2009

Cyber Terrorism

Allen Gnanam, *University of Windsor*

INTRODUCTION:

Modern society is experiencing a technological juggernaut effect and this effect needs to be accompanied by a counter- cyber terrorism agenda, that works to secure societies functional dependence and reliance on web based technology. Generally speaking cyber terrorism is more of a concern for western democratic nations, as result of their current and ever growing functional dependence on web based management and control computer systems (Furnell & Warren, 1999) (Goodman, Kirk & Kirk, 2007) (Jones, 2005) (Lin, Liou & Wu, 2007). In fact a former FBI director of the National Infrastructure Protection Centre stated that the United States, is hundred percent dependent on information systems (web/ internet based systems) to functionally operate (Goodman et al., 2007). Cyber terrorism is not a traditional physical attack that causes physical harm, rather it's a technological attack that has the potential to cause national, physically, psychological, and economic devastation (Furnell & Warren, 1999). This paper sets out to identify and explain the negative national security implications, negative physical & psychological implications, and the negative economic implications that society could face, as a result of a severe cyber attack against major sectors of a nations infrastructure. In addition instigating factors that lead to/ provoke cyber terrorism will be identified, in order to strategically influence counter cyber terrorism policy towards an offensive model. Along with that, this paper will present defensive/ target hardening counter- cyber terrorism policies that will enable proactive security mechanisms to be implemented, in order to secure web based services that are essential to western societies survival and existence. When reading this paper the term cyber terrorism will constantly be re-emerging and it is important not to formulate a tunnel visioned conceptualization, that solely links cyber terrorism to Islamic groups such as al Qaeda, as other organizations such as the Liberation Tigers of Tamil Eelam (LTTE), the Provisional Irish Republican Army (PIPRA), Marxist groups, separatist groups, racist groups, and other state and non state sponsered groups and individuals, are capable of violent cyber attacks depending on their level of technological knowledge and internet infiltration skills (Jones, 2005) (Weiman, 2008).

CONCEPTUALIZATIONS:

Before discussing the above mentioned implications of a severe cyber terrorism attack, such as an attack against a nations critical infrastructure, the terms media, worm, virus, infrastructure, cyberspace, and cyber terrorism will be conceptualized. For the purposes of this paper the interactive model of media will be used to discuss cyber terrorism, as this model not only defines media as web based computer technologies such as the internet, but is also defines media as a tool that can cause visual change through the physical operation of tangible computer related technologies such a mouse (Comstock & Scharrer, 2007). The interactive model's definition of media is ideal for this investigation of cyber terrorism, as cyber attacks cause security breaches in web (internet) based computer systems as a result of the physical operation of computer equipment (E.g. Keyboard).

A worm is considered to be a electronic program that has been instructed/ programmed to directly attack and damage the computer it has been send to, weather it be through email or an infected storage device, however, the infected computer cannot pass on the worm to other computers (Hinde, 2001). A virus on the other hand is an electronic program that can cause damage to a single computer, as well as multiple computers or web based management systems (Hinde, 2001). This is possible since virus's have the ability to transfer themselves from one computer to the next, through infected email attachments or documents saved on storage devices (Hinde, 2001) (E.g. Conflicker virus).

Infrastructure is defined as the necessary and essential facilities, institutions, and services that a country requires in order to functionally and coherently operate (Goodman et al., 2007). For example water turbine faciltities, major transportation services (E.g. Airplanes, subways, trains), financial institutions, electricity facilities, emergency services, and communication facilities and services (E.g. Air traffic control) (Boni, 2001) (Dwan, 2001) (Furnell &Warren, 1999) (Lin et al., 2007). These sectors of a nations infrastructure have be highlighted due to the fact that they have been noted be overly dependent on web based computer management and control (Furnell &Warren, 1999) (Lin et al., 2007), and because they are the most likely targets of a cyber terrorism attack (Hinde, 2003).

Cyberspace refers to a network of communication systems that allow for information and data to be transmitted and received (Goodman et al., 2007). The internet is a major component component of cyberspace as it allows for the reception and transmission of information and data, through communication technologies that enable the management and control of a nations web based infrastructure (Goodman et al., 2007). With that, individuals or groups who utilize the internet (cyberspace) as an instrument for invoking harm and injustices are dubbed cyber terrorists, and their actions are dubbed cyber terrorism (Dwan, 2001). Cyber terrorists can fall under two broad categories known as (a) insiders and (b) outsiders (Goodman et al., 2007). Insiders refers to employees of a company who engage in cyber terrorism against their company or against other targets using their company computers, where as outsiders refer to individuals not associated with the cyber target being infiltrated (Goodman et al, 2007).

Western democratic nations have defined cyber terrorism as an unauthorized and intentional threat or act of internet violence or disturbance (E.g. Denial of service virus's), against web based computer systems which in turn results in death, injury to humanity, property damage, societal disorder, or economic destruction (Jones, 2005). It is important to point out that there isn't a single agreed upon definition of what constitutes cyber terrorism, in fact there is much intra-national variation in defining cyber terrorism. For example in the United States the FBI, the U.S Department of Defense, and the U.S Department of State have varying definitions though similarities do exist (Ford & Gorden, 2002).

CATEGORIES OF CYBER-TERRORISM:

Cyber terrorism can be categorized under two forms of attack known as (1) targeted attacks and (2) opportunity attacks (Kshetri, 2005). Targeted attacks are committed by highly trained, skilled, and experienced individuals or groups such as computer corporations, terrorists, or governments who have strategically planned to attack a specific vulnerable target to cause significant damage (Kshetri, 2005). In contrast opportunistic attacks lack intensive planning, and are carried out by less trained and skilled personnel or groups when compared to those committing targeted cyber attacks, and opportunistic attackers are more likely to use malignant virus's that spread from computer to computer through documents, downloads, or emails (Kshetri, 2005). With that a reception analysis illuminates the reality that the media does not transcend human control, rather the media is a tool that is explicitly controlled by conscious individuals (Jewekes, 2004). This points out that cyber terrorism which can be seen as a form of media manipulation is a conscious and deliberate phenomenon, that is orchestrated by intentional agents to cause destruction and disorder. For the purposes of this paper cyber terrorism will mainly be discussed in relation to targeted cyber attacks, as these attacks are the most serious (Kshetri, 2005) and the most likely to cause negative national security, physical & psychological security, and economic security effects.

NATIONAL SECURITY IMPLICATIONS:

Negative national security implications linked to cyber terrorism can be discussed in relation to the functionalist framework, as cyber terrorism attacks that target and damage the critical sectors of a nations infrastructure may not only disintegrate essential social systems, but it may also cripple a nations ability to adapt to a large scale technological plight in a timely manner before societal functioning collapses. A large scale cyber terrorism attack has the potential to damage two of the four functional imperatives that are vital to a societies survival and functional operation. Parsons formation of the AGIL scheme illustrated that adaptation, goal-attainment, integration, and latency/ culture are the four needs required by a society to function (Trevino, 2005). A cyber terrorism attack against a western societies infrastructure has the potential to cause both the adaptation and integration component of the AGIL scheme to become severely damaged, to the extent that national security would be breached and society would be on the verge of social dis-functionality. Adaptation refers to a societies ability to adapt/ overcome an external problem and maintain social processes (Trevino, 2005). Research has found that western nations specifically, have become overly dependent on web based technologies for the purposes of managing and controlling critical sectors of infrastructure (Furnell & Warren, 1999) (Goodman et., 2007). As a result, a breach in web based management systems would destabilize the Capitalistic mode of production and leave a nation vulnerable to traditional/ physical forms of terrorism. Adaptation to a severe cyber blow would probably not occur as fast as Parsons would have deemed healthy, as a technological nation cannot fall back onto modern methods as a means to regain control over web based computer systems. In addittion the time taken to repair damaged infrastructure would most likely be a longer term project, and a long term project would leave a nation in a vulnerable state for far to long. In light of integration, referring to societies ability to functionally coordinate and cohesively operate in conjugation with societal institutions/ processes (Trevino, 2007), dis- integration would occur as a result of a nations inability to adapt to cyber terrorism in a reasonable amount of time. Damage to critical infrastructure and the inability to rapidly adapt to a cyber attack would prevent social, corporate, financial, and medical institutions from coordinating in a functional manner which in turn may cause society to become dis-functional/ disordered. Damage to the adaptional and integration functional imperatives of a nation would also put societal members into a state of confusion, and lead to the emergence of moral panics which in turn would further intensify the national security plight. The importance of a counter- cyber terrorism unit is not only essential for national security purposes, but also for the survival of a nation. It is surprising clear that western nations have undergone a technological transformation that requires society to operate under web based computer management systems, as a means to ensure functionality, survival, and existence.

Cyber- terrorism also poses a national security threat linked to the extraction of classified government and military information, found on web based computer data bases (Furnell & Warren, 1999). Malware which is a type of virus, is a computer program that once embedded into a web based computer system (E.g. Government computer) as a result of cyber terrorism, is able to surreptitiously send data into a computer system and/or extract data from a computer system

(Goodman et al., 2007). In addittion malware can negatively impact the transportation sector of a nations infrastructure, which in turn poses a national security threat as citizens within their homeland borders will be facing a risk of injury. In terms of communication networks such as air traffic control centers, it is vital that these communication networks send and receive accurate information verifying altitude and location coordinations in order to ensure a safe landing. Therefore cyber terrorism that embeds malware into air traffic networks will enable cyber terrorists, to send false information to either air planes or air traffic control centers which in turn could result in a catastrophic event (Goodman et al., 2007).

Cyberspace is an area that enables state or non state sponsored cyber terrorists to perform activities such as security breaches, from either domestic areas or foreign areas half way across the world without being traced and identified (Goodman et., 2007). Sophisticated technological devices used by cyber terrorists coupled with legal dilemmas pertaining to jurisdiction issues, have prevented officials from pursuing technological leads and identifying cyber terrorists (Furnell & Warren, 1999) (Goodman et al., 2007). With that the anonymity of cyber terrorism is another major national security threat, as it prevents governments from engaging in offensive technological or even physical military strategies against state or non state sponsored cyber terrorist groups or individuals. Further more, anonymity prevents governments from knowing weather or not friends, allies, or domestic corporations are actually plotting against them and infiltrating web/ internet managed infrastructure. In light of current economic, military, and political tensions evident between western nations and the rest of the world, it is highly necessary for western cyber security to be enhanced and prioritized as a national security agenda. For instance, research illustrates that political and military tensions between nations is correlated with the precipitation of cyber terrorism (Hinde, 2003), and Russian history illustrates that economic down turns result in an increase in cyber terrorism due to the increase in over educated and unemployed computer programmers (Kshetri, 2005).

PHYSICAL AND PSYCHOLOGICAL IMPLICATIONS:

Cyber- terrorism is not a physical attack that causes physical harm rather it is a technological attack that has the potential to cause physical (Furnell & Warren, 1999), and psychological harm (Goodman et al., 2007). The cyber terrorism phenomenon reflects Dwan's idea of a logic bomb that threatens the physical well being of individuals, and this ideal also reinforces the reality that cyber terrorism is intellectual might rather physical/ military might (2001). For example, Dwan illustrates how rouge manufactures can engage in cyber terrorism and cause physical harm by pre-programing computer equipment to overheat, and catch on fire once specific words or letters are inputed (2001). In addittion, Elsevier points out that cyber terrorists are capable of infiltrating the health care sector of a societies infrastructure, in order to alter patient hospital records as a means to cause humanitarian injustices and physical harm (2000). Due to the sophistication of technological devices, cyber terrorists are cable of remotely altering patient records and modifying a patients medical treatment, if web based health care computer data bases experienced a security breach (Elsevier, 2000) (Furnell & Warren, 1999). Further more, breaching web based transportation systems that manage and control railways in order to alter train routes and cause collisions, is another example of the potential physical harm cyber terrorism poses (Elsevier, 2000). The above examples almost seem as though they are fictional entertainment media phenomenon's, however, the reality is that society has built themselves into a technological iron caged world where web based and wire less technology rather than bureaucracy is dominating and operating society.

It is evident that cyber related physical victimization weather it be primary in the sense that one is physically harmed, or secondary in the sense that ones employee or friend was physically harmed, does result in some level of invisible psychological harm/ trauma. For example, cyber terrorists cause fear and anxiety among the general public as well as specific individuals (E.g. politicians) as a mechanism to highlight their political, religious, or social agenda (Goodman et al., 2007). The injection of fear should not be seen simply as a by-product of certain cyber terrorism attacks, as cyber terrorists understand how the media operates and as a result they intentionally propagate cyber threats and attacks in order to acquire media attention (Goodman et al., 2007). Cyber terrorists view the mass media as a tool that can aid in their political, social, or religious agenda as increased public fear equals increased media attention regarding their ideology (Goodman et al., 2007). In addittion to the injection of fear and use of cyber violence for social, religious, or political agendas, the cultural criminology perspective provides evidence of internal factors that instigate cyber violence. In taking a micro level perspective, it may be accurate to assume that select individuals are obsessed with carrying out violence and crimea as it provides a sense of power and grants psychological excitement and fulfillment (Jewekes, 2004). Therefore internally influenced cyber terrorism might be difficult to deter as psychological deterrence may require individualizing solutions for the the most part.

It is important to keep in mind that cyber terrorism can accompany traditional forms of terrorism as a means to increase the destructive force of a terrorizing event (Goodman et al., 2007). For instance, after a physical attack such as a bomb blast terrorists could infiltrate web based communication systems used by emergency response teams, which in turn would prevent rapid response time and further intensify the physical and psychological effects of a terrorist attack (Goodman et al., 2007) (Hinde, 2001). The National Infrastructure Protection Centre carried out a study and stated that dual terrorism would produce increased destruction (Goodman et al., 2007). This study stated that the 9/11 tragedy would have been significantly worse if a cyber terrorism attack also occurred simultaneously (Goodman et al., 2007). This again reiterates the major importance of exercising legal reform pertaining to cyber policy, in order to rapidly initiate a counter- cyber terrorism agenda that is both offensive and defensive.

ECONOMIC IMPLICATIONS:

Cyber attacks that target financial sectors of a nations infrastructure such as banks, forces the Capitalist mode of production to become challenged which in turn causes negative economic implications linked to profit/ financial decline (Forte & Power, 2006) (Hinde, 2003) (as well as national security implications). For example, if financial institutions lost important customer information such as bank balances or personal identification/ verification information, individuals as well as multi-national corporations would be in a major economic plight. Individuals would not be able to withdraw money, pay bills, and corporations would be unable to pay employees, order materials/ product, or operate efficiently. With that, the Capitalist mode of production would not only be challenges but it may even come to a halt if people and corporations are unable to stimulate the economy through the flow of money.

Web based banking systems have been infiltrated in the past and monetary funds have been illegally transferred to unknown bank accounts (Philippsohn, 2001). For example prior to the 2001 World Trade Centre attack an employee (insider) working for Citi Bank along with other individuals, infiltrated customer bank accounts and transferred around seventy- five million dollars U.S to different parts of the world (Philippsohn, 2001). However, Citi Bank was able to detect the security breach, identify the insider, and recover close to all of the money without causing customers to experience profit loss (Philippsohn, 2001). This example points out that enhanced proactive cyber security mechanisms are needed as a means to target harden web based financial systems, that are apart of a nations critical infrastructure. Therefore the destabilization of financial sectors in society can trigger large scale negative economic consequences (Furnell & Warren, 1999) (Hinde, 2003) (Power & Forte, 2006). It is evident that some of these cyber attacks might be viewed as white collar crime, however, in reference to the above citied conceptualization of cyber terrorism, white collar crime doesn't directly cause large scale economic destruction which could lead to societal disorder.

There have been many other reported cases of economic loss as a result of cyber terrorism. In 1996 the UK National Computing Centre was down 14,460 pounds due to hacking/ a cyber attack (Furnell & Warren, 1999). Secondly, a virus known as the Love Letter worm caused businesses around the world ten million too ten billion dollar U.S in damages, as worms are programs that damage the specific computer(s) they have infected (Hinde, 2003). In June of 2000 a cyber attacker/ hacker illegally obtained passwords, credit cards numbers, names, and address of twenty- four thousand people from a web server (Philippsohn, 2001). Some of the twenty four thousand primary victims were employees at a classified Defense Evaluation and Research Agency, and this depicts that class, prestige, or occupational status doesn't immune an individual from cyber attacks (Philippsohn, 2001). Another reported case illustrates how cyber attackers of an U.K brokerage and a defense law firm, demanded a payment of ten million euros in order for them to give back full control of the web based computer system (Philippsohn, 2001). Research also points out that gambling websites have payed and are paying cyber attackers an annually salary in order for them not to infiltrate the gambling website (Kshetri, 2005). One of the problems with the way in which vulnerable corporations handle cyber threats reflects their unilateral focus on defensive proactive strategies, rather than a dual focus that takes into account both defensive and offensive model strategies that would target the root causes of cyber terrorism (Hinde, 2003).

PROVOCATIONS TO CYBER-TERRORISM:

In connection to the cultural criminology perspective, it is evident that cyber violence can stem from an internal desire to fulfill psychological desires or gain a sense of power (Jewekes, 2004). Other internal motivations reflect a desire to challenge ones technological competencies, or fulfill ones obligation to a social, religious, or political group (Furnell & Waren, 1999) (Kshetri, 2005). Therefore the internal desire to fulfill radical instructions and/or cult like rites of passage ideologies may instigate cyber terrorism such as Cyber- Jihad. With that, preventive cyber terrorism policy should consider increasing the deterrence aspect of crime control/ prevention, by increasing the severity level of cyber terrorism punishments and by publicizing the severity of the new punishment for general deterrence potential (Goodman et al., 2007).

In connection to the external factors that instigate cyber terrorism, research presents that political tensions resulting from failed diplomacy (Lin et al., 2007), economic incentives when employment opportunities are lacking (Furnell & Warren, 1999) (Kshetri, 2005), the realization that cyber attacks are cost efficient in comparison to physical attacks (Furnell & Warren, 1999), and the fact that cyber attacks entail less physical and legal risk for the cyber attacker, as the attack can be committed from a distant and secure location where tracking in almost impossible (Jones, 2005), are all external instigators that increase the likelihood of cyber terrorism. In light of the first point regarding political tensions, it is critical that the United States prioritize the counter cyber terrorism agenda and place it at the top of their national security agenda, as many nations may be overly tempted to infiltrate America's web based infrastructure as well as the Pentagon in order to cause large scale harm.

In relation to the above mentioned instigating factors, it is evident that the counter cyber terrorism agenda needs to take an offensive stance against domestic and foreign religious and educational institutions, that inject propaganda vilifying the Western worlds and teachings that influence intentional terrorizing behaviours directed at the West. Hatred and resentment fostering institutions need to be either reformed or legally dismantled as a means to ensure the national, physical & psychological, and economic security of the West. It is important that these forms of offensive policies that target foreign institutions be accomplished through diplomatic channels. Diplomacy will ensure that the West is not using hegemonic behaviours as a means to secure their national security, which in turn will decrease the possibility of further propagation of resentment towards the West.

PROACTIVE SOLUTIONS:

Cyber terrorists should not solely be framed as foreign individuals or groups that operate in distant lands, as domestic workers known as insiders may potentially be cyber terrorists (Goodman et al., 2007) (Hinde, 2001). For instance due to fear/ coercion, black mail, or financial desperation company employees who have the authority to change software settings or internet connection settings may engage in cyber terrorism (Goodman et al., 2007). With that, it is important that corporations managing sectors of a nations infrastructure perform extensive criminal background checks on all their employees (Goodman et al., 2007). In addition, corporations should consistently evaluate the moods, behaviours, social changes, and personal life changes that each of their employees are undergoing. This will enable corporate security personnel or employee auditors to identify negative patterns and take proactive steps in helping the employee and preventing a potential cyber attack. It is essential that government policies provide infrastructure managing corporations with the tools and legal avenues needed to carryout extensive criminal background searches, and on going evaluations of their employees for national security purposes. In addition, corporations managing critical sectors of a nations infrastructure should be required by law to undergo routine cyberspace security audits, as this will verify weather or not web based computer management systems are vulnerable to cyber attacks or not (Goodman et al., 2007). In addition, these audits will ensure that infrastructure managing corporations will continually update security features and systems in order to protect against cyber infiltration.

Cyber terrorism is also thought to occur when their is (a) a vulnerable web based computer system present, and (b) when an individual or group is motivated to penetrate vulnerable web based computer systems (Goodman et al., 2007). In terms of factor (a), it is important that policy makers formulate proactive defensive/ target hardening strategies that decrease the vulnerabilities of critical web based computer systems. Government officials should be solely restricted to downloading only government approved software onto computers that contain sensitive government information. This will prevent potential cyber terrorists from embedding themselves into government computers. Also, government computers and laptops should only operate on unique hardware and software programs that members of society can not purchase, as this will reduce the risk of hardware and software vulnerabilities being identified. With that, government computers and laptops should be restricted only to government secured wireless networks as this would decrease the chances of a security breach. In addition, government laptops and computers should be equipment with USB drive internet capabilities, as this would disable deliberate hacking when computers are idling, since wireless connectivity could be disabled simply by removing the USB. Government agencies should also strongly consider implementing laws that hire special government engineers, that specifically analyze hardware and software programs that the government plans on purchasing from foreign or domestic corporations. In expanding Dwans concept of the “logic bomb”, it is safe to assume that foreign and domestic corporations can secretly manipulate computer software as a means to cause physical harm, or secretly view classified government information. With that, governments should fund educational programs that train individuals in the filed of counter cyber terrorism (Lin et al., 2007), as this will ensure that nations have individuals who not only understand the cyber terrorism threat but also have the knowledge to counter cyber terrorism.

Lastly, Dasgupta takes a biological immune system perspective in discussing potential security mechanisms that can be implemented to protected against cyber terrorism (2007). For example, just as the human body has white blood cells that detect and destroy foreign entities such as pathogens, there should be computer programs that detect and report foreign programing and software (Dasgupta, 2007). This strategy will prevent cyber terrorists from surreptitiously embedding malware into web based computer systems with the intention to cause national, physical & psychological, and economic insecurity. With that, legal policies should not only make certain security mechanism law but laws should also provide financial support that will enable corporations to engage in acquiring security enhancements, as profit is a significant barrier to enhanced security implementations (Goodman et al., 2007).

CONCLUSION:

Cyber terrorism is a not a new technological phenomenon as its existence has been documented since the middle of the 1990's (Jones, 2005), however, only recently has cyber terrorism largely become problematized as a threat to security. With that, government security personnel should not be solely focused on physical terrorism as other forms of terrorism including cyber terrorism, are equally threatening in todays day and age. It is vital that all aspects of terrorism such biological terrorism (e.g. Anthrax), cyber terrorism, nuclear terrorism, and traditional terrorism be given significant investigative attention as a multi counter terrorism agenda will heightened western societies national, physical & psychological, and economic security.

In close nation security, physical & psychological security, and economic security are interrelated components. For example, national security devastations will inevitably result in economic loss as well physical & psychological hardship. Large scale economic damage to the Capitalist mode of production would result in a national security crisis, as the economy may potentially freeze as in a depression, and as a result physical and psychological harm could result from looting and social disorder. With that, mass amounts of death as result of a cyber attack against air traffic control centers would also result in economic loss due to the destruction of aeroplanes, and nation security would be compromised as citizens would not be secure within their boarders. In the light of the current war against terrorism, it is evident that terrorists are mainly relying on physical elements such as improvised explosive devices (IED's), road side bombs, machine guns and other tangle elements that are destructive. However, as the war on terrorism continues and old terrorist leaders are no longer capable of running or planning terrorizing events, new terrorizers who have matured during the technological era of society may emerge in place of aging counter parts. With that, the war against terrorism may also become a war against cyber terrorism, as governments may not only be physically combating terrorists and defending against terrorists, but also technologically combating terrorists and defending against terrorists. Cyber terrorism as a form of interactive media is a destructive instrument that can potentially be used to destabilize western democratic nations, due to their over reliance and dependence on web based technological innovations (Furnell & Warren, 1999) (Goodman, Kirk & Kirk, 2007) (Jones, 2005) (Lin, Liou & Wu, 2007). With that, modern society is experiencing a technological juggernaut effect and this effect needs to be accompanied by a counter- cyber terrorism agenda, as it is crucial that western nations embark on both an offensive and defensive counter cyber terrorism agenda in order to secure societies long term web- based survival, existence, and functionality.

By: Allen Gnanam (2009)
University of Windsor

REFERENCES

Boni, B. (2001) Cyber - terrorists and counter spies. *Network Security,* 2001(12), 17-18

Comstock, G., & Scharrer, E. (2007) Demographics and preferences in media use, with special attention to the very young. *Media and the American Child,* Vol. 0, Pg. 1-41

Dwan, B. (2001) Cyber-terrorism- Virtual for who? *Computer Fraud & Security,* Vol. 2001, Issue 11, Pg. 12 - 14

Dasgupta, D. (2007) Immuno-inspired autonomic system for cyber defense. *Information Security Technical Report,* Vol. 12, Pg. 235 - 241

Elsevier (2000) Is it cyber- terrorism, techno- terrorism, or none of the above? *Computer Fraud & Security, 2000(7), 18-20*

Ford, R., & Gorden, S. (2002) Cyberterrorism? *Computers and Security,* Vol. 21, Issue 7., Pg. 636 -647

Furnell, S., & Warren, M. (1999) Computer hacking and cyber terrorism: The real threats in the new millennium. *Computers and Security,* Vol. 18, Pg. 28-34

Goodman, S., Kirk, J., & Kirk, M. (2007) Cyberspace as a medium for terrorists. *Technological Forecasting and Social Change,* Vol. 74, Pg. 193- 210

Hinde, S. (2003) Cyber- terrorism in context. *Computers and Security,* Vol. 22, Issue. 3, Pg. 188-192

Hinde, S. (2001) Incalculable potential for damage by cyber terrorism. *Computer and Security,* Vol. 20, Pg. 568-572.

Jewekes, Yvonne. (2004) “Chapter 1: Theorizing Media and Crime” (Pg. 2-33) in *Crime and Media.*

Jones, A. (2005) Cyberterrorism: Fact or fiction. *Fraud and Security.* Vol. 2005, Issue. 5, Pg. 4-7

Kshetri, N., (2005) Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management,* Vol. 11, Pg. 541- 562

Lin, C., Loui, D., & Wu, k. (2007) Opportunities and challenges created by terrorism. *Technological Forecasting & Social Change,* 74, 148- 164

Philippsohn, S. (2001) Trends in cybercrime- An overview of current financial crimes on the internet. *Computers and Security,* 20, 53-69

Trevino, A. (2005) Parsons's Action-System Requisite Model and Weber's Elective Affinity: A Convergence of Convenience. *Journal of Classical Sociology,* 5(3), 319-348

Weimann, G. (2008) They psychology of Mass- Mediated Terrorism. *American Behavioural Scientist,* Vol. 52, Issue, 1, Pg. 69 - 86