ATTACK WITHOUT BULLETS

11-01-2023

The notion that a terrorist is a person with a gun is changing with the advancement of technology.[1]

Cyber Terrorism as a word was coined in the late 1980s by Banny C. Collin of the Institute for Security and Intelligence (ISI), and the term was used most during the 9/11 attack. Thereafter, the world has faced many instances of cyber terrorism in the past. In India, misuse of technology has been observed in many cases and particularly in the Mumbai terror attacks of 26/11.

Thereafter, the government took some strong steps and the Information Technology (Amendment) Act, 2008 was introduced to include the definition of cyber terrorism under section 66F. A unique team (CERT) was also created under section 70 B and The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 were enacted.

Recently, there was a cyber-attack on AIIMS Hospital on November 23, rendering its systems inaccessible. Various day to day activities were paused because of the cyberattack and the FIR was registered by Delhi Police under Section 66 and 66-F of the Information Technology Act, 2000 ("Act"). Similarly, over the course of 24 hours, the website of Indian Council of Medical Research website was allegedly subject to 6,000 hacking attempts on November 30, 2022[2].

[1] This article reflects the general work of the authors and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice.

CYBER TERRORISM:

Cyber Terrorism is generally understood to mean misuse of internet to violate or threaten any person or organization to collect their data, information stored in the system to achieve certain unfair gains through this process.

Section 66F (1) (A) of the Act has included a broad definition to state that certain acts may come within the purview of cyber terrorism if:

a) Such acts are committed by any person with an intent to create threat to the unity, integrity, sovereignty and security of the nation or create terror in minds of people;

b) Such acts are committed by:

- denying or causing the denial of access to any person who is authorized to access computer resource; or
- attempting to penetrate a computer resource without authorisation or exceeding authorized access; or
- introducing or causing to introduce any Computer Contaminant.

AND such act causes or is likely to cause death or injuries to persons or damage to or destruction of property.

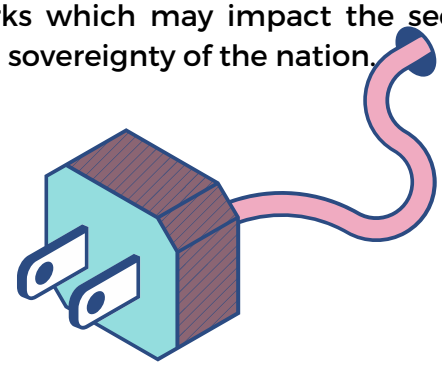
Section 66F (B) states that the offence of cyber terrorism is also committed:

- if a person knowingly or intentionally;

·penetrates or accesses a computer resource without authorization or exceeding authorized access,

- and by means of such conduct
- **obtains access to restricted information, data or computer database** and he/she has reason to believe that such restricted information is critical and may be used to cause injury to the sovereignty and integrity or may be misused by any foreign nation or group of individuals.

The main objective of Cyber Terrorism is to invade the critical networks or block access to such networks which may impact the security, integrity and sovereignty of the nation.



JUDGEMENTS:

To understand the concept of cyber terrorism better, let's look at the recent case law that came before the Kerala High Court- **Sumit Kumar Singh and Ors. Vs. Union of India[3]**. This case pertains to a theft of certain equipment like CPU/ SSDs/ processors at M/s. Cochin Shipyard Limited of the Indian Navy. The accused were appointed as contract workers to paint the I.A.C (Indigeneous Aircraft carrier).

One of the accused was self-trained in handling the computer hardware and together with second accused committed a theft of six components from the warships on different dates. Then the stolen equipment was formatted to delete the data and the same was put up for sale on OLX.

Considering the loss of valuable data and sensitive information that was lost, accused were sued under section 66F(1) (B) for cyber terrorism along with other offences under IPC and the Act.

The advocates for the accused claimed that there was no mens reus and it should be treated as a theft and not cyber terrorism and pleaded for discharge. The discharge application was dismissed, and the dismissal was upheld by the Appellate Court citing that the accused had undergone some training on safety and had an idea about the sensitive nature of the project. Considering the data about warships, the accused had every reason to believe that this information or data contained in the stolen components can be used in or can damage the sovereignty, integrity, security of India. The matter was remanded back to the Special Judge by the High Court for further investigations.

[3] In the High Court of Kerala (CRL .No. 865 of 2021)

Recently, newspapers reported that Anees Ahmad Ansari was convicted of cyber terrorism as he was conspiring to kill foreigners in an international school in Mumbai and was awarded life imprisonment by the sessions court at Mumbai.[4] It is reported that the accused had wrongly used his company's laptop to generate fake social media accounts with fake names and downloaded objectionable material from 2011 to 2014. It was found that he supported activities of terrorist organisation IS and with the help of one Omar Elhajj he was conspiring to attack foreign nationals in Mumbai at an international school in Bandra Kurla Complex. He was arrested in March 2018 for sending offensive messages on ideologies of IS to Omar with an intent to threaten the unity, sovereignty and security of India.

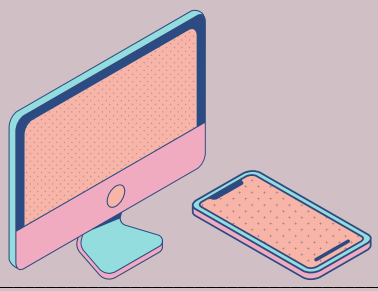
Another instance of usage of this section was under the judgement of **K. Divya Vs. The Bar Council of Tamil Nadu and Pondicherry and Ors[5]** when the Petitioner, a social activist was sued as she was part of the documentary on manual scavenging. The petitioner had recorded a documentary and published the same on YouTube for creating the awareness to abolish the manual scavenging. One of the respondents filed a complaint stating that the documentary published on You tube shows that this scavenging activities are done by a particular community and was thus defamatory and an attempt to create a conflict between the communities which ultimately disturbs the public tranquility. The FIR was filed by the police against the petitioner under section 153(A) & 505(1)(b) of IPC read with Section 66F of the Act.

After considering the submission of each party, the Court directed that section 66F deals with Cyber terrorism and in order to commit cyber terrorism, it must be that this particular action is done with an intention to threaten the integrity, sovereignty and security of India. The Court allowed the petition and observed that the complaint filed by the respondent does not in any way attract the provisions of Section 66F of the Act and the said FIR was quashed.

As per the report published the total cases of cyber terrorism of which trials are completed and disposed of is 6. The total cases pending for the trial at the end of the year is 30 and the pendency percentage of the case of cyber terrorism is 83.3 %[6].

PUNISHMENT:

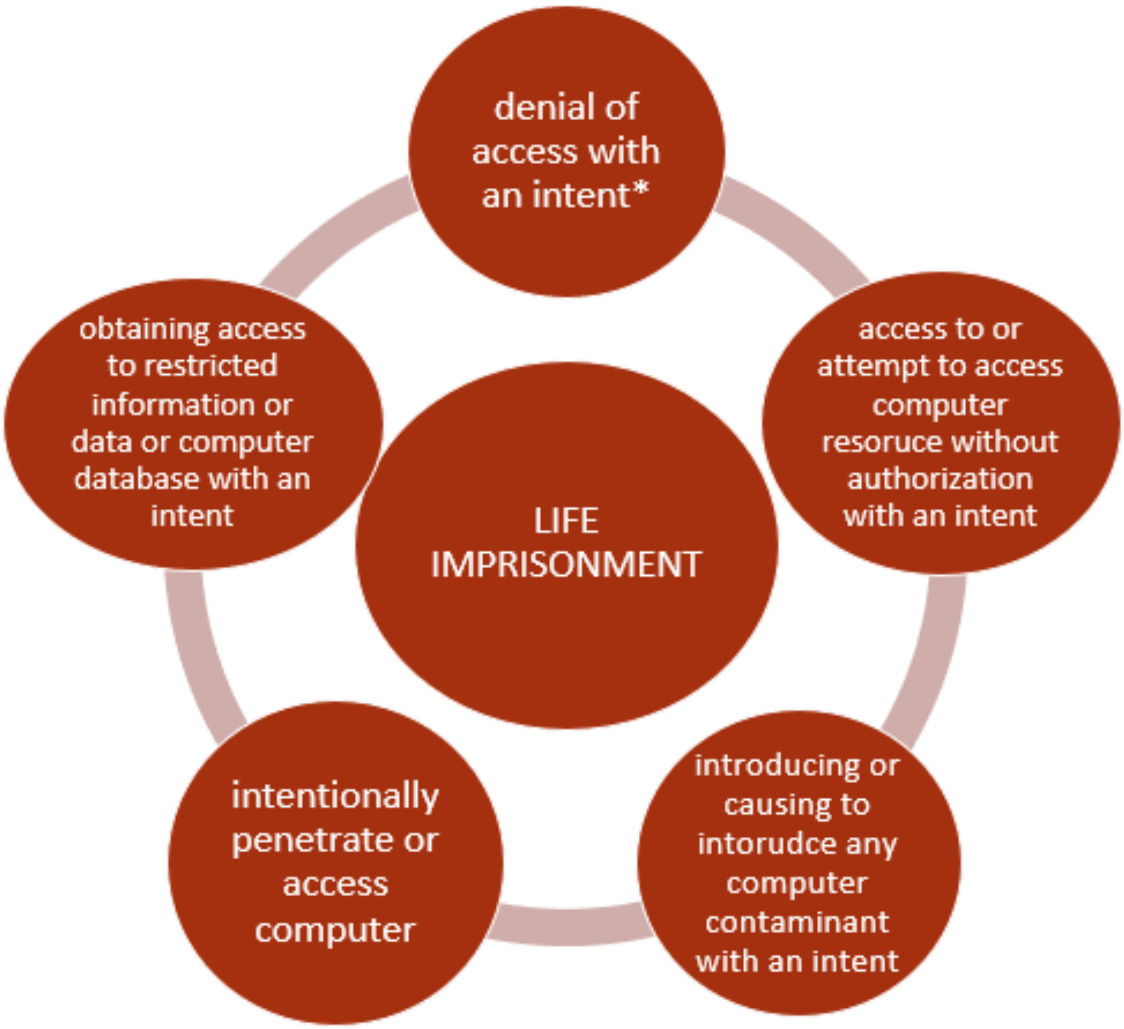
Cyber terrorism is punishable with life imprisonment under the Act considering the gravity of the offence. For other offences, the penalties range from imprisonment of a few years varying from 3 to 5 years as the offences pertain to misuse of any software, any computer resources, data related to any industry, etc. tampering, unauthorized access to the computer resources, any data or information or source code under the Act.



[4]https://www.thehindu.com/news/cities/mumbai/mumbai-court-awards-life-imprisonment-to-computer-engineer-in-cyber-terrorism/article66044201.ece

[5] IN THE HIGH COURT OF MADRAS (MADURAI BENCH) CRL.O.P(MD) No. 10701 of 2017 and W.P. (MD) No. 12774 of 2018 Decided On: 26.06.2018

[6] CII_2021Volume 2.pdf (ncrb.gov.in)



*MEANS AN INTENT TO CREATE THREAT

REPORTING CYBER TERRORISM

Reporting cyber terrorism is very important and to ease the mechanism, the victim of any cyber terrorism can report such actions or file a complaint online on National Cyber Crime Reporting Portal ("NCCRP").[1]

- A person can file all types of complaints related to mobile crime, online social media, any financial attacks, hacking and viruses. The portal is especially concerned with complaints related to cybercrimes or offences against women or children.
- Further for cases related to crimes committed against women and children, the victims can file their complaints anonymously.
- The complaints which victim/ complainants have filed are dealt by the law enforcement agencies.
- The victims can track their complaint by providing acknowledgement number which they receive while registering the complaint.

[7] https://cybercrime.gov.in/

For any feedback or response on this article, the author can be reached at sanika.phatak@ynzgroup.co.in

Sanika Phatak

is an associate at YNZ Legal. By qualification she is Master in Corporate Law from Vishwakarma University, Pune and Bachelor of Law from Pune University.