Author: F Cassim

ADDRESSING THE SPECTRE OF CYBER TERRORISM: A COMPARATIVE PERSPECTIVE

ISSN 1727-3781

2012 VOLUME 15 No 2

http://dx.doi.org/10.4314/pelj.v15i2.1

ADDRESSING THE SPECTRE OF CYBER TERRORISM: A COMPARATIVE PERSPECTIVE

F Cassim*

1 Introduction

Cyber space is regarded as the meeting place for criminal groups.[1] Cyber space has recently emerged as the latest battleground in this digital age.[2] The convergence of the physical and virtual worlds has resulted in the creation of a "new threat" called cyber terrorism.[3] Before 9/11, much apprehension arose about the threat of cyber terrorism including fears about a "digital Pearl Harbour".[4] The millennium bug further enhanced this fear. [5] In the context of post 9/11, the threat of cyber terrorism is often linked to Al- Qaeda and other terrorist organisations. [6] Cyber terrorists are regarded as computer savvy individuals who look for vulnerabilities that can be easily exploited.[7] Cyber terrorism is one of the recognised cyber crimes.[8] It has been defined as the "premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in the furtherance of such objectives.[9] Usually such attacks can take different forms: a terrorist could break into a company's computer network causing havoc, sabotage a country's gas lines or

* Fawzia Cassim, BA (UDW) LLB (UN) LLM LLD (UNISA)Associate Professor, Department of Criminal and Procedural Law, UNISA, cassif@unisa.ac.za

1 Tushabe and Baryamureeba 2005 *World Academy of Science, Engineering and Technology* 66.

2 Veerasamy 2009 *4th International Conference on Information Warfare and Security* 26-27 March.

3 It should be noted that the physical world refers to the place where we live and function, whilst the virtual world refers to the place in which computer programmes function.

4 The term "electronic or digital Pearl Harbour" was first coined by a tech writer one Winn Schwartau in 1991. See further, Stohl 2006 *Crime Law and Social Change* http://ceps.anu.edu.au/publications /pdfs/stohl.

5 The millenium bug which is also referred to as the Y2K problem, was the result of an outdated programming system which had not accounted for the transition from 1999 to 2000. Ofcourse, this problem soon came to pass without any major catastrophe. *Ibid*.

6 *Ibid*.

7 Raghavan 2003 *Journal of Law, Technology and Policy* 297.

8 It is important to distinguish between cyber crime and cyber terrorism. Cyber terrorism is usually restricted to activities which have a cyber component and the common components of terrorism. Therefore, it is submitted that a discussion of cyber terrorism cannot be divorced from a discussion of terrorism as the two concepts are linked together. This article will focus on cyber terrorism. However, it will also touch on terrorism where relevant.

9 Tushabe & Baryamureeba (n 1) 66-67. Also see Denning 2002 http://www/iwar.org.uk/cyberterror/resources/denning.htm.

wreak havoc on the international finance system.[10] These terrorist attacks against information infrastructures, computer systems, computer programmes and data may cause injury, loss of life and destruction of property. The aim of such unlawful attacks is to intimidate or persuade a government or its people to further a political or social objective.[11] Cyber attack methods are also said to possess many advantages over conventional methods of terrorism.[12] However, distinctions should be drawn between hacktivism and cyber terrorism, and the use of digital means for organisational purposes and the use of digital communications to actually commit acts of terror.[13]

The horrific events of 9/11 provided the impetus for many countries to introduce anti-terrorist legislation. Such anti- terrorist legislation not only focuses on legislation to criminalise cyber terrorist activity and impose penalties proportional to the act but also to prevent cyber terrorist activity or mitigate its impact by denying cyber terrorists materials, finance, support and equipment. The September 11 attacks illustrated that terrorism crosses national and ethnic boundaries and changed the prevailing attitudes to terrorism.[14] Indeed, after 9/11, the discussion about cyber security and cyber terrorism took centre stage.[15] The United States of America introduced the Patriot Act of 2001 in response to the 9/11 attacks on its soil. The United Kingdom has introduced a number of anti-terrorist legislation, namely, the Terrorism Act of 2000, the Anti-Terrorism, Crime and Security Act 2001 and the Terrorism Act of 2006. The Information Technology Amendment Act of 2008 in India contains a provision on cyber terrorism. South Africa has introduced a number of legislative measures to address the growing threat of cyber terrorism and terrorist financing such as the Prevention of Organised Crime Act 38 of 1999 ("POCA"), the Financial Intelligence Centre Act 38 of 2001 ("FICA"), the Electronic Communications and Transactions Act 25 of 2002 ("ECT), the Regulation of Interception of

10 Guru & Mahishwar "Terror networking" 71.
11 *Ibid*.
12 Terrorists find cyber attack methods to be cheaper than traditional methods; the actions can be difficult to track or trace; the actions can be done remotely anywhere in the world; a number of targets can be attacked effortlessly and it can affect a large number of people. See Garg "Cyber terrorism" 121. Also see Brunst 2010 "Terrorism and the Internet" 53-56.
13 See Stohl 2006 (n 4) 1. Also see Krapp 2005 *Grey Room Inc and Massachusetts Institute of Technology* 70-93.
14 Young 2006 *Boston College International and Comparative Law Review* 23-103 29.
15 Frauenheim 2002 http://news.cnet.com/2100-1001-977780.html?tag=fd_top.

Communications and Provision of Communications-Related Information Act 70 of 2002 ("RICA") and the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004 ("PCDTRA").[16]

The article examines the definition of cyber terrorism and different uses of the Internet by terrorist groups. The article also looks at measures introduced in the United States of America, United Kingdom and India to address the threat posed by cyber terrorism. The South African position is also examined. The study reveals that some confusion exists between the terms "hacktivism" and "cyber terrorism". This confusion together with media-induced fears about imminent threats about cyber terrorism has exaggerated the threat of cyber terrorism. Nevertheless, the study also demonstrates that while cyber terrorism does not pose an imminent threat, this could change in the near future. Therefore, the threat posed by cyber terrorism should not be taken lightly. To this end, proper and effective measures should be put in place to counteract such threats in the future. The article also contends that while the global fight against cyber terrorism is necessary, measures addressing cyber terrorism should not jeopardise basic human rights and fundamental freedoms. Therefore, countries need to ensure that a balance is maintained between the protection of human rights and the need for effective prosecution when enacting cyber terrorist legislation.

2 Definition of cyber terrorism

Terrorists are said to use the Internet to spread propaganda and conduct internal communications. However, threats resulting from terrorist use of the Internet have been strongly debated. According to Phillip Brunst, the difference in opinion is due to

16 It should be emphasised that these legislative measures do not refer to cyber terrorism specifically. However, they also contain measures or provisions to address terrorist financing and the protection of computer systems. The discussion on South Africa in section 6 will elaborate further.

a lack of exact terminology about the term "cyber terrorism".[17] Maura Conway defines cyber terrorism as "acts of terrorism carried out using the Internet and /or against Internet infrastructures".[18] Dorothy Denning defines cyber terrorism as "the convergence of terrorism and cyberspace. It is understood to mean unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in the furtherance of political or social objectives". [19] Mark Pollit defines cyber terrorism as a "premeditated, politically motivated attack against information, computer systems, computer programmes, and data which result in violence against noncombatant targets by sub national groups or clandestine agents".[20] Such attacks may lead to death or bodily injury, or cause explosions, plane crashes, water contamination, severe economic loss or serious attacks against critical infrastructure.[21] Cyber terrorism encompasses attacks against life and electronic infrastructure which are directed against national security establishments and critical infrastructure.[22] The aim of the attacks is to cause a state of terror and panic in the general public. Terrorists may also use information technology to perpetrate new offences or exploit cyberspace to commit more traditional activities such as planning, intelligence, logistical capabilities and finance.[23] Thus, terrorists may use computer technology to secure many of their organisational goals. However, attacks that disrupt nonessential services or present a costly nuisance do not amount to cyber terrorism.[24] Denning also maintains that while terrorists may use cyberspace to facilitate traditional forms of terrorism such as bombings, or use the Internet to spread their messages and

17 Brunst also maintains that the use of additional terminology such as "digital Pearl Harbour", "electronic Waterloo" and "electronic Chernobyl" which focus on possible future attacks by terrorists, has further complicated matters. See Brunst (n 12) 51.

18 Conway 2007 "Terrorism and the New Media" 1.

19 Denning (n 9) 2. Stohl sees no reason to reject Denning's definition. See Stohl (n 4) 8. Also see Gordon & Ford 2002 http://www.symantec.com/avcenter/reference/cyberterrorism.

20 Pollit 1998 http://www.scribd.com/doc/ ; Also see Goodman & Brenner 2002 *International Journal of Law and Information Technology* 150. However, Phillip Brunst regards Pollit's definition as being a narrow definition of cyber terrorism. He maintains that a broad definition of cyber terrorism might include other forms of terrorist use of the Internet. See Brunst (n 12) 51.

21 Gordon & Ford (n 19) 4; Goodman & Brenner (n 20) 145; Denning (n 9) 2. Also see Brunst (n 12) 66.

22 Goodman & Brenner (n 20). Weimann maintains that cyber terrorism involves the use of computer networks tools to harm or shut down critical national infrastructures such as energy, transportation and government operations. Weimann 2005 *Studies in Conflict and Terrorism* 130.

23 *Ibid*.

24 Denning (n 9) 2.

recruit supporters, there are few indications that they are actually pursuing cyber terrorism.[25] However, this could change in the future.

The blurring of the distinction between hacktivism and cyber terrorism has also fuelled the debate on cyber terrorism. The term "hacking" refers to the use of special software and techniques of a disruptive nature ('hacking tools') to exploit computers.[26] However, Peter Krapp maintains that hacktivists should not be regarded as secret agents, soldiers, terrorists or net warriors but rather as individuals or groups who strive to capture attention and achieve maximum media effect in their quest to raise the awareness of citizens regarding certain rights and liberties.[27] It is debatable whether hacktivists will succeed in changing government policy.[28] Nevertheless, hacktivism should be distinguished from cyber terrorism.

3 Different uses of the Internet by terrorist groups

Organised crime and terrorist groups are using sophisticated computer technology to bypass government detection and carry out destructive acts of violence. The actions of Rami Yousef who orchestrated the 1993 World Trade Center bombing by using encryption to store details of his scheme on his laptop computer, is a case in point .[29] It has also been reported that the first known attack by terrorists against a country's computer system took place in Sri Lanka in 1998, when the ethnic Tamil Tigers guerrillas overwhelmed Sri Lankan embassies with 800 e-mails a day over a two-week period.[30] These messages threatened massive disruption of communications,

25 Conventional terrorism is said to have a "greater dramatic effect" than cyber terrorism. Denning (n 9) 19-20; 22. Also see Stohl (n 4) 8; 11-13. However, Brunst reports that although many attacks have taken place, they have been kept confidential to avoid security lapses or breaches if such details were published. See Brunst (n 12) 53.

26 Hacktivism includes electronic civil disobedience. For more information, see Denning (n 9)12.

27 Krapp (n 13) 86-88. Also see Brunst (n 12) 56-57, regarding the blurring of the distinction between the terms "hacktivism" and "cyber terrorism."

28 Denning (n 9) 22.

29 Bazelon *et al* 2006 *The American Criminal Law Review* 306.

30 See Tushabe & Baryamureeba (n 1) 67; Also see Denning (n 9) 7. Also see Walker 2006 "Cyber –Terrorism: United Kingdom" 635.

and caused fear and panic among ordinary Sri Lankans as the rebel group was notorious for killing people. During the war in Kosovo in 1999, Serb sympathisers tried to target the NATO website with viruses.[31] In another incident, cyber attacks were launched against the Estonian state during April 2007. The targets were the Estonian Parliament, banks, media houses and government departments. These attacks affected critical services.[32] The events in Estonia illustrated how countries can be put at risk by attacks via the Internet.[33] Thus computers have been used as tools by terrorists to execute terror attacks and advance their particular agendas.[34] However, there is "little concrete evidence" to demonstrate that cyber terrorism has resulted in a catastrophic loss of life or physical destruction often associated with conventional terrorism.[35]

On the other hand, terrorists can also use the Internet for organisational purposes rather than to commit acts of terror. Terrorists can use the computer to commit various crimes such as identity theft, computer viruses, hacking, malware, destruction or manipulation of data.[36] Terrorists can use information communication technologies (ICTs) and the Internet for different purposes: propaganda, information gathering, preparation of real-world attacks, publication of training material, communication, terrorist financing and attacks against critical infrastructures.[37] This means that organisations or governments which depend on the operation of computers and computer networks can be easily attacked. The Internet has the advantage of being "a more immediate, individual, dynamic, in-depth, interactive,

31 Walker (n 30) 635. Chinese computer hackers also launched attacks on US web sites to protest against NATO's bombing of a Chinese embassy in Kosovo. See Krapp (n 13) 72.
32 See Veerasamy "Conceptual Framework" 4. Also see Brunst (n 12) 62.
33 Brunst (n 12) 52.
34 It has also been reported that computers and the Internet played a key role in the execution of the September 11 attacks in that computers were used to make travel plans and purchase air tickets. However, it is submitted that these acts can be distinguished from cyber terrorism in that computers are used here to **plan** acts of terror rather than to commit acts of terror. See Gordon & Ford (n 19) 4; also see Gerke 2009 "Understanding Cybercrime" http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html.
35 Stohl (n 4) 2. Computers are said to be the means to achieve terrorist purposes rather than the objects of attack. See Walker (n 30) 636.
36 "Malware" is the distribution of malicious codes to disrupt computer networks. See Raghavan (n 7) 299-300 regarding the different types of attacks that can be brought against computer networks. Also see Gordon and Ford (n 19) 7.
37 Gerke (n 34) 52-57. Also see Brunst (n 12) 70-73; 74-75; Walker (n 30) 635-642 and Conway (n 18) 4-10.

anonymous, unedited, cheaper and far-reaching process than conventional media". [38] These factors facilitate the task of terrorists to execute their plans unhindered.[39] Information on how to make bombs is also freely available on the Internet. [40] However, it should be borne in mind that "terrorist use of computers as a facilitator of their activities, whether for propaganda, recruitment, communication or other purposes is simply not cyber terrorism".[41] Similarly, protest action by way of" virtual sit-ins" on web sites (called electronic civil disobedience) does not amount to cyber terrorism.[42]

4 Cyber terrorism: Myth or reality?

Although cyber terrorism has become a more dominant force in the global battle between information and network warfare, much misconception still exists over what cyber terrorism entails. As stated earlier, it is important to recognise that all "cyberspace-based threats" are not necessarily terrorism.[43] According to Stohl, the concern with the threat of cyber terrorism stems from a combination of fear and ignorance.[44] Stohl maintains that the discussion about cyber security also involves some misinformation and the exploitation of fears of the general public.[45] The failure to distinguish between hacktivism and cyber terrorism has also contributed to the

38 Conway (n 18) 3-4.

39 Raghavan (n 7) 297. It should be stated that the general motivations to commit crimes via the Internet are: the lack of a definite physical location, the use of bandwidth and speed of third parties to perpetrate cyber crimes, the anonymity of cyberspace, the lack of physical borders or boundaries and the cost- benefit ratio. For detailed discussion about these issues, see Brunst (n 12) 53-56.

40 This includes material such as *The Terrorist's* Handbook, *How to Make Bomb: Book Two* and *The Anarchist's* Cookbook. See Walker (n 30) 645. The Internet also contains detailed instructions on how to establish underground organisations and execute terror attacks. See Conway (n 18) 17.

41 Weimann (n 22) 133. Attacks on critical infrastructure are said to fall under the domain of cyber terrorism. Also see Walker (n 30) 634.

42 For more information on electronic civil disobedience, see Dominguez 2008 *Third Text* 661-670.

43 For example, attacks on data contained within systems and programmes do not translate to "terrorist" acts. However, in some instances, the distinction between cyber crime (such as hacking) and cyber terrorism has also become blurred. See Brunst (n 12) 56-57.

44 This translates to a fear of technology and the fear of terrorism (both unknown factors). This results in the nature of cyber terrorism being misunderstood. Also see Embar-Seddon 2002 *American Behavioural Scientist* 1033-1043.

45 Stohl (n 4) 5. Also see Conway (n 18) 29.

fear and hype about the threat of cyber terrorism.[46] Some writers believe that the media has also exaggerated the possibility of cyber terrorist attacks causing much concern and panic in the public domain.[47] However, the number of potential targets and the lack of proper and adequate safeguards have also made addressing the threat a daunting task. One should also not underestimate the risk and potential of future threats.[48] Thus, a need arises for the re-examination of commonly held beliefs about the nature of computer systems and cyber terrorism.[49] To this end, measures to address cyber security, to introduce adequate cyber terrorist legislation and to make software safe and effective should be introduced. One should also bear in mind that the removal of technical information from the Internet (such as information on how to execute terror attacks), does not provide an adequate guarantee to safeguard the Internet as such material can be easily loaded onto offshore or other international severs.[50] Gordon and Ford maintain that an urgent need arises for the development of minimum standards of security for computer networks.[51] They also endorse the idea of negotiations to resolve long-standing disputes with terrorist groups, the careful use of surveillance techniques to gather information on terrorist communications and the sharing of information across various public and private sectors to combat terrorism.[52]

5 Comparative perspective

The following discussion will examine measures taken by the United States of America, the United Kingdom and India to address cyber terrorist threats. These countries have been the target of conventional terrorism; so it is not surprising that they are taking potential cyber terrorist threats seriously.

46 Hacking refers to activities conducted online that aim to reveal, manipulate and exploit vunerabilities in computer operating systems and software. Also see Denning (n 9) 12.
47 Veerasamy (n 2) 1. Also see Green 2002 *Washington Monthly* http://www.washingtonmonthly.com/features/2001/0211.green.html 1-8. Also see Frauenheim (n 15) 2.
48 The lack of a large cyber attack by terrorists should not make one complacent. See Brunst (n 12) 75.
49 Gordon and Ford (n 19) 14.
50 Conway (n 18) 19.
51 Gordon and Ford (n 19) 12.
52 *Ibid*.

5.1 United States of America

Since September 11, concerns about cyber terrorism in the United States have multiplied. [53] The USA Patriot Act of 2001 was enacted By President George Bush in response to the 9/11 attacks on the World Trade Centre and Pentagon.[54] Although the USA Patriot Act addresses several issues, certain key provisions relate to cyber security and other computer concerns. To this end, the Act has eased restrictions on electronic surveillance to facilitate the capture of terrorists.[55] The Act also contains anti-money laundering provisions in order to prevent terrorists from achieving any financial gain from their actions.[56] The Patriot Act also includes terrorism and computer crimes on its list of offences.[57] However, the Act has been criticised for violating the civil rights of ordinary American citizens.[58]

Cyber terrorists are said to have the ability to cripple critical infrastructure such as communication, energy and government operations. Cell phones have also been used to track terrorists and to provide evidence against them.[59] Terrorist websites are also under increased surveillance since 9/11 to strengthen the fight against

53 The September 11 hijackings led to an outcry that airliners are susceptible to cyber terrorism. See Green (n 47) 4.

54 The USA Patriot Act stands for: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. See Young (n 14) 75-76. Also Raghavan (n 7) 298; 304. The law protects the national infrastructure by easing the restrictions placed on electronic surveillance by amending provisions of the Computer Fraud and Abuse Act 1986 to increase penalties for cybercrimes.

55 The Act has expanded the powers of the federal government to combat terrorism in the area of surveillance and interception of communications; it provides for closer policing of financial transactions; it strengthens the anti-money laundering regulations to disrupt terrorist funding opportunities and it authorizes administrative detentions. See Young (n 14) 76. Alse see Raghavan (n 7) 305.

56 See ss 301-77. Raghavan (n 7) 305.

57 See s 814. The increase in vigilance against the threat of cyber terrorism has resulted in increased penalties for all forms of computer hacking including hacktivist activity. See Dominguez (n 42) 664.

58 To illustrate this, the expanded surveillance measure in the Act has been criticised because of its lack of adequate checks and balances. The government's ability to spy on suspected computer trespassers without a court order has also been criticised as it infringes on the civil liberties of suspected trespassers. Raghavan (n 7) 310.

59 Walker (n 30) 664. It is noteworthy that South Africa has introduced the Regulation of Interception of Communication Act 2002 (RICA) for this purpose. For further information on RICA, see the discussion in section 6.4 below.

terrorism.[60] A call has also been made for the development of cyber intelligence as a better co-ordinated government discipline to predict computer-related threats and deter them.[61] A bill on cyber security is currently being debated by the US Senate.[62] The bill is aimed at the protection of critical infrastructure such as power and phone companies, water and treatment plants and wireless providers. The enactment of the USA Patriot Act and other measures taken by the American government demonstrates the government's commitment to combat international terrorism including cyber terrorism.

5.2 United Kingdom

The Terrorism Act of 2000 was introduced to address terror attacks in the United Kingdom. The listed prohibited actions include endangering another person's life or creating a serious risk to the public health or safety, acts designed to seriously interfere with or disrupt an electronic system and acts involving serious violence to or death to another person or serious property damage.[63] Section 1(2)(e) of the Terrorism Act 2000 describes a terrorist act as one that "is designed seriously to interfere with or seriously disrupt an electronic system". The inclusion of this section is said to consider cyber terrorism.[64] This phrase might contemplate cyber terrorism including for example, attacks on banking services through the internet and destruction of computer-stored data. The emphasis on "serious" is said to be important as "a costly nuisance" does not amount to cyber terrorism.[65]

In response to the September 11 attacks, the British Government passed the Anti-Terrorism, Crime and Security Act of 2001. On 14th December 2001, the British Anti-Terrorism, Crime and Security Act became law. Its object is to ensure the Government has adequate powers to counter the increased threat of terrorism in the

60 Conway (n 18) 22-23; 28.
61 Anonymous 2011 http://www.eLaw@legalbrief.co.za.
62 See Anonymous 2012 http://www.csoonline.com/article/700397/liberman-cybersecurity-act-of-2012.
63 See s 1 of the Act.
64 Walker 2006 (n 30) 632.
65 *Ibid*. Also see Denning's definition, Denning (n 9) 2.

United Kingdom following the events of September 11th. This Act has also been the subject of criticism.[66]

The Terrorism Act of 2006 was introduced in response to the 2007 London bombings. Provisions in the Act now make it illegal to 'glorify terrorism' and distribute terrorist publications. [67] The Terrorism Act of 2006 also allows groups or organisations to be banned for those offences and covers anyone who gives or receives such training. The Act also creates new offences of undertaking terrorism training, preparation or planning of a terrorist act and disseminating terrorist publications. The Act has been criticised by human rights campaigners and concerns have been raised about the issue of "glorification".[68] Section 17 of the Act facilitates the prosecution of terrorist offences committed outside the United Kingdom.

Information available on the Internet is being used not only by sophisticated terrorist groups but also by disillusioned and unhappy individuals who are prepared to use terrorist tactics to pursue their agendas. To illustrate this, in 1999, a right-wing extremist David Copeland planted nail bombs in different areas of London.[69] His actions targeted multi-racial communities and the gay community, and he killed three people and injured 179 over a period of three weeks. At his trial, Copeland disclosed that he learned his deadly techniques from the Internet by downloading copies of *The Terrorist's Handbook and How to Make Bombs: Book Two.*[70]

Thus, the United Kingdom government is seeking protective measures against the cyber terrorist threat. To this end, the United Kingdom government has also set up

66 See Young 2006 (n 14) 73. The following criticism has been leveled: the fact that some of the proposed measures did not relate to terrorism at all; the exclusion of judicial review of the Home Secretary's power to order detention; and the introduction of European measures, including police co-operation and simplified extradition procedures without adequate parliamentary scrutiny. Also see Nicholls 2002 *CHRI News* http://www.humanrightsiniative.org/ publicatons/hl/1/5/2012.

67 See Anonymous 2012 http://www.news.bbc.co.uk.

68 *Ibid*.

69 Conway (n 18) 17.

70 According to Conway, these manuals are still available on the Internet. *Ibid*.

the National Technical Assistance Centre which is a surveillance advice and interception facility.[71] A call has been made to introduce a new offence that would render data inaccessible, introduce the use of more effective filtering mechanisms, educate the general public about cyber terrorism and create public-private partnerships to address security strategies in the computer industry.[72] Terrorists are said to be increasingly using online technology to perpetrate cyber attacks and communicate their propaganda. Hence, the British Government has also recently launched a counter-terrorism strategy to keep pace with evolving technology and counteract radicalisation on the Internet. [73] A Cambridge technology company Plextek is also urging the UK Government to create a Cyber Attack Prevention Agency to effectively protect the national critical infrastructure against cyber terrorism.[74] A recent proposal by the government to introduce a new strategy of interception of communication has been criticised by civil society as it will lead to a violation of people's privacy.[75] The above discussion demonstrates that the UK Government is taking the cyber terrorist threat seriously. The government has recognised that it has a primary duty to maintain security in all spheres of government. However, it remains the responsibility of human rights campaigners to monitor carefully the enforcement of anti-terrorist legislation and to ensure that miscarriages of justice are avoided.

71 See Walker (n 30) 661.

72 *Id* 662.

73 See "Al Qaida in the UK" *The Independent* mhtml:file: // E:\Warning of rise in cyber-terrorism – Crime – UK – The Independent .

74 It should be noted that this agency will train critical infrastructure staff in the departments of water, energy and finance. See "Cambridge Wireless debates UK Cyber Terrorism Agency" *Business Weekly* mhtml:file://E:\Cambridge Wireless debates UK cyber terorism agency Business Wee...

75The new law requires all UK Internet companies to install hardware which will enable the Government Communication Headquarters to intercept any phone call or text message. See Jalalzai 2012 *The Daily Outlook* http://outlookafghanistan.net/topics.php?post_id=3833. Also see Anonymous 2012 http://www.elaw@legalbrief.co.za . It is noteworthy that South Africa has introduced the Regulation of Interception of Communication Act (RICA) for this purpose. RICA has implemented most of the measures under discussion in Britain. For further information on RICA, see the discussion in section 6.4 below.

5.3 India

The Information Technology Act of 2000 contained no provision on cyber terrorism. However, this lack of cyber security strategy was rectified when the Information Technology Amendment Act of 2008 was promulgated. The Information Technology Amendment Act contains a provision on cyber terrorism. Section 66F defines and penalises cyber terrorism. In order to qualify as a cyber terrorist act, the act must be committed with the intention to threaten the unity, integrity, security or sovereignty of India by way of interfering with authorised access to a computer resource, obtaining unauthorised access to a computer resource or damaging a computer network. The acts are punishable if they cause death or injuries to persons or cause damage or destruction to property, disrupt essential supplies or services or affect critical information infrastructure. The penalties range from three years' imprisonment to life imprisonment and a fine depending on the seriousness of the crime.

India has been a target of conventional terrorism so it is not surprising that India is taking the threat of cyber terrorism seriously.[76] It is submitted that stringent measures are necessary to combat the threat of cyber terrorism and to act as effective deterrents. The imposition of stringent punishment for cyber terrorism demonstrates the Indian government's intention to prevent terrorists using the Internet to perpetrate crime. Whilst the provisions addressing cyber terrorism are welcomed, concerns have been raised about their potential abuse by government authorities.[77] Nevertheless, the Act has been welcomed as a step in the right direction.[78]

The above discussion demonstrates that the United States of America, the United Kingdom and India are taking potential cyber terrorist threats seriously. All these

76 The November 2008 Mumbai bombings is a case in point. The advent of the Information Technology (Amendment) Act 2008 has been described as a knee-jerk reaction to the November 2008 terror attacks in Mumbai. See Nappinai "Cyber Crime law in India" 405.
77 Nappinai (n 76) 411.
78 *Id* 414.

countries have introduced legislation to address terrorism, terrorist financing and cyber terrorism. The increase in vigilance against cyber terrorist threats, the increased surveillance of terrorist websites and the introduction of a cyber security bill in the United States demonstrates the American government's concern about cyber terrorism. Further steps taken in the United Kingdom include *inter alia*, the introduction of a surveillance and interception facility and the adoption of a counter terrorist strategy to combat terrorist activity on the Internet. The Information Technology Amendment Act in India contains a specific provision on cyber terrorism. Thus, protective measures are being taken to counteract terrorist threats on the Internet, address cyber security concerns and to keep abreast with evolving technology. However, legislation in these respective countries has also been criticized by human rights campaigners for violating the human rights and freedoms of their respective citizens. Thus, these countries need to ensure that their fight against cyber terrorism does not jeopardise basic human rights and fundamental freedoms. To this end, a balance should be maintained between the protection of basic human rights and the need for effective prosecution.

6 South Africa

Cybercrime is said to be growing faster in Africa than any other continent.[79] The advent of information technology has made Africans more dependent on the Internet. At the same time, the increase in untrained and apathetic users has made information infrastructures in African countries more vulnerable to attacks by criminals who can pursue their malicious agendas undetected. The absence of suitable legal frameworks and safe and effective computer software to address cyber terrorism at national and regional levels, inadequate telecommunication infrastructure, the pre-occupation of African countries with internal factors such as the Aids crisis, poverty, rising unemployment, basic service delivery, crime and corruption have all contributed to the continent becoming a "haven" for cyber

79 For further information on cyber crime in Africa, see Cassim 2011 *CILSA* 123-138. Also see Kumar 2010 "Africa" http: //www.psfk.com/2010/04.

criminals including cyber terrorists.[80] This has created an environment that is vulnerable to attacks by cyber terrorists.

The question arises how real is the threat of cyber terrorism in South Africa? There is presently no reported case of cyber terrorism in South Africa. Similarly, the nature of terrorist financing in South Africa is not well documented, although the spectre of terrorist threats looms in Africa. It has been reported that a number of Al-Qaeda or al-Qaeda-related operatives have been arrested in Southern Africa or being captured in transit.[81] Botha maintains that a likelihood of Al-Qaeda attacks against Western interests exists in South Africa, even though the South African government disregards such a threat because of its neutrality on the so-called "war on terror" and its pro-Palestinian stance.[82] Nevertheless, there are also reports of right-wing terrorism in South Africa with members of some right- wing organisations currently facing trial for sabotage and terrorism. Right wingers remain on trial for trying to overthrow the government in 2002 through many attacks. Such attacks included an explosion on a railway line at Soweto outside Johannesburg that killed a woman. The case is still continuing.[83] Despite reports of plots by terror groups ranging from Al-Qaeda to "home grown" white militants to attack the World Cup Soccer 2010 event, none materialised.[84] There have also been recent reports of the use of South African passports by terrorist groups.[85] However, the South African home affairs government has conducted an investigation concluding that the passports were fake.

South Africa has introduced the following legislative measures to counteract cyber terrorism and terrorist financing:

80 Also see Anonymous 2011 http://cbr.co.za/news.
81 Basdeo 2011 "Terrorist financing" 49.
82 Botha 2005 http://www.jamestown.org. Also see Cassim 2011 "Combating cyber terrorism" 96-105.
83 Anonymous 2011 http://mg.co.za/article/2010-04-19.
84 Anonymous 2011 http://mg.co.za/article/2010-05-31.
85 Anonymous 2011 http://mg.co.za/article/2011-06-17. The government is also tightening its counter corruption measures at its various home affairs departments. It is submitted that this strategy will strengthen the fight against terrorism and cyber terrorism at critical infrastructures.

6.1 The Prevention of Organised Crime Act 38 of 1999 ("POCA")

POCA contains measures to *inter alia* combat organised crime, money laundering and criminal activities. The Act also contains provisions to freeze and confiscate property, and forfeit it to the state if such property is acquired through criminal activities.[86] POCA requires businesses to report transactions involving funds or assets associated with criminal activities. This includes the financing of future terrorist activities. Thus, POCA targets organised crime, money laundering and terrorist financing both nationally and internationally.

6.2 Financial Intelligence Centre Act 38 of 2001 ("FICA")

South Africa is a country rich in mineral resources such as gold, diamonds, uranium and platinum. This makes the country vulnerable to clandestine business transactions which can be used to facilitate terrorist financing and money laundering. The advent of AML/CFT (anti money laundering and combating the financing of terrorism) regimes have thus become key tools in addressing terrorism in the post 9/11 era.[87] FICA outlaws money laundering and other unlawful actions. The aim of this legislation is to prevent and suppress terrorism financing.[88] To this end, the Act has introduced an anti-money laundering regime to encourage voluntary compliance and self-regulation by institutions (such as banks) which may be exploited for money laundering. To this end, all bank customers are required to be FICA compliant to operate their accounts. Section 21 of FICA requires banks or financial institutions to verify the identity and residential addresses or business addresses of all customers before rendering any financial service. Thus, stringent financial controls have been put in place to counteract the threat posed by terrorist financing.

86 See section 18.
87 Basdeo (n 81) 49-52.
88 Terrorist groups raise funds from third parties to finance their activities. Money is considered to be their lifeline in "their struggle". See Conway (n 18) 7-10.

6.3 The Electronic Communications and Transactions Act 25 of 2002 ("ECT")

The ECT addresses *inter alia*, "the facilitation and regulation of electronic communications and transactions in the public interest".[89] The ECT deals comprehensively with cybercrime in Chapter 13.[90] Denial of service attacks (DOS) are attacks that cause a computer system to be inaccessible to legitimate users. These actions include unauthorised access, unauthorised modification or the utilisation of a programme or device to overcome security measures.[91] It is submitted that DOS attacks are criminalised in sections 86(1) to 86(4) of the ECT. Penalties range from a fine or imprisonment not exceeding 12 months to a fine or period of imprisonment not exceeding five years.[92] These penalties have been criticised as not being stringent enough to deter cyber criminals.[93] Although, the ECT does not specifically refer to the offence of cyber terrorism, sections 86-88 may well be used to address the offence of cyber terrorism.[94]

Jurisdictional issues are addressed in section 90 of the ECT. Section 90 of the ECT provides that a court in the Republic (SA) trying an offence in terms of this act committed elsewhere will have jurisdiction in the following instances:

(a) where the offence was committed in the Republic;
(b) where part of the offence was committed in the Republic or the result of the offence had an effect in the Republic;

89 See s 2(1) of ECT. For further discussion on this Act, refer to Cassim (n 79) 127-129. Also see Cassim 2009 *PER* 21-25.
90 The following offences are regarded as punishable offences: ss 86(4) and 86(3) introduce new forms of crimes called anti-cracking (anti-thwarting) and hacking law, which prohibit the selling, designing or producing of anti-security circumventing technology; e-mail bombing and spamming are addressed in ss 86(5) and 45 of the ECT respectively, whereas the crimes of extortion, fraud and forgery are addressed in s 87.
91 Kufa 2009 http://umkn-lib01.int.unisa.ac.za/nxt/gateway.
92 See s 88.
93 Also see Van der Merwe *et al* (Lexis Nexis 2008) *Information Technology Law* 75-78.
94 However, it is submitted that more stringent measures are required to deter cyber terrorists.

(c) where the offence was committed by a South African citizen or a person with permanent residence in the Republic or a person carrying on business in the Republic;

(d) or the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight from the Republic at the time that the offence was committed .

It is submitted that section 90(b) facilitates the prosecution of cyber terrorists based abroad who may launch attacks against our local computer networks and critical infrastructure. A South African court will also be vested with jurisdiction in instances where an offence such as a cyber terrorist act "had an effect in the Republic".[95] A South African court will also be vested with jurisdiction if a South African national commits a cyber terrorist act abroad based solely on the nationality of the perpetrator.[96]

6.4 The Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002 ("RICA")

RICA requires all customers with cell phone numbers on cellular networks in South Africa to register their details with their respective networks as from 1 August 2009. Section 39 of RICA provides that before a telecommunication service provider must register a contract, the customer is required to furnish the service provider with his or her full name and address and a copy of his or her identity document. Section 40 of RICA contains a similar requirement but it is directed at the sellers of cellular phones and SIM cards. The aim of RICA is to help make South Africa a safer country. The objective of the Act is to help law enforcement agencies identify users of cell phone numbers and track down criminals using cell phones for illegal activities. The failure to comply with this law will result in the disconnection of cellular numbers from their cellular

95 See s 90(c) of the ECT.
96 *Ibid*. It is noteworthy that this provision is similar to s 17 of the UK Terrorism Act of 2006.

networks. Thus, this Act can also be used to track down cyber terrorists using cell phones to plan their malicious agendas and commit illegal activities.

RICA prescribes harsher measures than the ECT. To illustrate this, section 51 of RICA prescribes fines not exceeding R 2000 000 or imprisonment not exceeding 10 years. Regarding juristic persons, fines may increase to a maximum of R 5000 000. Thus, the criminal sanctions in the ECT appear to be inadequate when compared to RICA. RICA legislation has proved to be useful to police in securing convictions with intercepted cell phone evidence. It has been reported that convictions in numerous cases have depended on cell phone evidence either in terms of the communication between individuals involved in crime or determining the location of individuals who were involved in crime.[97] However, the implementation of the Act is not without criticism. It has been reported that South Africa has no system in place to reel in cell phone customers who are in possession of RICA-registered SIM cards even if their personal information have not been entered into the network databases as required by law. Unscrupulous traders have also sold RICA-registered SIM cards without asking buyers for their personal information and documentation in contravention of the law. Thus, a national audit of the RICA system is due to be debated to discuss the scope of the problem.[98] RICA has implemented most of the measures presently being introduced in the United Kingdom.[99] However, the routine abuse of such measures in South Africa should be investigated to determine the extent of the problem.[100]

97 Anonymous 2011 http://www.elaw@legabrief.co.za.
98 *Ibid*.
99 Anonymous 2012 http://www.elaw@legalbrief.co.za.
100 *Ibid*.

6.5 The Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004 ("PCDTRA")

This Act provides measures to *inter alia* prevent and combat terrorist and related activities; it gives effect to international instruments addressing terrorist and related activities; provides measures to prevent and combat the financing of terrorist related activities and provides investigative measures in respect of terrorist and related activities. The term "terrorist activity" is widely defined in Chapter 1.[101] The list of prohibited actions is contained in (i)-(viii).[102] The prohibited action listed in (vi) is relevant to the offence of cyber terrorism: The term "terrorist activity" is defined *inter alia* as any act which "causes serious interference with the disruption or delivery of an essential service, facility or system, whether public or private". It should be noted that "an essential service, facility or system" refers to an electronic system, including an information system, a telecommunication system, a banking or financial service or system, an essential government service system, an essential public utility or transport system, an essential infrastructure facility or any essential emergency services such as the police, medical or civil defence service. Thus, this phrase covers critical infrastructures such as banks, communications systems, government departments and computer networks. The harm or activity must threaten the unity and territorial integrity of the Republic, intimidate or cause insecurity within the country or have a negative impact on the public or the operation of state organs or international bodies. From the above, it can be ascertained that any act which causes interference with an essential service, facility or system may be regarded as an act of cyber terrorism.

Section 18 of the Act contains a range of penalties. The penalties range from a period of life imprisonment in the High Court to a five year sentence in the magistrate's court for a section 2 offence (offence of terrorism) or section 5 offence (offence relating to explosive or other lethal device). Section 4 offences (offences associated with the financing of specified offences) are considered to be more serious. Such offences carry a fine of R100 million or a period of imprisonment of 15

101 See ch xxv in the Act.
102 Refer to the Act for further information about these actions.

years in the High Court or regional court. A similar offence in the magistrate's court will attract a fine of R250 000 or five years' imprisonment. [103] The stringent penalties in the Act demonstrate that the government is taking terrorism and the cyber terrorist threat seriously.

7 The way forward for South Africa

South Africa has ratified numerous international instruments on terrorism such as the International Convention on the Suppression of the Financing of Terrorism, which was adopted by the United Nations in 1999 and ratified by South Africa in May 2003. South Africa has entered into bilateral agreements with other Southern African states such as Lesotho, Swaziland and Namibia regarding financial policy measures implemented in the Southern African region including the prevention of terrorism. Thus South Africa is taking steps to address the spectre of terrorism.

A Computer Security Incident Response Team (CSIRT) has been established to address cybercrime, avert cyber attacks and apprehend computer criminals.[104] It is noteworthy that an organisation called SABRIC (South African Banking and Risk Information Centre) was established to combat cyber crime in the banking industry through effective public private partnerships. Its key stakeholders are the major banks in the country, such as Absa, Standard, Nedbank and First National Bank.[105] It is submitted that SABRIC can also counteract terrorist financing measures.

South Africa has ratified or become a member of international bodies engaged in combating terrorism. The Financial Action Task Force ("FATF") is an inter-governmental body that facilitates the development and promotion of national and international policies to address money laundering and terrorist financing

103 It should be stated that a court can together with any punishment, order the forfeiture of any property believed to be used in the commission of the offence on conviction. See s 19.
104 Anonymous 2011 http://www.defenceweb.co.za/index.
105 SABRIC 2011 https://www.sabric.co.za .

measures.[106] FATF recommendations comprise the 40 Recommendations on money laundering and 9 Special Recommendations on terrorist financing. These recommendations also contain a set of guidelines for member countries to incorporate when drafting the contents of their respective legislation. South Africa is a member of FATF. This demonstrates that South Africa is taking steps to address terrorist financing measures.

The Convention on Cyber Crime (ETS no 185) ("ECCC") is the first international treaty addressing crimes committed via the Internet and other computer networks. It was signed by member states of the Council of Europe and by non-member states in Budapest on 23 November 2001. It came into force on 1 July 2004.[107] It deals specifically with infringements of copyright, computer-related fraud, child pornography and violations of network security.[108] It is submitted that articles 2-6 which address offences against the confidentiality, integrity and availability of computer data and systems, may be used to address the offence of cyber terrorism. The Convention also contains a range of powers and procedures addressing the search of computer networks and the interception of computers.[109] Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[110] An international 24/7 network of contacts requires all participating countries to establish points of contact for transnational investigations that are accessible 24 hours daily, 7 days a week.[111] South Africa is the only African country to sign the European Convention on Cyber crime (ECCC). However, it still needs to ratify and accede to the ECCC.[112] Its ratification of the ECCC will garner much needed support in its fight against cyber terrorism. International co-operation is also necessary to fight cyber terrorism.

106 FATF 2011 http://www.fatf-gafi.org.
107 Convention on Cybercrime 2011 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
108 See s 1 – substantive criminal law, articles 2-13.
109 See s 2 – procedural law, articles 14-21.
110 Convention on Cybercrime 2011 (n 107) 2; Also see Bazelon (n 29) 309.
111 See article 35.
112 Both the United States and the United Kingdom have ratified the ECCC. See Cassim (n 89) 13.

A global security agenda (GSA) was launched by the International Telecommunication Union in Geneva during May 2007. The GSA strives to provide a global framework for dialogue and international cooperation. Its objective is to coordinate an international response to the increased challenge to cyber security and to enhance confidence and security in the information society. [113] The GSA also calls for the development of cyber crime legislation that is globally applicable and consistent with existing national and regional legislative measures. It is submitted that South Africa should become involved in such an initiative to enhance its cyber security measures.

It is submitted that South Africa can also learn from the approaches followed in other countries such as the United States, the United Kingdom and India. To this end, South Africa can also use increased surveillance measures against terrorist websites and set up a counter terrorist strategy to address radicalisation on the Internet. Indeed, South Africa should not become complacent. South Africa can also examine the success of Internet filtering measures introduced in countries like Saudi Arabia. Saudi Arabia introduced the Internet Service Unit during 2000 to filter web traffic from ISPs (Internet service providers) before permitting users access to the contents. The result is that if the requested URL is blacklisted, then the user is directed to a page that informs him or her that access to the requested page has been denied.[114] It is submitted that such measures may prevent access to illegal websites that promote cyber terrorism and pose a serious threat to the government's national security. However, such measures may well infringe the constitutional right to privacy in section 14 of the South African Constitution of 1996. It is noteworthy that the USA Patriot Act, the UK's anti- terrorism laws and the Information and Technology Amendment Act 2008 in India have all been criticised for violating the constitutional rights of citizens in their respective countries. Therefore, South Africa needs to be wary of jeopardising basic human rights and freedoms in its quest to tackle cyber terrorist threats in the future.

113 Gerke (n 34) 13.
114 Tushabe & Baryamureeba (n 1) 67.

8 Recommendations and conclusions

The debate about the threat that cyber terrorism poses will continue into the future. Cyber terrorism is a global menace which requires a united, global response. One should not underestimate the risks and potential of future threats. Countries must work together to introduce a set of core consensus crimes that can be enforceable against cyber criminals in any jurisdiction.[115] The events in Estonia during 2007 demonstrated that governments are vulnerable to attacks by digital means. Every state should enact legislation denying cyber terrorists 'safe havens' and safe places of operation. However, "law alone is insufficient; it must be buttressed with faithful enforcement and effective prevention strategies".[116] Therefore, it is also important to build defences against cyber criminals and cyber terrorists. The convergence of terrorism and the cyber world has created a new threat that has to be taken seriously.[117]

South Africa can learn from the approaches followed in other countries. We can take note of the United States initiative to develop and enhance cyber intelligence and cyber security measures in order to better predict computer-related threats and deter them and we can investigate the possibility of introducing a similar model to the National Technical Assistance Centre in the United Kingdom to counteract and avert potential cyber terrorist threats. It is noteworthy that South Africa has introduced RICA which can be used to track down cyber terrorists using cell phones to plan their illegal activities or agendas. However, South Africa should also follow the United States and the United Kingdom and ratify the ECCC as the treaty offers a global approach to the global problem of cyber terrorism.

Although attempts by countries such as the United States, United Kingdom, India and South Africa to address cyber terrorism are laudable, there is room for

115 See Goodman & Brenner (n 20) 223.
116 See Young (n 14) 28.
117 See Brunst (n 12) 76.

improvement. It is submitted that this problem can be addressed not only though enacting stringent legislation and enhancing cyber security measures but also through international cooperation. Although the global fight against cyber terrorism is necessary, combating cyber terrorism should not jeopardise basic human rights and fundamental freedoms. To this end, "the urge to restrict, prohibit and to curtail must be resisted".[118] Therefore, countries need to ensure that a balance is maintained between the protection of human rights and the need for effective prosecution. The following steps should be taken by countries to combat the spectre of cyber terrorism globally:

- Countries should ensure that its cyber terrorism legislation is compatible with international -human rights instruments. It appears that adequate legislation has been introduced by the South African government, the United States, the United Kingdom and India. While the protection of cyber systems is a major concern, this security should not prejudice the fundamental rights and freedoms enshrined in our Constitutions and human rights instruments.
- Countries should educate the public about the threat of cyber terrorism as vigilance is a key factor in addressing the potential threat of cyber terrorism. Users of the Internet should also be encouraged to adopt stronger security measures.
- The role of the media is critical in the fight against cyber terrorism. The media should follow a concise and sensible approach rather than exploit the fears of the ordinary public.
- Countries should regulate cyber cafés as these cafés are popular internet access points.
- Countries should explore the feasibility of introducing internet filtering measures to control access to websites that pose serious threats to their national security.
- Countries should introduce specialised law enforcement and training skills, and improve computer forensic capabilities. The respective governments must also initiate support and training within government, with the help of the

118 See Walker (n 30) 663. As stated earlier, measures taken in the United States, the United Kingdom and India have all been criticised by human rights campaigners.

private sector and international enterprises. Crime and corruption at various government departments should also be rooted out.

- Countries should develop cyber intelligence as a new and better co-ordinated government discipline to predict computer-related threats and deter them.

- Countries should enter into partnerships with other countries to provide technical and material support and increase cooperation among the intelligence agencies of different countries to facilitate exchange of sensitive information to counter cyber terrorist threats. International cooperation is important to ensure the integrity of the Internet. There should also be cooperation to secure networks.
  - Countries should encourage reconciliation and respect for diversity, and bridge gulfs between different countries in the broader international community to counteract terrorist threats. To this end, negotiations should be explored as a way to resolve long-standing disputes. A country should also engage all its citizens in its counter terrorist strategies.
  - Countries should keep pace with evolving technology to counteract potential cyber terrorist threats. New technologies need to be developed and enhanced in the global fight against terrorism.
  - Countries such as South Africa should follow the United States and the United Kingdom and ratify and accede to the ECCC to avoid becoming vulnerable to cyber terrorism. The Convention is also open to accession by non-member states.

Bibliography

Basdeo 2011 *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)*

Basdeo V "Terrorist financing in Southern Africa: African commitment to combating terrorism" *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)* 15-17 January 2011 Jaipur 49-52

Bazelon D *et al* 2006 *The American Criminal Law Review*

Bazelon D *et al* "Computer crimes" 2006 *The American Criminal Law Review* 43 260-308

Brunst P W 2010 Springer

Brunst PW "Terrorism and the Internet: New Threats Posed by Cyber terrorism and Terrorist Use of the Internet" in *A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications* Wade M and Maljevic A (ed) (2010 *Springer*) 51-78

Cassim F 2009 *PER*

Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study" 2009 *PER* 36-79

Cassim F 2011 *CILSA*

Cassim F "Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players" 2011 *CILSA* XLIV 123-138

Cassim F 2011*Proceedings of the Third Annual Conference of Asian Criminological Society (ACS)*

Cassim F "Combating Cyber Terrorism in South Africa: Are Adequate Measures in Place?" *Proceedings of the Third Annual Conference of*

Asian Criminological Society (ACS) 17-19 December 2011 Taiwan 96-105

Conway M 2007 *Praeger Security International – Greenwood Publishing*

Conway M "Terrorism and New Media: the Cyber Battle Space" in *Countering Terrorism and Insurgency in the twenty first century* James F Forest (ed) (2007 *Praeger Security International – Greenwood Publishing*) 1-31

Dominguez R 2008 *Third Text*

Dominguez R "Electronic Civil Disobedience Post 9/11: Forget Cyber-Terrorism and Swarm the Future Now!" 2008 *Third Text* 22(5) 661-670

Embar-Seddon A 2002 *American Behavioral Scientist*

Embar-Seddon A "Cyber terrorism: Are we under siege?" 2002 *American Behavioural Scientist* 45(6) 1033-1043

Garg N 2011 *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)*

Garg N "Cyber terrorism: The advent of E-War" *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)* 15-17 January 2011 Jaipur 121-123

Goodman MD and Brenner S 2002 *International Journal of Law and Information Technology*

Goodman MD & Brenner S "The Emerging Consensus on Criminal Conduct in Cyberspace" 2002 *International Journal of Law and Information Technology* 139-223

Guru & Mahishwar 2011 *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)*

Guru A & Mahishwar U "Terror Networking via Social Networking: Are the Laws adequate" *Proceedings of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)* 15-17 January 2011 Jaipur 71-73

Krapp P 2005 *Grey Room Inc and Massachusetts Institute of Technology*

Krapp P "Terror and Play, or What was Hacktivism?" 2005 *Grey Room Inc and Massachusetts Institute of Technology* 70-93

Nappinai NS 2009 *International Association of IT lawyers*

Nappinai NS "Cyber crime law in India: Has Law Kept Pace with Emering Trends? - An Empirical Study" in *Legal Discourse in Cyberlaw and Trade* Kierkegaard SM (ed) (2009 *International Association of IT lawyers*) 405-414

Raghavan TM 2003 *Journal of Law, Technology and Policy*

Raghavan TM "In Fear of Cyberterrorism: An Analysis of the Congressional Response" 2003 *Journal of Law, Technology and Policy* 297-312

Tushabe and Baryamureeba 2005 *World Academy of Science, Engineering and Technology*

Tushabe F & Baryamureeba V "Cyber Crime in Uganda: Myth or Reality?" 2005 *World Academy of Science, Engineering and Technology* 8 66-70

Van der Merwe *et al* 2008 *Information and Communications Technology Law*

Van der Merwe D *et al* 2008 *Information and Communications Technology Law* (Lexis Nexis)

Veerasamy 2009 *4th International Conference on Information Warfare and Security*

Veerasamy N 2009 "Towards a Conceptual Framework for Cyber- terrorism" *4th International Conference on Information Warfare and Security* 26-27 March 2009 Cape Town

Walker 2006 *Pennsylvania State Law Review*

Walker C "Cyber-Terrorism: Legal Principle and Law in the United Kingdom" 2006 *Pennsylvania State Law Review* 110(3) 625-665

Weimann G 2005 *Studies in Conflict and Terrorism*

Weimann G "Cyber terrorism: The sum of all fears?" 2005 *Studies in Conflict and Terrorism* 129-149

Young R 2006 *Boston College International and Comparative Law Review*

Young R "Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislations 2006 *Boston College International and Comparative Law Review* 29(1) 23-103

Register of legislation

South Africa

Constitution 108 of 1996

The Electronic Communications and Transactions Act 25 of 2002 ("ECT)

The Financial Intelligence Centre Act 38 of 2001 ("FICA")

The Prevention of Organised Crime Act 38 of 1999 ("POCA")

The Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004 ("PCDTRA")

The Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002 ("RICA")

International

Convention on Cybercrime ETS 185
Information and Technology Amendment Act of India, 2008
UK Anti-Terrorism, Crime and Security Act of 2001
UK Terrorism Act of 2000
UK Terrorism Act of 2006
USA Patriot Act of 2001

Register of Internet sources

Anonymous 2011 http://www.defenceweb.co.za/index; http://cbr.co.za/news.aspx ; http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm ; http://www.elaw@legabrief.co.za ; http://mg.co.za/article/2011-06-17; http://mg.co.za /article/2010-05-31 ; http://mg.co.za/article/2010-04-19

Anonymous 2011 "South Africa to establish a national computer security incident response team" http://www.defenceweb.co.za/index [accessed on 6 October 2011]

Anonymous 2011 "SA takes first steps towards Computer Security Incident Response Team (CSIRT)" http://cbr.co.za/news.aspx [accessed on 6 October 2011]

Anonymous 2011 "European Convention on Cyber crime" http://conven tions.coe.int/Treaty/en/Treaties/Html/185.htm [accessed on 16 February 2011]

Anonymous 2011 "eLaw and Management" http://www.elaw@legabrief.co.za [accessed on 14 September 2011]

Anonymous 2011 "Terrorists favour "easy" fake SA passports" http://mg.co.za/article/2011-06-17 [accessed on 5th October 2011]

Anonymous 2011 "There is no World Cup terror threat" http://mg.co.za/article/2010-05-31 [accessed on 3rd October 2011]

Anonymous 2011 "Right-wing link in arms cache found"

http://mg.co.za/article/2010-04-19 [accessed on 3rd October 2011]

Anonymous 2011"eLaw and Management" http://www.elaw@legabrief.co.za [accessed on 3rd October 2011]

Anonymous 2012 http://www.csoonline.com/article/700397/liberman-cybersecurity-act-of-2012; http://www.elaw@legalbrief.co.za; http://wwwnews.bbc.co.uk

Anonymous 2012 "Lieberman: Cybersecurity Act of 2012 will help us protect critical infrastructure" http://www.csoonline.com/article/700397/liberman-cybersecurity-act-of-2012 [accessed on 23 April 2012]

Anonymous 2012"eLaw and Management" http://www.elaw@legalbrief.co.za [accessed on 4 April 2012]

Anonymous "New terror laws come into force" http://wwwnews.bbc.co.uk [accessed on 1 May 2012]

Anonymous 2012_mhtml:file: // E:\Warning of rise in cyber-terrorism – Crime – UK – The Independent; mhtml: file: //E:\Cambridge Wireless debates UK cyber terrorism agency Business Wee...

Anonymous 2012"Al Qaida in the UK" *The Independent*
mhtml:file: // E:\Warning of rise in cyber-terrorism – Crime – UK – The Independent [accessed on 23 April 2012]

Anonymous 2012 "Cambridge Wireless debates UK Cyber Terrorism Agency" *Business Weekly* mhtml: file: //E:\Cambridge Wireless debates UK cyber terrorism agency Business Wee... [accessed on 23 April 2012]

Botha A 2005 http://www.jamestown.org

Botha A 2005 "PAGAD: A Case study of Radical Islam in South Africa" *Terrorism Monitor* 3(17) **http://www.jamestown.org** [accessed on 5th October 2011]

Denning D 2000 http://www/iwar.org.uk/cyberterror/resources/denning.htm

Denning D 2000 "Activism, Hacktivism, and Cyber terrorism: The Internet as a Tool for Influencing Foreign Policy" http://www/iwar.org.uk/cyberterror/resources/denning.htm [accessed on 3 October 2011]

FATF http://www.fatf-gafi.org

FATF http://www.fatf-gafi.org [accessed on 5th October 2011]

Frauenheim E 2002http://news.cnet.com/2100-1001-977780.html?tag=fd_top

Frauenheim 2002 "IDC: Cyber terror and other prophecies" http://news.cnet.com/2100-1001-977780.html?tag=fd_top [accessed on 07 April 2012]

Gerke M 2009 http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html

Gerke M 2009 "Understanding Cybercrime: a guide for developing countries (ITU 2009)" http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/html [accessed on 29 September 2011]

Gordon S & Ford R 2002 http://www.symantec.com/avcenter/reference/cyberterrorism

Gordon S & Ford R 2002 "Cyberterrorism?" *Computers and Security* 21(7) 636-647 http://www.symantec.com/avcenter/reference/cyberterrorism [accessed on 29 September 2011]

Green J 2002 http://www.washingtonmonthly.com/features/2001/0211.green.html

Green J 'The Myth of Cyberterrorism' http://www.washingtonmonthly.com/features/2001/0211.green.html (accessed on 17 April 2012).

Jalalzai MK http://outlookafghanistan.net/topics.php?post_id=3833

Jalalzai MK "Britain faces the Threat of Cyber terrorism and Economic Warfare" *The Daily Outlook* http://outlookafghanistan.net/topics.php?post_id=3833 [accessed 23 April 201]

Kufa M 2009 http://umkn-lib01.int.unisa.ac.za/nxt/gateway

Kufa M 2009 "Cybersurfing without boundaries" http://umkn-lib01.int.unisa.ac.za/nxt/gateway [accessed on 7th October 2009]

Kumar N 2010 http://www.psfk.com/2010/04

Kumar N "Africa could become the cybercrime capital of the world" http://www.psfk.com/2010/04 [accessed on 6 December 2010]

Nicholls 2002 *CHRI News* http://www.humanrightsiniative.org/publicatons/hl/1/5/2012

Nicholls C" UK Anti-Terrorism Crime and Security Act 2001: Too much…too soon" *CHRI News* http://www.humanrightsiniative.org/publicatons/hl/1/5/2012 [accessed on 1 May 2012]

Pollit MM 1998 http://www.scribd.com/doc/

Pollit MM 1998 "Cyber Terrorism-Fact or Fancy?" http://www.scribd.com/doc/ [accessed on 3rd October 2011]

SABRIC https://www.sabric.co.za

SABRIC https://www.sabric.co.za [accessed on 16 February 2011]

Stohl M 2006 *Crime Law and Social Change* http://ceps.anu.edu.au/publications/pdfs/stohl

Stohl M "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?" *Crime Law and Social Change* http://ceps.anu.edu.au/publications/pdfs/stohl [accessed on 17 April 2012]

ADDRESSING THE SPECTRE OF CYBER TERRORISM: A COMPARATIVE PERSPECTIVE

F Cassim*

SUMMARY

This article looks at the definition of cyber terrorism and terrorist use of the Internet. The article evaluates cyber terrorist threats facing countries such as the United States of America, the United Kingdom, India and South Africa. The article also examines measures introduced by the respective governments in these countries to counteract cyber terrorist threats. Finally, the article will propose a way forward to counteract such possible threats in the future.

The face of terrorism is changing. The convergence of the physical and virtual worlds has resulted in the creation of a "new threat" called cyber terrorism. Cyber terrorism is one of the recognised cyber crimes. The absence of suitable legal frameworks to address cyber terrorism at national and regional levels, the lack of adequate safeguards, the lack of cyber security strategies and the pre-occupation of countries with internal factors have all contributed to the creation of an environment that can be easily infiltrated by cyber terrorists.

The horrific events of 9/11 provided the impetus for many countries to introduce anti-terrorist legislation. The United States of America, United Kingdom, India and South Africa have introduced legislation to address the threat of cyber terrorism.

KEYWORDS: Cyber space, cyber terrorists, cyber crime, cyber terrorism, hacktivism; legislation, international legislation; anti-terrorist legislation, cyber security, computer networks, critical infrastructure; United States of America, United Kingdom, India, South Africa.

* Fawzia Cassim, BA (UDW) LLB (UN) LLM LLD (UNISA)Associate Professor, Department of Criminal and Procedural Law, UNISA, cassif@unisa.ac.za