Cyberterrorism is real – is it?

Introduction:

In the 1980s, Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term 'cyberterrorism' in reference to the confluence of cyberspace and terrorism. Even so, it was only during the 1990's that the concept began to develop in response to the growth in internet usage and associated cyber threats. In 1998, the Global Organised Crime Project of the Center for Strategic and International Studies in Washington D.C published a report entitled 'Cybercrime, Cyberterrorism and Cyberwarfare: Averting an Electronic Waterloo', which was the first major contribution to the field, and since then there has been a scarcity in academic books. A government reluctance to disclose threats and vulnerabilities coupled with media hype – for instance describing it as an 'Electronic Pearl Harbour', have fostered an uninformed general public who display scepticism about what to believe. This uncertain climate has led to erosion of some civil liberties, and raised suggestions resources are better distributed elsewhere, which, in combination with the context of a modern society increasingly reliant on IT and cyberspace, ensure it is timely and pertinent to question reality of the cyberterrorism spectre.

This paper will explore the question at hand through construction of a three part model, dichotomising operational and rhetorical realities and threat perception. Firstly, operational reality will contrast actual terrorist intent and capability with Critical Infrastructure Protection (CIP) systems, which if secure, ensures irrelevancy of terrorist capability, the second part will present rhetoric from the government, the IT industry, the media and academia, and thirdly, the paper will explore how target perception impacts on reality. Within the literature, a lacuna on state cyberterrorism is evident, (see for instance Conway 2002, Weimann 2006, Denning 2007), and so, to add analytical depth, the paper will appraise reality of this phenomenon, to avoid erroneous omission. Firstly however, a clear definition will clarify the concept at hand and set the boundaries from which reality can be determined or falsified, and therefore, the paper will open with discussion of definitional issues and establish a working definition.

Definitions:

Cyberterrorism can be defined as:

'the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not'.

The definition above, whilst useful, fails to incorporate state actors or those sponsored by a state, something particularly problematic given such actors arguably have motive and increased capability to conduct such attacks. Therefore, perhaps the concept can be more workably defined as:

Electronic attacks underpinned by political, social or ideological motives that are designed to generate fear amongst the target. Attacks that lead to death or bodily injury as well as those that damage digital property, physical property, or a combination of both, can be included. Crucially, the cyberterrorist actor can function at sub-state or state levels, while state – sponsored actions would also comprise cyberterrorism.

There is of course a very real debate whether cyberterrorism can ever actually exist. A consensus on traditional definitions of terrorism posits composition of two essential elements, namely the politically motivated use of force or violence. Whilst physical violence is real and understood, such 'cyber violence' is vague and problematic to clarify. Additionally, most domestic laws define terrorism as the threat to or taking human life for political or ideological motivations, and so there is no specific legal grounding either.

Having discussed definitional issues and outlined a working definition, the paper will determine if any operational reality exists in cyberterrorism, opening with discussion of terrorist intent.

Operational reality - Terrorist intent:

Arguably terrorists have intent, as suggested by the following examples, despite the fact the attacks never materialised. In October 2008, a Fatwa issued on the website of the Egyptian Muslim Brotherhood movement authorised cyber terrorism against American and Israeli websites, and Al Qaeda planned cyberterrorism against the US economy during 2010-13.

Yet, current terrorist modus operandi undermines such intent. For terrorists, the importance of a tactic depends on whether it is beneficial over other forms of terrorism, with lower costs both in response (victim and bystander response) and in production (financial and manpower). Traditional attacks have lower costs, for example, the 1993 World Trade Center bombing cost only $400 to construct, resulting in 6 dead, more than 1,000 injured, and $550 million damages. In comparison, the average salary of IT staff is $55, 100 - $155,100, so to employ such people as a possible means to conduct cyberterrorism, a terrorist group would have to pay several times that rate, not to mention other operational costs. It is also important for terrorists to advertise the group and their cause and therefore, terrorists prefer fast moving high profile dramatic events that can be recorded live with resulting casualties to maximise their publicity, for instance the Al Shabaab Westgate Mall attack. Furthermore, there seems to be a preference for traditional weapons including the gun and bomb, as suggested in an Al Qaeda training manual, which stressed preference for explosives as they create heightened fear and terror in the enemy.

An obvious question here is why would terrorists go to such trouble when simpler traditional attacks cost far less and prove far more effective? In other words, terrorists arguably believe financial and manpower costs are too high to justify any resulting 'pay-off.' It appears therefore that terrorist 'intent' is limited to a number of statements, which to carry them out would make no strategic or tactical sense – intent only makes sense rhetorically. Nevertheless, it would be more worrisome if intent were matched by capability, to which the attention now shifts.

Operational reality - Terrorist capability:

Much of the literature contains hypothetical predictions and case studies of terrorist capability. For instance, a common articulation details it's only a matter of time before cyberterrorism occurs, suggestive that capable terrorists are waiting for an opportune moment, while for others, website hacking or terrorist communication and radicalisation processes online is categorised as cyberterrorism. Therefore, one could argue terrorists are capable, and yet, such activity is not cyberterrorism as it lacks both political motive and fear generation. The important point here is that hypothetical predictions and allegations lack substance, are not grounded in reality and cloud understanding regarding actual terrorist capability.

Even so, there is always chance that intelligence agencies lack awareness of some terrorist cyber action, which could result in the unknown unknowns scenario Donald Rumsfeld articulated whereby there are threats we don't know we don't know, (i.e. cyberterrorism), as opposed to known unknowns, as for instance, when a terrorist group leader dies, the enemy knows they will be replaced, the question is by whom.

To be truly capable, one would expect terrorist acquisition of cyber tools and to display competency in their use, which does appear to be the case. For instance, Al Qaeda provided training in cyber surveillance of infrastructure and Supervisory Control and Data Acquisition (SCADA) systems, which explored the controls of electrical power grids and dams. Additionally, Ali S. Marri, was trained in hacking and met Bin Laden, who reportedly wanted him to attack computer systems of US banks. Despite this, such attacks never materialised and anyway, it is unclear whether this would merely have resulted in hacking, or indeed whether Al Qaeda and other groups have acquired the cyber tools required. The fact that Marri is perhaps the only example tells its own story in that there capable terrorists are few or none – existent.

Various mitigating factors undermine terrorist capability. For instance, terrorists would have to operate in misleading and terms such as 'information security' or 'cyberspace security' should be used instead. Clarke believes most terrorist groups have only utilised the Internet for propaganda, communications, and fundraising, a finding corroborated by former head of the US National Infrastructure Protection Center, Michael Vatis. As we have seen, whilst there is some evidence of terrorist intent and capability to conduct attacks, it remains very limited and largely rhetorical. Even so, such considerations are somewhat irrelevant in the face of an effective CIP, which the next section attempts to validate.

Operational reality - CIP systems:

Clearly, assessment of CIP systems generally would be a substantial work in its own right, and while the cyberterrorist threat is arguably posed mainly towards the US, this paper will assess US CIP systems. With regards to civil aviation, the most common concern is terrorist control of an air traffic control system. However, pilots rarely, if ever, rely solely on this system, and so even if terrorists did hack into this, pilots would still be able to land planes safely. Therefore, as the biggest concern is a misnomer, civil aviation seems well protected at least from cyberterrorism.

It is alleged that cyberterrorists could attack the US water system. However, the US has over 54,064 separate water systems, many relying on technology not easily disrupted, while another supposed target, the US electricity grid, comprises 3000 electrical power providers each with their own unique control system. Successful cyberterrorism against either US water or electricity would have to coordinate simultaneous and sustained attacks, extremely countries with good communication infrastructure, and arguably employ highly trained personnel. Given there are perhaps only 1, 000 highly experienced net engineers with a further 5,000 – 10, 000, mostly American, capable net users and administrators, it is difficult to see how terrorists could manage to employ such people initially, and then to overcome the advanced protections of advanced societies. Additionally, terrorists remain highly suspicious of outsiders and view unfavourably anyone lacking their beliefs, and so would be even less likely to employ such people on ideological grounds.

Indeed, a qualification on terrorist capability is provided by Richard Clarke, former White House special adviser for Cyberspace Security, who stated that the term 'cyberterrorism,' is

unlikely given the inbuilt protections coupled with the lack of terrorist competency or tools, as we have seen. Furthermore, the US Defence Department quarantines critical programs and systems and also the Pentagon's internal network from the internet, which highlights the extreme difficulty in conducting such attacks against a government department.

The paper has so far evaluated actual CIP protection as being healthy, which posits redundancy of terrorist threat, but does rhetorical reality reflect this?

Rhetorically real:

Government statements usually present a vague narrative of potential threats, effects, precautions and cyber security requirements, as for instance, Richard Clark, then special advisor on cyberspace security under President Bush Jr. repeatedly hyped up the threats, without many concrete justifications. In another, particularly vague example, the US Government concluded there was a threat during December 2006, against US online banking and stock market industry, which was based on uncorroborated evidence, as they admitted. Such statements lack substance for security and other reasons, and therefore, the presented threat can only really be categorised as rhetorically real.

IT security companies sometimes also promulgate cyberterrorism. For instance, a former president of the Internet Software Consortium (an industry group) in the US once equated cyberterrorism with being a threat to civilisation, whilst Gary Kaspersky, a leading cyber security specialist claimed the cyberterrorist threat was rising. However, Kaspersky has vested financial interest in promoting cyberterrorism so people buy his IT protection software. In any event, such public statements are rather vacuous.

The academic community appears split on the issue. For instance, Lacquer (1999), highlights the conjunction of technology and terrorism, while others, see for instance, Collins, 1997, have predicted cyberterrorism in the future, but that fails to establish it as a present reality. The majority view is of course that cyberterrorism is a myth; see for instance Denning, (2007) and Pollitt, (1998).

Media reports on cyberterrorism tend to headline for instance: 'Cyber terrorism is 'biggest threat to aircraft' or 'Cyber terror threatens UK's biggest companies'. Such reports frequently and wrongly, conflate hacking, denial of service attacks, terrorist communications online, or other nefarious activity with cyberterrorism, for instance that a teenager broke into the SCADA system at Theodore Roosevelt Dam in 1998. Such articles are largely descriptive opinion pieces, consisting of public statements from governments, or employees in relevant industries including civil aviation, critical infrastructure or IT.

Threat perception - Targets themselves:

The reality of a phenomenon also depends on how the target defines it, and within cyberterrorism, the two main targets are government and the general public. Firstly, within a government, the differing arms of state alter threat perception and therefore reality. Legally speaking, a nation state will define as cyberterrorism even a solitary attack on infrastructure or service disruption, while, from a militaristic standpoint, attacks that fail to undermine national security are thus insignificant. Finally, at the national security level, infrastructure comprises many dozens of differing systems. This means that each level of state has different thresholds to define cyberterrorism, ranging from a single attack to lengthy, simultaneous, multiple attacks. In other words, where a single attack happened, legally it would be cyberterrorism, but not militarily or from national security perspective.

For the public, does cyberterrorism ever have to actually happen to be real? A key aspect of terrorism is the wider fear it engenders amongst the target audience. Allegedly, cyberterrorism amplifies the sense of fear as it combines fears of terrorism and technology (a fear of the unknown). Definitional confusion compounds the consternation, as people tend to conflate hacking, terrorist research, planning and radicalisation and online communication with cyberterrorism, thus widening exposure to it. Therefore, as long as terrorists periodically repeat even vague promises to conduct cyberterrorism, then the fear is real, even where actual incidents are absent. In other words, cyberterrorism creates tangible fear and so is tangible, a proposition with some truth behind it, according to a June 2001 study, whereby 75% of worldwide Internet users believe in cyberterrorism.

However, it is questionable whether catastrophic attacks would actually cause such tremendous fear. For instance, the US and UK saturation bombing during World War II was intended to cause German moral to collapse, but instead, industrial production increased and resilience hardened until invasion by ground force troops, a notion corroborated by the US in Vietnam during aerial bombing. Furthermore, in the blackout that covered New York City, five U.S. states, and Eastern Canada in August 2003, some 50 million people were affected, most of whom reacted calmly, with very few resulting injuries or fatalities. This latter incident reinforces the notion that people appear unafraid of such incidents and their aftermath. Therefore, even if cyberterror did happen, arguably no real fear would be generated. Cyber terrorism can be considered too far removed from 'normal' life to generate fear.

So far, the paper has established that non – state cyberterrorism is really only rhetorically real, but what about such activity at state level? Could it even exist, and if so, can any comparisons be drawn?

State cyberterrorism:

In June 2010, the Stuxnet computer virus was discovered which had damaged over 1000 centrifuges in the Natanz uranium enrichment facility, and was the first computer based attack known to have caused physical damage. Application of the working definition above categorises this as a cyberterrorism incident. This computer based attack caused physical damage and was motivated by the political goal of coercing the Iranian Government and the Iranian nuclear industry to halt work on nuclear technology. In this regard then, cyberterrorism is real. Additionally, several Chinese based attempts to infiltrate Western networks have been noted including Titan Rain, Byzantine Haydes, Aurora, and Shady RAT, which could be examples of state cyberterrorism, but the motives and/or damage is unclear.

Another potential form of state cyberterrorism stems from the hype given by governments about sub-state cyberterrorism. This raises the question whether governments are deliberately creating fear for to coerce publics for political purposes? For instance, Richard Clark, then special advisor on cyberspace security to President Bush Jr. regularly hyped up the threat of an 'electronic Pearl Harbour' during budgetary cycles. Furthermore, the Code Red (potential computer virus), during July – August 2001, provided a useful backdrop to former President Bush Jr signing a new Executive Order on Cyber Security. A further question concerns whether state cyberterrorism real only when considered in this vein?

Conclusion:

At a sub-state level, with no real terrorist intent or capability and due to the fact that CIP systems seem particularly thorough, it is fair to argue that operationally, cyberterrorism is a chimera. Rhetorically however, it very much depends on whom one wants to listen to. The government, IT industry and media tend to suggest it is real, while the public influenced by such platforms, show inclination for a belief in reality as well. Conversely, the consensus in academia highlights the mythological nature of the phenomenon. Furthermore, there is very little agreement amongst academics over the precisely what cyberterrorism comprises and therefore, the question what is cyberterrorism, and by extension whether it is real, remain problematic to answer.

Exploration of specific branches of government reveals divergence of opinion between the law on the one hand and the military and national security services on the other. The idea that within one state, an incident of cyberterrorism may be categorised as such by the legal apparatus, but not by the military seems quite ludicrous and so, it is highly timely for governments and the international security community to draft effective definitions and laws to add clarify to this otherwise bizarre situation.

Conversely, state cyberterrorism is real, with various incidents being conducted in recent years – most notably the Stuxnet worm, which is odd considering the almost complete absence of coverage in the literature. Therefore, there is significant scope for governments to incorporate this aspect into cyberterrorism definitions and for researchers to develop further study.

Bibliography:

Ackerman, Spencer. 2013. *Cyber-attacks eclipsing terrorism as gravest domestic threat*. Guardian Newspaper. 14th November. Available at: http://www.theguardian.com/world/2013/nov/14/cyber-attacks-terrorism-domestic-threat-fbi. Accessed 9th April 2014.

Adams, Jonathan and Guterl, Fred. 2003. *Bringing Down the Internet*. Newsweek 3. November.

Anderson, Alison G. 2003. *Risk, Terrorism, and the Internet*. Knowledge, Technology & Policy. Volume 16. Issue 2. Pp. 24-33

Arquilla, John, Ronfeldt, David and Zanini, Michele. 2001.*Networks, Netwar, and Information Age Terrorism*. Networks and Netwars: The Future of Terror, Crime, and Militancy. 75 – 111

BBC. 2006. *US warns of al-Qaeda cyber threat*. December. Available at: http://news.bbc.co.uk/1/hi/world/americas/6197446.stm. Accessed: 10th April, 2014.

Brunst, Dr. Phillip W. *Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet*. A War on Terror?: The European Stance on a New Threat. Eds by M. Wade and A. Maljevic´. Changing Laws and Human Rights Implications. Springer Science+Business Media, LLC 2010. Pp. 51 -78

Cavelty, M.D. *Cyber-Terror: Looming threat or phantom menace? The framing of the U.S. cyberthreat debate*. Journal of Information Technology and Politics 4. 1.2007.

Chen, Dr. Hsinchun, Qin, Jialun, Reid, Edna, Zhou, Yilu. 2008. *Studying Global Extremist Organizations' Internet Presence Using the DarkWeb Attribute System*. Terrorism Informatics. Integrated Series In Information Systems Volume 18. Pp 237-266

Collins, Barry. 1997. *The Future of Cyberterrorism*. Crime and Justice International. March 1997. Pp. 15–18. Available at: http://www.cjimagazine.com/archives/cji4c18.html?id=415. Accessed 5th March 2014.

Collins, Nick. 2013. *Cyber terrorism is biggest threat to aircraft*. Telegraph Newspaper. December 27th. Available at: http://www.telegraph.co.uk/finance/newsbysector/transport/10526620/Cyber-terrorism-is-biggest-threat-to-aircraft.html. Accessed 9th April 2014.

Conway, Maura. 2002. *Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet*

Conway, Maura. 2005. *The media and cyberterrorism: a study in the construction of 'reality*

Copeland, Lee. 2001. *More for the Money*. ComputerWorld. 3rd September. Available at: http://www.computerworld.com/careertopics/careers/story/0,10801,63423,00.html. Accessed 30th March 2014.

Adnkronos International. *Egypt: Sunni scholars sanction electronic Jihad*.

http://www.adnkronos.com/AKI/English/Security/?id=3.0.2595019598. Accessed 23/02/2014.

Denning, Dorothy. 2000. *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Available at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html . Accessed 2nd February 2014.

Denning, Dorothy. 2001. *Activism, Hacktivism, and Cyberterrorism: The internet as a tool for influencing Foreign policy*. Networks and Netwars: The Future of Terror, Crime, and Militancy. Eds by John Arquilla and David Ronfeldt. Pp. 239 – 288.

Denning, Dorothy. 2007. *A View of Cyberterrorism Five Years Later*. Internet Security: Hacking, Counterhacking, and Society. K. Himma ed. Jones and Bartlett Publishers.

Desmond, Dennis. 2001. *Sytex, Inc*. Cyber Terrorism and Information Warfare: Threats and Responses. Eds by Alexander, Yonah and Swetnam, Michael. S. Transnational Publishers. Pp. 29 - 37.

Embar-Seddon, Ayn. 2002. *Cyberterrorism: Are We Under Siege?* Cyberterrorism. Ashgate Publishing Limited. Pp. 11 – 21.

Ganor, B. 2002. Terror as a Strategy of Psychological Warfare. July 15. Available at: http://www.ict.org.il/var/119/40015-Terror%20as%20a%20Strategy%20of%20Psychological%20Warfare.pdf. Accessed 7th April 2014.

Giacomello, Giampiero. 2004. *Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism*. Studies in Conflict & Terrorism. 27. Pp 387–408.

Hall, Allan. 2005. *Al-Qaeda Chiefs Reveal World Domination Design*. The Age, August 24, 2005. Available at: http://www.theage.com.au/news/war-on-terror/alqaeda-chiefs-reveal-world-domination-design/2005/08/23/1124562861654.html. Accessed 4th March 2014.

Hoffman, Bruce. 1999. *Terrorism Trends and Prospects*. Countering New Terrorism. Ian O. Lesser et al. Eds Santa Monica, CA: Rand. Pp. 7–38.

Hoffman, Bruce. 2014. *Low tech terrorism*. Fortunas Corner. February 26th. Available at: http://fortunascorner.com/2014/02/26/low-tech-terrorism-by-bruce-hoffman/. Accessed 9th April 2014.

Hopkins, Nick. 2001. *Cyber terror threatens UK's biggest companies*. Guardian Newspaper. 3 April. Available at: http://www.theguardian.com/technology/2001/apr/03/internetnews.uknews. Accessed 9th April 2014.

Kaspersky, Gary. 2013. *Cyber espionage and sabotage 'on the rise'*. BBC News. 26th January. Available at: http://www.bbc.co.uk/news/business-21211618. Accessed 11th April, 2014.

Kearney, Paul. 2012. *Towards a C2I Platform for Combating the Cyber-Threat*. Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems. Lecture Notes in Computer Science Volume 7322. Pp 17-19

Kizza, Joseph Migga. 2013. *Security Threats to Computer Networks*. Guide to Computer Network Security .Computer Communications and Networks. Pp 63-88

Laqueur, Walter. 1999. The New Terrorism: Fanaticism and the Arms of Mass Destruction. Oxford University Press.

Lewis, James A. 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Center for Strategic and International Studies

Lindsay, Jon R. 2013. *Stuxnet and the Limits of Cyber Warfare*. Security Studies. Vol. 22. No. 3.Pp. 365 - 404.

Luiijf, Eric. 2012. *Understanding Cyber Threats and Vulnerabilities*. Critical Infrastructure Protection Lecture Notes in Computer Science. Volume 7130. Pp 52-67

Minei, Elizabeth and Matusitz, Jonathan. 2012. *Cyberspace as a new arena for terroristic propaganda: an updated examination*. Poiesis & Praxis . Volume 9. Issue 1-2. Pp 163-176.

Minei, Elizabeth & Matusitz, Jonathan. 2011. *Cyberterrorist Messages and Their Effects on Targets: A Qualitative Analysis*. Journal of Human Behavior in the Social Environment. 21.8. Pp. 995-1019.

Nelson, Bill; Choi, Rodney; Iacobucci, Michael; Mitchell, Mark and Gagnon, Greg. 1999. 'Cyberterror: Prospects and Implications'. The Center for the Study of Terrorism and Irregular Warfare, Monterey, California. White Paper. Available at: http://www.nps.edu/Academics/Centers/CTIW/files/cyberterror%20prospects%20and%20implications.pdf. Accessed 8th April, 2014.

Pollitt, M.M. 1998. Cyberterrorism - Fact or Fancy. Computer Fraud and Security. February.

Rattray, G. J. 2001. The Cyberterrorism Threat. The Terrorism Threat and US Government Response: Operational and Organisational Factors. James M. Smith and William C. Thomas. Eds. US Air Force Institute for National Security Studies. Colorado. Available at: http://www.au.af.mil/au/awc/awcgate/usafa/terrorism_book.pdf. Accessed: 9th April 2014.

Rollins, J and Wilson, C. 2005. *Terrorist capabilities for cyberattack: Overview and Policy Issues.* Congressional Research Service, October 20, 2005. Available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf. Accessed 5th March 2014.

Rumsfeld, Donald. 2002. DoD News Briefing. US Department of Defense. February 12th. Available at: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636. Accessed 10th April, 2014.

Savas, A. 2006. *IBM launches internal network protection*. Computer weekly.Com. Monday, 27 February 2006. Available from http://www.computerweekly.com/Articles/2006/02/27/214429/IBMlaunchesinternalnetworkprotection.htm. Accessed 6th March 2014.

Soriano, Manuel R. Torres. 2012. *The Vulnerabilities of Online Terrorism.* Studies in Conflict & Terrorism. 35:4. Pp. 63-277

Stanton, John. J. 2002. *Terror in Cyberspace: Terrorists Will Exploit and Widen the Gap Between Governing Structures and the Public*. American Behavioral Scientist. Vol. 45. Pp. 1017 – 1032.

Stern, J. 1999. The Ultimate Terrorists. Harvard University Press. Cambridge MA.

Stohl, M. 1988. *Demystifying terrorism: The myths and realities of contemporary political terrorism.* The politics of terrorism. 3rd Ed. In M. Stohl Eds. New York: Marcel Decker

Stohl, Michael. 2006. *Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?* Crime Law Soc Change. 46. Pp. 223–238

Yunos, Zahri, Ahmad, Rabiah, Mat Ali, Syahrir, Shamsuddin, Solahuddin. 2012. *Illicit Activities and Terrorism in Cyberspace: An Exploratory Study in the Southeast Asian Region*. Intelligence and Security Informatics . Lecture Notes in Computer Science Volume 7299. Pp 27-35

Valerie, L and Knights, M. Affecting Trust: Terrorism, Internet and Offensive information Warfare. Terrorism and Political Violence. Vol. 12. No. 1. Pp. 15 - 36

Vatis, Michael. 2001. *Government Perspectives*. Cyber Terrorism and Information Warfare: Threats and Responses. 3 – 12. Eds by Alexander, Yonah and Swetnam, Michael. S. Transnational Publishers.

Weimann, Gabriel. 2006. *Terror on the Internet: The New Arena, the New Challenges*. United States Institute of Peace Press.