had a 'massive and ongoing'[24] impact on society, it is natural, as Knight and Ubayasiri suggest, that terrorist groups have 'embraced the Internet'[25] and have challenged the existing balances on information flow and news coverage. This point is further emphasised by Scott and Street,[26] who suggest that the Internet has shifted 'editorial' control to activists, allowing them to present news and opinion as they like. As a result, terrorist use of the Internet is very vibrant; websites appear, change format and disappear or simply change their addresses to avoid closure.[27] This equates to normal progression in regard to the development of protest politics, as noted by Dahlgren, as cyberspace has become a 'vital link and meeting ground for the civically engaged and politically mobilized'.[28] Weimann[29] further expounds the idea that terrorists are drawn to the web to target three main audience categories:

- *Supporters*: Terrorist websites keep supporters informed of their (recent) activities. Merchandise can be sold to help raise funds. Organisations localise their site in order to provide more detailed information; this often is done in minority languages. Al Qaeda is one such group which employs this tactic.
- *Public opinion*: Even those who are not directly involved may be affected. Most sites offer information in a number of languages in order to draw as wide an audience as possible. The Basque Separatist Group (ETA), for example, has pages in Basque, Castilian, German, French and Italian. The main premise of this is perhaps to capture international journalists' attention and hence get the organisation into the traditional media. One of the Hezbollah's websites is aimed exclusively at journalists, inviting them to email the group's press office.
- *Enemy publics*: This is one of the less obvious targets, but an equally important one. Sites will aim to promote the past activities of the terrorist group and threaten more, wider and dangerous campaigns. The idea is to try to demoralise the enemy. This is turn gathers media attention and begins debate and may weaken the governments' rule, which is the ultimate aim of most groups. An example of this is the 11 March 2003 bombings in Madrid. The ruling People's Party maintained through the state-run news agency EFE that ETA were behind the attacks; however, various wings of Al Qaeda began to spread news via the web that they were responsible. The commercial, non-state-run media began to publish this and the citizenry began to doubt the government. This contributed to the ruling party being ousted in favour of the Socialist Party in the 13 March election.

Attractions of cyberspace

Heralded as the integrator of cultures, the Internet[30] has also been the 'instrument of a political power shift'.[31] As one of the first many-to-many broadcasting systems, as opposed to the one-to-many systems, it has opened up numerous possibilities for

groups of activists to freely air their views and opinions.[32] It has become a medium in which businesses, consumers and governments communicate with each other. It is, as such, unparalleled in its creation of a truly global forum which provides for the virtual existence of McLuhan's much-quoted 'global village'.[33] However, as positive a development as the Internet has been, utopian visions were quickly challenged by the proliferation of sites such as those which contain (child) pornography, violence and extremist aims.[34] That said, the Internet remains an exciting proposition as it challenges existing regimes of power and presents information and opinion in a less hierarchical way than traditional media.[35]

The attractions that the Internet holds for terrorist are manifold. It is an ideal arena for activity as it offers the advantages shown in Figure 15.1.[36]

In their approach to combat terrorist use of the Internet, governments have had to be imaginative and creative in their policy-making. An evaluation of the mechanisms introduced and their wider implications is put forward later in this chapter.

How do terrorists use the Internet?

There is a clear lack of an answer to the above question when considering modern, or rather post-September 11, terrorism, and the obvious difficulties the Internet has presented in policing terrorism. How does one identify a terrorist using a computer to further their aims, as distinct from an ordinary user? The actual identifying of a terrorist remains a perilously difficult thing to do and has been the subject of many heated debates. Consequently, a broad-brush approach is often taken by authorities, who categorise all members of particular ethnic or religious groups by the actions of a few. The dangers of 'risk-profiling' potential terrorist suspects are highlighted by Kip Viscusi and Zechauser,[37] as well as by Muhammed Abdul Bari, head of the Muslim Council of Britain, who feels the current climate of 'unease' may only 'help some people to recruit young [people] to terrorism'.[38] This is further illustrated by the shooting of Jean Charles de Menezes, who was wrongly identified as a terrorist suspect partially due to his appearance after the 7 July 2005 bombings in London.

- Easy access
- Little or no regulation/government control
- The potential for huge global audiences
- Anonymity (false identities are easy to create and use), unsecure networks open to abuse and distortion
- Speed of information flow
- Inexpensive to develop and maintain
- Multimedia possibilities (websites can combine text, graphics, films and sound, which can be downloaded by users)
- Ability to gather attention (mass media increasingly use the Internet as source for news stories)

Figure 15.1 Advantages of the Internet

Source: Amended from Weimann (2004), Knight and Ubayasiri (2002).

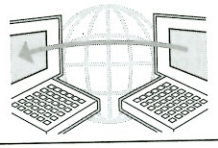
Terrorist websites are rife and appear in all shapes and forms. Almost all major terrorist organisations have websites; many have more than one and appear in several languages. Terrorist organisations have embraced the Internet as a vital cog in their machinery, as shown in Figure 15.2.[39]

Although the use of the Internet as a tool may be new, terrorist groups have always sought to spread propaganda by whatever means possible. The appeal of the Internet is that it goes beyond the means of traditional media and 'allow[s] for completeness of storytelling'.[40] It means that the terrorists can now bypass media controls and edit their own news agendas; one should consider the potential of social-networking sites such as Facebook and the group possibilities that exist here.

One of the earliest known postings by terrorists was back in March 1996 when the 'Terrorist's Handbook' was placed online. The handbook contained guidelines on how to make a bomb – the same type of bomb as was later used in the Oklahoma bombings.[41] With today's advances in technology, the handbook has now been supplemented by training videos which can be uploaded onto video-hosting sites. An obvious candidate here would be sites such as YouTube; however, these sites are regularly monitiored. In an interview with a web analyst[42] it was revealed to me that terrorists prefer to use 'unmonitored' porn sites such as Red Tube, where videos are hidden away in the annals of the back catalogue.

Another example of how terrorists use the Web aside from creating websites is by registering blogs. 'Blogging', as it is commonly referred to, offers terrorists the potential to air their views and present information is an unedited way, while at the same time allowing others to voice their support by joining in discussions held in the forum. It would appear that all viewpoints are available and given equal space and prominence; however, the owner of the blog can decide whose viewpoints he/she wishes to publish, hence there is a form of editorial control in the hands of the terrorist blogger. The examples of the French bloggers arrested on suspicion of inciting violence given earlier in this chapter[43] and the proposed €70 million expenditure of the British government 'to undermine extremist influences' in 'ungoverned' online spaces illustrate how seriously the authorities take this potential threat.[44]

It is further argued by Weimann[45] that terrorists seek to use the Internet to maintain their 'psychological warfare'. Their websites will not only re-enact past actions, but also present more general threats aimed at illustrating to the public the potential of their reach (i.e. disabling air traffic, destroying networks, etc.). An example of this was the airing of the murder of the American hostage Daniel Pearl in 2004, which was issued on several terrorist websites. Groups can also spread disinformation, which exaggerates the scope of their potential attacks and can generate cyberfear. Al Qaeda has been particularly successful at this, continually talking of the impending attack on



- Transmit propaganda on their aims and objectives
- Raise money by selling articles, merchandise or asking for donations
- Attract new members
- Communicate with existing activists

Figure 15.2 Why terrorists use the Internet

the United States, which has kept the nation on high alert since September 11 2001. Moreover, many terrorist organisations have created their own newsgroups to counter the power of traditional journalists.[46]

Al Qaeda has proven to be an excellent example of how a terrorist group can utilise the Internet. According to Knight and Ubaysiri,[47] the structure of this organisation is in many ways parallel to the Internet, which affords limitless possibilities for it. They are listed in Figure 15.3.

Consequently, we can say that Al Qaeda is 'simultaneously everywhere and nowhere'.[48] National governments often complain of the lack of wherewithal to control the Net due to its borderless, translucent world; the United States government has found it tough to eliminate and negate the threat Al Qaeda poses.

Mechanisms of government control

Thus far this chapter has only really examined the measures that terrorists take in using the Internet. It has also looked at the weakness that governments feel they have in their arsenal in being able to deal adequately with the potential threats. However, the picture of a meek, mild and limited executive does not really fit the mould. The somewhat considerable powers that government have are considered in this section and I challenge the notion the Internet is a wilderness beyond control.

Internet regulation and governance

One of the greatest myths of the Internet age is that there is no control over the Internet whatsoever. Sunstein argues that mechanisms exist to monitor and regulate the Internet: '[it] is hardly an anarchy or regulation free'.[49] The Internet Corporation for Assigned Names and Numbers (ICANN), based in California, has long since been the main body which has regulated how Internet domain names and addressing systems function, as well as managing how email and Net browsers direct their traffic. It was established in 1998.[50] ICANN has a direct link to the United States government.[51]

It is this very issue – the United States' relationship with ICANN – which formed the basis of heated debate during the World Summit on the Information Society (WSIS) held in Tunis in November 2005. Nations such as Brazil, China, France, Iran and South Africa wanted a more neutral body to be created under UN auspices to oversee the Net,[52] while others, such as the Internet think tank group the Internet Governance Project (IGP), wanted greater reforms of ICANN's powers and a democratisation of its structure.[53]

- Is transitional
- Lacks a geographic centre
- Consists of disparate nodes or activist cells
- Relies on software of ideas, rather than hardware of the military (e.g. aeroplanes as bombs)

Figure 15.3 Analogies between Al Qaeda and the Internet

A concept paper prepared by IGP identified the main criticisms of ICANN to be:[54]

- the unilateralism of the United States government in its control and supervision of ICANN;
- dissatisfaction with ICANN's Government Advisory Committee (GAC), where governments have only advisory powers;
- that ICANN does not reflect the needs and interests of developing countries in balance to those of developed countries;
- the general feeling that ICANN lacks legitimacy.

This concept paper was mooted during WSIS in attempt to create an agreement which would see the development of an internationally and legally recognised body to replace supervision by the US government with a more multi-lateral body similar to the International Telecommunications Union, which was founded in 1865.[55] It was further suggested that ICANN, while being central to Internet governance, does not meet all of the challenges that are faced, and indeed lacks transparency, accountaliblity and legitimacy itself. These ideas were substantiated by the Working Group on Internet Governance (WGIG), which last met in June 2005, and presented four models for Internet governance.[56]

However, despite these pressures for reform of ICANN, the outcome of WSIS resulted in little change to the current situation. ICANN remains in the hands of the United States, although an agreement was reached to set up an Internet Governance Forum (IGF) under the guidance of the United Nations Secretary General.[57] Kawamoto argues that a body that satisfactorily regulates the Internet should be created. Kawamoto points to the role of the UN as being a key international body in the past when looking to form a global consensus; these experiences should not be lost and the UN should have a major role in his opinion.[58] The IGF has a tough task ahead of it.

In addition to the ICANN provisions, however, there are other ways in which the Internet is regulated. The Security Intelligence Products and Systems (SIPS) framework has been in operation since 1995. It forms part of the British-based mi2g Intelligence unit and boasts 'the world's largest digital attack database'.[59] SIPS contains information on all major hacking groups and Internet malware attackers (sabateurs) and has relationships with virtually all global actors in order to maintain a peerless status in holding confidential information with regard to digital risk.[60]

A secondary wing of the above-mentioned intelligence unit is the Asymmetric Threats Contingency Alliance (ATCA), which was initiated post-September 11. ATCA monitors activity throughout the world, focusing on terrorist and organised crime cartels. ATCA draws up a thorough database of potential threat by compiling monthly reports on posting of information gathered through monitoring of terrorist groups, websites and intercepted communications of terrorist organisations. However, a fundamental criticism of ATCA is that it continually infringes civil liberties and confuses protest with terrorist activity.

Control of Internet users

As important as it is that cyberspace is regulated, it it is also of equal importance to monitor the users that surf the World Wide Web. A simple reason for this is highlighted by the fact that the September 11 hijackers booked at least nine of their airline tickets online a few weeks prior to the attacks.[61] It is further suggested that the hijackers set up a number of 'largely anonymous . . . temporary [email] accounts' such as Hotmail accounts, and accessed the Web from public places such as libraries. Notably, these are all actions which are perfectly legal. Had the tickets been booked in the conventional way with a travel agency, would we now want to control travel agencies' services more stringently?

In order to combat this element of Web abuse, authorities are beginning to introduce a number of new measures. One such example is in Italy, where anti-terror laws affect how people can access the Internet in public places. Celeste[63] suggests that these new laws are part of the most extensive anti-terror packages introduced in Europe. While encompassing more than Internet use, these laws now require people who wish to use the Internet in public places such as libraries or Internet cafés to submit a photocopy of their passport before being allowed to log on. Moreover, Internet cafés have to obtain public communications business licences and install expensive tracking software, or so-called 'eavesdropping technology',[64] costing up to US$1,400.[65]

Additionally, the European Union introduced a directive which will allow police authories to access users 'traffic data'.[66] The directive, which was introduced in every member state of the European Union by the deadline of July 2007, compels every telephone company and Internet service provider (ISP) to save call and Internet records for up to two years. The ISP data is comprehensive and includes websites visited and header information of email correspondence detailing the sender, recipient, date, time and Internet address.[67] Whereas law enforcement agencies welcomed the new legislation, privacy advocates fear for the wider implications. The prospect Gibb presents of our communication tools forming part of the largest surveillance system ever created in the near future surely is enough reason to worry.[68]

One could ask whether these restrictions are enough when we once more analyse the use of technology by terrorists in reality. As reported by Spanish media following investigations into the 11 March 2003 train attacks by Al Qaeda in Madrid, it was found that in order to not have their messages intercepted on Hotmail, the terrorists merely amended their use of the free email service. Current legislation allows authorities to monitor inboxes and no more. The Madrid attackers simply used one email account which was accessed by all and stored messages in the 'drafts' folder of the account. Once more, legislation seems to be one step behind.

Do governments pose a threat to cyberfreedom?

Government controls and their ensuing implications for society have left spectators lamenting the abuses of privacy and freedoms that governments can now legitimately undertake under the guise of protecting their citizens. Indeed, as noted by the Geneva-based NGO International Commission of Jurists, many governments have used the anti-terror drive as an excuse to curb freedoms and limit the use of domestic opponents on the Internet – a charge levelled most acutely at the US and UK executives.[69] These initiatives, which have introduced surveillance and removed the protection of privacy, may threaten the healthy existence of democracy.[70] The benefits of E-Government in making society more open and democratic may be undone by E-Policing and E-Control.

The dynamics at play here bring together the divergent needs of government and society. On the one hand, as mentioned earlier, the Internet has enabled society to freely express its opinions at a global level. Borders have been in some cases rendered irrelevant. On the other hand, as positive an element for society as this may have been, it has also triggered a need for governments to adjust antiquated laws and regulations, which the existence of the Internet has challenged. For example, it is illegal to own a copy of Adolf Hitler's *Mein Kampf* in Germany. In the pre-Internet world this was a simple policy to implement and maintain, as the book was not available. However, in the new Amazon.com age it was easy to order a copy of the book online without the authorities ever knowing about it. A law change was needed.

Post-September 11 the world seemed to legitimise the opportunity for governments to make these changes due to the large-scale public fear that was generated by the media for potential terrorist threats, although the actual desire to adjust laws pre-dated September 11 – indeed, the British government has been interested in the idea of data retention since 1998,[71] as has the German government.[72] However, as Loundy suggested before September 11 2001, the Internet must not be made a scapegoat ahead of other methods of communications, despite concerns over its mis-use being 'legitimate'.[73] If there are concerns that terrorists communicate using email, why are there no such concerns that they may communicate using regular mail? It is this question which guardians of Internet privacy ask in retort to the clampdown and ultra-secure era that is dawning in the cyberworld. Indeed, as noted by Loader, the Internet has presented a 'paradigmatic change in the constellation of power relations'[74] between governments and individuals. This is perfectly illustrated by Williams, who argues that post-September 11, the Internet became an invaluable source for 'neutral' information as the traditional media was seen as the mouthpiece of the US government.[75]

However, the opportunities to harness the new cyberworld were only fully grasped by governments post-September 11. The fear of terrorism, in all its forms, has heightened since September 11, becoming part of our daily political diet and thus becoming the '*raison d'être* for countless examples of political excess'.[76] Cynics have argued that there has been an over-emphasis of the threats faced so that the public would accept a diminishing of rights without a public outcry – although, as Sunstein argues, free society has always known some form of regulation.[77]

Legislation passed in the United States, Britain, France, Germany, Spain, Italy and Denmark, tied in with policy from the European Union, the Council of Europe and the G8, has limited cyber freedoms in some way.[78] The danger of many of these law changes is that not only do they challenge personal freedoms, but they also risk turning ISPs and telecommunication companies into a potential arm of the police. The upshot is that governments seem to be willing to exact 'a high price in terms of liberties to the high toll of terrorism'.[79] Many well-meaning initiatives have fallen 'far

short'[80] of promises made and have created new problems of limiting freedom and augmenting the unaccountability of government and corporations.

The risk is that society has accepted changes without much debate, whereas had changes been introduced to control more traditional media and methods of communication, discussion would have been rife.[81] The need for a legitimate form of developing E-Identities has never been greater. As presented by Fishenden,[82] the need for E-Identities to monitor online government services and online commerce now encompasses online security.

Can the ordinary citizen do more?

As illustrated above, governments across the world have been keen to introduce restrictions in order to protect the citizenry from the terrorist potential. However, these restrictions, though accepted without discussion at their inception, have been rounded on as curbing our natural freedoms. Nevertheless, the threat exists and something needs to be done. However, perhaps there is something that we, as ordinary citizens, can do to limit the possibilities that terrorists have of using the Internet to meet their needs.

A first and very simple step is to limit the visibility of our own digital equipment. Many of us enjoy simple, easy access to the Internet through our domestic wi-fi environment; however, we extend this courtesy to all and sundry when we do not secure our networks. As mentioned earlier, the potential terrorist thrives on anonymity and an unsecured network allows them to have access to an ISP which cannot be traced back to them – better still, it can be traced to an unsuspecting innocent citizen caught in the crossfire. This is, incidentally, also true for the Bluetooth facility on mobile devices, which, as factory default, come as 'visible to all' and should be set to 'password protected'.

We can also make sure our information is safe by making sure our access to the Internet is safe too. Increasingly, as illustrated by other chapters in this volume, we turn to the online world for our interaction with government (i.e. for taxes, health, education, etc.). By filling in an online form for a tax return, for example, we send out vital information about ourselves which can be adopted and used to criminal, and potentially terrorist, use. So-called 'blaggers' wait to prey on any lapse of security in order to gain personal information which they can sell on to the highest bidder.[83] The problem is so rife that the British Information Commissioner's Office published a 'Personal Information Tool-Kit' in January 2007. Unfortunately, two years after its publication the success of this leaflet was not as widespread as the leaking of personal information or indeed the 'cybercrime tool kits' which can be easily purchased.[84]

In short, the citizen can never safeguard everything; we will always need government protection too, but by being aware of our actions and their implications we can begin to remove some of the threat to our online security that we face. We must also apply common sense when we interact over the Internet. We would never post money in an unsealed envelope through regular post, so why transact over unsecure Internet sites? Public complacency sits oddly with public paranoia.[85]

Conclusions

We have reached an important juncture in the so-called 'zeitgeist' of cyberterrorism. Governments have acted and their policy-making counteracts the growing prospective threats of cyberterror, but terrorists continue to seek a safe haven in the dark corners of cyberspace to advance their campaigns based on creating fear and panic.

However, as Matai notes, 'physical terrorism and digital attacks go hand in hand',[86] thus the potential of cyberterror should not be overestimated and exaggerated, which has been the case with politicians 'using fear of terror'.[87] Terrorists will continue to use violence to overcome their 'invisibility'.[88] However, the use of the Internet by terrorists is a far more alarming prospect and one which is tougher to combat. It is here that a delicate balance needs to be addressed. On the one hand, restrictions need to be tough enough to serve as an adequate deterrent, but on the other hand, they need to maintain the existing freedoms and allow cyber society to develop. Mechanisms to monitor public Internet access points, as in Italy, can work. However, they should not burden the host (i.e. Internet café) to the extent that the host is impeded by the requirement for financial capital needed to meet modern regulations, as this may only lead to closure of much-needed public access points, which help address the issue of the digital divide.[89]

In our fight against modern terrorism and its role in cyberspace, a few things must be noted. The War on Terror has not been a watershed, it has been an excuse. The threat existed before September 11, and nothing since this date has heightened its potential as a threat. However, events since this date have legitimised government attempts to implement restrictive legislation which they have wanted to introduce for some time now (see the above-mentioned examples of the UK and Germany). The simple fact remains that we (both government and citizen alike) need to better monitor how the Internet is used and limit its capacity to be abused by Internet-savvy terrorists. However, heavy-handed restrictions will only hand the initiative to authoritarian governments that may violate privacy, curb the free flow of information and hamper freedom of expression – ironically, the very core values of the society we are claiming to be trying to protect. Moreover, it will enable undemocratic regimes to refer to our own counter-terror mechanisms as examples to justify their own abusive practices. As noted by Moore,[90] the relationship between democracy and cyberspace is a complex, multi-dimensional one, and we must all engage in nurturing it.

Key points

- Governments have readily highlighted that terrorists have been quick to utilise the potential that the cyberworld has to offer them to deliver their messages, communicate with each other and retain their anonymity.
- Terrorist groups have embraced the Internet and have challenged the existing balances on information flow and news coverage. The Internet has shifted editorial control to activists. This allows them to present news and opinion as they like.

- Terrorist use of the Internet is very vibrant. Websites appear, change format and disappear or simply change their addresses.
- Mechanisms do exist to monitor and regulate the Internet – '[it] is hardly an anarchy or regulation free'. Such mechanisms include ICANN, SIPS and ACTA. There are also numerous national surveillance tools used the world over.
- In order to combat this element of Web abuse, authorities are beginning to introduce a number of new measures. For example, eavesdropping technology is used in public access points and the European Union introduced a directive which will allow police authories to access users' traffic data, which compels every telephone company and Internet service provider (ISP) to save call and Internet records for up to two years.
- Government controls and their ensuing implications for society have left spectators lamenting the abuses of privacy and freedoms that governments can now legitimately undertake under the guise of protecting their citizens.
- Citizens can limit the visibility of their own digital environment. They can also make sure their information is safe by making sure their access to the Internet is safe too. Common sense must be applied when interacting over the Internet.
- The simple fact remains that we (both government and citizen alike) need to better monitor how the Internet is used and limit its capacity to be abused by Internet-savvy terrorists.

Notes

1 BBC Newsonline (2009) 'Obama Begins Cybersecurity Review', *BBC News*, 10 February, http://news.bbc.co.uk/go/pr/fr/-/hi/technology/7880695.stm.
2 Buckler, S. and Dolowitz, D. (2005) *Politics on the Internet*. Abingdon: Routledge.
3 Knight, A. and Ubayasiri, K. (2002a) 'eTerror: Journalism and the Internet', *Ejournalism* 2/1, http://www.ejournalism.au.com/ejournalist_v2n1.htm.
4 Scott, A. and Street, J. (2001) 'From Media Politics to E-Protest?', in *Culture and Politics in the Information Age*, Webster, F. (ed.) London: Routledge. pp. 32–51.
5 Bradbury, D. (2009) 'The Fog of Cyberwar', *Guardian*, 5 Februray.
6 Cukier, K. N. (2005) 'Who Will Control the Internet? Washington Battles the World', *Foreign Affairs* 84/6 November/December: 7–13.
7 Segoviano Monterrubio, S. (2005) 'Al Qaeda en la Red', *Papeles de Cuestiones Internacionales* 89, Primavera.
8 Matai, D. K. (2005) *Cyberland Security: Organized Crime, Terrorism and the Internet*. Oxford Internet Institute, University of Oxford, 10 February.
9 BBC Newsonline (2009) 'Obama Begins Cybersecurity Review', *BBC News*, 10 February, http://news.bbc.co.uk/go/pr/fr/-/hi/technology/7880695.stm.
10 Bradbury, D. (2009) 'The Fog of Cyberwar', *Guardian*, 5 February.
11 Conway, M. (2002) 'Reality Bites: Cyberterrorism and Terrorist 'use' of the Internet', *First Monday* 7/11 (November), http://firstmonday.org/issues/issue7_11/conway/index/html.
12 Painter, A. (2001) 'The Contagious Campaign (part 2)', in *Viral Politics*, Painter, A. and Wardle, B. (eds) London: Politicos Publishing. pp. 154–167.
13 Denning, D. quoted in Conway, M. (2002) 'Reality Bites'.
14 Denning, D. quoted in Conway, M. (2002) 'Reality Bites', p. 6.
15 BBC Newsonline (2005) 'Spammer Convicted of £1.6m Scam', *BBC News*, 16 November, http://news.bbc.co.uk/go/pr/fr/-/1/hi/england/cambridgeshire/4442772.stm.
16 Conway, M. (2002) *Reality Bites*; Weimann, G. (2004) *www.terror.net: How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report 116, March 2004, www.usip.org.
17 Rosenkrands, J. (2004) 'Politicizing Homo economicus' in *Cyberprotest – New Media, Citizens and Social Movements*, van de Donk, W., Loader, B.D., Nixon, P.G. and Rucht, D. (eds) London: Routledge. pp. 57–76.
18 Plunkett, J. (2005) 'French Bloggers Held after Paris Riots', Guardian Unlimited Special Reports, November, http://www.guardian.co.uk/story/0,11882,1638520,00html.
19 Weimann, G. (2004) *www.terror.net*.
20 Louw, E. (2005) *The Media and Political Process*. London: Sage Publications.
21 Conway, M. (2002) *Reality Bites*.
22 Lanzone, R. (2005) *Cyberjihad*. Indiana: AuthorHouse.
23 Weimann, G. (2004) *www.terror.net*.
24 Webster, F. (2001) 'A New Politics?', in *Culture and Politics in the Information Age*, Webster, F. (ed.) London: Routledge. pp. 1–13.
25 Knight, A. and Ubayasiri, K. (2002b) 'Reporting On Line: The Internet and Terrorism', *ON LINE opinion – Australia's e-journal of social and political debate*, http://onlineopinion.com.au/view.asp?article=1101.
26 Scott, A. and Street, J. (2001) 'From Media Politics to E-Protest?'
27 Weimann, G. (2004) *www.terror.net*.
28 Dahlgren, P. (2001) 'The Transformation of Democracy?', in *New Media and Politics*, Axford, B. and Huggins, R. (eds) London: Sage Publications. pp. 64–88.
29 Weimann, G. (2004) *www.terror.net*.
30 Ibid.
31 Conway, M. (2002) 'Reality Bites'.
32 Dahlgren, P. (2001) 'The Transformation of Democracy?'
33 McLuhan, M. (1964, 2002) *Understanding Media: The Extensions of Man*. London: Routledge.
34 Weimann, G. (2004) *www.terror.net*.
35 Stevenson, N. (2001) 'The future of public media cultures', in *Culture and Politics in the Information Age*, Webster, F. (ed.) London: Routledge. pp. 63–80.
36 Weimann, G. (2004) *www.terror.net*; Knight, A. and Ubayasiri, K. (2002b) 'Reporting On Line: The Internet and Terrorism'.
37 Kip Viscusi, W. and Zechauser, R. Z. (2003) *Sacrificing Civil Liberties to Reduce Terrorism Risks*, John F. Kennedy School of Government, Harvard University Faculty Research Working Paper RWP03-017.
38 BBC Newsonline (2007) 'UK Terror Tactics create unease', *BBC News*, 10 Novermber, http://news.bbc.co.uk/go/pr/fr/-/hi/uk/7088325.stm.
39 For an elaborative review of terrorist websites and their aims and objectives please refer to Conway 2002, Knight and Ubaysiri 2002a, Weimann 2004.
40 Kawamoto, K. (2003) *Media and Society in the Digital Age*. Boston: Allyn and Bacon.
41 Sunstein, C. (2002) *Republic.com*. Princeton, NJ: Princeton University Press.
42 The web analyst prefers to remain anonymous.
43 Plunkett, J. (2005) 'French Bloggers Held after Paris Riots'.
44 BBC Newsonline (2007) 'Internet Used to Target Extremism', *BBC News*, 31 October, http://news.bbc.co.uk/go/pr/fr/-/hi/uk/7070416.stm.
45 Weimann, G. (2004) *www.terror.net*.
46 Knight, A. and Ubayasiri, K. (2002b) 'Reporting On Line: The Internet and Terrorism'.
47 Ibid.
48 Ibid.
49 Sunstein, C. (2002) *Republic.com*.
50 Internet Corporation for Assigned Names and Numbers (ICANN) (2004) *Fact Sheet*, http://www.icann.org/general/fact-sheet.html.

51 BBC Newsonline (2005) 'US Retains Hold of the Internet', *BBC News*, 16 November, http://news.bbc.co.uk/go/pr/fr/-/hi/technology/44441544.stm.
52 Cukier, K. N. (2005) 'Who Will Control the Internet? Washington Battles the World' BBC Newsonline 'US Retains Hold of the Internet', *BBC News*, 16 November, http://news.bbc.co.uk/go/pr/fr/-/hi/technology/44441544.stm.
53 Klein, H. and Müller, M. (2005) *What to Do about ICANN: A Proposal for Structural Reform*, A Concept Paper by the Internet Goverance Project, 5 April, http://www.InternetGovernance.org; Working Group on Internet Governance (WGIG) (2005), Château de Bossey, June, http://www.wgig.org/; Drake, W. J. (2005) *Reforming Internet Governance: Perspectives from WGIG*, ICT Task Force Series 12, Working Group on Internet Governance (WGIG).
54 Klein, H. and Müller, M. (2005) *What to Do about ICANN: A Proposal for Structural Reform*.
55 Cukier, K. N. (2005) 'Who Will Control the Internet? Washington Battles the World'.
56 Reporters Without Borders (2002) *Anti-terrorism Drive Threatens Internet Freedoms*, www.ThinkCentre.org, 12 September, http://www.thinkcentre.org/article.cfm?ArticleID=1724.
57 BBC Newsonline, 'US Retains Hold of the Internet'; World Summit on the Information Society (WSIS) (2005) *Tunis Agenda for the Information Society*, Document: WSIS-05/TUNIS/DOC/6(Rev.1)-E, http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf.
58 Kawamoto, K. (2003) *Media and Society in the Digital Age*.
59 Matai, D. K. *Cyberland Security: Organised Crime, Terrorism and the Internet*. p. 1.
60 Ibid. p. 2.
61 Conway, M. (2002) 'Reality Bites' p. 11.
62 Ibid.
63 Celeste, S. (2005) 'Want to Check Your E-Mail in Italy? Bring Your Passport', *The Christian Science Monitor*, October, 4 http://www.csimonitor.com/2005/1004/p07s01-woeu. html.
64 Gibb, J. (2005) *Who's Watching You?* New York: Conspiracy Books.
65 Celeste, S. (2005) 'Want to Check Your E-Mail in Italy? Bring Your Passport'.
66 Grossman, W. M. (2006) 'Will Logging Your Email Combat Terrorism in Europe?', *Guardian Unlimited Technology Section*, January, http://technology.guardian.co.uk/weekly/story/0,16376,1683944,00.html.
67 Ibid.
68 Gibb, J. (2005) *Who's Watching You?*
69 BBC Newsonline (2009) 'Anti-terror Tactics Weaken Law', *BBC News*, 16 February, http://news.bbc.co.uk/go/pr/fr/-/hi/world/europe/7892387.stm.
70 Raab, C. D. (1997) 'Privacy, Democracy, Information', in *The Governance of Cyberspace*, Loader, B. D. (ed.) London: Routledge. pp. 155–174.
71 Grossman, W. M. (2006) 'Will Logging Your Email Combat Terrorism in Europe?'
72 Gibb, J. (2005) *Who's Watching You?*
73 Loundy, D. (1995) 'Constitution Protects All Modes of Speech', *Chicago Daily Law Bulletin*, 11 May, accessed http://www.loundy.com/CDLB/Terrorism.html.
74 Loader, B. D. (1997) 'The Governance of Cyberspace', in *The Governance of Cyberspace*, Loader, B. D. (ed.) London: Routledge. pp. 1–19.
75 Williams, B. A. (2003) 'The New Media Environment, Internet Chatrooms and Public Discourse after 9/11' in *War and the Media*, Thussu, D. T. and Freedman, D. (eds) London: Sage Publications. pp. 176–189.
76 Gibb, J. (2005) *Who's Watching You?* p. 20.
77 Sunstein, C. (2002) *Republic.com*.
78 Reporters Without Borders (2002) *Anti-terrorism Drive Threatens Internet Freedoms*.
79 Weimann, G. (2004) *www.terror.net*. p. 12.
80 Lyon, D. (2004) *Surveillance after September 11*. Cambridge: Polity Press.
81 Loundy, D. (1995) 'Constitution Protects All Modes of Speech'; Celeste, S. (2005) 'Want to Check Your E-Mail in Italy? Bring Your Passport'; Reporters Without Borders (2002) *Anti-terrorism Drive Threatens Internet Freedoms*.
82 Fishenden, J. (2005) 'eID: Identity Management in an Online World', in *Proceedings of the 5th European Conference on E-Government*, Remenyi, D. (ed.) University of Antwerp, June 2005.
83 BBC Panorama (2008) 'You Can Run . . . but Can You Hide?' *BBC News*, 24 October, http://news.bbc.co.uk/go/pr/fr/-/hi/programmes/panorama/7685043.stm.
84 BBC Newsonline (2007) 'Cyber Crime Tool Kits Go on Sale', *BBC News*, 4 September, http://news.bbc.co.uk/go/pr/fr/-/hi/technology/6976308.stm.
85 Economist (2008) 'Identity Parade', published in *The Electronic Bureaucrat: A Special Report, The Economist*, 16 February.
86 Matai, D. K. *Cyberland Security: Organised Crime, Terrorism and the Internet*. p. 3.
87 BBC Newsonline (2009) '"Ministers 'Using Fear of Terror"', *BBC News*, 17 February, http://news.bbc.co.uk/go/pr/fr/-/hi/uk/7893890.stm.
88 Louw, E. (2005) *The Media and Political Process*.
89 Nixon, P. G. and Rawal, R. (2005) 'From e-Gov to we-Gov: Social Inclusion, Government and ICTs', in *Proceedings of the 5th European Conference on E-Government*, Remenyi, D. (ed.) University of Antwerp, June 2005.
90 Moore, R. K. (1999) 'Democracy and Cyberspace', in *Digital Democracy*, Hague, B. N. and Loader, B. D. (eds) London: Routledge. pp. 39–59.

Further reading

Dahlgren, P. (2001) 'The Transformation of Democracy?', in *New Media and Politics*, Axford, B. and Huggins, R. (eds) London: Sage Publications. pp. 64–88.
Gibb, J. (2005) *Who's Watching You?* New York: Conspiracy Books.
Weimann, G. (2004) *www.terror.net How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report 116, March, www.usip.org.