Internet Journal of Criminology © 2014
ISSN 2045 6743 (Online)

DEBATING THE TERM CYBER-TERRORISM: ISSUES AND PROBLEMS

By Imran Awan[1]

Abstract

The UK Defence Review in 2010 shed light on the real concerns that Britain could be facing a new threat from cyber-terrorists. Indeed, extremist groups and organisations are increasingly using cyberspace for terrorist purposes and as a result the role of the Internet has meant that terrorist are able to play the role of hostile actors willing to cause mass carnage and destruction through technological means. This threat has led to many questions for example, what the term cyber-terrorism means? The paper examines the case for two schools of thought. It concludes that the current nature of terrorism provides more support for the Weimann argument, but that things could change if terrorists are given more appropriate training and skills in cyberspace.

[1] Senior lecturer in Criminology, Birmingham City University

Introduction

According to Dorothy Denning the phrase cyber-terrorism was first coined in 1982 by Barry Collin who argued the term meant the convergence of the physical and cyber world (Denning 2010). Colin argued that this future cyber warfare would involve terrorists conducting a cyber-terrorist attack against critical infrastructure, for instance causing large civilian aircraft to crash with the click of a mouse. Thus the debate over what the term cyber-terrorism means has begun to permeate itself in legal, political and criminological discourse i.e. whether it includes aircraft falling from the sky or just simply the use of the Internet for terrorist purposes? The paper attempts to answer this question; using empirical case studies (Altheide 1997; Foltz 2008; Weimann 2005; Denning 2000) which might help to explain what is cyber-terrorism? Notwithstanding the serious threat posed by cyber-terrorism critics argue cyber-terrorism is nothing more than sensationalized fear mongering conducted through a platform for the media, and politicians who aim to use it to enact draconian pieces of counter-terrorism legislation.

There is no universal definition of cyber-terrorism, instead we have a myriad of definitions, from both security agencies such as the FBI and CPNI in the UK, politicians and academics who have attempted to define it (Yar 2006). For Verton (2003) cyber-terrorists are people who execute surprise attacks that use computers and the Internet to cripple a nation's infrastructure. Furthermore, there are conflicting viewpoints of the term, as highlighted by Pollitt (2001), who like Denning (2000) argues that cyber-terrorism is an attack which uses the computer as a weapon of warfare. In contrast, Bronskill (2001) and Weimann (2004) argue that cyber-terrorism is used for recruitment, propaganda purposes and gathering support through websites. While these activities do provide a provocative analysis of what cyber-terrorism might mean, they are murky in the sense that some fit the Weimann (2005) argument of cyber-terrorism, but they do not, however fit Denning's (2000) interpretation of the computer being the deadly weapon. Therefore in helping get a better understanding of the terminology, the theoretical arguments made by social constructionism theorists allows us to have a more nuanced opinion on the terminology cyber-terrorism. Given, the fact that types of behaviour can be linked to social problems and social movements, this allows us to look at cyber-terrorism, through the lens of social change (Spector and Kitsuse 1973). At present, the threat of cyber-terrorism is now emerging in the UK, and thus becomes relevant, in the present discourse and requires a deeper critical reflection of the terminology.

In Britain, the fight against cyber-terrorism has meant a review of national security strategies. The Strategic Defence and Security Review in October 2010 highlighted a grave warning that the UK was facing a serious threat from cyber-terrorism. The fear is that after the death of Osama Bin Laden terrorists would have the capacity to play the role of hostile actors capable of conducting a major cyber-terrorist attack (Grabosky, 2007). The National Security Strategy in 2010 sets out two clear objectives: (i) firstly, to make sure the UK is resilient and secure by protecting the public, economy and infrastructure; and (ii) to build a stable world, by reducing the likelihood of risks affecting the UK or its interests overseas (National Security Strategy 2010). In a joint statement the coalition government in Britain stated that;

"We are entering an age of uncertainty. This strategy is about gearing Britain up for this new age of uncertainty – weighing up the threats we face and preparing to deal with them" (National Security Strategy 2010: 4).

The paper will explore the debate around what cyber-terrorism is and its meanings; by examining two different and prominent definitions. Dorothy Denning argued, in a speech given before the US Congress, that cyber-terrorism was a means "…intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples" (Denning 2000: 1).

Denning's argument is that cyber-terrorism directly causes loss of life or other serious damage. This means the 'threat of attack on computers, networks' and attacks that could lead to 'explosions, plane crashes, water contamination or severe economic loss and even death' would constitute an act of cyber-terrorism (Denning 2000:1). This conjures up an image of devastation and graphic violence, of computer technology used as a lethal weapon. Furthermore, her definition raises real technical, legal and social issues. For example, she argues that attacks against critical infrastructures, such as electric power or emergency services, are acts of cyber-terrorism. Is Denning's description valid? Weimann for example, takes a different view. He states that, "Some fears are simply unjustified, while others are highly exaggerated" (Weimann 2005; 132). When Weimann uses the term, "cyber-terrorism" he uses it in a different sense, arguing that: "terrorist use of computers as a facilitator of their activities, whether for propaganda, recruitment, defaming communication or other purposes is not simply cyber terrorism" (Weimann 2005: 132).

To substantiate his argument, Weimann would need to show how terrorist's use of online videos and websites constitute the act of cyber-terrorism. For example, are online videos of terrorist attacks a form of cyber-terrorism? What both of these views raise are questions about cyber-terrorism, whether cyberspace is confined to the use of the Internet or also covers modes such as television, radio, fax, and email etc? This article examines the case for both these schools of thought but concludes that the current nature of terrorism provides more support for Weimann's argument, but that things could change if terrorists acquire more sophisticated skills in new technology (Weimann 2004).

Terrorism and Cyberspace

As noted above, according to Denning, cyber-terrorism is capable of reeking actual damage on critical infrastructures of society, such as telecommunications, water supply, and economic and financial institutions. Denning argues that if terrorists are given the right training and acquire the appropriate technological skills then this would be dangerous for the whole world. Denning states that: "To understand the potential threat of cyberterrorism, two factors must be considered: first, whether there are targets that are vulnerable to attack that could lead to violence or severe harm, and second, whether there are actors with the capability and motivation to carry them out" (Denning 2000: 1).

Denning therefore argues that a cyber-terrorist attack could lead to death or bodily injury, through 'explosions, plane crashes, water contamination, or severe economic loss.' As regards her first claim, that cyber-terrorism causes explosions, it is clear that any explosive device (whether homemade or more sophisticated) is likely to cause severe damage. It is not clear, from Denning's writings, how this would actually work (Flemming and Stohl 2001). One possibility is that, she is referring to a hacker, breaking into the FBI or MI5 computers, and successfully unlocking passwords and letting off a nuclear weapon or bomb. Embar-Seddon (2002) stress it could include non-state actors getting unauthorised access, and therefore launching a cyber-terrorist attack.

Therefore terrorist use of the Internet as a facilitator to get instructions on building a nail bomb, mounting to an explosion might be part of a cyber-terrorist attack. David Copeland, for example, used online material to make a nail bomb with the intention of blowing up various locations in London (Hopkins and Hall 2000). Though he used cyber technology to aid his bomb making, it is questionable whether he would fall within the definition of a terrorist in the usual meaning of the word today (Stohl 2007). Similarly, in July 2009 a Muslim convert by the name of Andrew Ibrahim attempted a terrorist attack by making explosives which he intended to detonate in Bristol. He also like Copeland had found material on the Internet which had helped him create these explosives (Gardham 2008).

One question is, therefore, if somebody gets instructions on the Internet on how to make a bomb, are they a cyber-terrorist? For Denning's argument to hold, computers should be directly used for the cyber-terrorist attack. Copeland therefore is not a cyber-terrorist because the computer in his case acted as a knowledgeable database on how to make a bomb. Denning argues that the computer must be the weapon. Something that might help understand this link is the understanding of this process of why terrorists (for instance Copeland and Ibrahim) might choose the Internet to promote violence as a strategy through the social learning theory (Freiburger and Crane 2008). This theory asserts that individuals learn deviant behaviour from other groups, which may lead to extremist learning that is categorised by association, definitions, differential reinforcement, and imitation. They argue that mechanisms of the social learning theory are used by terrorist groups on the Internet as a tool to facilitate attacks and recruitment. This perspective of deviant behaviours offers a thought provoking insight into the processes that transform naive individuals like Copeland and Ibrahim into violent extremists (Desmond 2002).

Indeed, Freiburger and Crane refer to a European case study where Peter Cherif was recruited by Al-Qaeda over the Internet through a similar learning process (Powell et al., 2005). They argue that if groups become marginalized they become more susceptible to using the Internet for terrorist purposes. The use of social constructionism as a mechanism to understand the competing definitions of cyber-terrorism is crucial in getting a better understanding of the phenomena. Clearly, social practices and social behaviour change with time and thus our understanding of cyber-terrorism will also evolve as shown by the definitions discussed above. Within this context social constructionism offers both criminologists and sociologists a means to examine the various social processes that emerge when looking at interpretations of cyber-terrorism (Felson 2002).

McKenna and Bargh (1998) research suggests cyber space and terrorism have converged thus allowing terrorists to use the Internet for terrorist purposes. Despite this, cyber-terrorism, has

divided opinion; on one hand it is seen as a real threat to security and on the other it is seen as a myth (Wykes 2010). As a result of such conflicting opinion there is a real and present fear, which critics argue means the Internet has become a safe haven for potential extremists to 'groom' vulnerable people. Moreover, Tsfati and Weimann (2002) argue that terrorist groups are using the Internet to groom vulnerable individuals by justifying violence against innocent civilians as a retribution for the invasions and crimes committed against Muslims across the globe.

Hackers and Terrorism

Another problem with defining cyber-terrorism is often the blurring of different terminologies within the same context. For example, hacking has been defined as "operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software ("hacking tools"). Hacktivism includes electronic civil disobedience, which brings methods of civil disobedience to cyberspace" (Denning 2000: 263).

Therefore hackers are motivated by a variety of different reasons, one of the most common of which is fun and the challenge of hacking (Levy, 1984). For example, Gary McKinnon, a UK resident, who caused major damage to US security computers in the Pentagon, was wanted by the US on extradition charges for breach of US computer laws. On the 31st July 2009, McKinnon lost his appeal against extradition, but following the British Home Secretary's recent intervention, his appeal was granted. Despite this, his case does demonstrate further, that even if someone is not a terrorist but has used cyberspace for hacking purposes then they will also be treated as a cyber-terrorist.

Indeed, the association of hackers as potential cyber terrorists is often glamorised by the media. Yar refers to the mediatisation of hackers that contributes to this populist image of wizards and techno-geek's intent on causing carnage as dangerous cyber-terrorists (Yar 2006). This embodiment of media frenzy surrounding hackers is aligned according to him by themes of fear, crime and terror (Pool 2005). More recently, hackers have now been aligned to terrorist organisations using 'electronic jihad' to create forums and chat rooms used to distribute manuals and tools for hacking and cyber attacks. For example, Denning (2010) found that the Al-Farouq website allowed hackers the ability to use information that would enable disruption of electronic resources and a report by the Jamestown Foundation (2008) found many Jihadi forums had devoted entire sections to hacker warfare.

There is however some evidence to suggest that Denning's doomsday scenario has already happened. In Australia, in the Maroochy Shire, an individual successfully hacked into the water systems and caused severe problems and water contamination. The attack was conducted by Vitek Boden who was a disgruntled council worker and unleashed this major cyber attack. Using a laptop, he disrupted the central pumping system and caused major damage to the sewage systems in rivers and parks all across Queensland (The Age 2003). The worry about Boden's attack is that he was very skilful and had training in the use of computer technology. If the same skills were given to terrorists, then what happened in Australia may be a footprint for future cyber warfare.

The Motives of Hackers and Cyber-terrorists

The above example supports the claim that hackers with access to powerful computers could cause huge harm, but as much of the literature shows that the people with skills to do this do not have the same motivations as terrorists. Hacker's motivations are testing systems and not bringing down an aircraft as a number of studies have shown (Verton 2003). They have a high level of technological knowledge, spending endless hours honing their skills. They simply enjoy the challenge of trying to get into cyberspace. Their aims are not the same as extremists (Furnell and Warren 1999). Denning states that, cyber-terrorism "covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide" (Denning 2000: 241). But there is no evidence to suggest an aeroplane has fallen from the sky because terrorists have hacked into air traffic control systems and been able to bring it down. It is true that critical infrastructure can be vulnerable to a cyber attack, but no incident of magnitude has occurred. This must be because, cyber-terrorism can be a complex system of encryption and has little psychological impact and appeal when people are not injured. This gives groups like Al-Qaeda having to use the old trusted and relied upon methods; namely suicide attacks (Internet Haganah 2008).

This critical infrastructure is vulnerable and the Centre for the Protection of National Infrastructure in the UK have argued that electronic attacks on air traffic control are possible, citing the key vulnerable areas as 'malware, hacking, botnets, keystroke logging, phising and denial of service' as a threat if bringing down an aeroplane. Indeed, insiders may well be the new main threat as they have the key information at their fingertips. For example, the case of a computer analyst who worked at British Airways and had been sending sophisticated encrypted messages to Al-Qaeda on how to cause a major terrorist attack at Heathrow airport would be an example of the dangers of this (BBC News 2011).

To support Denning's argument that computers can be used as weapons in cyber-terrorism, we must examine the CRS Report for Congress 'Computer Attacks and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress' in October 2003, where there were various simulation exercises undertaken as a way of highlighting the potential threat of cyber-terrorism. Part of the exercises involved, the US Department of Defense undertaking a simulation exercises where they examined whether or not there ICT systems would be able to protect itself from such an attack. This exercise was called 'Eligible Receiver 1997' and gave crucial information that helped the US administration address their limitations in cyber security.

Part of the process included using hacker's and practitioners with experience of warfare to be part of the experiment. Members included the PLO, LTTE, Basque Fatherhood, ETA-PM and FARC, and the exercise was based on a virtual situation in Chechnya. The report showed that terrorists do not yet have the sophisticated skills in information technology nor are they willing to use these tactics. This example also shows that terrorists lacked the skills to use cyber technology in the manner in which Denning predicts. Furthermore, as noted above, to date, no terrorists have used cyberspace in this way. Terrorists aim to use tried and tested methods. Bringing down an aeroplane might kill innocent civilians and result in a loss of support from the community. A bomb against a legitimate target is preferable. This is because a target outside Parliament is more symbolic than bringing down an aeroplane.

Recruitment and Propaganda in Cyberspace

The alternative approach to Denning is Weimann's argument where cyber terrorism means terrorists use of the Internet to pursue their ideological aims. This includes terrorists using the Internet as a tool for propaganda via websites, sharing information, data mining, fundraising, communication, and recruitment (Conway 2003). For Weimann (2004) however it means terrorists using the Internet for psychological warfare, publicity, propaganda, fundraising, recruitment, networking, sharing information and planning (Lachow and Richardson, 2007; Whine, 1999).

Recruiters therefore may use more interactive Internet technology (Kohlmann 2008; 2006) to go through and use online chat rooms and cyber cafes (Furnell and Warren 1999), therefore looking possibly for enlisting support from vulnerable people. Marc Sageman states that this form of interaction and chat rooms helps build ideological relationships and are a key tool in radicalising the youth (Sageman 2008). Critics argue the Internet has changed dramatically in the past decade, and what was written about it seven to ten years ago is not as relevant today. Thus Al-Qaeda have used cyberspace in the past, but there are very few reported incidents of their online activity now. The nature of participation on the Internet, participation in online discussion is political activism. This is the process of turning to political violence is an active one, and not a passive one as portrayed in the Weinmann argument. The recent events in the Middle East show the murky lines between participation in social media and physical demonstrations.

Indeed, following the murder of Lee Rigby in Woolwich, the British Home Secretary, Theresa May was quick to identify the Internet as a potential source for radicalisation. She stated that: "There is no doubt that people are able to watch things through the internet which can lead to radicalisation" (Cited by Wintour and Jones in the Guardian 2013). As a result the UK government has announced a new taskforce called TERFOR which will examine ways of restricting what people can see on the Internet as a means of tackling the form of cyber-terrorism described by Weimann. The British government is also considering a new Communications Data Bill which it hopes will allow the state the power to filter extremist content and the flow of content and work more closely with Internet Service Providers in helping remove material which is considered to be inciting people to commit acts of terrorism or violent extremism.

There is however a third alternative approach to Denning and Weimann's argument, which is that cyber-terrorism, is a myth (Kohlmann, 2006). Critics argue the media has sensationalized the threat level and raised a public alarm which has been used to strike fear. Thus for Klang (2005), cyber-terrorism is a 'ghost' in a machine whilst Vegh (2002) describes cyber-terrorism as anti-hegemonic use of the Internet.

This form of cyber-terrorism thus has been associated with stereotypes of criminality that often identify terrorism and Muslims as Cyber-Jihadists and allows for draconian legislation. As Wall points out, discussion around cyber crime and indeed cyber-terrorism are often transcended through the media and politicians who use fear to overrate the actual nature and scale of the problem. This he argues leads to unnecessary legislation which is aimed at addressing the interests of the State (Wall 2001).

Anonymity

The Internet is a safe haven for terrorists (McKenna and Bargh, 1998) as they can remain anonymous, do not need to travel, do not need to show their passports (Weimann, 2004) but with the click of a mouse they can send messages of hate. For example, the online terrorist Younis Tsouli who used the name Irhaby (terrorist) 007 to hide his details ran extremist material online, promoting the cause for Al-Qaeda and was planning a major terrorist attack. In 2007, he was convicted in the UK for inciting terror through the use of the Internet. He had helped prepare Al-Qaeda's online propaganda campaign (including translation of al-Qaeda's online e-book into English). Geltzer (2008) however argues that such online material is still not a substitute for physical training camps and he uses the example of the July 7/7 bombers in the UK who took part in a number of rigorous physical training sessions as opposed to using online material for training and terrorist purposes.

Websites and Radicalisation

Websites are a powerful tool for extremist organisations. They can secure membership without directly approaching potential recruits (Tsfati and Weimann, 2002). The messages on websites can also reach thousands of people across the world. Online recruitment by terrorist organisations using websites and chat rooms is said to be widespread. These websites contain crucial information with historical accounts, statistics and with pictures and images of terror that can be downloaded and sent to millions of people. This creates support and act as a recruitment tool. The key to such extremist ideology over the Net is to create websites that cause resentment (Innes et al. 2011) for the West and allows international support to reach to millions.

Al-Qaeda's media operations are supported by a network of productions which include the al-Fajr and Global Islamic Media Front (Denning 2010). Al-Qaeda's most prominent media arm however is the As-Sahab institute for Media Productions which has had a leading role in recruitment of a wider audience. According to IntelCentre, As-Sahab releases more than 58 videos every six days (Intel Centre 2007). Furthermore, SITE an institution in Washington monitoring terrorist use of the Internet, found in 2009 online interactive question and answer session with Al-Qaeda's main leaders. They described the question and answer session with Ayman al-Zawarhi, as deeply 'disturbing'. These videos of Al-Qaeda act as propaganda tool and aim to use information technology as a way for Al-Qaeda to reach a global audience.

Within this paradigm, social constructionist theories are helpful in us having a better grounded understanding of the lone wolf analysis of self-radicalisation. For example, this is where individuals, might be subjected to radical ideologies and discourses that subsequently lead them down the process of self-radicalisation. In terms of having this isolated virtual environment, it allows individuals to meet like minded people who are able to 'groom' them and help create powerful social identities for disaffected individuals. This is clear in the case of Hamid Munshee, who remains the youngest person ever convicted of a counter-terrorism offence after being radicalised through websites and the online extremist material that was available to him.

Communication in Cyberspace

Al-Qaeda are now using the Internet to promote and indoctrinate their audience by propaganda means through; videotapes of its leaders condemning the West, t-shirts with slogans, flags, CD Roms, DVD's and photographs which all aim to advertise the Al-Qaeda brand globally. For instance, videotapes of the Baghdad sniper Juba are readily available on the Internet (Juba 2000). These videos show Juba killing American soldiers and as such Juba has become an immortalized figure described as a freedom fighter. The key aim of this propaganda is to disseminate information through various online terrorist means.

Furthermore, Omar Bakri, - (who was barred from entering the UK) - continued to use emails, chat rooms and online seminars to promote and broadcast his message of terror online using emails and chat rooms to keep in contact with those sympathetic to his cause. This use of the Internet allowed Omar Bakri to continue to preach his extremist views for recruitment purposes. It is also possible to use these chat rooms for terrorist funding online. For example, Paltalk which has been heavily criticised for its unwavering regulation of its members and the messages its members are able to post (Mosquewatch 2007).

The Evidence for Cyber-terrorism

If we examine the use of the Internet for terrorist purposes, most of the activity fits Weimann's argument. The evidence for Denning's argument is more limited. The first reported incidence of a so called 'targeted orientated' cyber-terrorist attack was in 1997 when groups aligned with the Liberation Tigers of Tamil Eelam claimed responsibility for suicide email bombings against Sri Lankan embassies over a two week period. Another more recent example is the Estonia conflict. In May 2007, Estonia was under siege for almost 3 weeks from hackers using sophisticated modes of technology to deface and cripple governmental and financial sectors. This attack is not the first of its kind as similar incidents of cyber attacks have taken place against different States. Before this incident, the Estonian government had invested heavily in protecting itself from such cyber attacks. It had mechanisms which, it argued, could combat this threat which included an Information Computer Technology infrastructure in place to deal with this and had created the Estonian Computer Emergency Services (CERT), a body committed to thwarting hackers.

Moreover, the Stuxnet virus which infected an Iranian power station and gained control of the system leaving the Iranian government's nuclear programme in turmoil. This was a complex and sophisticated attack on the Iranian industrial control systems in the Middle East which the UK government feared would increase the threat landscape for the UK. This is a clear demonstration of what a computer attack can look like. Also, the take down of the Internet in various Arab countries in 2011 by various governments show the problems of denial of services attacks.

All of these recent events demonstrate that an analysis of the arguments about cyber-terrorism must be viewed in a temporal context as the technology evolves. Therefore Weimann's view of the Internet participants acting as passive recipient of propaganda is somewhat problematic since it appears all participants are active participants, as they log on to various sites and may be transformed in the process of participation. They are active shapers of their own lives, not passive victims 'at risk, or susceptible'.

Conclusion

It appears that cyber-terrorism is omnipresent. It is a buzzword that seems to be fashionable in political discourse but has such a nebulous meaning that it has managed to become a 'poisoned chalice' when trying to define its true meaning. It is thus not a surprise that many academics have also weighed in on the debate. Our understanding of the term cyber-terrorism has and will continue to evolve. Within the paradigm of social constructionism, the increasing level of threat means that academics such as Denning (2000; 2009; 2001) and Weimann (2008) have both argued that cyber-terrorism is a real threat. The Denning argument has always placed the threat on the use of computers to destroy critical infrastructure, such as financial, military and governmental sectors. Conversely, the Weimann argument is that terrorists use the Internet as a means of propaganda and recruitment. Moreover, a line has to be drawn between hackers and terrorists whose aims and goals are incomparable and different. The first problem with answering such a question is how do you define a cyber-terrorist? Many countries have their own jurisdictions that define cyber-terrorism the concern being that the discourse on cyber-terrorism might actually alienate Muslim communities. Either way the government's new strategy of defence and security clearly puts cyber-terrorism as a potential danger.

The aim of this paper was to highlight two of those definitions raised with empirical evidence in order to try and establish the real truth about cyber-terrorism. The old and new technology of subversion and terrorism remains a threat and the use of steganography or mobile phones (as in the Mumbai attacks) means that there is a new form of technological threat. Therefore, the current nature of terrorism provides more support for Weimann's argument but things could change if terrorists become more sophisticated in their skills (Grabosky and Stohl 2010). Therefore I agree with the Weimann argument of what is cyber-terrorism and what it entails, although both arguments have their merits, there is a grey area but the Weimann argument holds a stronger connection to the term cyber-terrorism. The US and the UK have been heavy handed when it comes to dealing with those involved in cyber space (take the example of Gary McKinnon) and are seemingly using a heavy handed approach and regard everything at the moment as cyber-terrorism and this includes anyone downloading information from the Internet for research purposes as cyber-terrorists.

References

Altheide, D., (1997) 'The news media, the problem frame and the production of fear.' *The Sociological Quarterly*, 38 (4): 647–668.

BBC News. (2011) '*Rajib Karim: The terrorist inside British Airways',* [Online]. Available at: http://www.bbc.co.uk/news/uk-12573824 [Accessed: 9 June 2011].

Bronskill, J. (2001) 'CSIS on alert for cyber saboteurs: spy agency monitors threat to computer networks', *Ottawa Citizen*, 9th January: 3.

Conway, M. (2003) 'What is Cyberterrorism? The Story so Far.' Journal of Information Warfare 2(2) (March 2003): 33 - 42.

Denning, D. (2000) 'Cyber terrorism Special Oversight Panel on Terrorism Committee on Armed Services.' U.S. House of Representatives May 23, 2000. [Online]. Available at: http://www.cs.georgetwon .edu/~denning/inforce/cyberterror.html [Accessed: 20th May 2012].

Denning, D. (2010). 'Terror's web: how the Internet is transforming terrorism' In Majid Yar and Yvonne Jewekes *Handbook of Internet Crime*, Willan Publishers: 194-212.

Denning, D. (2009). 'Activism, Hacktivism, And Cyberterrorism: The internet as a tool for influencing foreign policy' Chapter 8 [Online] Available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf [Accessed: 15th February 2011].

Denning, D. (2001). Is Cyber Terror Next?, New York: US Social Science Research Council [Online] Available at: http://www.ssrc.org/sept11/essays/denning.htm [Accessed: 10th March 2009].

Desmond, P. (2002). 'Thwarting cyberterrorism,' *Network World*, Vol. 19, No. 7: 72-4.

Embar-Seddon, A. (2002) 'Cyber-terrorism: are we under siege?'*American Behavioural Scientist*, Vol. 45, No. 6: 1033-44.

Flemming, P, & Stohl, M, (2001) *'Myths and realities of cyber terrorism'*, In A. P. Schmid (Ed.), *'Countering terrorism through international cooperation',* Vienna, Austria: ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program: 70–105.

Felson, M., (2002) *Crime and Everyday Life',* (3rd Ed), California: Sage.

Foltz, B. (2008) 'Cyber-terrorism, Computer Crime, and Reality', *Information Management and Computer Security',* Vol. 12, No 2: 154-166.

Freiburger, T. and Crane, J. (2008). 'A Systematic Examination of Terrorist Use of the Internet' *International Journal of Cyber Criminology*, Vol. 2, Issue 1: 309-319.

Furnell, S., & Warren. M., (1999) 'Computer Hacking and Cyber Terrorism: The real Threats in the New Millennium.' *Computers and Security* 18 (1): 28-34.

Gardham, D. (2008). 'Al-Qaeda Terrorists who brainwashed Exeter Suicide Bomber Still on the Run,' *Daily Telegraph* [Online]. Available at: http://www.telegraph.co.uk/news/uknews/law-and-order/3204139/Al-Qaeda-terrorists-who-brainwashed-Exeter-suicide-bomber-still-on-the-run.html [Accessed: 3rd July 2013].

Geltzer, A. (2008). 'Six rather unexplored assumptions about Al Qaeda', *Critical Studies on Terrorism,* (December): 393-403.

Grabosky, P, (2007) "Requirements of prosecution services to deal with cyber crime"; *Crime Law Social Change,* 47: 201-223.

Grabosky**,** P. and Stohl**,** M.**,** (2010) *Crime and Terrorism.* Sage: London.

Hopkins, N. and Hall, S. (2000). 'David Copeland: a quiet introvert, obsessed with Hitler and bombs' *The Guardian* [Online] Available at: http://www.guardian.co.uk/uk/2000/jun/30/uksecurity.sarahhall [Accessed: 18 June 2011].

Innes. M., Roberts, C. & Innes, H. With Lowe, T. and Lakhani, S. (2011). *'Assessing the Effects of Prevent Policing A Report to the Association of Chief Police Officers';* Also See Innes, M. and Innes, H. (2011). '*Police Presence and Public Confidence in Local Policing: An Analysis of the British Crime Survey'*. HMIC.

IntelCentre. (2007). Al-Qaeda Messaging Statistics. [online]. Available at http://www.intelcenter.com/QMS-PUB-v3-3.pdf [Accessed 19 June 2011].

Internet Haganah (2008) 'Portrait of Rats, Preparing to Drown' 10th October 2008, [Online] Available at:http://internet-haganah.com/harchives/006420.html [Accessed: 15 January 2011].

Jamestown Foundation., (2008) 'Hacking Manual by Jailed Jihadi Appears on Web', *Terrorism Focus,* 5 (9) Jamestown Foundation 4th March.

Juba pictures. (2000). [Online]. Available at: http://www.blackflag.wordpress.com/2007/07/19/juba-the-baghdad-sniper-video/ http://blackflag.wordpress.com/2007/07/19/juba-the-baghdad-sniper-video/ [Accessed: 10th February 2010].

Klang, M, (2005). *'Virtual Sit-Ins civil disobedience and Cyberterrorism'* in M Klang and A Murray *Huaman Rights in the Digital Age*, London: Glasshouse Press.

Kohlmann, E.F. (2008). Al Qaida's MySpace: Terrorists Recruitment on the Internet. *CTC Sentinel*, 1:2 January; also see Kohlmann, E. (2006). The Real Online Terrorist Threat. *Foreign Affairs, 85*(5): 115-124.

Lachow, I., & Richardson, C. (2007) 'Terrorist use of the Internet: The real story'. *JFQ: Joint Force Quarterly, 45*: 100-103.

Levy, S. (1984). '*Hackers: Heroes of the Computer Revolution',* NY, Anchor Press.

McKenna, K.Y.A. & Bargh, J.A. (1998) 'Coming out in the age of the Internet: Identity "demarginalization" through virtual group participation.' *Journal of Personality and Social Pyschology, 75*(3): 681-694.

Mosquewatch.blogspot.com.(2007). 'Paltalk hosts Al-Qaeda, Hizballah, and Hamas chat rooms' [online] http://mosquewatch.blogspot.com/2007/12/exclusive-paltalk-hosts-al-qaeda.html [Accessed 15 June 2011].

National Security Strategy (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, HM Government: London. Cm 7953.[Online]. Available at: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy [Accessed: 29th June 2010].

Pollitt, M. (2001) *'Cyberterrorism-Fact or Fancy?*' [Online] Available at: http://www.csgeorgetown.edu/~denning/infosec/pollitt.html [Accessed: 12 February 2011]

Pool, J., (2005) 'Technology and Security Discussions on the Jihadi Forums', *Jamestown Foundation* October 11.

Powell, B., Carsen, J., Crumley, B., Walt, V., Gibson, H., Gerlin, A. (2005) 'Generation Jihad.' *Time*: *166,* 56-59.

Sageman, M. (2008). *Leaderless Jihad,* Philadelphia: University of Pennsylvannia Press.

Spector, Malcolm, and John I. Kitsuse. (1973). Social problems: A reformulation. *Social Problems* 21:145–159.

Stohl, M. (2007). 'Cyber terrorism: A clear and present danger, the sum of all fears. Breaking point or patriot games?', *Crime, Law and Social Change.* Vol. 46: 223-238.

The Age. (2003). 'The cyberspace invaders' (June 22) [Online] Available at: http://www.theage.com.au/articles/2003/06/21/1056119529509.html [Accessed: 16 June 2011].

Tsfati, Y., & Weimann, G. (2002). 'www.terrorism.com: Terror on the Internet.' *Studies in Conflict & Terrorism, 25*(5): 317-332.

Verton, D., (2003) '*Black Ice: The Invisible Threat of Cyber-Terrorism'* New York: McGraw-Hill Osborne.

Vegh, S. (2002). Hactivists or cyber-terrorists? The changing Media Discourse on Hacking, *FM* Volume 7, Number 10-7th October.

Wall, D. (2001) (Ed.) '*Crime and the internet'*, NY, Routledge,(2001).

Weimann, G. (2005). 'The sum of all fears?' *Studies in Conflict and Terrorism*, 129, 135.

Weimann, G. (2008) 'Al Qaida's Extensive Use of the *Internet' CTC Centenial* 1(2):607

Weimann, G. (2004) 'US Institute of Peace December' Special Report 119, [Online] Available at: http://www.usip.org/pubs/specialreports/sr119.html [Accessed: 5 August 2009].

Wintour, P. and Jones, S. (2013) Theresa May's measures to tackle radicalisation come under fire, *The Guardian*, [Online] Available at: http://www.guardian.co.uk/uk/2013/may/27/theresa-may-woolwich-radicalisation [Accessed: 2 July 2013]

Whine, M., (1999). Cyberspace-A New Medium for Communication, Command, and Control by Extremists' *Studies in Conflict & Terrorism 22*(3):231-246.

Yar. M (2006) *'Cybercrime and Society'* London, Sage Publications.