Research Guru
Online Journal of Multidisciplinary Subjects (ISSN : 2349-266X)
Volume-13, Issue-1, June 2019
Impact Factor: 4.081
www.researchguru.net

CYBER TERRORISM: A COMPARATIVE PERSPECTIVE BETWEEN UNITED STATES OF AMERICA AND UNITED KINGDOM LEGAL SYSTEM

Misha Bahmani
Research Scholar, USLLS, GGSIPU, Delhi

ABSTRACT: *The author demonstrates the impact, which has been caused by terrorist activities by making use of digital technology. The emphasis is made on how the lives of the people have changed and why there is a need to have effective measures to control such activities in order to make people feel secure and safe in society.*

The author postulates the measures that are taken by the United States of America and the United Kingdom in order to deal with threats caused by cyber terrorism. There will be a short analysis of the definitions given by different authors and organizations stating the concept of cyber terrorism. Further, the concern is made on to find out whether these efforts which are made by these countries are helpful in combating such activities. There is a need to focus on such practices and the authorities should not take it lightly. The article depicts that it is essential to fight back against cyber terrorism. It is important to protect human life from any form of threat caused by terrorist groups. There is a need to understand the difference between cyber terrorism and hacktivism. Additionally, one should have a balanced system which could protect human rights and could make effective laws against cyber terrorist activities. The countries should make joint as well as individual protective measures in order to attain their goal of maintaining peace and order in this world.

Keywords: *Cyber Terrorism, Human Rights, Internet, Protective Measures, Terrorist*

1. Introduction

It has been a matter of concern nowadays humans will cope with fast changes that have taken place in society with the passage of time. With the beginning of the use of the Internet the founders would have never thought that specific people would have later misused this technology at a certain stage than utilizing it in a proper manner. There has been a rise in a number of crimes, which are not only physical, but there is now the use of technology to cause harm to society as a whole. The term 'Cyber Terrorism' is becoming progressively common in popular culture, yet a solid definition of the word seems hard to come by. Although the phrase is loosely defined, there is a large amount of subjectivity in what exactly constitutes cyber terrorism. This term was first coined in 1997 by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California. It was considered to be the convergence of cybernetics as well as terrorism.[1] The United States (U.S.) Federal Bureau of Investigation defines cyber terrorism as any premeditated, politically motivated attack, which is against computer systems, computer programs as well as data and results in violence toward non-combatant targets by sub-national groups either clandestine agents.[2]

There is a difference between cybercrime and cyber terrorism, although both are the crimes of the cyber world there is a difference of intention of the preparatory and

motive. We can say that cybercrime is an unlawful act wherein the computer is either a tool or a target or both. Whereas, cyber terrorism requires a more detailed definition and hence we can define it as the intentional use of turbulent activities in cyberspace with the intention to further causing harm to social, religious either political aspects or related motive, or alarms any person concerning such matters.

According to NATO, cyber terrorism is considered to be a cyber attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal.

Moreover, cyber terrorism is usually not intended for physical harm but its intention is to attack the work of computer or devices to gain access to confidential data or financial information. There is a difference in cyber terrorism and cyber attack. Cyber terrorism is an act of sabotage that is carried out to cause terror and loss to infrastructure and computers are used to store, process and communicate information between groups of individuals. Therefore, computers are not the problem but it is the people who manipulate them for cyber attacks.

2. Why Cyber Terrorism occurs?

Cyber terrorism appears to be an attractive option for terrorist groups. While analyzing the reasons for the occurrence of these terrorists' activities we need to focus upon basically five factors. These factors comprise of the destruction factor, complexity factor, cost factor, media-impact factor and preparation factor.

To begin with, the first factor is the destruction factor which covers the destruction caused by the use of online nicknames as screen names by the terrorists or internet surfers. Additionally, they log on to a website as an unidentified guest user and making it extremely difficult for the security agencies and police forces to track down the terrorists' real identity. Whereas, in the situation of cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, no customs agents to outsmart. Secondly, complexity is the other factor. The variety and number of targets are tremendous. The cyberterrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines as the case may be. Subsequently, the sheer number and intricacy of potential targets guarantee that terrorists can find vulnerabilities and weaknesses to exploit. Thirdly, there is a media impact factor also. As the I LOVE YOU virus[3] showed, cyber terrorism has the capability to affect directly a larger proportion of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want. Cyber attacks are relatively less expensive than traditional methods. All that the terrorist require is a personal computer and an online connection. They do not need to buy any sort of weapons such as guns and explosives; rather, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection is in relation to the fourth factor which is cost. [4] It depends on preparatory factor where cyber terrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers. In other words, it can be conducted remotely, a feature that is especially appealing to terrorists.

3. The Rise of Cyber Terrorism

A series of cyber attacks were launched against popular government websites in the United States and other countries, effectively shutting them down for several hours

with devastating consequences for the United States economy and national security.[5]

Additionally, there was one message released in a video in 2015, from a hacker group that claimed to be affiliated with the Islamic State. The video showed a digitized, hooded and faceless figure, akin to the symbol of the hacker collective Anonymous, reading out a prepared speech in Arabic with English subtitles. Also, a group had declared itself as Islamic State's Defenders by a video online however it was not later supported by any organization.[6]

There was another incident of a cyber attack, which included the famous case of Estonia. The cyber attack took place in 2007 which had unknown attackers who launched a full-scale cyber attack against the Estonian government. The cyber attack remained relatively unnoticed for the first twenty-four hours but was discovered soon thereafter when Estonian Minister of Defense Jaak Aaviksoo found himself unable to log into the Prime Minister's Reform Party website. Due to such unfortunate events, a cyber attack in Estonia has stressed the severity of threats posed by cyber warfare to the United States and the international community at large.[7]

U.S. is not new to such attacks one such event in the history is known as 'Titan Rain' where the code name U.S. analysts gave to a series of 2004 cyber attacks in which Chinese Web sites targeted computer networks in the U.S. Department of Defense and other U.S. agencies, compromising hundreds of unclassified networks. However, one needs to understand that even misuse of small information can be an advantage for the enemy to know the weakness of the American administration.[8]

4. What is Hacktivism?

The rise of Internet technology has brought many changes in several fields including activism. These new technologies have given protestors a background to spread and mobilize their ideas. Also, technical innovations have given them the ability to employ hacking tools in directing cyber operations analogous to their protests. This merging of hacking and activism is known as Hacktivism. Worms Against Nuclear Killers (WANK) is a great example under this aspect.[9] It is noteworthy that Hacktivism can be for anything it could be either for documents, data or for dollars. The clear example is the Aaron Swartz case in which Carmen M. Ortiz stated that stealing is stealing, whether you use a computer command or a crowbar, and whether you take documents, data or dollars. It is injurious for the victim when a stolen good is also sold again either it has been given to someone else.[10] However, there are also instances of hacktivism in the cricket rivalry between India and Pakistan. In 2014 Pakistani cricket team defeated Indian team for Asia Cup held in Dhaka. Next day in Meerut unfortunately 67 Kashmiri students were suspended as they were supporting Pakistani cricket team and they were distributing sweets when the Pakistani team won. It was found that later the website of student's University was hacked by a group who claimed themselves as Pakistan Cyber Army.[11]

i) Difference between Hacktivism and Cyber Terrorism

Although, the boundary between hacktivism and cyber terrorism is blurred as both are involved in disruptions by different techniques. To elaborate, the difference between hacktivism and cyber terrorism it is essential to know that hacktivism has resorted for a political cause, it is usually done in a peaceful way. The level of collaboration and information sharing is relatively high among hacktivists than among cyber

terrorists.[12] Nevertheless, cyber terrorism is grabbing the attention of the public through aggressive ways, specifically instilling fear into the hearts and minds of the general public.[13] Hacktivists have four main weapons at their disposals such as virtual sit-ins and blockades, automated e-mail bombs, web hacks and computer break-ins, and computer viruses and worms. The first weapon is virtual which includes generation of traffic towards the website that other users losses their access to that site and hence gain publicity via media. Regarding the second weapon that is e-mail bombing, there was an incident in 1997 when an e-mail bombing was conducted against the Institute for Global Communications (IGC), a San Francisco-based Internet Service Provider (ISP). The attackers wanted ETA's site pulled from the Internet. To accomplish this they bombarded IGC with thousands of spurious e-mails.[14] The third weapon covers web hacking and computer breaking, whereby they hack into computers to access stored information. For instance, ISIS 'Hacking Division' claims to have hacked the personal information of hundreds of military, political and diplomatic personnel and released it online in a report with a hit list. The list was in the form of a spreadsheet and was shared by the so-called Islamic State Hacking Division which contained the private details of 1,400 individuals.[15] Lastly, the fourth weapon comprises of the malicious code that could infect computers. The Code Red Worm has infected about a million servers in 2001 and has caused damage of $2.6 billion by destroying the computer hardware, software, and networks.[16]

ii) Measures to control

While dealing with the future capabilities of cyber terrorists we need to focus upon, what effect terrorist organizations can have against critical infrastructures and also how could such a major cyber attack play out in the future in real time. The aim of cyber terrorism is not necessarily mass destruction but the mass disruption of an opponent by corrupting its information. The aim of cyber terrorism is to damage, misuse, confuse, and hijack our information and communications infrastructure and that damage could, if unchecked, have far-reaching and catastrophic results.[17] There is an urgent need to stop these cyber terrorist activities. In 2012, a video from al-Qaeda's as-Sahab media outlet calling for an electronic Jihad was released to the FBI. The chilling video showed an unnamed al-Qaeda operative directing covert mujahidin to launch waves of cyber attacks against U. S. networks which included critical infrastructure such as the power grid and water supplies.[18] There can be two strategies which can be active and another can be passive defense, the only difference is the imposition of the penalty. For instance, in Active defense deterrent theory plays an important role and strict risk or penalty is imposed on the attackers.[19]

For example, Jay P. Kesan once warns that an active self-defense regime, which he termed as 'Mitigate Counterstriking' and emphasized that it is a necessity in cyberspace to protect critical infrastructures such as banking, utilities, and emergency services. According to him the threat from cyber attack is real and harm is greater in real sense.[20] However, Steven Chanbinsky stated that one should follow active defense rather than passive defense. In his view, the passive defense does not work well against cyber threats. From this, we can understand that we should not expect any difference in cyberspace.[21]

5. Laws in relation to Cyber Terrorism- A Comparative Perspective

The paper focuses on the measures, which are taken by the United States of America, and the United Kingdom legal system in order to tackle the problem related to cyber terrorist activities. It is noteworthy that these countries are taking the matter seriously and have emphasized the importance of having stringent laws for the welfare and protection of society. Moreover, they have joint their hands together as well as individually to safeguard society from any form of unwelcoming activities caused by the terrorist by making use of digital technology. Today, most of the experts believe that the Internet is not only a tool for international organizations but also central to their operations.[22] This has established a threat to the cyber world and the lives of the people too.

i) United States of America

The U.S. government had budgeted $14 billion for cybersecurity in 2016.[23] The cyber threats are still not controlled and many federal agencies have not taken two-factor authentications where one requires a card and a PIN number. According to the American Gallup polls cyber terrorism is a serious threat to American growth and interest. Gallup for the first time has asked to consider the matter related to cyber terrorism, where it has been stated that the use of computers has caused disruption or fear in society.[24] It has considered cyber terrorism to be among the top three threats in the upcoming years. As per the polls that were taken in 2016 where the result showed that 73 % of U.S. adults had considered cyber terrorism to be a serious matter of concern.[25]

Subsequently, the Global Risk Report of 2016 illustrated that cyber attacks are most likely to occur in America. The World Economic Forum stated that this Report is an eye opener for the business community and the society has to act responsibly while they are working. They believe terrorism is one of the risks which they carry on their head while doing business there.[26] When we look at the cyber terrorism definition under Cyber Insurance Policy the standards changes significantly. This policy is applied to disruptive activities against a computer system.

The Homeland Security Department is responsible for the regulations related to the acting of cyber terrorism where the concern has been made on protection of people from cyber terrorist activities which are domestic as well as international. Additionally, the concern is made on the maintenance of the digital world and safety which can be electronic and national in nature. The focus is made on the preservation of the liabilities and freedom established by the American Constitution. The signing of the Homeland Security Act was the first effective step taken by the authorities to create an organization which receives funds and other resources for keeping a check on the security of the nation. Today, they have PATRIOT Act, Tools Required to Intercept and Obstruct Terrorism which allows the Department of Homeland Security to collect information related to prevention of terrorist activities. After the unfortunate event of 9/11 attacks on the World Trade Centre and Pentagon, the Former President Georg W. Bush had signed the PATRIOT Act. From this now the government authorities have the right to search various communications like emails, telephone records, medical records and more. Also, Former President Obama had signed an extension of the Act. The Act at present also includes anti-money laundering provisions in order to stop the terrorist from obtaining money by their actions. The

Act includes terrorist and cyber crimes as crimes under the Act. However, the Act has been criticized for violating the civil rights of the people who are an American citizen. In 2010 the protecting cyberspace as National Assets Act amended Title 11 of the Homeland Security Act of 2002. According to this Act, cyber-aggression would be considered an act of war.[27]

Section 814 under Title VIII of the PATRIOT Act shows that punishments will be applied to those situations which either damage or gain unauthorized access to a protected computer and can cause a person an aggregate loss greater than $5000, where there is an adverse effect on medical examination, diagnosis or treatment, causes a person to be injured, causes a threat to public health or safety, or causes damage to a governmental computer which is used as tool for administration of justice, national defense or national security. In other words, this provision encourages the practice of check and balance where the concern is made on maintaining peace and order in society. Furthermore, it prohibits any extortion through a protected computer. Any attempt to cause damage to the computer by viruses or other software mechanisms will be punishable for imprisonment, not more than 10 years. In case matter related to unauthorized access and damage to the protected computer the punishment will be more than 5 years imprisonment. When the offense is committed the second time the punishment will not increase more than 20 years imprisonment. Also, Section 814 shows that there has been a rise in criminal penalties for Computer Fraud and Abuse Act where the computers which are located outside the U.S. are also included under the term of protected computers.

Recently, the Cyber Security Information Sharing Act of 2015 gives significance to improve cybersecurity in the United States by sharing information about cybersecurity threats and for other purposes. The Act permits to share information related to Internet traffic between the US government and technology as well as manufacturing companies. The Bill was passed in 2015 by the Senate which was later signed by Barack Obama in December of the same year. This Act is based on Senate Intelligence Committee Bill which provides an opportunity to the Homeland Security to act as a central system for sharing information. Former President Barack Obama has said that it is the time now to consider cyber threat to be one of the most serious economic and national security challenges for the nation.[28]

There was a project by Arizona University known as ‘Dark Web Project’ which claimed that on the Internet there are 50 crores pages, 10 lakh pictures, 15 thousand videos, 300 forums which are related to terrorist activities and more than 30,000 terrorists exist.[29] After the event of Estonia, the world is now keeping a check on the activities prevailing through the use of the Internet. One needs to learn a lesson from this event which took place in 2007 and still is an eye-opener for the authorities fighting which is against cyber-terrorist activities at present. One should not make the Internet a battlefield to win over the population or the territory in order to exploit the nation and its resources.

ii) United Kingdom

National Crime Agency’s Cybercrime Assessment in 2016 illustrated that society needs strong law enforcement in order to fight cybercrime. It was reported that almost 17% percent of crimes were committed through the use of computers in 2015.[30] After the events of 7/7 where the London underground bomb blast took place in 2005,

the authorities have become more active in order to protect the society from any form of terrorist activities which also include cyber terrorism. Under Section 1 of the Terrorism Act, 2000 defines terrorism with reference to cyber attacks which are related to the government and would apply against an international governmental organization such as NATO or the United Nations. Additionally, a cyber attack would be included in terrorism where the attack would involve anything which the court considers to be an electronic system.[31] In 2013, RAND Corporation conducted an investigation in related to the role of Internet use and it was found that 15 cases were there in relation to extremism, terrorism, radicalization which were earlier identified by UK Counterterrorism Units.[32]

With the Terrorism Act of 2000 and Terrorism Act of 2006, we are now able to address the matters related to cyber terrorism in the United Kingdom. Under Section 1(2) (e) the term 'Terrorism' includes the act of cyber terrorism under Act of 2000. It is broadly drafted so that it will include threats by cyber terror.[33] This Section imposes serious penalties to the offenders for using computers and internet technology where harm is caused in such way that they do not cause any direct harms to others such as posting on YouTube which leads to a terrorist act.[34]

Similarly, the Act of 2000 contains offenses which give the basis for charging individuals who have made use of the internet to support terrorist activities. Section 54 provides an offense to provide, receive or invite others to receive instructions or training in the making or use of firearms, radioactive material or related weapon, explosive or chemicals, biological or nuclear weapons. Namely under Section 57 if a person carries articles which can give rise to a reasonable suspicion that person shall be in connection to preparation, instigation or commission of the act of terrorism. For instance, carrying a hard drive, DVDs, any form of instructional document related to a suicide vest, mortars. In other words, anything specific in connection to acts of terrorism will be considered under the Act. Although, Section 58 deals with there is no evidence that the individual was engaged in the activities related to terrorism. If there is collect, make or have in one possession without any reasonable excuse any record of information which likely to cause or preparation of an act of terrorism or possession of any document or record of such information will be considered under this aspect. There is no need for the prosecution to prove that the accused is a terrorist or he possesses any item, which leads to terrorist activities.

The Terrorism Act of 2006 is an excellent example which provides information related to committing acts in preparation for terrorism.[35] Part I makes it an offense for a person to publish a statement which is meant directly or indirectly encourage the members of the public to do an act of terrorism which includes encouragement that glorifies terrorist acts or for a person to be reckless as a result of such conduct has an effect.[36]

For example, in case of R v. Bilal Zaheer Ahmad[37] where the defendant was charged with soliciting murder in relation to the article and with three offense possession of material likely to be used for the terrorist activities under Section 58 of 2000 Act. He was held liable for 12 years' imprisonment with an additional 5 years' period on the license.[38]

In 2000 the United Kingdom came up with Regulation of Investigatory Powers Act which is a remarkable example of a legal framework for regulating the five types of

surveillance activities which are considered by the government agencies are as follows:

a) Interception of communications, which includes intercepting telephone calls or accessing the contents of e-mails

b) Intrusive surveillance, which shows covert surveillance in private premises or vehicles.

c) Directed surveillance where the covert surveillance against an identified target in a public place.

d) Covert human intelligence sources, which cover undercover agents.

e) Communications data includes matters such as records related to communications but not the content of such communications.[39]

The British Foreign Secretary William Hague stated that cyber threat is a serious issue for the country and there is need to take quick steps in 2011. Hague said that a globally coordinated response is the basic requirement to combat cyber threat.[40] From this, we can observe that the use of the internet by the terrorist has risen with the passage of time.

6. Conclusion

There has been an increase in the numbers of Internet users around the world among which is the terrorists. The use of technology has caused greater harm to society through involvement of terrorist activities. The United States of America has considered cyber terrorism to be their major concern nowadays. With reference to the United Kingdom, their Former Prime Minister in 2015 has stated that cyber terrorism is a serious matter of concern for both the nations. The most welcoming step which these countries can make is to work together in harmony to fight back against cyber terrorist activities. The United States of America needs to develop their laws in relation to cybersecurity as well as cyber intelligence and this can be an inspiration for the United Kingdom to have a similar model. There is need a to have a balance between the protection of human rights and the need for effective prosecution. There is an urgent need to have developed technology which could help in fighting against cyber terrorist activities. We should learn lessons from our past events such as Estonia, 9/11 attacks on the World Trade Center and Pentagon, 7/7 attack in London in order to safeguard the future generation from any form of exploitation. Moreover, recently in 2019 the Global Cyber Innovation Summit took place in New York with an objective to encourage better enforcement of laws in order to fight against such evils that have been are prevailing in the society for a very long time.[41] There is a need to have strict laws and skills training should be given to those authorities who are dealing with this matter. The countries need to regulate the services which are provided by the cyber café so that terrorist cannot easily access to internet facilities. The people should encourage the practice of having strong security measures while surfing on the internet in order to maintain peace and order in society.

References

1.Barry C. Collin, *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, Annual International Symposium Criminal Justice Issues, 11 (1996), http://www.crime-research.org/library/Cyberter.htm.

2.GENERAL SECURITY, (Dec. 21, 2012), http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/.

3.Mark Ward, *A decade on from the ILOVEYOU bug*, BBC News (May 4, 2010), http://www.bbc.com/news/10095957.
4.GABRIEL WEIMANN, *Cyberterrorism: The Sum of All Fears*, 28 STUDIES IN CONFLICT & TERRORISM 129, 137 (2005) , https://www.princeton.edu/~ppns/Docs/State%20Security/Cyberterrorism%20-%20sum%20of%20all%20fears.pdf.
5.The Lipman Report (2010) , Cyber crime and cyber terrorism: inducing anxiety and fear on individuals, (Feb. 3, 2011), http://iconof.com/blog/cybercrime-cyberterrorism-inducing-anxiety-fear-on-individuals/.
6.Allesendria Masi, *ISIS-Affiliated hackers threatens cyberattacks on U.S*, INTERNATIONAL BUSINESS TIMES, Nov. 5, 2011, http://www.ibtimes.com/isis-affiliated-hackers-threaten-cyberattacks-electronic-war-us-europe-1917320.
7.International Affairs Review, *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security*, (April 26, 2007), http://www.iar-gwu.org/node/65.
8.The lesson of Titan Rain: Articulate the dangers of cyber attack to upper management , HOME LAND SECURITY NEWS WIRE, 14 Dec., 2005, http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management.
9.Dorothy Dennings ,*The rise of hacktivism*, Georgetown Journal of International Affairs, (Sep. 8, 2015) http://journal.georgetown.edu/the-rise-of-hacktivism/.

10.John Schwartz, *Open-Access Advocate Is Arrested for Huge Download* , N.Y. TIMES, (July 19, 2011), http://www.nytimes.com/2011/07/20/us/20compute.html?_r=0.
11.RFSID , *Cyber Threat intelligence*, (Feb. 11, 2016), https://www.recordedfuture.com/india-pakistan-cyber-rivalry/.
12.STEFANO BALDI ET AL. , HACKTIVISM , CYBER TERRORISM AND CYBERWAR:THE ACTIVITIES OF THE UNCIVIL SOCIETY IN CYBERSPACE, http://baldi.diplomacy.edu/italy/isl/Hacktivism.pdf, 18 (2003).
13.Infobarrel technology, *The difference between hacktivism and cyber terrorism,* (Nov. 13, 2013), http://www.infobarrel.com/The_Difference_Between_Hacktivism_and_Cyberterrorism.
14.GABRIEL, *Supra* note 4.
15.ISIS Hacking Division' claims to have leaked names and addresses of at least 100 military personnel, DAILY MAIL ONLINE , (Aug.13, 2015, 6.12 PM), http://www.dailymail.co.uk/news/article-3195974/ISIS-hack-compromises-State-Department-personnel-s-private-information.html.
16.GABRIEL, *Supra note* 4.
17.Frank Fiore & Jean Franco, *How Cyberterrorism Can Affect You?* (Mar. 1, 2002), http://www.informit.com/articles/article.aspx?p=25739&seqNum=3.
18.Cloherty & Jack , *Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad*, ABC News (May 22, 2012) , http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875.
19.S.E. Goodman, *Cyber terrorism and security measures, Science and technology to counter measures workshop* (2007), https://www.nap.edu/read/11848/chapter/6.

20.*Active cyber-defense strategy best deterrent against cyber-attacks* , HOME LAND SECURITY NEWS WIRE, 28 June 2011, http://www.homelandsecuritynewswire.com/active-cyber-defense-strategy-best-deterrent-against-cyber-attacks.
21.Steven chabinsky, *Passive Cyber Defense: The Law of diminishing and negative returns*, (May 6, 2013), http://econwarfare.org/passive-cyber-defense-the-laws-of-diminishing-and-negative-returns/.
22.DAVID TALBOT, TERROR'S SERVER ANNUAL EDITIONS: VIOLENCE AND TERRORISM 130 (2007).
23.Daniel Bukszpan, *The new era of cyber terrorism*, CNBC News (Sep. 25, 2015), http://www.cnbc.com/2015/09/25/biggest-cyberthreats-to-watch-out-for-in-2016.html.
24..American considers cyber terrorism the top threat, SECURITY MAG. (Feb. 15, 2016), http://www.securitymagazine.com/articles/86920-americans-consider-cyberterrorism-the-top-threat.

25.Justin Mc Carthy, *American Cite Cyber terrorism among top three threat to U.S.,* (Feb. 10, 2016), http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three threats.aspx?g_source=Politics&g_medium=newsfeed&g_campaign=tiles.
26.Denise Johnson, *Cyber terrorism a major concern for U.S. Businesses*, Claims Journal, (Aug. 15, 2016) http://www.claimsjournal.com/news/national/2016/08/15/272825.htm.
27.MAURICE DAWSON & MARWAN OMAR, NEW THREATS AND COUNTERMEASURES IN DIGITAL CRIME AND CYBER TERRORISM 5 (2015).
28.60 Minutes : Former Chief of National Intelligence Says U.S Unprepared for Cyber Attacks (CBS television broadcast 6 Nov., 2009), http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

29.Maneela, *Cyber Crimes: The Indian Legal Scenario*, 11 US-China L. REV. 570, 579 (2014).
30.NATIONAL CRIME AGENCY STRATEGIC CYBER INDUSTRY GROUP, CYBER CRIME ASSESSMENT, NEW FOR A STRONGER LAW ENFORCEMENT AND BUSINESS PARTNERSHIP TO FIGHT CYBER CRIME ,2016,NCA ,at 6 (UK), http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.
31.CYBERTERRORISM - UNDERSTANDING, ASSESMENT AND RESPONSE 6 (Thomas M. Chen et al. , 2014).
32.RAND CORPORATION, RADICALISATION IN THE DIGITAL ERA, THE USE OF INTERNET IN 15 CASES OF TERRORISM AND EXTREMISM, 28 (2013) , http://www.rand.org/pubs/ research_reports/RR453.html.
33.Clive Walker, *Cyber Terrorism: Legal Principle and law in UK*, 110 PENN. STATE L. REV. 625, 629 (2006), http://www.leeds.ac.uk/law/court21/penn07d.pdf.
34.MAURICE, *supra* note 27, at 9.
35.Susan Hemming, *The practical application of counter-terrorism legislation in England and Wales: A Prosecutor's perspective*, 86 INTER. AFFAIRS, 955-969, 964 (2010).
36.UNODC, The use of internet for terrorist purpose 39 (Sep., 2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.
37.2012 WL 5995906.
38.UNODC, *supra* note 36, at 36.
39.LIBERTY , NATIONAL COUNCIL FOR CIVIL LIBERTIES,SUMMARY OF SURVEILLANCE POWER UNDER THE REGULATION OF INESTIGATORY POWERS ACT, 2016,(UK), https://www.liberty-human-rights.org.uk/sites/default/files/Liberty's%20summary%20of%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf.
40.*GCHQ chief reports 'disturbing' cyber-attacks on UK*, BBC News (Oct. 31, 2011), http://www.bbc.co.uk/news/uk-15516959.
41. Daily Briefing, (May 10, 2019), https://thecyberwire.com/issues/issues2019/May/CyberWire_2019_05_10.html.