A Comprehensive Review of Cyber Terrorism in the Current Scenario

Prashant Vats,
Research Scholar,
prashantvats12345@gmail.com

Abstract: *In this research paper we have discussed about the phenomenon of Cyber terrorism and its growing impact in the current scenario. We have reviewed the laws and acts in various countries like US, UK, Canada, Australia and in India. We have also tried to review the Cyber terrorism from the aspect of the Indian IT Act 2000. We have carried out a comparative review of the various laws made by these individual countries to deal with the Cyber Terrorism. In the end we have concluded that The existing laws in various countries are not efficient to restrain the cyber crimes and, thus urging a need for implementing modifications through which these activities can be prevented. There is a need of international cooperation of nations to crack down the efficiency on the cyber crime.*

Keywords: Cyber Terrorism, Internet, Denial of Service (DOS), Electronic Surveillance,

1. INTRODUCTION

Today, with the increase in use of the Information and Communication Technologies (ICTs) and the on growing trend towards the digitization of the Information resources has resulted in using the advanced computational techniques like Distributed and Cloud Computing for the storage and retrieval of data on the public and private infrastructures. The availability and advancements of ICT's has provided a base for development in the creation, availability and use of network-based services. The ICT applications, like as e-governance, e-commerce, e-education, are seen as enablers for development, as they act as an effective channel provider to deliver a wide range of basic services in the remote and rural areas of our nation. The use of ICT applications can facilitate the achievements of one nation's development targets, reducing poverty and improving health and living conditions in the various developing countries across the globe. Given the right approach, in right context and implementation processes, the investments in the ICT applications and tools have resulted in the increasing productivity and quality improvements of the common man.

But, at the same time, the growth of the information society is accompanied by the upcoming new and serious threats as well. The increasing attacks against the public informational infrastructure and the use of the growing effective internet services has resulted in serious increased potential to harm the Human society in many various new and critical ways. The International Terrorist Groups like AL Qaeda or ISIS has already started using such kind of cyber attacks against the existing informational infrastructure and Internet services in various developing nations across the globe. The use of online fraud and hacking attacks merely are examples of computer-related crimes that are committed by these international hacking groups on a very large scale increasing day by day. The financial damage caused by these cybercrime is has been reported to be enormous.

The Cyber terrorism can be defined as using the global Worldwide Internet Services for the motives and agenda propagating the inhumane motives and agenda of the various terrorist organizations and their illegal activities [1], which includes the use of acts like deliberately causing the large-scale disruption of the public computer networks, especially of the personal computers of the citizens of a particular nation which are connected to the Internet, by the means of tools like as computer viruses. The Cyber terrorism can also be defined as the intentional use of computer, computer networks, and Public Internet Infrastructure to cause the public destruction and harm to the personal objectives of a Nation. The objectives behind the propagation of these kinds of terrorist activities through the use of Information Infrastructure and interconnected communication channel like World Wide Web (WWW) may be a result of the ideological or political belief, and depending upon the form of terrorism and motive of a terrorist organization. There are much concerns given by the governments of various nations and United Nations about the potential damages that can be caused by the cyber terrorism, and It has prompted in the generation of official responses from the local government agencies in various nations like Federal Bureau of Investigation (FBI) in the United States and in countries like India as well in the form of the National Investigation Agency (NIA) [2].

The use of information technology by the terrorist groups and individuals to further their agenda, can include use of information technology to organize and execute attacks against the Government networks, their existing computer systems and the telecommunications infrastructures, or for exchanging the information or by making terroristic threats via use of electronic communication like WWW. The international terrorist organizations nowadays no longer use the local electronic media to dilute their messages and spread their propaganda. Nowadays they insists on the disseminate information of their choice which aids to their causes. This is usually accomplished by publication of various articles combined with pictures galleries on the social networking sites like a Face book, or using social android based apps like Whatsapp etc., this further is supplemented by adding video and audio files in which these terrorists themselves tries to orally defend their actions by brutally killing innocent peoples. The terrorist organization spreads their messages on these sites by using symbols and imaginary of the victimization and empowerment. This all in result raises the emotions of future supporters.

The first type of cyber terrorism was created by the Al-Qaeda group which has established the Al-Qaeda Center for Islamic Study and Research [3], which was created by the former bodyguard of the Bin Laden, Shekh Yussuf -Al-Ayyiri. They have created a video on the internet which was based on the Al-Qaeda's propaganda and had several audio messages from the Al-Ayyiri [3], insisting on the use of cyber terrorism acts by trying to recruit more individuals for their cause, and giving instruction for the future terrorists to increase their potential on the use of cyber attacks against the developed nations.

The cyber terrorists use certain tools or methods and posses efficient computer programming skills for exploiting the government and personal computer networks and infrastructure to cause this new age terrorism. These are:

(a) Hacking. This the most popular and common methods used by the terrorists to hack into the Government official sites. Some technologies like packet sniffing, tempest attack, cracking of secure firewalls and highly encrypted passwords and buffer outflow, all these facilitates hacking.

(b) Trojans. It contains of self initiated computer programs written in any computer programming language, which pretends that they are doing the one meant thing but while actually they are meant for doing something different, like the use of wooden Trojan horse in the 10th Century BC by the Greeks.

(c) Computer Viruses. It is a self initiated computer program, which infects the other computer programs by modifying their code structures.

978-1-4673-9080-4/16/$31.00 ©2016 IEEE

(d) Computer Worms. These are self contained computer programs or a set of programs which is able to spread the functional copies of it replicating itself or its segments to other computer systems usually via use of computer network connections to the other computers.
(e) Crimes related to the Hacking of Emails or Online Identity Theft (ID Theft) – In this case usually threats like worms and viruses attach themselves to any host program to be injected as a suspicious code to infect any given computer system connected over the Internet. Certain e-mails are also used as host by viruses and worms for spreading the disinformation by the anonymous terrorist organization, or posing electronic threats and spreading their defamatory stuff.
(f) Denial of Service (DOS) attacks. This kind of cyber attacks are aimed at denying authorized person's or government officials to access to the computer attached to governmental hosted computer networks.
(g) Cryptology. The international terrorist groups have started to use the encryption methodology for encrypting their voice or data links etc at higher frequencies.
The most concerning threat in the cyber terrorism against the Public Key Infrastructural support (PKI) is the use of computer viruses and worms. The attacks or methods on these governmental PKI's can be classified into three broad categories.
(a) Physical Attack. In this the PKI is damaged by using conventional methods like bombs, fire etc.
(b) Syntactic Attack. The PKI is damaged by performing modifications into the logics of the given governmental system by using malicious software codes by introducing delay or making the system in an unpredictable state. It includes malicious computer viruses and Trojans.
(c) Semantic Attack. These kinds of cyber attacks exploit the confidence of the user in the system. In this case the security is breached by entering malicious software codes during entering and exiting the system at the connecting gateways in governmental network like routers of firewalls and the contents of the given computer system are modified without inducing errors, without the users' knowledge.

2. CHALLENGES ENCOUNTERED IN DEALING WITH CYBER TERRORISM

The word cyber terrorism includes the use of warfare attacks against the sovereignty of a nation's state and forcing the use ICT's against the public and private PKI's and their assets in order to create panic and destroy them. Based on the nature of the globalization of the terrorism, challenges that the local authorities of a nation may face in dealing with cyber terrorism are as follows:
(a) A clear definition of activities related to Cyber Terrorism is very necessary in defining the cyber terrorist activities [4]. It is important to differentiate between the action and motive of these activities. In most cases, the motive involved in the increasing cyber attacks is more of computer-related crimes which may include cases like as Theft of Identity (TOI) and the illegal hacking into the bank's system to gain money for funding their motives.
(b) The advanced technical impediments may be used by the terrorist groups by using ICT in conducting their illegal modes of operation conduct operations without being detected by the local investigation and monitoring authorities like Electronic surveillance. They may utilize the advance network security features of the Internet technology that may enable them to remain anonymous and hidden over the internet. Therefore, it is hard for the local investigating authorities to trace or detect such kind of suspicious activity over the internet or detection of any suspicious link and collection of any related information that may assist in identifying these criminal offenders.
(c) The Legislative is the most prominent against aspect against all the odds posed by the increase in the cyber terrorism across the various nations. It's a fact that some the existing legislation in many countries deals with computer-related crimes, but most of the legislation are conventional laws and may not be adequate to address issues that are related to the use of the Internet for the terrorist activities. These conventional laws do not include the ICT and are confined to the physical boundaries of their countries. In many circumstances, the enforcement of these conventional laws and prosecution of the Cyber offenders poses a serious challenge, especially in case of the investigations which are related to offence of cyber crimes made by cross border terrorist organizations.

3. LAWS RELATED TO CYBER TERRORISM IN VARIOUS COUNTRIES

In this part, we have discussed laws related to encounter the Cyber terrorism in various countries.

3.1 Laws related to Cyber terrorism in United States [5].

3.1.1 The Computer Fraud and Abuse Act (CFAA) [5], 18 U.S.C. 1030, outlaws conduct that exploits the governmental or personal computer systems. It is a cyber security law. It protects federal computers, computers that are installed in the banking organizations, and the personal computers which are connected to the internet. It provides a protective shield for them from the cyber attacks like trespassing, threats, damage, espionage of the computer systems, and from being used as an instruments of fraud in a corruptive manner. The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030,1 protects the computers systems in which there is a federal interest or the federal computers, banking computers, and the computers which are used in or affecting the interstate and the foreign commerce. The provision made in the paragraph (a) (3) of the CFAA makes it unlawful for anyone to intentionally misuse a federal or any personal computer which is of the federal importance without authorization of the notifying federal agency. If such attempts are performed than he shall be punished as provided in subsection (c) of the said paragraph.
As per this para, whom so ever attempts to commit such offense under the subsection (a) of this section shall be punished with up to maximum life imprisonment.

3.1.2. The USA PATRIOT ACT [6] The USA PATRIOT Act [8] was implemented by the US Government as a counter response to the cruel events attacks on the Twin towers of the World Trade Centre(WTC) in the New York City that took place on the black day of the September s11th, 2001. The full abbreviation for the Act stands for "Uniting and Strengthening America by Providing Appropriate Tools Required for Intercepting and Obstruct Terrorism Act of 2001". This Act was passed by the Federal American Congress Govt. on the date of the 26th October in 2001after the 9/11 incident took place in the US. This Act addresses various issues that were related to the terrorism and the terrorist activities, but it was having very few provisions that were addressing the issues related to cyber terrorism like cyber threats and other cyber security concerns. In this Act, provisions has been made to ease out the restrictions made by the federal laws the on electronic surveillance of the mobile and the computer resources which can facilitate the capturing of the terrorists. The USA PATRIOT Act enables such computer surveillance allowing the federal authorities to intercept the communications made be computer system trespasser. This Act also contains legal provisions for preventing the anti-money laundering activities made by the terrorist groups in order to gain financial benefits for funding from their actions. Previously the Title III of the U.S. Law Code was lacking to include the terrorism and computer related cyber crimes from the predicate offense lists, but now the USA PATRIOT Act includes such cyber crimes as serious offences and is included under punishable offenses.
The Title I of this Act is enhancing domestic security against terrorism. It authorizes the federal agencies to take preventive measures for enhancing the capability of the domestic security

services for preventing terrorism. This title establishes a funding mechanism for the counter-terrorist activities and for the Terrorist Screening Center which is administered and monitored by the FBI. The American military is authorized to provide assistance in some situations that may involve detection of the weapons of mass destruction when so requested by the Attorney General of USA.

The Title II of this Act is meant for the Surveillance procedures and is called the "Enhanced Surveillance Procedures". It includes all the technical aspects of the surveillance of the suspected terrorists like Online Internet Network traffic monitoring, Mobile phone tapping procedures etc. It helps in detection of the suspects who are engaging themselves in some kind of computer frauds or computer abuse, and the agents of anonymous foreign power who are engaged in such destructing activities. In particular, this title allows the federal agencies to gather the foreign intelligence information from both, the U.S. and the non-U.S. citizens.

The Title VIII of this Act includes a Terrorism criminal law which alters the definitions of the cyber terrorism and defines the rules to deal with the Domestic and International terrorists who tries to damage or gain unauthorized access to a protected federal computer and then tries to commit a number of cyber criminal offenses. It also includes the actions that may cause a personal to be got injured or any kind of a public threat to the public health or safety. It also includes the attempts to gain the access of the federal computers, for using them as a tool to administer the local justice, the U.S. A. national defense and the U.S. national security. The penalty which is imposed under this law for attempts made by terrorist groups to damage protected federal computers through the use of malicious computer virus programs or other malicious software mechanism, is set to provide a punishment of imprisonment for up to 10 years, while the penalty for the unauthorized access and subsequent damage to a protected federal computer has been increased to more than five years imprisonment. This act also specifies the development and support of cyber security forensic capabilities by US national government.

3.1.3. The Cyber Security Research and Development Act (CSRDA) [7]

The CSRDA has allowed the American Congress to provide funds for over a period of five years for research and development in the area of computer security. The National Science Foundation and the National Institute of Standards and Technology will coordinate the use of the funds. Along with earmarking funds for research, the Act also encourages grants to higher education institutions for programs that would increase the number of students interested in studying computer and network security. One of the controversial aspects of the Act is that it prevents certain foreign individuals from receiving grants if they were found to be connected with any terrorist funding state.

3.2 Laws Related to Cyber terrorism in Australia:

According to the Federal Laws of Australia they have defined terrorism into the section 100.1 of their Federal Criminal Code Act 1995 (‘Australian Criminal Code’) made as per by the Security Legislation Amendment (Terrorism) Act 2002 (Cth) (‘SLAT Act’) [8]. The SLAT Act is their main legislation package of five government bills which was formed after the events of September, 2011 attacks occurred in the USA. As amended by the SLAT Act, the Australian Criminal Code provides a maximum penalty of life imprisonment for the ‘terrorist acts’ committed in any jurisdiction.

As per SLAT Act the Terrorist act is defined as an action or threat of action where an action is performed or a threat is made with the intention of posing a threat to sovereignty of the government of the Commonwealth or a State, Territory of the Australian government, Foreign country, or of part of a State. The public Subsection (2) of this Act lists the possible harm requirements specifically related to the cyber terrorism that prohibits the acts of terrorism against the Federal electronic systems. It includes interference and disrupting, or destroying, an electronic information system or a governmental financial system. The Sec.100.1 (2) (f) of this Act covers the politically motivated Denial-of-service attacks against the federal websites and email systems under the label of cyber-terrorism. This law has a maximum penalty of life imprisonment for cyber-attacks against the federal infrastructure in Australia or any foreign country.

3.3 Laws related to Cyber Terrorism in United Kingdom (UK)

3.3.1 Terrorism Act 2000[9].

The UK’s interpretation of Cyber Terrorism includes the use or threats of suspicious actions which are intended to influence the government of UK or to the public of a country other than the UK which is a Part of the UK or of a country other than the United Kingdom by a means of politically motivated cyber-attacks directed against its governmental bodies of importance like the NATO headquarters, the World Bank Organization etc. The Sec. 1(2)(e) of this Act deals with intended cyber attacks which are meant to seriously interfere with or to disrupt an electronic system. It includes the possible threats to their internet facilities, their governmental financial exchanges, their federal computer systems or the governmental controls of their national power The government of the United Kingdom govt. has announced their National Security Strategy [9] into which they have stated that the potential cyber-attacks by a state and non-state actors as Tier-1whchi is among out of one on four, ‘highest priority risks’ to their national security. The Sub.Sec. (2) (e) of this Act does not only criminalize the cyber-attacks that were meant to destroy the federal electronic systems but it also extends to cyber criminals who are really intended to seriously interfere with their federal electronic systems.

As per the laws in both the countries i.e., the Australia and the UK they have a drawback that they need to satisfy the other requirements to qualify as the terrorist acts like whether the offences were politically motivated and intended to impact on a government or they just meant to intimidate a civilian population. In both the countries if a cyber-attack in either jurisdiction has not caused any major impact to interfere with their federal or civilian population, wouldn’t qualify as an act of cyber terrorism.

3.4 Laws related to Cyber Terrorism in Canada

In the Canada the definition of the cyber terrorism is contained defined by the Anti-Terrorism Act 2001 (‘ATA’) [10]. It defines the cyber terrorism as an act of causing interference with the disruption of essential service by using the Internet facilities or a computer system, to result in the conduct of harm to the federal government of Canada and its citizens. As per the ATA, 2011 it provides a maximum penalty of life imprisonment for anyone who commits an indictable offence for a group that is engaged in terrorist activities by means of the cyber warfare against Canada or its favoring countries.

The Canadian Law is extending to politically motivated cyber-attacks against the Internet services and Computer based Defense facilities, and not merely ‘systems’. The Canadian definition of Cyber terrorism provides a higher standard than its Australian and UK counterparts, but efforts are needed for the possible scope of applying cyber terrorism to the cyber- attacks made against private business infrastructure, including acts of political protest like hacking of personal computer systems in Canada.

4. LAWS IN INDIA FOR CYBER TERRORISM

The Indian government has taken a number of counter measures to prevent the use of cyberspace for the terrorist-related activities, especially in the after facing the use of internet facilities in the terrorist attack that were made in Mumbai in November 2011. The Indian Parliament has passed amendments to its IT Act, with addition on emphasizing on the cyber terrorism and cyber crime, in to the existing sections the IT Act and by addition of new sections, against these cyber threats. Further actions have been taken to include the passing of rules like as the Information Technology

(Guidelines for Cyber Cafe) Rules, 2011 under the IT Act. In doing so, the government has had made a fine line to differentiate between the fundamental rights to privacy under the Indian Constitution and national security requirements.

4.1. **The Indian IT Act 2000[11].**

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

It has various sections that deal with the activities that will constitute Cyber terrorism."[11]

The Sec. 66 of the IT Act deals with the unauthorized hacking with a computer system. In this section who ever performs an unauthorized access willingly that is intended to cause a loss or damage to the public or any person who commits hacking with the intention to temper or harm the information content of a governmental or a personal data, is punishable with an imprisonment up to 3 years in Jail, or with imposing a fine of which may extend up to 2 Lakhs Indian Rupees (INR), or with both.

Further as per amendments made by the Indian government in the later on stages various provisions has been added in the Indian IT Act 2000 to deal with the increasing cyber threats.

The Sec. 66 C. deals with the punishment imposed for the Identity theft with an amendment made in 2008. As per this section who ever fraudulently attempts to use the electronic signature or a other unique identification feature of any other person, is punishable with an imprisonment of either for a term which may extend up to 3 years and by imposing a fine which may be extend up to 1 Lakhs in INR.

The Sec. 66D. deals with cheating a person by using the computer resource or by using computer resource like sending fish mail, is punishable under IT Act, with a term of imprisonment which may be extend up to 3 years and liable to pay a fine which may be extend up to 1 Lakhs in INR.

The Sec. 66 F. of the Indian IT Act specifically deals with the Cyber terrorism. In its subsection 66 F(A) , it defines that whom so ever who is intended to hamper and wants to pose a threat on the unity, security and the sovereignty of India or attempts to strike terror in its citizen by means of using cyber threats like Denial of Service (DOS) to any authorized person to access governmental computer resource; or attempts to breach the security of a governmental computer resource without the authorization of the concerned agencies; or causes to introduce any malicious code into the governmental computer systems, and by using such attempts, is likely to cause or causes death or injuries to its citizens or trying damage to destruction of property ; or disrupts or causing disruption of supplies or services essential to the life of the community or adversely impacts on the Critical Information Infrastructure (CII) specified under the Sec. 70. of the IT Act is termed to include in the act of Cyber Terrorism activities

The Sec. 66 F defines that any person who willingly penetrates or accesses into a computer resource without the authorization of the concerned agencies, and by means of such acts tries to obtains access to information which is restricted for the reasons of the security of the Indian State or its foreign allies; to use such information to cause or likely to cause injury to the sovereignty and the security of India and tries to hamper its friendly relations with the foreign States. Such attempts made by any foreign nation or certain groups of individuals, are come under the offences of the cyber terrorism. As per Sec. 66 F, who so ever commits such kind of cyber terrorism is liable for a punishment which may be extend to the imprisonment for his entire life.

Under Sec. 69., special provisions have been made for issuing directions by the Central Govt. to the National Investigation Agency (NIA) for intercepting or monitoring or decryption of any information through any computer resource. The Sub. Sec. 69 A. empowers the central agencies to issue directions for blocking any content or information onto the websites on the internet, which may cause or are intended to cause threat to the internal security of the nation. The Sub. Sec. 69 B authorizes the Govt. Agencies for the centralized monitoring or collection of information from any computer resource which may pose harm to the cyber security and the sovereignty of the nation. As per the Sub. Sec. 69 (f) of this Act, if any person who refuses to assist the investigating agency, is liable for a punishment with an imprisonment for a term which may be extend to 7 years and shall also be liable to imposing a fine.

The Sec. 70 of the IT act clearly defines that any computer information system that is of nation's importance and is essential for supporting the facility of CII, as to be a protected system. Such information systems may have the impact on the public security and safety of the Nation. Any person who attempts to hamper such protected systems is liable for with an imprisonment for a term which may be extended up to 10 years and shall also be liable to fine. The Sec. 70A of the IT act deals with the appointment of a National Nodal Agency (NNA) by the Indian Central Govt. for the protection of the CII. The NNA would be the responsible agency for all the research and development needed for the protection of the CII. The Sec. 70B notifies for the appointment of Indian Computer Emergency Response Team (CERT) by the Indian Central Govt. for serving as a national agency for the incident response in case of a cyber security breach. The Indian CERT team is responsible for the analysis and collection of information on cyber incidents. It forecasts and alerts the concerned facilities for the cyber security incidents by time to time. It performs emergency counter measures for handling the cyber security incidents performed against the Indian state.

5. A TABULAR COMPARISON BETWEEN LAWS RELATED TO DEAL WITH CYBER TERRORISM.

In this portion, we have carried out a tabular comparison between the laws to deal with cyber terrorism in various countries and are presented in Table.1.

6. CONCLUSIONS

From the above study we conclude that as we are growing more dependent on the Internet for our daily life activities, we are also becoming more vulnerable to any disruptions caused in and through cyberspace. The cyberspace is becoming an important area for large number of terrorists to attack on crucial information infrastructure. The existing laws are inefficient to restrain the cyber crimes and There is a need of international cooperation of nations to crack down the efficiency on cyber crime, thereby ensuring a development of the internet cybercrime is not limited to states of boundaries, thus it requires a universal collaboration of nations to work together to reduce the ever growing threats and risk to a manageable level.

REFERENCES:

[1] Pub. In "Tcp_ip-protocol-suite"-4th-ed-b-forouzan-mcgraw-hill-2010-bbs

[2] Pub. In proceedings of "cyber terrorism-threats" , pp. 4–5, 2011.

[3] Alex P. Schmidt, "Al-Qaeda's "Single Narrative" and Attempts to Develop Counter Narratives: The State of Knowledge", pub. in ICCT Research Paper, Netherlands, January 2014.

[4] Pub. in "Common Cyber Attacks: Reducing The Impact" by GCHQ and Cert-UK, 2015.

[5] Pub. in "Computer Fraud and Abuse Act" in Fraud and Related Activity in Connection with Computers Title 18 Sec. 1030.US Code, 1999.

[6] Pub. in "The USA Patriot Act: Preserving Life and Liberty" pub. by Department of Justice, Federal Govt. of United States.
[7] Pub. in "Federal Cybersecurity Research and Development Strategic Plan" by the National Science and Technology Council, US Govt., 2016.
[8] Pub. in "Australia's Cyber Security Strategy" by Govt. of Commonwealth of Australia, 2016.
[9] Pub. in "Terrorism Act 2000" in Legislation passed by the UK Govt., 2000.
[10] Pub. in "Canada's Anti-terrorism Act: an unjustified limitation of freedom of information and privacy rights" by The House of Commons Subcommittee on Public Safety and National Security, Canadian Govt., 2005.
[11] IT Act Notified with Gazette of Govt. of India, 2000.

Table 1.1 A Tabular Comparison Between the Laws related to Cyber Terrorism into Various Countries.

Sr. No:	Country	USA	UK	CANADA	Australia	India.
1.	Laws Implemented	The Computer Fraud and Abuse Act (CFAA). The USA PATRIOT ACT . The Cyber Security -Research and Development Act (CSRDA).	Terrorism Act 2000[9].	Anti-Terrorism Act 2001 ('ATA') [10].	Federal Criminal Code Act 1995. The Security Legislation Amendment (Terrorism) Act 2002 ('SLAT Act').	IT ACT 2000
2.	Judicial Implications Area	Within the Jurisdiction Range of USA	Inside & Outside UK, NATO as well.	Inside or outside Canada	Within the Jurisdiction Range of Australia	Within the Jurisdiction Range of India
4.	Threats Covered	CFAA shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud USA PATRIOT Act enables such computer surveillance allowing authorities from intercepting communications to and from a computer system trespasser. CSRDA provides funds for research and development in the area of computer security.	cyber-attacks that destroy electronic systems, interfere with national power and water supplies, cause major economic harm, physically injure civilians, or create a national public emergency	politically motivated cyber-attacks against 'services' and 'facilities'	politically motivated denial-of-service attacks	
5.	Penalties	The penalty for attempting to damage protected computers through the use of viruses or other software mechanism was set to imprisonment for up to 10 years, while the penalty for unauthorized access and subsequent damage to a protected computer was increased to more than five years imprisonment	Not Addressed	The Canadian legislation provides a maximum penalty of life imprisonment for anyone who commits an indictable offence for the benefit of, at the direction of, or in association with a group that engages in terrorist activity.	a maximum penalty of life imprisonment to cyber attacks against nonessential infrastructure in Australia or any foreign country.	Cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.
6.	National Security Policy	Yet to be needed.	Clearly Announced	Yet to be needed.	Yet to be needed.	Yet to be needed.
7.	Provisions of Monitoring & Electronic Surveillance	Yes	Yes	Yes	Yes	Yes
8.	National Nodal Agency.	Federal Beuro of Investigation (FBI), Central Investigation Agency (CIA)	Not Addressed	Not Addressed	Not Addressed	National Investigation Agency (NIA). CERT (Computer Emergency Response Team.
9.	Implementation of Computer Emergency Response Team.	YES	YES	YES	YES	YES