TRENDING TERROR

Raghav Sharma
Under Graduate B.B.A L.L.B (Hons)
Vatsala Sharma
Under Graduate B.A. L.L.B (Hons)
Uttaranchal University,Law College Dehradun
Dehradun, India

Abstract-

This research looks at the "**Challenges to Human Security in 21st Century**", focusing on a world epidemic, "**Terrorism and Cyber Terrorism**". Our work has Terrorism at its foundation with an emphatic emphasis on Cyber Terrorism. Apart from myriad challenges, the world is in clutches of Terrorism and Cyber Terrorism, making it a pressing issue for our research. Ironically, we could not find a comprehensive definition of the term "Terrorism", due to lack of universal agreement, however, certain legislations, giving individual **definitions** of the same exist. Prominent ones amongst them are - "Comprehensive Convention on International Terrorism" on which negotiations are taking place, Title 22 Chapter 38 US Code 2656f, 18 Chapter 113 B US Code 2331 and NATO 2008 Document. The paper also covers various terrorist groups operating within India with specific mention to Indian Mujahidin, LeT and ISIS.

The research further lays structure of Cyber Terrorism stating the intersection of physical and virtual worlds, which are inherently disparate yet, form the vehicle for it, as its major cause. In absence of its universal definition, our search converges on **Section 66(f) of IT Act, 2000** for Indian Territory. Since, every cyber-attack does not constitute cyber terrorism, making it a controversial term in itself, bringing us to the point of connecting the words "Cyber" and "Terrorism" to create a comprehensive definition. Aforementioned legislations were a precaution step to instances like- **WannaCry Ransome Ware Attack, 2017.** The paper studies Cyber Terrorism into three heads- **Domestic, Global and International Terrorism.**

After instances of Cyber Terrorists and attacks – **hacking, malware, Botnet** etc, the leading cases- **Ardit Ferizi's** Case, etc, the paper **concludes** with useful findings of **methods of protection** against this technological catastrophe. Since "Cyber war is the battlefield of now."

Terrorism is the tactic of demanding the impossible, and demanding it at gun-point
- *Christopher Hitchens*

Terrorism is one such world epidemic that has in its clutches, global communities, at large and seldom can any victim of it escape from the same. In broader sense, terrorism can be said to divided into myriad kinds- cross-nation terrorism, ethno-centric terrorism, state sponsored terrorism, whose meaning is latent in their names itself. However, in layman language, "any act that strikes fear in a person's mind, or terrorizes any person, can be said to defined as terrorism- generating or creating terror".

Etymologically, in Latin, the word "**Terrere**", means to frighten, which is similar to the English meaning which translates into "alarm", "anguish", "fear", or "panic". However, the word "Terrorism" has its roots in the French Revolution in the late 18th Century. The primary meaning of the word was "supporter of Jacobians", or "Adherent". The term "Jacobians" related to the groups surrounding Maximilien Roberspierre. The said group was held responsible for violence and rebellion in the French Government between June 1793 till July 1794. The given period got named, hence, as "Reign of Terror". Since then, the term is in vogue and strikes almost instantly, as an immoral act. The term is now exploited by the governments and non-state groups to demean the opposing groups.

As per the report of **November 2004** by a **Secretary-General** of United Nations, **Kofi Atta Annnan** defined "Terrorism", as "any act intended to cause death, or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organisation to do or abstain from doing any act."

With these conflicting yet similar opinions of world leaders one is left to wonder as to which acts can directly constitute as terrorism. To sum that up, if we take the world to be a stage then each terror attack accounts for a performance with an intent to affect many large audiences negatively, that is, an attempt to dismantle the foundation of a country while glorifying themselves and their ideologies.

With the advancement in technologies, the terrorists who have been known to have great degrees to their credit, have used media as a channel to spread, enhance their ideologies and ingratiate people and thereby, to convince them to believe in and follow their fanatic cause. Hence, media, unknowingly serves as "*oxygen of terrorism"*[1]. The "media" here, includes not only the print media and broadcasts, but also electronic media and use social networking sites, as well, for its propagation. The ease of accessibility has helped terrorism to branch out into another sphere which is popularly being termed as "**Cyber Terrorism".**

[1] Margret Thatcher- "Speech to American Bar Association"

Cyber Terrorism in its simplest form means "internet vandalism". Another famously used synonym for the same is "information war" or "electronic terrorism", because it majorly associates itself to the acts of deliberate and large scale attacks upon the computer networks by inducing viruses, causing malware, to cause disruption in the functioning of government organisations and individuals.

The word was first coined by **Barry C. Collins** of the "Institute for Security and Intelligence"[2] in the late 1980s. However, the term "Cyber Terrorism" must not be misinterpreted as "Cyber- attack" Addressing the gray area of cyber terrorism and cyber-attacks the thin line that differentiates them is the intent as; in the former- the motive is to create a feeling of terror while the later sprouts from financial or egoistical motive.

The face of terrorism is changing while the motivation remains the same because, of this it is mandatory to understand "Cyber Terrorism". As per the **National Information Protection Centre (NIPC)**[3], Cyber Terrorism is, "A criminal act perpetrated through computers resulting in violence, death and / or destruction, and creating terror for the purpose of coercing a government to change its policies."

Definitions of Terrorism

It is not just the individuals in a government system, even experts and scholars have failed to reach a consensus regarding definition of terrorism. Thus, ironically, we could not find a comprehensive definition of the term "Terrorism", due to lack of universal agreement, however, certain legislations, giving individual definitions of the same exist. Prominent ones amongst them are-

"The word **International Terrorism** means activities that-

Involve violent acts or acts dangerous to human life that are a violation of criminal laws of the United States or of any State or that would be criminal violation if committed within the jurisdiction of United States or any State;

a. Appear to be intended-
   1. To intimidate or coerce a civilian population;
   2. To influence the policy of government by intimidation or coercion; or
   3. To effect the conduct of a government by mass destruction, assassination, or kidnapping; and
b. Occur primarily outside the territorial jurisdiction of United States, or transcend National boundaries in terms of the means by which they are accomplished, the persons they appear to intended to intimidate or coerce, or the locale in which they are perpetrators operate or seek asylum." [4]

- "**Terrorism** is defined as political violence in an asymmetrical conflict that is designed to induce terror and psychic fear (sometimes indiscriminate) through the violent victimisation and destruction of non-combatant targets (sometimes iconic symbols). Such acts are meant to send a message from an illicit clandestine organisation."[5]

- "The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in furtherance of political or social objectives."[6]

- "Premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents."[7]

The given definition has been on the negotiating table of the **Comprehensive Convention** (proposed by India in 1996) since 2002, still waits to seek universal approval-

- "Any person commits an offence within the meaning of this convention if that person, by any means, unlawfully and intentionally, causes-

a. Death or serious bodily injury to any person; or
b. Serious damage to public or private property, including a place of public use, a state or government facility, a public transportation system, an infrastructure facility or the environment; or
c. Damage to property, places, facilities, or systems referred to Paragraph 1(b) of this Article, resulting or likely to result in major economic loss,

When the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act."[8]

[2] 11th Annual International Symposium on Criminal Justice Issues- "The Future of Cyber Terrorism"
[3] Department of Homeland Security, U.S
[4] 18 Chapter 113 B US Code 2331
[5] Carsten Bockstette at The George C. Marshall European Centre for Security Studies
[6] 28 U.S Code of Federal Regulation Section 0.85
[7] Title 22 Chapter 38 US Code 2656f

Terror Groups and Instances of Terrorism

Depending upon the kinds of various terrorist activities, their place of origination and reason of promotion, we have various terror groups operating at National and International levels.

At National Level –

There are following terror groups operating in India, under following sub-heads of different kinds of terrorism-

- **Lashkar-e- Taiba-**
  1. Formed in 1987.
  2. Current Leader- Hafiz Mhd. Saeed.
  3. Is one of the largest terrorist group in India.
  4. Received funding from Osama Bin Laden.
  5. Attacked Indian Parliament in 2001. (31st December 2001).
  6. Aim- To separate Jammu and Kashmir from India and merge it with Pakistan.
- **Hizbu-ul-Mujahideen-**
  1. Founded in late 1980s.
  2. Leader man is **Sayeed Salahudeen.**
  3. Aim- to Separate Kashmir from India.
- **Indian Mujahideen-**
  1. Formed in 2007.
  2. Leader man is **Abdul Subhan Qureshi.**
  3. Aim- to create an Islamic Caliphet across South- Asia.
  4. Responsible for **Jaipur Bombing and Ahmedabad Serial Blast, Banglore Bombing** all in 2008.

On 4th June, 2010 the Indian Mujahideen was declared a terrorist organisation and was banned by the Indian Government. The same was followed by New Zealand and the United Kingdoms. Some of the attacks claimed by them, apart from the ones above, are **2011 Mumbai Serial Blast, 2013 Bodhgaya Blast**,

Ethno-Centric Terror Groups-

- **Khalistan Zindabaad Force-**
  1. Formed in 1988.
  2. Current Leader- **Ranjeet Singh Neeta.**
  3. Aim- is to create a Sikh Independent State in Punjab, named "KHALISTAAN".

There are some other ethno-centric terrorist groups operating in the **North Western** region of India, apart from the aforementioned, such as, **Khalistaan Commando Force, International Sikh Youth Federation, Babbar Khalsa International**, lie in the same genre of acquiring Khalistaan.

i. **National Liberation Front of Tripura-**
  1. Formed in 1989.
  2. Current Leader- **Biswamohan Debbarma**
  3. Aim to establish an independent Tripura State.
  4. Held responsible behind assassination of Shanti Kaali- a tribal Hindu spiritual leader, Labh Kumar- religious leader of the State's second largest Hindu group.

ii. **National Socialist Council of Nagaland-**
  1. Formed in 1980.
  2. Current Leader- **S.S Khaplang.**
  3. Aim at securing Naga-State by unifying the Nagaland inhibited areas in the North-East of India and Northern Burma.
  4. Responsible for Insurgency in North-East India and Internal Conflicts in Myanmar.

There are some other ethno-centric terrorist groups operating in the **North-Eastern region**, apart from the aforementioned, such as, **National Democratic Front of Bodoland, Manipur People's Liberation Front, United Liberation Front of Assam, Tripura Tiger Force,** etc..

iii. **Maoist Communist Centre of India-**
  1. Formed in 1975.
  2. Merged with Communist Party of India (Maoist), in 2004.
  3. It is declared as Terrorist Organisation in India under Unlawful Activities (Prevention) Act,
  4. Aim- to overthrow the Indian Government through a civil war.

[8] UN General Assembly Resolution 51/210 of 17th December 1996, Sixth Session (28th January to 1st February 2002) Annex II art 2.1

At Inter-national Level –

There are following terror groups operating at international level, under following sub-heads of different kinds of terrorism, as declared by various Governments-

iv. Al-Quaeda-

1. Formed in- 1988.
2. Current Leader- **Ayman al-Zawahiri** (2011-present times)
3. First Attack on December 29, 1992 at Aden, Yemen (Movenpick Hotel).
4. Nations where it operates- U.S.A, U.K, U.A.E, Australia, Canada, India, Iran, Japan, New Zealand, Kazakhstan, etc.
5. Designated as Terrorist Group by the U.N Security Council, The NATO, The E.U, Russia, India, Australia, France, Israel, Ireland, Switzerland, and the like.
6. Aim- To establish Islamic Rule over the world.
7. Prominent Attacks-
   i. The Pentagon (U.S)- September 11, 2001
   ii. World Trade Centre (U.S)- September 11, 2001
   iii. Istanbul (Turkey)- November 15, 2003; November 20, 2003.
   iv. Aden (Yemen)- October 12, 2000.
   v. Nairobi (Kenya)- August 7, 1998.
   vi. Dar es Salaam (Tanzania)- August 7, 1998.

v. ISIS- Islamic State of Iraq and Syria

1. Formed in 1999
2. Current Leader- Abu Bakr al-Baghdadi
3. They were initially establish under the name of **Jama'at al-Tawhid wal-Jihad** and later joined Al-Quaeda from 2004 to 2014.
4. Nations where it operates- Islamic state of Iraq and levant, Syria majorly with others being Afghanistan, Pakistan, Egypt, Bangladesh etc. Their headquarters are at Baqubah (Iraq), Raqqa (Syria) and Mayadin (Syria).
5. Aim- to claim religious, political, and military authority over all Muslims Worldwide.
6. Prominent attacks-
   i. Corinthia hotel attack (Libya)- January, 2015
   ii. Orlando nightclub shooting (USA)- June, 2016
   iii. The berlin attack (Germany)- December, 2016
   iv. Kabul Supreme Court bombing (Afghanistan)- February 2107
   v. Manchester Arena Bombing (UK)- May, 2017

The below mentioned are some of the major terror attacks in India:

i. Delhi bombings 2005
ii. Mumbai train bombings 2006
iii. Jaipur bombings 2008
iv. Mumbai attacks 2008
v. Uri attacks, 2016

International Conventions to Combat Terrorism-

Established by the U.N and other International Organizations, there are twelve major International Conventions in existence which stand against terrorism. Though not all states are a signatory to it, but they are relevant in certain circumstances, such as Vienna Convention on Diplomatic Relations, 1961.

The list given below contains a number of conventions against terrorism, having a brief about each convention's major terms, aims, and signatories for better comprehension-

1. Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo Convention, 1963—Safety of Aviation):-

- The Convention is applicable for the safety of flights and aviation.
- Contains provisions by which aircraft commanders can impose restrictions on any person, if he has reason to believe that s/he has committed any act which is against aircraft's safety.
- The aircraft must be returned to lawful commander after custody of offender is taken by the contracting states.

2. Convention for Suppression of Unlawful Seizure of Aircraft ("Hague Convention", 1970—aircraft hijacking):-

- It is considered as offence if a person on board or flight, "unlawfully by force, or threat thereof, or any other form of intimidation, [to] seize or exercise control of that aircraft",[9] or makes an attempt of doing so.
- Makes it necessary for the signatories to make hijacking a severely punishable offence.
- Make its necessary for signatories to take custody of offenders and to extradite them, or to prosecute them.
- Makes it necessary for parties to assist each other, if criminal proceedings are brought.

3. **Convention on the Prevention and Punishment of crimes against Internationally Protected Persons (1970—Outlaw Attacks on Senior Government Officials and Diplomats):-**
   - The Internationally Protected Person is defined as "Head of a State, Minister for Foreign Affairs, a representative or official of the State, or an international organization which is entitled to protection."[10]
   - The crimes of intentional murder, kidnapping, a violent attack upon the official premises, the private accommodation, or the means of transport of such person; a threat or attempt to commit an attack, and other attacks upon the person or liberty of an internationally protected person, and an act constituting participation as an accomplice, shall be made punishable by the signatories to this convention.
4. **International Convention against taking of Hostage (The Hostages Convention, 1979):-**
   - The main objective of the convention is to define the meaning of "hostage taking", within the scope of this convention, stating- if "any person who seizes or detains or threatens to kill or injure, or continue to detain a person in order to compel a third party, namely, a state, an international intergovernmental organization, a natural or judicial person or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage commits the offence of taking hostages".[11]
5. **International Convention for the Suppression of Terrorist Bombing 1977 (UN General Assembly Resolution) –**
   - Provides a universal platform for jurisdiction of unlawful use of bombs and explosives and other lethal devices, in any place with intention to kill or cause serious bodily injury and destruction of that public place.
   - It enables the State parties to establish the aforementioned criminal offences under their domestic law, punishable by appropriate penalties accounting for their gravity.[12]
6. **International Convention for the Suppression of the Financing of Terrorism, 1999-**
   - It make the signatories to hold the ones who finance terrorism "criminally, or civilly" liable.
   - "measures to eliminate international terrorism, the UN General Assembly called upon all states to prevent and counter-act through appropriate domestic measures, the financing of terrorist and terrorist-organisations, whether such financing is direct or indirect through organizations which also have or claim to have charitable social, or cultural goals or which are also engaged in unlawful activities.. including the exploitation of persons for purposes of funding terrorist activities."[13]

Definitions of Cyber-terrorism

Since there is no finality on the definition of terrorism, similarly, there is no concrete definition of the term cyber terrorism which has sprouted from the technological advancement. We try to put forth of the definitions that lay down the as to what constitutes cyber terrorism.

The only definition given in any codified law is under Information Technology Act, 2000-

"*If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty, or security of India, then he commits cyber terrorism.*" [14]

Technolytics Institutes defines it as, "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to immediate any person in furtherance of such objectives.

National Conference of State Legislatures laid down the following definition – "the use of information technology by terrorist groups and individuals to further their agenda. This can include the use of information technology to organise and execute attacks against the networks, computer systems and telecommunications infrastructures or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to the vulnerable networks, website defacing, Denial-of-service attacks, or terroristic threats made via electronic communication."

[9] Article 1 (a)- 2. Convention for Suppression of Unlawful Seizure of Aircraft ("Hague Convention", 1970—aircraft hijacking)
[10] Article 1 (1) (a), Outlaw Attacks on Senior Government Officials and Diplomats, 1970.
[11] Article 1 of the Hostage Convention, 1979.
[12] Article 4 of International Convention for the Suppression of Terrorist Bombing 1977 (UN General Assembly Resolution)
[13] Para 3(f) of the 2 declarations adopted on report of the sixth committee annexed respectively to GA Resolution 49/60 and 51/210 of December 9, 1994 and December 17, 1996 respectively.
[14] Section 66(f) of Information Technology Act, 2000.

NATO defines it as - "*a cyber-attack using or exploiting computer or communication networks to cause sufficient disruption to generate fear or to intimidate a society into an ideological goal.*"[15]
FBI defines it as, "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non- combatant targets by subnational groups or clandestine agents."

Kinds of Cyber Terrorism-

There are broadly three kinds of cyber terrorists- Domestic, Global and International Cyber Terrorists. They are explained by following examples and under following heads-

1. Domestic Cyber Terrorists-

They are primarily the part of the society that we live in, hence, their main motive is to collect data regarding trade secrets, employees and any other secret information from a private server of any corporation. They attack a particular corporation that operates within their own society.

2. Global Terrorists-

Unlike the private server, the global terrorists, operate with an aim of creating public nuisance or causing inconvenience by destructing a major website, in order to bar traffic to that website, thereby, not letting the publication of the content which does not align with their ideology and modus operandi. They have a far reaching effect in comparison to domestic terrorists.

3. International Terrorists-

Their attacks are the most lethal from all other forms of terrorist attacks, as they are capable of putting the nation's security at stake. If they succeed in getting access and thereby disabling the signals required to fly drones, or technology used for military control and safeguarding of the nation, it could lead to a major physical war that would lead to loss of thousands of lives!
The above three kinds and their explanations clearly gives us a point of conversion that we mentioned in our abstract, whereby, when the physical and the virtual world coincide, it's not just smart cities and modern military equipment that sprout, but it also comes with it fair share of drawbacks, like acts of destruction and alteration which can cripple the economic, military and civilian infrastructure, if not, dealt with in due time, with effectiveness and efficiency.

How Terrorism and Cyber Terrorism -threat to Human Security?

The question "Is Terrorism and Cyber Terrorism, a threat to Human Life and Security?", holds the connotation itself that terrorism and cyber terrorism- a threat to human security. The daily newspapers are in themselves evidences to the connotation mentioned above. Given below are the instances which will prove how these two concepts are making human life, security and finance vulnerable and susceptible to threat-

1. Morris, 1988.

The first computer worm was transmitted in 1988, with a credulous intention to determine the expanse of the cyberspace. However, things went topsy-turvy, when the worm morphed into a virus, replicated and began infecting computers. The master-mind behind it was Morris, a student at Cornell University, U.S.A.
6000 computers were reported to be effected causing an estimate of $10-$100 million in repair bills. This event was the beginning of Ddos (Distributed denial-of-sevice) types of attacks that we witness today.

2. Jonathan James hacks NASA and US Defence Department, 1999-

James managed to sneak into computer of US Department of Defense Division and install a "backdoor" at its servers. This paved way for him to sneak a peek into thousand government emails and get usernames and passwords of various military computers. This made him steal a NASA software which amounted the space exploration $40,000 on grounds of system being shut for three weeks.
According to NASA, "the software (purported to be worth $1.7 million) supported the International Space Station's physical environment, including control of the temperature and humidity within living space."
Apart from these, the most recent Cyber Attacks are the ones which gave the most serious blow to the Cyber Headquarters of almost every nation.

3. WannaCry, 2017

The most recent and most disastrous cyber attack faced by the world on May 12, 2017 is a string of ransomware called WannaCry. 200,000 systems in 100 countries were affected with this attack. In total WannaCry netted almost 52 bitcoins, or about $ 130,000!It is alleged to have been committed by **Shadow Broakers**- unidentified hackers who leaked **EternalBlue** developed by US National Security Agency. EterenalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block Protocol.
The notable disaster (apart from computers) in this case was caused to The National Health Service Hospitals and Facilities in U.K, by creating chaos in emergency rooms, delaying vital medical procedures, and the like. This clearly underlines the idea of Cyber Terrorism being a threat to "Human Life and Security".

[15] NATO 2008 Document

4. Petya/ NotPetya/ Nyetya/Goldeneye, 2017-

A couple of months after WannaCry attack, another ransomware infection that followed was Petya, NotPetya, Nyetya, Goldeneye, which was more advanced than the WannaCry ransomware. Petya consists of ransomware which propagates via email attachments. On 27th June, 2017 France, **Germany, Italy Poland, U.K and US** and majority infections targeted **Russia and Ukraine**. It infected networks in many countries- US Pharmaceutical Company- **Merck**, Danish Shipping Company- **Maersk** and Russian- Rosnoft. However, more than 80 companies were attacked initially.

However it is alleged that the attack was targeted against **Ukraine.** The ransomware hit the Ukranian infrastructure, disrupting power companies, airports, public transit and central bank! The **Chenrobly Nuclear Power Plant went offline.** Considering the world, the Petya infected 2000 computers in U.S.

5. Vault 7, 2017-

On March 7, data trove containing 8,761 documents were stolen from the CIA that contained extensive documentation of spying operations and hacking tools. There were detailed files laying down the capabilities of the agency for the term 2013 to 2016 with regard to operating systems of the leading smart phones, web browsers-Microsoft Edge, Opera Software ASA, etc. as well as other operating system of macOS, Microsoft Windows and Linux.

Robert M. Chesney, Director of technology and public policy program MME at CSIS (Centre for Strategic and International Studies) alleged a group called Shadow Brokers linked to vault 7 by NSA hacking tools.

6. Ardit Ferizi Case-

21 year old Ardit Ferizi was sentenced for "providing material support to Islamic State of Iraq and levant (ISIL) and accessing a protected computer without authorisation and obtaining information in order to provide material support to ISIL.[16]

According to the US Intelligence, he was arrested in September 2015, for providing data that included names, email addresses, passwords, locations and phone numbers of 1,351 U.S. Military and other government personnel to popular I.S militant Junaid Hussain, who disclosed it on the web.

7. North Korea's Sony Picture's Hack-

In November 2014, a hacker group which identified itself by the name of **"Guardians of Peace" (G.O.P)**, leaked a release of confidential data from the computers of Sony Pictures Ent. Employees got locked out of their computer networks and red skeletons started appearing on their screens. After hacking internal data, movies like, "*Still Alice*", "*Annie*" and "*To Write love on her arms"* were leaked online. According to a theory, North Korea is to be blamed because, Sony's upcoming comedy "*The Interview*" was about an assassination attempt on Kim Jong Un, to stop the telecast of which the said attack was devised.

Apart from the cyber-attacks which are the most common aspect of cyber terrorism, which basically deals with satisfaction of the ego on the part of the attackers who aimed at causing economical loss to the target which maybe business houses, government or an individual, another major impact and which happens to be a lasting one is on the **psychology** of the public at large when terror groups like Al Quaeda do not shy away from uploading videos of brutal execution in the name of religion and upload it on the internet where at zero or bare minimum cost they reach out to billions of people thereby leaving an impact on the viewer which is not like an **economical loss** that can be recovered. How they operate is by collecting personally identifiable information which is later on sold in the black market, catering to the opportunists who aim at stealing identities, to drain the back accounts and charges on the credit card of the individuals whose identity has been stolen.

There was an incident when the branch of the same terrorist group AQAP published articles stating their intent to attack or strike on the US. Also, they used social media to impart their knowledge and share the intention with people of similar ideologies.

Yet another impact is that there is no territorial boundary to their crimes as they are not area specific. They might be sitting in one continent and cause a major malware in the other that to in seconds and before the person can even comprehend as to what went wrong, they are already celebrating their victory and aiming at yet another site. The problem amplifies when the countries where they take place might not have an extradition treaty with the other from where they are operating.

Analysis and Conclusion-

After stating as to what terrorism is and what cyber terrorism translates into and the various terrorist groups operating in India and on international level. We lay down the various cyber-attacks with the special mention of Ardit Ferizi's case. The entire research boils down to not just the impact that it has on India but how can we successfully combat it. There is always a beginning to everything and if we cut the roots there shall be no tress and no branches to it. These cyber terrorists are criminals who hack small websites and computer systems and have a meagre income. This income over the time is then used to set up a lager base and then they knows no ends as these petty criminals turn into dangerous terrorists, their meagre incomes into large fund base and their small websites into the entire computer server. Below mentioned are some of the safeguards that can be effectively applied in order to get control over these acts of threat and crisis in the 21st century:

1. International organisations should be independent of the influence of the world super powers to achieve the goal of supervising and securing the world as the scale of terrorist activities, frequency of attacks, and many other factors vary from nation to nation, therefore, if a nation has a comparatively lesser acts of terrorism to another, it should not stop them from formulating a common policy or law. Also, the nations must be brought to a common consensus at UNO and

[16] Department of Justice, Federal Court of Alexandria

should come up with a comprehensive definition and better ways to fight them by providing armies with latest technologies, improved training program and above all proper allocation of the funds and implementation of the laws.

2. World states should amplify their internal security systems which would in turn multiply the international security. The army must be given enough freedom and liberty to take necessary actions as and when required and the act of curbing it at its nascent stage should not in any way be hampered by the tedious hierarchy that needs to be followed before they get into action and by that time it's too late.
3. Governments of sovereign states need to be flexible enough to take into consideration the rationale that would cater the interest of majority of local citizens and hence would avert crisis resulting out of terrorism.
4. Nuclear disarmament should be practised by nations in turn contributing to descending arms race by way of certain agreements and treaties with deterrent enforcement agencies.
5. There must be proper rehabilitation facilities IF any terror attack happens so as to safeguard the generations to come and must be provided with counselling sessions so that the seed of hatred and a feeling of revenge does not settle in the mind as we would then be dealing with future terrorists who would be convinced that it is fine to take lives as they no nothing better to look for.
6. The government must put absolute ban with no loopholes in its application when it comes to the kind of content which must be displayed on the public platform. There have been various instances of videos, photos, interviews and open threats going viral over the internet which has a negative impact on the viewer as the feeling of insecurity, danger and fear seeps within.
7. There are many faces to a cyber-attack, which cannot be ignored. Not only states, nations and computer systems are exposed to its threat but also financial companies are not immune to it. For instance- a business could attack by cyber terrorists because of its contribution to nation's economy. In order to prevent this, the entire nation state needs to have such resources and be vigilant so much so that a second line of defence should be established in worst case scenario of the cyber invasion.
8. The oxygen of these agencies are the funds that are required by them at every stage of their operation and what we need to focus on is that the sources must be cut down and there must be a vaccum created so that their funds are drained and they can no longer support the people working for them and stop them from further expansion.
9. We have ourselves provided them with easy access to acquire a workforce whom they brain wash and manipulate into doing as they are ordered to do by facebook, twitter etc. There have been instances of professionals being approached by such agencies to join them by giving them lucrative career options and persuade them to work towards a greater cause while they are earning good. The government should therefore try and create better employment opportunities for the youth so that their vigour and energy can be channelized and they will not be swayed by such baits. They biggest example of unemployment turning into an epidemic is the situation in Kashmir where the people are bombarding stones over the military personnel and other officials just for a small sum of Rs 500.