Shahzad et al LGURJCSIT 2019

LGU International Journal for
Electronic Crime Investigation

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

Research Article

Vol. 3 Issue 2, April - June 2019

Cyber-Terrorism Law, Implementation and Ways Forward

Amir Shahzad
DDPP Sargodha
7th Batch specialized Training of Counter Terrorism Prosecution
aamirshahzad510@yahoo.com

Abstract:
This research paper is concerned with focused critical analysis of cyber terrorism laws in Pakistan. Cyberspace is now becoming a battlefield where terrorists are active on dark net and using digital tunnel for which every country of the world has to take necessary steps for global peace, in the same way Pakistan needs an effective legislation and its efficient implementation. We explore here some crucial questions regarding cyberterrorism threats, cyber terrorism laws, implementation challenges and some recommendations based on current situation as well as a slight glance on future perspective of the topic Cyber terrorism law, implementation and the ways forward.

Keywords:

1. Introduction

Before the promulgation of prevention and electronic crime act (PECA) in 2016, there was a law namely Electronic transaction Ordinance 2002 (ETO) to deal with the unauthorized and unlawful access to information system. However, ETO was an incapable law to cope the multidimensional nature of cybercrime. An increasing use of internet at one click is at the same time a phase of new challenge for the globe as well as in Pakistan which enforced legislature to draft a legal framework to protect the legitimate digital media users as the modern school of thought now tells that "digital rights are basically human rights in the internet era". Accordingly elaborating 25 new offences and their punishments, Prevention of Electronic Crime Act 201 6 was passed on August 11, 2016 in Pakistan, first comprehensive law in our history to encounter cybercrime as well as cyber terrorism. Much has been said on the issue of "Electronic Pearl Harbor" before and after Washington and New York attacks of September 11, 2001 but thereafter apprehensions raised a bitter question to the whole world as alarming notion that "what would be the probabilities and trepidations of terrorist attacks in cyberspace in future"? As reported by Carnegie-Mellon Computer Emergency Response Team Coordination Center, about 200000 cyber security incidents took place within the first three quarters of 2003 by nasty programmers? Hackers? Or script kiddies? The answer is not so simple. The person behind cyber-attacks could belong to any terrorist organization, intending to cause widespread damage to the peace and prosperity of the world. So here we are with a law Prevention of Electronic Crime Act 2016 in Pakistan to deal with this modern challenge of digital era i.e. Cybercrime & Cyber terrorism.

Obviously, implementation of PECA,2016 in letter and spirit would remain a challenge for Pakistan, as we are a country victimized most by terrorism and unfortunately, we are now placed in the grey list of Financial Action Task Force (FATF) with allegation of terrorism financing. So, to curtail our victimization, to get out from the grey list and to protect our future we need to protect our country from cyber terrorism. Accordingly, we need an efficient comprehensive moderate legal framework and

its effective implementation, hence this study aims to review this law in this perspective.
This law is multifaceted in nature dealing with the cybercrime in general, cyber terrorism and with other legal and procedural aspects. This review only focusses on provisions related to the cyber terrorism and its implementation issues. Firstly, sections related to cyber terrorism are analyzed. Secondly investigation, procedure and related issues are critically reviewed. Thirdly, legal, investigative, administrative, and technical challenges to implement this law, particularly to encounter cyber terrorism. Lastly, ways forward to these challenges are proposed.

2. Research Methodology

Research methodology for this paper is a combination of primary and secondary research. Interviews have been conducted of the legal, computer sciences and digital forensics experts from the different practical fields. As a secondary source, benefits have been obtained from different research articles, thesis, different statutes and other sources from all over the world. Proper references have been made accordingly.

3. What is Cyber Terrorism?

Before going to discuss the concept of cyber terrorism we need to pass the bridge of complexity i.e. the definition "terrorism" which is not only different among the different countries but also an absolute clarity in the definition is still needed. Pakistan has longest definition of terrorism under section 6 of Anti-Terrorism Act 1997. Accordingly, for a general understanding it can be inferred that if an act is terrorism for a country and if the same is done by using any information system, the offence would be cyber terrorism. Let's have a look on few important definitions of cyberterrorism to understand its scope.
Dorothy E. Denning, defined cyberterrorism in year as: "Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives".
Websites hacked by terrorist organization are often political or social and are used as tactics of cyber terrorists. In the word of J.T Caruso:
"Cyberterrorism – meaning the use of cyber tools to shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of coercing or intimidating a government or civilian population".
In the advent of 21st century, there remained a debate to define the cyber terrorism between the thinktanks around the world. Media used to derive the definition of cyber terrorism from the above notion e.g. in 2001 Business World Report publish a list of cyber terrorism attack, two of which given below:

a. Dutch hackers made theft of information from the U.S. Department of Defense computers about U.S. troop movements during the 1990-91 Persian Gulf War and tried to sell the information to the Iraqis but the Iraqis thought it was a trick.

b. Disfigurement of U.S. Web sites after the April 1, 2001 crash between a Chinese jet fighter and a U.S. investigation plane.
However, these examples remained failed to qualify Denning's definition: "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, plane crashes, water contamination, 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"
As observed above, media reporting was cited misleading and arguments were offered that there was no specific example of cyberterrorism which qualified Denning's prerequisites till that time. So, there are various concepts on this issue considering cyber-terror, cyberterrorist and cyberterrorism. While PECA 2016, reveals the definition of cyberterrorism in the following words under section 10
"Cyber terrorism. Whoever commits or threatens to commit the offences under sections 6. 7, 8 or 9, where the commission or threat is with intent to-

"(a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or in the public or a section of the public or community or sect or create a sense of fear or insecurity in

society; or

b) advance interfaith, sectarian or ethnic hatred

c) advance the objectives of organizations or individuals or groups proscribed under the law"

While the corresponding provisions referred above, section 6 deals with offence "Unauthorized access to critical infrastructure information system or data". Section 7 deals with offence "Unauthorized copying to critical infrastructure information system or data". section 8 deals with offence "Unauthorized interference to critical infrastructure information system or data". section 9 deals with offence "glorification of an offence".

So mainly offences are defined in section 6,7,8,9 but if these offences are committed or threaten to commit with the Mens rea as revealed in section 10 above, would amount to cyberterrorism under the perspective of PECA, 2016. However, it extends its perspective in section 10A & 10B in the following manner:

Section 10A reveals the concept of Hate Speech, "whoever prepare or disseminate information through any information system or device that advances or likely to advance inter-faith, sectarian or racial hatred"

Section 10B divulges the offence of that recruitment, funding and planning of terrorism, preparing or disseminating information, through any information system or device, that invites or motivates to fund, or recruits people for terrorism or plans for terrorism.

So, a wider scope definition we have now under PECA but still there is much to say about it. Some of the critics considered it as a law full of vagueness and the scope of cyber terrorism is contradictory with the fundamental human rights guaranteed by Constitution of Pakistan. Concept of terrorism entailed by section 10 of PECA is criticized for its too much broader scope which makes it unclear. It's a general principle to test the unclear legislation on the basis of vagueness doctrine. The essence of this doctrine is based on clarity of criminal law. It requires an explicit clarity that a criminal legislation must answer clearly that what type of conduct is punishable?

The mindset correlated to terrorism, hate, cyber terrorism, cyber hate is sightseen as well as scrutiny of wider theories which relate to cybercrimes such as "social influence", "social identity theory" and "social identity model of individualism", belongings and discriminatory moral disentanglements. An efficient implementation of any law is always a slave of its given scope and definition. It's now universal reality that cyber space in a parallel universe within the human world which is much wider and bigger indeed. Terrorist are part of this world and they do have complementary opportunity to use cyberspace for their ulterior causes which is much easier to do as compare to physical actions and may be more fatal than ever before. Anti-terrorism legislation always adversely affects the human fundamental rights. Peace and prosperity of a state is more valuable then freedom of speech or freedom of using digital media.

After facing almost two decades of worst terrorism, we are forced to have such wider scope definition of cyber terrorism with vast powers of investigation agencies. However, probability of political misuse of any criminal law cannot be ruled out. More the wider scope definition more chances of its misapplication.

4. Historical Review of Cyber-Terrorism

The importance of cyberspace can be well adjudged that almost each of the frontline terrorist organization has Web site(s). These sites even cannot be forced off because these terrorist groups are genius enough that they use to operate their web sites from the countries with wide scope freedom of speech laws e.g. alneda.com of Al-Qaeda group used at first Malaysia as its host country then Taxas and thereafter Michigan. It was forced off in 2002.

Web sites were used by terrorist groups for various causes. Few examples from the history are listed below:

a. hizbullah.org was used by Hizballah as its central press office.

b. moqawama.org was used to present the details of its attacks on Israel

c. Jehad.net, aloswa.org were established by supporters of Al Qaeda to support Osama bin Laden.

d. Al-Farouq website was used by Osama bin Laden to publish 39 principles of jehad

e. 7hj.7hj.com was used to impart the skills of hacking for Jehad purpose.

f. Alneda.com notable most with reference to its multi-features i.e. cyber-planning through use of internet via publication of terrorist cause and propaganda, recruitment, information gathering, internet techniques to hide identities, fund raising, control and mobilization etc.
Talking about 9/11 attacks, Muhammad Atta placed his final instruction via email, as reported:

"the semester begins in three more weeks. We have obtained 19 confirmations for the studies in the faculty of law, the faculty of urban planning, the faculty of arts, and the faculty of engineering"

The code words used, encapsulated, it is said that four targets or four airplanes to be used for attacks

Obviously, it's a natural progression for terrorist groups to target /use cyber space for their attacks. Hence cybersecurity is a global issue, it must be treated globally. Not only every state is required to have an efficient and moderate anti cyberterrorism legislation but there is also a crucial need to have a global legislation with mutual integration of all countries of the world for global peace and prosperity. PECA ,2016 by Pakistan is first-rate step, in line with this mutual global mission.

5. Cyber Terrorism Laws in Pakistan:

As said earlier sections 6,7,8,9,10,10A,10B of Prevention of Electronic Crime Act, 2016 with section 11W of Anti-Terrorism Act 1997 are the direct provisions to encounter cyberterrorism in Pakistan. Let's have a gist of understanding of these provisions:

5.1 Section 2(c) of PECA, 2016:

The basic prerequisite of sections 6,7,8 is "critical infrastructure" which is broadly defined in section 2(c). It encapsulates all those processes, networks, assets, systems, facilities, if they got loss or their integrity is compromised, the consequences would might be in all or any of the followings:

1. Substantial causalities or loss of life
2. Substantial adverse impact(s) on economic or social situation
3. Substantial adverse impact(s) on national security
4. Substantial adverse impact(s) on national defense
5. Substantial adverse impact(s) on functioning of the of the state

Its scope has been made wider by proviso of this subsection where its provided that it is authority of the Government to declare any private or Government infrastructure as critical infrastructure based on its objectivity in purview of above-mentioned criteria.

5.2 Section 2(k) of PECA 2016:

It further extends and specify this concept by giving the gist of critical infrastructure information system and critical infrastructure data. These terms are specifically used in penalizing sections this Act.

5.3 Section 6 of PECA:

Incriminates the unauthorize access to critical infrastructure system or data and provides punishment of imprisonment up to 3 years or fine up to one million rupees.

5.4 Section 7 of PECA

Section 7 incriminates the unauthorize copying or transmission of critical infrastructure data and provides punishment of imprisonment up to 5 years or fine up to 5 million rupees.

5.5 Section 8 of PECA

Section 8 incriminate the interference with the critical infrastructure system or data and provides punishment of imprisonment up to 7 years or fine up to 10 million rupees. These three sections penalize a cybercrime without its node with any kind of cyberterrorism.

5.6 Section 9 of PECA

Section 9 is directly related to terrorism activity and incriminate a pet activity of terrorist i.e. glorification of an offence. From all the history of terrorism it is evident that every terrorist group needs its glorification to flourish and to fascinate the attentions. This section reveals in the following way:

- Whoever prepares or disseminates information,
- Through any information system or

device,

- With the intent to glorify an offence related to terrorism or
- With the intent to glorify any convicted terrorist who is convicted for terrorism charge
- With the intent to glorify activities of proscribed organization
- With the intent to glorify activities of proscribed individual
- With the intent to glorify activities of proscribed group

It further explains the word "Glorification" as praise or celebration in any form of description. The punishment provided under this section is an imprisonment up to 7 years or fine up to 10 million rupees. This section in fact is very important with reference cyber terrorism as history tells us that terrorist groups used their web pages for their glorifications

5.6 Section 10 of PECA

Then section 10 comes with the proper term of "cyber terrorism" and encapsulates the scope of the offence of cyber terrorism. It focuses on "intent" or we may say "Mens rea" to create nexus of offences under sections 6,7,8,9 particularly with cyber terrorism. It covers both commission of offence or threat to commit which makes this section wider in scope in term of its implementation. A cybercrime under the aforementioned sections becomes cyber terrorism under this section mainly because of the intention of the offender. It elaborates in clause (a) that intention of offender is:

- Creation of coercion
- Creation of intimidation
- Creation of sense of fear
- Creation of sense of panic
- Creation of sense of insecurity

For:

- The Government
- The public
- Any section of public
- The community
- Any sect
- The society

So, in clause (a) of section 10, clear details come across, what terrorist groups usually aim to do ever. Clause (b) specifically emphases sectarianism, like intention to evolve hate or to spread hate between the sects or ethnic groups. It is pertinent to mention here that; this focus is one of the prerequisites provided in the preamble of Anti-Terrorism Act 1997 to encounter the intense abuse of sectarianism in Pakistan.

Every terrorist organization or group has its objectives for which terrorists strive for. They need to spread their objective notion at its maximum to achieve them. Clause (c) speaks about such objectives. It relates Mens rea of offender to advance the objective of proscribed individuals or proscribed groups or proscribed organizations. So, to stop the advancement of objectives of terrorist, this clause is emerged wisely. Punishment provided under section 10 is imprisonment up to 14 years or with 50 million rupees.

5.9 Section 10-B of PECA

The section deals with the offence of recruitment of people for their terrorist group, generation of funds for their terrorist activities and terrorism planning vide using information system. As said earlier, now it easier for the terrorist groups to motivate people to join their cause and to invite their financial support by interacting with them through internet devices as everyone have now this source in his hand round the clock in the shape of cell phones. At the same time, it has become an effective way then ever before, for their planning. This section provides 7 years or fine as punishments for the offenders.

5.10 Section 11W of Anti-Terrorism Act 1997

Section 11W of Anti-Terrorism Act 1997 was emerged to encounter the projection of any kind of terrorism or terrorist or proscribed organization or even organization under observation due its suspicious activities or funding etc. via publication, dissemination or any other such like sources. As mentioned above, facing new wave of terrorism in the leadership of Maulvi Fazlullah in Sawat, who used FM radio channel to motivate people in the name of jehad against the Government of Pakistan by declaring this country as Darul Harrab etc, Government emerged specifically the word FM radio by amending this section in 2009 but thereafter it was repealed in 2010. The scope of this section is very broad by including about all types of source of communication and about all types of possible acts to use these sources with the multi-motive(s) behind related to terrorism behind.

Actions:

1. Glorification of terrorist
2. Glorification of terrorist activities
3. Projection of any convicted terrorist who is convicted under the charge of terrorism
4. Projection of any proscribed organization
5. Projection of any proscribed person
6. Projection of any organization which is under the observation

Methods or Source of Communication:

a. Printing
b. Publishing
c. dissemination
d. Audio cassettes
e. Video cassettes
f. Any form of data device
g. Any form of storage device
h. Any kind of visible sign
i. Written photographic
j. Electronic
k. Digital
l. Wall chalking
m. Any other source or method

The punishment provided under the charge 11W ATA is 5 years imprisonment with fine. News report is exception of this law provided in this section but with the condition of "good faith". So, all the news channels and newspapers etc. are exempted from this penalized section when they are reporting to the general public. However, on the part of reporting agency would be observed in any adverse circumstances46.

5.11 Section 24 & 25 of PECA, 2016

All the offences under this Act may be read in the light of above both the sections of PECA. Scheme of this law reflects that substantive offences like terrorism would be tried along with sections of this law if the information system was also used for commission of terrorism. Offences of terrorism, for example glorification, hate speech are tried under the Anti-Terrorism Act 1997, if the mode of committing does fall under the ambit of ATA,1997 and would be punished under the same Act only, but if any information system is used or any other mode provided in PECA 2016 is used the offender shall additionally be punished under this PECA 2016 as well.

5.12 Sections 26 (3)(4), 28 & 37 of PECA, 2016

Collection, preservation and production of digital forensic evidence is a significant subject of any cyber law as well as cyber terrorism law. Sub-section 3 & 4 of Section 26 of PECA, 2016 caters to the requirement of scientific standards for admissibility of forensic evidence. Even preservation of data under Section-28 is also an enabling provision along with successive sections. Section 37 also help in this context which authorizes the government for establishment of forensic Laboratory.

So as afore discussed there are bunch of sections to face the challenges of cyber terrorism. This law provides much more but, for an effective delivery of any law, it has to pass through its implementation challenges.

6. Implementation of Cyber Laws in Pakistan – Problems

Talking about cybercrime and cyber terrorism, our country does have its history without any combatable law in hand. PECA, 2016. A late legislation is now a comprehensive law to cope this modern scientific contest. Obviously, there are series of hurdles and glitches on the way of its effective implementation:

6.1 Legal Complications

1. Chap-V speaks about all offence are non-cognizable, compoundable and bailable, except offences u/s 10, 19 & 19-A; this chapter is somewhat defective as does not talk about application of code of criminal Procedure expressly; though an attempt has ben made to highlight it in section 47 but it does not serve the purpose. Even who would compound the offence is a big question,offences which are non-cognizable obviously would be investigated if they are annexed with any offence under PPC or any other law which are cognizable. Question of jurisdictions would arise if the offence is added by any other law; section 41 would be a great hurdle in this respect. Unnecessary litigation would reduce the efficacy of this law.

2. No appointment of prosecutor is highlighted as it is mentioned in ATA & CNSA;

which would open a debate for prosecution of offences.

3. Trend of investment, use and speculations in "digital currency" is increasing day by day which is an offence on one side but it has other worst faces like it is being used for money laundering as well as it can be used for terrorism financing. No specific provision, definition or penalized section has been emerged in this regard. More over in the current era, money laundering and cybercrime should be seen together. These offences, in this cyber dependent modern world, should be understood together and dealt accordingly. Unfortunately, Anti-Money Laundering, 2010 is also silent on this issue.

4. Section 27 of PECA, 2016 reveals "power to investigate" and start with the word "only an authorized officer of the investigation agency shall have power to investigate under this Act". This might be problematic. In the current scenario FIA has power to investigate offence under this Act. For instance, if any terrorist attack is happened in any area of the country and CTD is dealing with that, according to this section if that terrorist activity is also related with some cyber terrorism activity then CTD is unable to investigate or collect evidence up to that extent?? Obviously, this would amount to loss of evidence and other procedural complications. In the same way concept of joint investigation team under this section is also unclear. It becomes more confused once again with the compulsion of authorized person.

5. Preservation of Data etc. is being regulated through the intervention of court under section 30, as its give power to authorized officer to dispense with such warrant if he apprehends destruction of data. Seeking permission from court in such like cases would be a futile exercise because destruction of data is one click away in the system; until the warrant is obtained, data would be no more in the system. It should be the prerogative of Investigating officer to directly approach the unit for data where ever it may be. We have seen the misuse of section 94 & 95 of Cr. P.C which is not being effectively applied and accused gets the benefit.

6. Sub-section 3 & 4 of Section 26 of PECA, 2016 provides the requirement of scientific standards for admissibility of forensic evidence. Conservation of data under Section-28 is also an enabling provision. Section 37 also helps in this context which authorizes the government for establishment of forensic Laboratory. Here it's important to understand that digital evidence is not tangible. By taking into possession any kind of device vide recovery memo is not a digital evidence preservation. Digital evidence is intangible content, it cannot be dealt under police rules or any other such like law for the time being enforced rather it needs customized rules and regulations. Its admissibility would remain in question. This law is silent and there are no such framed rules about the stander of admissibility of evidence i.e. Procedure of preservation of digital evidence and its production before the court of law etc..

7. According to the IT experts, terrorist groups uses or can use digital tunnel or dark net to be remained untraceable. PECA 2016 does not define even these terms. This would remain a complicated issue unless properly legislated.

8. There are voices which considered that cyber terrorism clauses under PECA 2016, as against the fundamental human rights, ensured by the Constitution of Pakistan 1973 like freedom of speech etc. the broader powers of investigation agency or authorized officer are also criticized from the same house accordingly.

6.2 Issues Related to Investigation

1. Contrary to the provisions of PECA, 2016, power to investigate is devolved to Federal Investigation Agency (FIA) rather establishment of an independent investigation agency as required by this law. A wing namely NR3C is established within FIA to investigate cybercrime. It's astonishing fact that a proximately thirty thousand application pertaining to cybercrime are pending with FIA while there are only 10 investigation officers to deal with cybercrime. Accordingly, the question arises about investigation of cyber terrorism cases and how can cyber laws implemented in letter and spirit?

2. History tells us that terrorists groups operate wisely and now they are very keen to use cyberspace for their all types of activities like planning, recruiting, fund raising, training, and glorifying etc. While we do have an old wine in a new bottle. FIA has no capacity, skills and infrastructure to combat this challenge. Moreover, the human resource working as

Authorized officer is unqualified, unskilled and untrained. So, FIA is lacking not only quantitatively but also qualitatively.

3. As discussed earlier, collection of digital evidence, its preservation, transmission, its forensic analysis and its presentation to the court need a complete package of legal and technical skills so that it can be admitted by the court of law is completely a scientific process. Neither we do have any trained force to do so nor have any set of rules for this purpose. So even FIA arrests an offender, there is minimum chance of his conviction. Worries becomes more bitter when we see our capacity with reference to the giant of cyber terrorism.

By virtue of subsection 3 of section 26, PECA requires the establishment of an independent digital forensic lab which is yet to be established. We are depending on PFSA Lahore for digital forensic analysis which is already overburdened. Moreover, it has no complete digital forensic infrastructure and compatible capacity. So, there is dire need of an independent digital forensic lab for effective implementation cyber terrorism laws.

7. Ways Forward – Future Perspective

At first, we must realize the significance of cyberspace, cyber evidence in connection with the terrorism. Even now and onward we need digital evidence or we can use cyber evidence to prove petty offences in the court of law. To stop the cyber based terrorism, we need to a proactive approach by all means. We can't wait for the incidences. More over its an easy way to drag the culprits into the prison and save the innocent people from fake accusations. Followings are the endorsements in the light of aforementioned issues:-

a. PECA is a law, based on technology, not easily understandable by the investigating officers, prosecutor and the judges. Frequent meetings of these three, combined trainings with respect to understanding of protocols applied for arriving at the results and calling of experts in the courts only in critical cases. The most important area for presentation of evidence be focused in such efforts.

b. As aforesaid, this is a technology-based law, hence cannot be implemented without relevant infrastructure for possible monitoring of cyberspace with proactive approach, effective investigation, collection, preservation and presentation of digital evidence.

c. The necessity of digital evidence will increase day by day with high pace in the upcoming times. We were late in legislating proper cyber law and now we must not get late in establishing an efficient well equipped digital forensic lab. Without such lab cyber laws or cyber terrorism laws would remain dreams to be implemented.

d. Legislation flaws as aforementioned, need a dire attention of Government. A body consisting technical experts, legal experts and others may be constituted to work on these legal complications and framing of the proposal of solutions.

e. As required by the Act, an independent investigation agency may be established with skilled and qualified sufficient strength of work force.

For effective implementation of cyber terrorism laws, a customized special wing comprising technical experts and counter terrorism trained personnel may be established within CTD so that terrorism activities may be deal efficiently.

8. Conclusion

Pakistan is a frontline country fighting with the 21st century monster i.e. terrorism, at the same time we are a Nation victim most in war against terrorism as we have lost more than 80000 lives and much more. Lacking of infrastructure and an expert team, incidents of cyberterrorism are not properly reported or even screened and understood in Pakistan. Terrorist has an open opportunity in the shape of cyber world for their all types of activities e.g. recruiting, training, fund raising, funds transferring, planning, and operations etc.

We are having legal, infrastructure and investigation issues along with other systematic problems due to which we remained unable to take effective steps to counter cyber terrorism. We do not have a proper investigation agency to investigate and to properly implement cyber-terrorism laws. What we need to do is to create infrastructure with sophisticated tools to

monitor cyberspace at maximum, to detect and to prevent cybercrime as well as cyber terrorism. We also need an efficient legal framework compatible to the future cyber terrorist attacks. Our general public and institutions may also be sensitized regarding the understanding, sensitivity and apprehensions of cyberterrorism.

9. References

[1] Electronic Transaction Act 2002

[2] Hutt, Rosamund. 2015. "digital Rights Are Basically Human Rights In The Internet Era." World Economic Forum.

[3] National Assembly Secretariat. (2016). "prevention Of Electronic Crime Act" May 2016. Islamabad. Available At: http://www.na.gov.pk/uploads/documenTs/1472635250_246.pdf

[4] Tan, Kheng Lee Gregory. 2003. Confronting Cyberterrorism With Cyber Deception . Monterey, California .

[5] Karim, Shahid. 2019. Www.dawn.com. Jun 10.

[6] Anti-terrorism Act 1997 Of Pakistan.s.6

[7] http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[8] Forno, Richard. 2002. "Shredding The Paper Tiger Of Cyberterrorism ."

[9] Tan, Kheng Lee Gregory. 2003. Confronting Cyberterrorism With Cyber Deception . Monterey, California

[10] Ibid

[11] Http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[12] National Assembly Secretariat. (2016). "prevention Of Electronic Crime Act" May 2016. Islamabad. Available At: Http://www.na.gov.pk/uploads/documen Ts/1472635250_246.pdf

[13] Prevention Of Electronic Crime Act 2016, S.6

[14] IBID, S. 7

[15] IBID, S. 8

[16] IBID, S. 9

[17] IBID, S. 10A

[18] IBID, S. 10B

[19] Khan, Eesha Arshad. N.d. "the Prevention Of Electronic Crimes Act 2016: An Analysis." 1-10.

[20] Faisal Daudpota, 'an Examination Of Pakistan's Cybercrime Law' (2016) Ssrn 14 <http://dx.doi.org/10.2139/ssrn.2860954> Accessed 16 May 2018.

[21] Blakmore, Brain. 2016. Policing Cyber Hate, Cyber Threat And Cyber Terrorism. New York: Routledge.

[22] Timothy L. Thomas. Al Qaeda And The Internet: The Danger Of "cyberplanning". Parameters. Spring 2003.

[23] Dorothy E. Denning. Cyberterrorism. Testimony Before The Special Oversight Panel On Terrorism, Committee On Armed Services, Us House Of Representatives, May 23, 2000. Http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, Accessed July 2003.

[24] IBID

[25] IBID

[26] Joel Leyden. Al-qaeda : The 39 Principles Of Holy War. Israel News Agency. 4 September 2003

[27] Ibid

[28] Bradley K. Ashley, Lt. Col, Usaf. Anatomy Of Cyberterrorism: Is America Vulnerable? Research Paper, Air War College, Air University, Maxwell Afb, Al. 27 February 2003.

[29] Timothy L. Thomas. Al Qaeda And The Internet: The Danger Of "cyberplanning". Parameters. Spring 2003

[30] Timothy L. Thomas. Al Qaeda And The Internet: The Danger Of "cyberplanning". Parameters. Spring 2003.

[31] Prevention Of Electronic Crime Act 2016, S. 2(c)

[32] IBID, S. 2(K)

[33] IBID, S. 6

[34] IBID, S 7

[35] Prevention Of Electronic Crime Act 2016, S. 8

[36] IBID, S 9

[37] [Denning1, 2000] Dorothy E. Denning. Cyberterrorism. Global Dialogue, Autumn 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror-gd.doc, Accessed July 2003.

[38] Prevention Of Electronic Crime Act 2016, S. 10

[39] Anti-terrorism Act 1997

[40] Zuberi, Kokab Jamal. 2018. "use Of Cyber Space By Terrorist Organization." Electronic Crime Investigation.

[41] Prevention Of Electronic Crime Act 2016, S. 10a

[42] IBID, S. 10B

[43] Zuberi, Kokab Jamal. 2018. "use Of Cyber Space By Terrorist Organization."

Electronic Crime Investigation.
[44] Khan, Yousaf Ali & Ijaz. Winter 2018. "uses And Abuses Of Fm Radiaos By Mreasiitants In Former Federally Administered Tribal Areas (fata) Ans Provincially Administered Areas (pata), Pakistan." Central Asia Journal No. 83.
[45] 2003 P.cr.l.j 277
[46] Anti-terrorism Act 1997, S. 11w
[47] Prevention Of Electronic Crime Act 2016, S. 24
[48] IBID, S. 25
[49] Rafiq, Amjad. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 10)
[50] Prevention Of Electronic Crime Act 2016, S. 26
[51] IBID, S.28
[52] IBID, S.37
[53] Rafiq, Amjad. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 10)
[54] Rafiq, Amjad. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 10)
[55] Ibid.
[56] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7).
[57] Anti-money Laundering Act 2010
[58] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7).
[59] Prevention Of Electronic Crime Act 2016, S. 30
[60] Code Of Criminal Procedure 1898, S. 94
[61] Ibid S. 95
[62] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7)
[63] IBID
[64] Khan, Eesha Arshad. N.d. "the Prevention Of Electronic Crimes Act 2016: An Analysis." 1-10.
[65] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7)
[66] Zuberi, Kokab Jamal. 2018. "use Of Cyber Space By Terrorist Organization." Electronic Crime Investigation.
[67] Rafiq, Amjad. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 10)
[68] Malik, Muhammad Baqir. N.d. "pakistan And India Cyber Security Strategy." 1-5
[69] Zuberi, Kokab Jamal. 2019. Critical Review Of Prevention Of Electronic Crime Act 2016 (may 7)
[70] 2018. International Journal For Electronic Crime Investigation Vol.2. Lahore: Lgu International Journal For Electronic Crime Investigation .
[71] Mr. Muhammad Usman Akram, Mr. Tahir Abdullah. 2011. "effective Enforcement Of Cyber Laws In Pakistan ." International Journal Of Science And Technology 1-15.
[72] Zuberi, Kokab Jamal. 2018. "use Of Cyber Space By Terrorist Organization." Electronic Crime Investigation.
[73] Sue, Siman Shecliff. 2012. "the Use Internet For Terrorist Purpose." United Nations, Unodc 7-12.