INDIA AND CYBERTERRORISM

Colonel B S Nagial (Retd)

Director: Academy of Proficiency & Training,
SCO-743, Tricity Trade Tower
Zirakpur Punjab-140603

***Abstract*: To live peacefully in this world of danger and uncertainty, courage is prerequisite. There are two way to meet the danger: one, remain indifference to danger and two, prepare and motivate yourselves through knowledge and training and face the danger head-on. Technology is a double-edged weapon, which can used for both constructive as well as destructive work. Cyberterrorism is the fine example of destructive use of technology, which is posing threat to humanity. To defeat your enemy, first you know your enemy well. So, the aim of this paper is to understand the concept of cyberterrorism, its effect on the world community including India and how to counter this menace. Digital world is being exploited by the terrorist' organisations for radicalisation, recruitment, propaganda, fundraising, training, etc. These organisations use the darknet to carry out terrorist activities so not visible on the public platform. Time plays the biggest role in any combat and certainly it has greater significance when countering cyberterrorism wherein technology is changing very fast. This paper will also discuss the possible defences available against the cyberterrorism.**

***Keywords*: Terrorism, Cyberterrorism, Cyberattacks, Radicalisation, Digital Infrastructure, Use of Internet by terrorists and other criminals.**

Introduction

Terrorism is an unlawful use of violence and threat especially against civilians for achieving the political goals. Terrorism is as old as the human history itself. After Sept 11, 2001 terrorists' attack on United State of America, the world community has come together to solve the problem of International Terrorism. It is pertinent to mention that there are different types of terrorism so profiling is not an easy task. Since different terrorist' organisations have different ideologies therefore operate differently, even individual terrorist work differently. Terrorism is very dynamic in nature, changing its strategies very fast and always look for weak target/targets to strike. These targets may include power stations, military assets, banking industry, air-traffic controls, radio and television stations, etc. Digital world is providing many opportunities and new battlegrounds to these terrorist' organisations. Through digital infrastructure these terrorists are targeting people for radicalisation, recruitment, fundraising, propaganda, training and other nefarious activities. As world is evolving and becoming dependent on technology more and more, threat posed is no longer physical but extended to digital world also. Like conventional warfare we can secure our digital infrastructure and any intrusion by inimical elements can be checked, pursued and destroyed. Awareness among the people is very essential.

What is terrorism?

For formulating any kind of strategy, especially when doing so for addressing the security threat such as terrorism, it is important that threat be minutely examined and defined. In fact, defining terrorism is a war on terrorism itself so we shouldn't be wrong. Beauty and terrorism both are as far as their definitions are concerned not easy to describe. As beauty lies in the eyes of beholder so the concept of terrorism lies with the nation/nations which have faced it. Let us examine a few definitions of terrorism to under the basic concept of terrorism.

"Terrorism is a form of violent struggle in which violence is deliberately used against civilians in order to achieve the political goals (nationalistic, socioeconomic, ideological, religious, etc)." [1]

The United Nations General Assembly adopted the resolution 49/60(Measures to eliminate the International Terrorism) on December 9, 1994 which states 'terrorism' as the criminal acts intended or calculated to provoke a state of terror in the general public or a group of persons or particular persons for political purposes are in any circumstances unjustifiable, whatever the considerations of political, philosophical, ideological, racial, ethnic, religious, or any other nature that may be invoked to justify them.

United Nation Security Council Resolution 1566(2004) gives a definition of terrorism: "Criminal acts including civilians, committed with the intent to cause death or serious bodily injury or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a govt or international organisation to do so or to abstain from doing any act." Further improving up on the definition of 'terrorism' a United panel, on March 17, 2005 stated that terrorism is an act "intended to cause death or seriously bodily harm to civilians or non-combatants with the purpose of intimidation a population or compelling a govt or international organisation to do so or abstain from doing any act."

FBI (Federal Bureau of Investigation), U.S.A, terrorism as under:

"**International Terrorism**: violent criminal acts committed by individuals and/ or groups who are inspired by or associated with, designated foreign terrorist organisation or nations (state sponsored)."

"**Domestic terrorism:** violent, criminal acts committed by individuals and/ or groups to further ideological goals stemming from domestic influences, such as those of political, religious, social, racial, environmental nature."

In India, Terrorism as an offence doesn't figure in the Indian Penal Code of 1860 which was amended from time to time. For the first time the term terrorism was described in Terrorist and Disruptive (Prevention) Act, 1987 but this act was repealed in 1993. Again, the word 'terrorism' found its place in Prevention of Terrorist Act, 2002. This act also got repealed in 2004. Finally, on Aug 02, 2019 Unlawful Activities (Prevention) Act, 1967 was amended and passed which contains the definition of terrorist act. "Under this Act, the Central government may designate an organisation as a terrorist organisation if it:

- Commits or participate in act terrorism or
- Prepares for terrorism or
- Promotes terrorism or
- Otherwise involved in terrorism.

The act additionally empowers to designate individuals as terrorists on the above mention grounds."

It is very essential to define the word 'terrorism' because it will help us to understand the problem of terrorism and make strategy to eliminate such blot from the face of humanity. It is very surprising that so far, we haven't reached at the consensus of defining terrorism. Basically, this is because of two main reasons: one, a terrorist in one country is a 'freedom fighter' for other country and two, some nation sates carry out clandestine operations against another country through terrorist' organisations. The fact is terrorism is a terrorism irrespective of its shape, size or form. There can't be 'good-terrorism' or 'bad-terrorism'. Terrorism is a crime against the humanity. All actions of terrorism should be considered as illegitimate irrespective of nature and goal/goals. And I think the most appropriate definition of the terrorism proposed so far is: "An act of terrorism=Peacetime Equivalent of War Crime" This short but most appropriate definition was proposed by Alex. P Schmid to United Nation Crime Branch in 1992.[2]

Cyberterrorism

Cyberterrorism is a genuine danger, which is spreading its roots in society very fast. There is an urgent requirement of world attention and action to contain this menace. The potential targets of the cyberterrorism are the frameworks which control country's resistance and provide resilience. Internet dependency has increased significantly and also the horizons of security threat have expanded. The traditional concepts and methods of terrorism are giving-in to new opportunities provided by the digital world. In this age of information most of the terrorist' organisations have developed a deadly combination of weapons and technology. Information Technology is a double-edged weapon, which can be used for constructive as well as destructive work. Awareness among the people is the only answer to this problem. It is an hour of need to formulate the safety networks in anticipation of invisible threats of terrorists' organisations. Cyberterrorists may win the war without firing a shot by crushing the fundamental foundation, which is mainly dependent on the use of data science. Definitely, a society without protection in the form of 'self-help', in this era of technology can't be imagined. Internet doesn't respect the boundaries created by nation states hence attackers can attack at will all over the world. If it is not tackled sooner than later then definitely it would become irreversible and catastrophic in nature worldwide.

As compared to other terrorist' activities, cyberterrorism is new phenomenon. Since there is no common acceptability to the term terrorism therefore consensus on the definition of cyberterrorism can't be reached. Cyberterrorism is the convergence of technology and terrorism. It is an unlawful attack or threat of attack against computers, networks and other paraphernalia and carried to intimidate or coerce a govt or the people for furtherance of their cause their (terrorist' organisations) goals and objectives. Let's examine a few definitions available to understand the concept of cyberterrorism.

As per Lexicon-a US Dictionary powered by OXFORD, "Cyberterrorism is the politically motivated use of computers and information technology to cause severe disruption or widespread fear in the society".

"[G]et ready…… terrorists are preparing …...cyberspace-based attacks…." (John Arqiua, Waging War through Internet).

The term 'cyberterrorism' appeared for the first time in defence literature in1998 in U S Army War College.[3]

Prof. Dorothy Denning offered definition of terrorism in testimony before the House Armed Services Committee in May 2000 that has been widely cited:

"Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks and information stored therein when done to intimidate or coerce a govt or its people in furtherance of its political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property or at least cause enough harms to generate fear. Attack that leads to death or bodily injury, explosion, plane crashes, water contamination, or severe economic loss…... would be examples. Serious attacks against critical infrastructure could be acts of terrorism, depending on their impact. Attack that disrupt non-essential services or that are mainly costly nuisance would not." [4]

Federal Bureau of Investigation, a U S investigating agency define "cyberterrorism as a premediated, 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." [5]

Bruce Hoffman defines terrorism as “the deliberate creation and exploitation of fear through violence or threat of violence in the pursuit of political change.” [6]

From above mentioned definitions certain activities which form part of the cyberterrorism are inciting, recruitment, radicalisation, financing, planning, communication, etc, these activities can be grouped under Enabling Cyber Terrorism (ECT). In general, we use the terms such as cyberwar, cyberterrorism, cybercrime, hacktivism, etc interchangeable but there are inbuilt insidious differences. The term cyber is generally used for computer but it could also include other information technology including people who have the capacity to interpret the information. Cyberspace is a global domain where interdependent network of information technology infrastructure including internet, telecommunication networks, computer system, etc exists. The aim of the terrorists using cyber destructive terrorism is to manipulate the computer code and corrupt the information networks to destroy or damage the virtual as well as physical national assets. The internet has allowed for exchange of vast exchange of information. Thus, created space for both criminals and terrorists to operate individually or collectively. It is very important to understand the motives behind such attacks this will facilitate to grasp the term cyberterrorism properly. While all cyberterrorism could be attributed to cybercrimes but all the activities of cybercrimes can’t be attributed to cyberterrorism. The threat of cyberattacks are continuous on rise and online users are vulnerable to such attacks. Our dependency on cyber-world is increasing day by day. In fact, it is impossible to think of life without internet. Different countries have developed various rules and regulations to combat cyberterrorism but at international level we lack coordination. Before agreeing up on the counter cyberterrorism measures first of all we must reach at an acceptable definition of Terrorism as well as Cyberterrorism.

Motives, Interests of Terrorists in Cyberattacks.

There could be many logical reasons of terrorist’ cyberattacks. The first and the foremost motive could be to gain visibility and influence people by creating fear among them. Destroying things and killing people could be the other reasons. [7] Other lesser goals could be in relation to the maintenance and upkeep activities such as fund raising, planning, recruitment, intelligence gathering, etc. The cyber domain provides various benefits which are enumerated as under:

- Anonymous communication with other terrorist’ organisations and own cadres within the organisations.
- Because of personal safety as compared to physical attacks
- Can access the target/targets easily
- It is a cost-effective as only PC or Mobile Hand Set with internet facilities is required.
- Availability of various attacking tools
- Vulnerable targets could be accessed through remotely connected networks.
- A person with an average skill can operate without much knowledge. Its user friendly.
- Propaganda can be spread worldwide with speed.

Terrorists can plan and coordinate cyberattacks and other physical attacks through covert use of communication networks. In asymmetrical warfare, even a small group of terrorists can carry out a largescale cyberattacks as well as physical attacks thus inflicting serious damage. Some thinkers and strategists think that the term “cyberterrorism” is not justified because a well-planned cyberattack may only produce annoyances, not the terror as a bomb or Improvised Explosive Devise (I ED) would have done. But according to other thinkers and strategists, since computer networks attack produces enough of disruption in economic activities, spread fear amongst the targeted population and may cause death to civilians and non-combatants thus qualifies as “terrorism”. Cyberterrorism could be considered as an act of terrorism if it fulfils the following criteria.

- Effects based event. Cyberterrorism exists when computer-based attacks result in the effects that are disruptive enough to produce fear in the minds of targeted people as compared to traditional acts of terrorism.
- Intent -based event. Cyberterrorism exits when unlawful or politically motivated computer attacks are done to intimidate or coerce a govt or organisation or section of people to achieve a political objective or inflict injuries or cause severe damage the assets of the targeted nation.

The uses of internet by terrorist for cyberterrorism.

“The Internet is a prime example of how terrorists can behave in a truly transitional way; in response, States need to think and function in an equally transitional manner.” (Ban Ki Moon, Ex Secretary-General of U N O).

Peter Flemming and Michel Stohi identify two components of Cyberterrorism.[8]

- Computer technology as a facilitator of terrorism: It is used for political propaganda, terrorist recruitment and financing, intra and inter-group communication and coordination, intelligence gathering, etc. This enables the terrorist’ groups to maintain anonymity in routine activities and tactical operations, and also carry out their operation in cost-effective manner.
- Computer technology as a specific component of terrorist weapons or targets: This includes computer technology-based attacks or threats or public utilities and transportation, commercial institutions, individuals, political or ethnic groups, security forces, nation-states or far that any ‘perceived enemy’.

It is well known fact that terrorists possess the knowledge about computers, internet and various other tools and their usages in furtherance of their cause of terrorism. Such causes could be anything ranging from social goals to political gaols. [9]

As per the United Nation Office of Drugs and Crime report, terrorists use the internet for following reasons:

- Spreading propaganda relating to institutions, explanations, justifications or promotion of terrorist' activities
- Incite violence
- Recruitment and radicalisation of individuals
- Fund raising through direct solicitation, e-commerce, online payment modes, charitable organisations, etc.
- Training for the followers for combat tactics, use of explosions and weapons

Objectives of cyberattacks.

There could be many objectives of inimical elements for carrying the cyberattacks such as intentional disruption in the digital infrastructure, to cause economic losses, destroying of military assets, luring people to join the terrorist' organisations, etc. Cyberattacks are defined as deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and /or transiting these systems or networks. [10]. Cyberattack is deliberate exploitation of computer systems, technology dependent enterprises and networks. As per U.S. Army Training and Doctrine Command, cyber operation and cyberterrorism Handbook No.102, Aug15, 2005, p-ii-1 and ii-3 following objectives may drive terrorists to carry out the cyberattacks.

- Loss of integrity- unauthorised changes made to the data or IT system can result in accuracy, fraud or error in decision making that bring the integrity of the system under suspicion.
- Loss of availability- an attack on mission or computer system makes it unavailable for the end users.
- Loss of confidentiality-the consequences of unauthorised discloser of information ranges from loss of public confidence to national security threats.
- Physical destruction- ability to create actual physical harm through computer hardware or IT Infrastructure.

A cyberattack, disrupts the integrity and authenticity of the data mainly through malicious code that alters the program system software, thus leading to disruptive or incorrect output. Whole internet network is scanned completely through security software manipulation. Once infected, the machine can be manipulated remotely via internet. Cyber-weapons and ammunitions are the subdivisions of computer/machine codes intended to be used with aim of terrorising people and disruption or destruction of cyber-infrastructure.

Cyberattacks have the ability to disrupt the way in which ordinary individuals live (e.g. the chaos that would arise if none of the automatic teller machines (ATMs in country were operational). The interconnectedness of global financial institutions, enabled by modern communication technology increase the risk. [11]

Cyberattacks weapons are easy to use and can produce results such as defacing of website to steal data and sensitive information, intellectual property, spying on targeted system and disruption of essential services. On the other hand, cyberattack as a mode of conflict raises many operation related issues, such as origin or roots of such attack, whether done by terrorist' organisations or any particular nation state. Very difficult to prove all this. But definitely cyberattacks can support military operations. They are capable to disrupt and destroy the target/targets Command, Control and Communication (C3). And can also support covert operations to influence government, group of people, any particular organisation, etc. Valuable information and state secret can be obtained through cyberespionage.

How cyberattacks work?

If we understand the different types of attacks and how they are carried out then certainly we can take preventive measures to safeguard our digital infrastructure and can take care of vital & essential resources. A cyber-attack is generally carried out by a trained handler and may consist of many stages. As per National Cyber Security Centre, United Kingdom, the cyber-attack could be grouped in two categories:

1. **Un-targeted cyber-attacks.** Under this category attackers indiscriminately target as many devices, services or users as possible. Victims are not identified. For such attacks they use the following techniques: -

- **Phishing-** sending emails to large numbers of people asking for sensitive personal information such as bank details, PAN, Aadhaar, etc.
- **Water holing-** setting up a fake website or compromising a legitimate one in order to exploit visitors to such website.
- **Ransomware-** which could include disseminating disk encrypting exploiting malware
- **Scanning-** attacking wide swathes of internet at random

2. **Targeted Cyber Attacks.** In such attacks target is identified and attacker has specific interest in such target. For this preparation may take for months even years. It is often more damaging than untargeted attacks. It is customised or tailormade for the specific target. These attacks may include:

- **Spear-phishing.** By sending emails to targeted individuals that could contain an attachment with malicious software or a link that downloads malicious software.
- **Deploying a botnet**. To deliver a DDOS (Distributed Denial of Service) attack.
- **Subverting the supply chain-** to attack equipment/ software being delivered to the organisation/target.

Stages of a cyber-attack.

In our cyberworld, cyberattacks are taking place almost daily in every organisation weather civil or military and to thwart such attacks such attacks we have to think and act like a military mind. These attacks occur at different stages depending upon the target and aim chosen by the terrorists. The term cyber Kill-Chain originally came from military environment, which is according to Joseph Raczynski a chain of stages leading to cyberattack [12]. A cyberattack takes place at 7 stages which are enumerated as under:

- **Reconnaissance.** Initially hackers begin with searching for the profile of the target, which include names, titles, e-mail addresses, telephone/mobile numbers, etc. They identify the target/targets and then plan the attack.
- **Weaponisation.** Hackers have the libraries of codes at their disposal which they use and tweak their attacks. They consider the networks, system software and operating system used by the victim/ victims. Then hackers customise their own codes and attack the unpatched software system.
- **Deliver.** Through research the hackers know the names of CEO and various other functionaries of the organisation. Get their particulars from the google search. And then lure the boss and other employees through various phishing tactics.
- **Exploitation**. The hackers send perfectly feasible emails to CEO and other employees with attachments.
- **Installation**. Maximum chances are there that boss and other employees of the organisation will click the e-mail with link provided therein. Once clicked malicious software takes the root.
- **Command and Control**. Once the malicious code has been established, it sends the messages to remotely computer station set-up by the hackers. Then hackers get activated extract the information and data as per their need and requirement.
- **Action on the objectives**. Finally, hackers are able to establish the contact with target/targets and carry out the desired operations.

Now, many proactive institutions are attempting to ‘break’ an opponent’s ‘kill-chain’ as a defence method. One of the leaders in this area of the concept of Information Security is Lodheed Martin. He suggests the following defence mechanism:

- **Survey**- investigation and analysis of available information about the target/targets. Also, vulnerabilities are identified at this stage.
- **Delivery**- getting to the point where vulnerability could be exploited.
- **Breach**- exploitation of vulnerabilities to gain an un-authorised access.
- **Affect**- carrying out the designated activities for desired results.

After attacking, the capable attacker would exit without leaving any source of evidence or attacker may create an access for future visits. On the other hand, other attackers may encash it and publicise widely, to garner more support in term of men and material.

Methods of cyberattacks.

Today, technology is changing very fast, this world is driven by social networks, online-transactions, cloud-computing and many other automated processes. Good and bad always progress at the same rates. On the one hand this technology has facilitated smoothness in our life, at the same time it has given birth to new types of threat in our life. If you have ever studied the history of battles in this world, then you will realise that no two battles employed the same tactics. But similar strategies and tactics have been used again and again in many battles because they are time-proven to be effective. Similarly, when terrorists and criminals carry out cyberattacks, they use different strategies and tactics to re-invent the wheel. Common types of cyberattacks are mentioned under:

- **Malware**. Attackers love to use malware to gain foothold in users’ computer networks and consequently the offices they work in. This type of attack is very effective. Malware is kind of harmful software which damage the digital infrastructure. Viruses, spyware, worms, ransomware are the popular examples. Malware is installed emails in attachments. Once malware is there in the computer it can cause the havoc beyond imagination. It silently steals the data from the computer system. Blocks the way to essential components of a network. Creates networks of other malicious software.
- **Phishing**. It is process of sending the fraudulent communication that appears to be come from reliable sources. It is generally sent through emails. The goal is to steal the confidential information or install malware on the victim’ computer. Advanced Persistent Threats (APTs) and ransomware often start with phishing.
- **Man-in-the-middle-attacks.** Also known as eves dropping attacks, occur when attackers insert themselves in a two-party-transaction. Once the attackers interrupt the traffic, they can filter and steal the data. They can basically enter through two routes. One, through free public Wi Fi and two, when malicious malware is installed. An attacker can install software to process the information and data.
- **Denial of service attack.** Through this they attack the floods systems, servers or networks with traffic to exhaust the resources and bandwidth. As a result, system is unable to fulfil the legitimate requests. Attackers can also malicious software and devices to block the genuine information to the user/users. This is also known as denial of information.
- **SQL Injection Attack.** A Structure Query Language (SQL) injection occurs when an attacker inserts the malicious code into a server that uses SQL and forces the server to reveal information it would not normally. This can be done through injection of malicious code in website search box.
- **DNS Tunnelling.** It utilises the DNS protocol to communicate to non-DNS traffic port number 53. It sends the HTTP and other traffic over the protocol. There are various reasons for using DNS Tunnelling. But there are different reasons use the malicious DNS Tunnelling VPN services. They are used to disguise the outbound traffic as DNS, concealing data through internet connection.

For malicious use DNS requests are manipulated to extract information from the compromised computer system. Through this process a command and control station could be established.

- **Zero-day exploit.** Attackers do this when a compromise is established and patching work or remedial measures are initiated. They exploit the vulnerabilities during time available.
- **Cross-Site Scripting (XSS).** Under these malicious scripts are injected in otherwise benign or trusted websites. Attackers use web application to send malicious code, generally in the form of browser side script, for different end using.

Cyberattacks in India.

Cyberattacks exploit reported vulnerabilities in the system and its users. Indian telecom service providers offer the lowest data rates in the world. India has the population more than 1.3 billion, internet users would increase definitely and the vulnerabilities would also increase in future.

As per the information provided by Computer Emergency Response Team (CERT), 50,362 cases of cyberattacks were reported in the year 2016. The number increased to 53,117 in the year 2017 and rose drastically in the year 2018 with 2,08,456 cases. Till Oct 2019, the number of cases reported are 3,18, 649, which is the highest in last four year. Major incidents of cyberattacks happened in India are enumerated in succeeding paras:

“The Indian Army has faced 23 attempted cyberattacks so far, this year or 2 cyberattacks every month. The number of attempts were sustainably higher than witnessed last year.” [13]

“In 2016, it was found that cybercrooks stole thousands of files that reveal the compatibility of Indian scorpene class submarine fleet. It was around 22,400 pages.” [14]

“On May 23rd 2017, a SUKHOI 30 aircraft which was meant for air warfare crashed on Indo-China border under mysterious conditions. The wreckage of the plane was discovered three days after crash and an analysis of the crash was carried out by Indian Air Force (IAF). The internal inquiry made by IAF led to believe that flying aircraft was cyberattacked by when it was airborne.” [15]

Union Bank of India heist. Through a phishing e-mail was sent to an employee, hackers accessed the credentials to execute fund transfer, swindling Union Bank of India $ 171 million, but prompt action helped the bank to recover almost the entire amount. In June 2017Petya Ransomware, this made its impact felt across the world, including India, where container handling functions at terminal operated by the Danish firm A P Moller Maersk at Mumbai Jawaharlal Nehru Port Trust got affected.

“Kundankulam Nuclear Power Plant (KNPP) came under cyberattack in the last week of Oct, 2019. The damage was in the form of data theft, the same data can used to enhance future attacks. Even ISRO faced attacks prior to Chandrayan-2 mission.” [16].

In late Feb 2019, Pakistan based threat actor Green Havildar (a.k.a Goron Group) used to lure related to airstrikes conducted by Indian Military within, Pakistan, airspace, allegedly targeting a Jaish-e-Mohammad training camp. The lure document delivered crimson RAT payload to victims. [17]

Rise in sophisticated attacks, botnet works, attacks on critical infrastructure using evolved malware dominated the threat landscape in 2019 as reported by Subex-a internet and telecommunication analytics company based at Bengaluru, its report Dated Feb 27, 2020. The report was prepared using threat intelligence gathered from Subex global honeypot network operational in 62 cities globally. The report highlighted that malware complexity and sophistication on rising, increasing reconnaissance capabilities of hackers, increasing common attacks on Internet of Things (IOT) devices, critical infrastructure as areas require tremendous actions. Major cities which were attacked globally in 2019 are New York, New Delhi, Atlanta, London, Kyiv. Recently there have increased incidents in South Asia, in Middle East and North America.

Countering Cyberattacks in India.

As per Dr V K Saraswat, member, NITTI Aayog, the state cyberattacks and cyber security are enumerated as under:

- India ranks 3rd in forms of the highest number of internet users in the world after USA and China, the number has grown six-fold from 2012-2017 which is compounded 44% annually.
- India secures a spot amongst the top 10 spam-sending countries in the world alongside USA.
- India was ranked among top five countries to be affected by cybercrime, according to 22 October report online security firm “Symantec Corp”.

Major players in cybercrimes usually belongs to organised criminal groups, criminal societies, criminal’ organisations operational both at national and international level. Almost all countries of the world recognise the inherent criminal liabilities of the terrorist’ organisations. After terrorists’ attack on USA on Sept 11, 2001, the fight against terrorism was hardened worldwide. Terrorism is considered as a threat to humanity. Many countries amended their existing laws and some brought new legislations to weed out the terrorism from the society. India has been suffering mainly due to state-sponsored terrorism since 1947. India has been tough on terrorism and to counter cyberterrorism she brought out the amendments in Information Technology Act 2000 in the year 2008.

66F. Punishment for cyber terrorism (1) Whoever, - (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource;

or (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access;

or (iii) introducing or causing to introduce any Computer Contaminant. and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70,

or (B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly 26 relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Various agencies in India which are working in tandem with another to meet the challenges thrown by cyberterrorism.

1. **Indian-Computer Emergency Response**. It was established in 2004 and placed under the Ministry of Electronics and Information Technology. It is nodal agency to deal with cybersecurity threats like hacking, malware, spam, phishing, etc and strengthen the security related defence of India Internet Domain.
2. **National Cyber Coordination Centre.** It received an in-principle approval in 2013 and would come under National Information Board. It is an operational cybersecurity and e-surveillance agency in India. It is intended to screen communication metadata and coordinate other intelligence gathering activities of other agencies.
3. **Cyber and Information Security Division**. It forms part of Ministry of Home Affairs of India and deals with matter related to cybersecurity, cybercrime, National Information Security and Policy & Guidance, NATGRID, etc. Also acts as a nodal agency to fight against cybercrime. To prevent the misuse of cyberspace for furthering the extremists and terrorists.
4. **National Technical Research Organisation.** It was established in 2004 under National Security Adviser in Prime Minister's office, India. It also included the National Institute Of Cryptology Research and Development, which is first of its kind in Asia. It is a national intelligence agency.
5. **Defence Intelligence Agency (India).** It was established in 2002, and is responsible for providing and coordinating military intelligence for Indian Defence Forces. It also deals with technical assets of our defence forces. Generally, handles the information warfare including psychological operation, cyber-war, electronic interception, etc.
6. **National Crime Records Bureau.** It was set-up in 1986 to function as a repository of Information on crimes and criminals so as to help the investigating agencies in linking crime to the preparators. It is responsible for monitoring, coordinating and implementing the crimes and criminal tracking networks & systems.
7. **Defence Cyber Agency.** It was established in 2018 as a tri-services agency of Indian Defence Forces. It would have the capacity and capability to hack into networks, mount surveillance operations, lay honey-pot, recover deleted data from the hard disks and other hardware, break into encrypted communication channel, etc. When fully functional will definitely become a force-multiplier.
8. **Defence Space Agency.** It was established in the year 2018, entrusted with responsibility of operating and maintaining Space Warfare Assets of the country. Months before coming into being DSA conducted and Anti-Satellite Weapon (ASAT) Test in Mar 2019. Test was conducted demonstrate the India's anti-satellite capabilities. This was in response to Ballistic Missiles System of China and Pakistan. With launching of ASAT, India has become 5th country in the world to have such capability.

International Collaboration.

- The commonwealth countries have unanimously agreed to take action in the field of cybersecurity by 2020. Nations agreed to work closely to evaluate and strengthen their cybersecurity frameworks and response mechanism.

- As governments the world over deliberate over how to tackle growing nation-state cyber-attacks and protect sensitive data, a top Microsoft official said on Tuesday that collaborations between the governments, tech companies and third-party cybersecurity agencies can help address the growing menace. According to Rob Lefferts, CVP-Program Management M365 Security at Microsoft, the company takes nation-state cyber-attacks very seriously. [18]
- In the third Indo-French cyber dialogue which was held in Paris on 20 June 2019, India and France have joined hands to work closely in the areas of cybersecurity.
- India and Japan have decided to collaborate in the areas of cybersecurity and outer space as part of their growing security partnership in the Indo-Pacific region, a development that comes in the backdrop of increasing violation of social media platforms by extremists and India's successful Anti-Satellite Weapons (ASAT) test.[19]
- "It is not well known that cooperation on cyber issues constitute an important aspect of the India-UK security relationship. Opportunities to enhance cyber cooperation relating to threats, challenges, defence, crime, international law, diplomacy, governance and prosperity could ensure substantive bilateral security convergences post-Brexit. Both India and the UK share a common vision

and principles for cyberspace. These include a commitment to a free, open, peaceful and secure cyberspace; recognition of the importance of cooperation for combating cyber threats; promotion of cyber security; and a commitment to the multi-stakeholder approach to internet governance.” [20]

- India and USA have renewed their agreement to cooperate in the field of cyber security. On Wednesday, a MoU was signed between the Indian Computer Emergency Response Team (CERT- India) under the Ministry of Electronics and Information Technology and the Department of Homeland Security, Government of the United States of America. [21].
- India and Israel on Monday signed nine agreements, including in the areas of cyber security and oil and gas, following delegation-level talks headed by Prime Ministers Narendra Modi and Benjamin Netanyahu in Delhi. A memorandum of understanding (MoU) on cooperation in cyber security was signed. A second MoU was signed between the Ministry of Petroleum and Natural Gas and Israel's Ministry of Energy in oil and gas sector.[22]

Conclusion.

The topic of terrorism is both complex and emotive. It is complex because it involves many other subjects such as politics, psychology, philosophy, military strategy, history, etc. On the other hand, it is emotive because an act of terrorism (through any means) evoke sentiments/emotions from the various sections of the society. As and when such acts of terrorism are discussed evoke different feelings.

Terrorism poses a great threat to humanity. The aim of the terrorism is to create disruption and instil fear in the minds of people. Reasons for such drastic actions could be anything ranging from political motives to religious motives. History is full of evidences that some nation-states have also been involved in using physical violence against the other countries through preparators. Nation states and terrorist’ organisations who get involved in such activities, violate the laid down legal system of the established governments. Such countries and terrorist’ organisations then face the counter reactions both from within and from outside.

In the recent past many such organisations have come up in many parts of the world and posing great challenges. These terrorist’ organisations go against the grain of country pose a serious threat to security and integrity of the nations. When confronted with terrorism, the affected nation states have two options: one, they can yield to the demands of terrorists, two, face the challenges thrown by terrorists boldly and crush all such groups. Only weak nations could think of first option. On the hand, strong nations would crush such terrorist’ groups with carrot and stick policy. India is one of those countries which is facing the problem of terrorism for the last seven decades or so. Country faces the multifarious challenges in dealing with homeland security/ internal security. A stable and comprehensive ant-terrorism measures are required to be undertaken with adequate safety provisions for the public. Terrorists’ violence has to dealt with an iron hand. An effective, efficient and responsive administrative setup works as an antidote to terrorism. Outdated laws don’t help to fight terrorism so legislations should be updated regularly. No terrorism can survive without the support of local people hence along with tough laws to deal with terrorism we must formulate policy win the hearts and minds of the local people. Inclusive and sustainable developmental policies must be implemented to keep the people in the national mainstream. Violation of human rights is a big issue in fighting against terrorism so we must endeavour to safeguard the basic human rights of the people. Media should be encouraged to carry out self-regulated code of conduct to make people aware of terrorists’ violence.

Internet has grown, primarily unregulated & unstructured and it has given a new lease of life to terrorism There has been exponential growth in data transfer rates and volume. We face a new threat of cyber terror related activities not only from our adversaries only, but amateur hackers, disgruntle people within the society, unemployed youth etc. With the help of digital world terrorist’ organisations can reach to the targeted population with speed and volume of information. By using the digital infrastructure terrorists can spread their propaganda, carryout recruitment and training, lure young people to join their outfits and reach out to people for fund raising and launching pads. They collude with criminals for conception and implementation of clandestine operations which generally result in killing of people and destruction of resources. Criminal activities help these terrorists to hide their true identities and divert the attention of law enforcing agencies.

Knowledge and synchronisation of various agencies fighting cyberterrorism is very essential. But it is easier said than done, lot of efforts are required for such combined strategy. For centuries we thought that we could win the battle if we were to from the ground of tactical importance. Now that physical place has been shifted to digital space. There are many issues and intricacies involved in the studies of intelligence & terrorism, international security, cyberterrorism, internet security in India as well as world over which have been researched and discussed by the various social scientists and cybersecurity techies. Proper cyber hygiene for all organisations is essential with well-defined policies and protocols. Training to update on technology changes is another aspect which to be looked into. Cybersecurity should form part of any organisational culture. After addressing these, attention may be given to software developments to defeat the more cultured threats by invoking distracting tools such as honey traps & dummy sites for hackers, bounties to trap bugs, sandboxing to trap malware, and security holes. To tackle the cyberterrorism, we need to be proactive and to be ready and organised with a set of controls, trained personnel, and a well-established security policy, with defined legislations, rules, regulations, roles and responsibilities. Cybersecurity management policy should be based upon the principles of good Information Technology governance and be based upon recognizable standards that give assurance given to all stakeholders. There is a need of cooperation and coordination among the nations to defeat the cyberterrorism in totality.

Bibliography

1. Boaz Ganor Page-17, The Counter-Terrorism Puzzle, A Guide for Decision Makers, 2007 Transaction Publishers, New Brunswick (U.S.A) and London (U.K).

2. Source: Alex. P Schmid: http://en.wikipedia.org/wiki/Definition of Terrorism.

3. (While, Kenneth C 1998. Cyberterrorism: modern mayhem, US Army War College. Retrieved on 13 March 2015 by Wikipedia-The Free Encyclopaedia).

4. Dorothy Denning, "Cyberterrorism- Testimony before Special Oversight Panel on terrorism, Committee on Armed Services, US House of Representatives." Washington DC. US House of Representatives, May 23, 2000, available on www.stealth-iss.com/documents/pdf/cyberterrorism.pdf.

5. (Centre for Excellence, Defence Against Terrorism, ed. (2008) Responses to Cyber Terrorism, NATO science for peace and security series, Sub series E: human and societal dynamics, ISSN 1874-6276.34, Amsterdam: I O S press page 119).

6. Bruce Hoffman Inside Terrorism-New York: Columbia University Press, 2006, page no.40.

7. (G. Giacomello, "Bangs for the Buck: A cost Benefit Analysis of Cyberterrorism", studies in Conflict and Terrorism, vol27, 2004 page 387-408).

8. (Flemming, Peter, Michel Stohi, " Myths and realities of Cyberterrorism" Available at http://www.comn.ucsb.edu/Research/Myths/Realities/Cyberterrorism.pdf as reflected in para 2.5.1.6.4 8th Report, Second Administrative Reform Commission, Combating Terrorism, Protecting by Righteousness, June 2008).

9. [P.Brunts, " Terrorism and Internet: New threats posed by cyberterrorism and terrorist using internet, " M. Wadea and A.Malijevic, eds, A war on Terror: The European Stance on a New Threat, Changing Laws and Human Rights Implications, New York: Springer 2010].

10. Data Security Council of India (D S C I), Promoting Data Protection.

11. Orman, L. 2013 "Technology at Risk", IEEE Technology and Society magazine, 23-31.

12. Killer Chain: The 7 stages of cyberattack, October 12, 2018, Thomson Reuters.

13. Amrita Nayak Dutta, The Print, India 25 Nov, 2019.

14. Economic Times CIO.com, 09 Dec, 2019.

15. Naveen Gaud, Cybersecurity Insiders, May 23, 2017.

16. Analytics India Magazine, Dec19, 2019.

17. Cyber Threats 2019: A year in Retrospective. Cyber threat operations Feb 2020 by PWC.

18. Outlook, India dt Jan 28, 2020.

19. The Economic Times, India dt July 02, 2019.

20. Rahul Roy Choudhary, Senior Fellow, South Asia, IISS dt Nov 22, 2019.

21. The Economic Times, Delhi, Jul 12, 2018.

22. The First Post, India, Jan 15, 2018.