



# Cyber Laws For CxO

*Be Aware... Be Empowered*

May-June 2010

**Editor**

**Naavi**

[www.naavi.org](http://www.naavi.org)

**Publisher**

**Ujvala Consultants Pvt  
Ltd**

[www.ujvala.com](http://www.ujvala.com)

Terrorism is a curse for the society that we live in.

Our lives have changed irrevocably today because of the terrorism threats which surround all of us.

We don't know if there could be a terrorist attack in the plane we plan to catch or on the train we commute or even in the mall which we regularly shop or the hotel where we stay.

While the physical world struggles to cope with the problems of terrorism, the cyber world has its own concerns on "Cyber Terrorism".

ITA 2008 has defined an offence under Section 66F called "Cyber Terrorism".

This issue tries to explore the legal aspects of this clause particularly how it may impact a corporate entity.

**Theme**

**Cyber  
Terrorism**

**In This Issue**

**Editorial: Jihadi Phishing**

**News Snippets: Manchurian Chip and others**

**Knowledge+: Human Bombs within an Organization**

**Knowledge++: Section 66F Analysed**

**Laugh and Learn**

**Questions and Answers**

P.S: This is a combined issue for May and June

Archived Issues will be available at  
<http://www.cyberlaws4cxo.com>

*Dear Readers,*



*Cyber Terrorism has been a term which is engaging our attention for quite some time. While terrorism on the physical space has been an inevitable part of our life, as we move some of our critical economic activities such as Banking, Investment and E-Governance on to the Cyber Space, the threats of Cyber Space being used to further the cause of terrorism looms large on the society.*

*After the terrible 26/11 attack in Mumbai, there was sudden realization that misuse of Cyber Space for terrorist objectives need to be tackled with an appropriate legislative response. This resulted in the then pending amendments to ITA 2000 being speeded up and passed by the Parliament in December 2008.*

*One of the key changes that were made to the legislation in the amendments (ITA 2008) was the introduction of section 66F which described an offence titled “Cyber Terrorism” and prescribed “Life Imprisonment” as the possible punishment.*

*We have completed more than an year after the definition of “Cyber Terrorism” was inserted into our statute and the Kasab trial has been successfully completed without the invoking of Section 66F (Which incidentally became effective only from October 27, 2009 and is relevant for future attacks of similar nature). It is time now to examine the Section 66F of ITA 2008 on how it has addressed the issue and how it impacts the Corporate sector in particular.*

*The first thought that occurs to the ordinary observer is “Whether Cyber Terrorism is different from Terrorism as we know today?”, “Is it meant to protect the Physical Space? Or Cyber Space?”, “If Cyber Terrorism is terrorism with Cyber Tools, is it not already covered under IPC or UAPA? (POTA)”, “Does Section 66F also cover Cyber Warfare?” etc.*

*An attempt is made here to throw up some discussion points which hopefully will provide a platform for analyzing the impact of Section 66F on Corporate and also indicate some remedial action that can be contemplated in an organization.*

*In addressing the Cyber Terrorism aspects under law, it is also necessary to address the dismantling of the support structure for Cyber Terrorism. In this context we need to discuss the growing tendency of Cyber Crimes that indicate a fund raising effort for terrorist activities. “Phishing” in India is being used extensively to generate such funds and a few Banks appear to be in the forefront of being a support base for a network of Phishing fraudsters who systematically execute phishing frauds. A few E-Commerce businesses such as Traveling agencies are also being systematically exploited by terrorists. Companies in such businesses therefore need to address this problem on a priority basis.*

*In finding a solution to the problem, this issue also focuses on mitigation of “Insider Threats” and approaches to mitigate them.*

June 14, 2010

### Manchurian Microchip

Viruses and Trojans that come via e-mail attachments or SQL injections have been known for some time. However, as Cyber Crime developed as an industry, new dimension of Cyber Crimes as “Cyber Terrorism” followed. In these new avatars of Cyber Crimes, the resources available to criminals increased manifold.

In the last few years, yet another up gradation occurred to Cyber Crimes with the evolution of Cyber Wars where the State supported setting up of an infrastructure within the enemy territory which could be exploited in times of need.

“Manchurian Chip” is the outcome of such a development. It represents the rogue microchip embedded in hardware devices, programmed to provide a backdoor entrance to a designated network. While it could be useful for remote servicing by the manufacturer, it could also be used maliciously by any person to steal the information of the user or otherwise usurp control of the user’s computer.

A concept which emanated out of a 1959 novel “The Manchurian Candidate”, where a POW is brainwashed to act under the control of an enemy force upon a trigger, has now assumed greater relevance because of the exploits of Chinese in the hardware market.

According to highly placed intelligence sources in USA there is a distinct possibility of Computers assembled in China and using Chinese made hardware could be embedded with such spying microchips.

Scotland Yard has identified such chips in the Credit Card swiping machines supplied to the UK market by a Chinese firm. It was speculated that these machines were doctored to send credit card information to a Chinese IP address and could have been used by AlQueda for terror funding.

Hardware related risks are therefore the biggest challenge to Information Security professionals. Just as we need to insist on “Source Code Audit” in respect of Software, it has become necessary for hardware purchasers to extensively check for possible presence of Manchurian Microchips in the hardware supplied to them.

### Telecom Security Certification Authority

In order to overcome the risks of secret codes embedded in software and hardware supplied by international vendors it is necessary to ensure that any software or hardware used in India in the telecom industry, should be subject to a “Security Certification” where an accredited agency would check the software/hardware appropriately and certify them as safe to use.

Indian Government has recognized this risk and has initiated some counter action in this regard. Accordingly, the Telecom Regulatory Authority has made it mandatory for Security Certification in respect of Telecom equipments supplied to Indian service providers.

Presently, the Telecom industry proposes to use British Telecom to check the security of Chinese Telecom equipments.

Such certification is also necessary for the IT industry particularly in Government establishments and other “Critical Infrastructure Resources” as defined in ITA 2008.

While ITA 2008 takes the responsibility of introducing enabling provisions in law to make the suppliers of such software or hardware liable under Section 66F of ITA 2008 for Cyber Terrorism and impose a maximum of “Life Imprisonment”, the mechanism for implementing the certification is still in its infancy.

Will the Indian Government develop in-house capability for such testing and certification? Or will it depend on commercially available international security certification agencies? Or will it take the assistance of US Security agencies that otherwise provide such support to the US Government? are some of the issues which still require to be sorted out.

### Terrorists use Hacked Website to Mobilize Resources

Some of the recent Phishing and hacking of E-Commerce websites in India indicate that the offence was committed by persons who used the benefits for either raising cash for the terrorist operations or to meet some of its expenses.

Unfortunately, neither the affected Banks nor E-Commerce Websites seem to have understood the seriousness of such attempts and refuse to even keep the authorities informed. Reserve Bank of India has also failed to impose the necessary discipline in the industry to ensure that all Cyber Crimes in the banks are appropriately reported though a system for such reporting does exist on paper. Hope this comment will wake them up at least now.

### Cyber Security Summit in Dallas

In the first week of May, a Cyber Security Summit was held in Dallas USA in which experts from many countries participated and discussed relevant issues. Though the organizers hailed it as the “First” Cyber Security summit, people in India remember that Karnataka Government organized Cyber Security Summit 2009 last year in Bangalore which was a highly successful event and a path breaking event in India.

What was interesting to observe was that many of the Security functionaries in the Indian Government who skipped the Bangalore Summit did not miss an opportunity to attend the US summit.

Hopefully they have come back with an International Perspective which they can share with the Indian public when the next Cyber Security Summit is held in Bangalore.

### US Military Will Respond to a Cyber Terrorist Attack

Indicating the seriousness which US attaches to Cyber Space security, the US Military has confirmed that it would use full force if necessary in response to a Cyber attack against United States.

India needs to appreciate that the kind of attacks we experience from Pakistan is in the form of a proxy war and what we face from China is in the form of a preparation for a future dominance. We need to retaliate on both fronts.

Today US Cyber assets reside not only within the US geography but also elsewhere. India is one of the major outsourcing partners for US and holds a big chunk of US Cyber Assets in a proxy form. If an event where US Cyber assets in India are attacked, the US military may consider it as its right to intervene in the defense.

Indian Companies who hold US cyber assets and US companies in India need to recognize the US approach and develop suitable compliance mechanisms.

### Dow Jones Drops by 1000 points

Week ending 15<sup>th</sup> May saw a huge drop of over 1000 points in the Dow Jones industrial index in US raising speculation of a possible Cyber Terrorist attack. The Securities Exchange Commission (SEC) has denied any confirmation of a cyber terrorist attack which triggered 17 million transactions within 1 hour and 66 million transactions on a single day. However the abnormal activity which overcame the circuit breaker mechanisms also indicates the vulnerability of the stock market system to software induced crashes. Whether the reason was an error in entry of some transaction or a cyber terrorism attack or a kind of virus, only further investigations would reveal.

### What is the Next Target for Cyber Terrorists in India?

Security analysts predict that the next target for Cyber Terrorists in India is the UIDAI which is setting up a database of Indian residents with sensitive information which would in due course be the base information for issue of Passports, Driving Licenses and to perform KYC for Bank accounts.

It is suspected that terrorists would be planting some of its sympathizers into UIDAI as employees and registration agencies and ensures that in a couple of years the “Human Bombs” inside UIDAI would help the terrorist organizations to access information from UIDAI which can be misused.

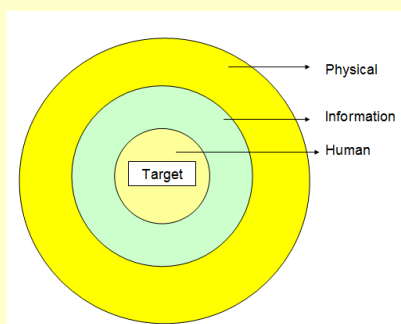
Let’s watch how UIDAI is addressing the security issues both from Technical, Legal and Human angle.

## Human Bombs Inside an Organization

Terrorism is the bane of the modern society. Whether we are in business or Governance or we are simply the common men on the street, we need to worry about the impact of terrorism on our lives. As organizational heads we often see that our business goals need to be modified because we need to guard our back against the effect of terrorism that is in the environment.

In manufacturing companies, there was a time when “Security” meant preventing stealing of some of the products of the company. A good frisking at the exit gate was all that was required to manage. Today, this is least of the botherations. A reputed company today has to guard against a Bomb being placed in a Car which is parked in the basement, A truck laden with explosives ramming into the building or even a computer virus that disrupts the activity. Hence in addition to the Physical security with Armed Guards, Electronic and Chemical sensors, CC TV monitoring systems etc there is a complete layer of information security with Firewalls and other gadgets.

Despite the large investments made by Companies in Physical security devices and Information security, the CEO is still not confident that the security is reliable. The reason is that all the security measures indicated earlier tries to guard the Company against external threats.



But a major part of the threat to a Company comes from within. It may not be a Kasab who rams into the Company walls in a Truck to create problem, but a trusted car driver who drives the CEOs car with his wife and children in the back seat and RDX inside the boot.

In such a scenario, Security in Corporate Space requires a holistic approach which combines Physical, Information and Human Aspects.

In 2007, FBI and Critical Infrastructure Threat Analysis division of US found that Mr Dhiren Barot, a notorious Al-Qaeda agent who was arrested in UK had instructed one of his terror team mates to secure an employment in a hotel in UK to learn how to deactivate fire and security systems. In 2008, we saw the happening of the 26/11 attack on Mumbai hotels where the terrorists displayed a remarkable knowledge of the interiors raising suspicions that some of them had perhaps collected information after working in the hotel for some time in the house keeping section.

Again the 2007 plot to explode Jet fuel pipelines at JFK International Airport was masterminded by Russel Defreitas who had been a Cargo handler at the Airport. Recently we observed a crude bomb in the cargo section of a plane in Cochin which could perhaps be a trial run to test the security at the airport.

In our own country the Rajiv Gandhi assassination plot succeeded because of the role Nalini played as an insider.

Such Human Bombs are sitting inside many of our organizations, receiving pay packets from our companies and acting as the agents of the external terrorists. Unless we identify and eliminate these inside threats who are sitting as human bombs within our organizations, the security strategy of a Corporate is incomplete.

### **Approach to Defusing the Human Bombs**

As a first step towards eliminating the insider threats to terrorism, we need to identify the employees who have a propensity for “Deviant Behaviour” and classify them as “No Threats”, “Probable Threats”, “Potential Threats” and “Real Threats” and then initiate appropriate actions. This is a very sensitive operation HR persons will jump at the security person when such a suggestion is made. Many CEOs also may consider this atrocious. Unfortunately, the threats are so serious that even atrocious measures need to be tried if we need to limit the risk of terrorist attacks.

In order to reduce and eliminate if possible the possibility of errors, the findings in the Classification exercise needs to be validated with a suitable observation of the behaviour of the short listed persons more closely and the classification reviewed before crystallization.

Once the classification is complete, corrective action plan has to be initiated. While real threats need to be kept at a distance and sent packing, the potential threats need to be avoided from sensitive positions while continued to be put under surveillance. The probable threats may contain those who need guidance and self improvement behavioural training to bring them back from “Deviant” to “Normal” status.

The whole exercise of weeding out people on the basis of a behavioral trend classification needs to be addressed in close association with the HR department and as a part of the regular corporate training programmes. Like all behavioural tests, they would be administered by experts in a different non-work environment through games and exercises and extrapolated to work situations.

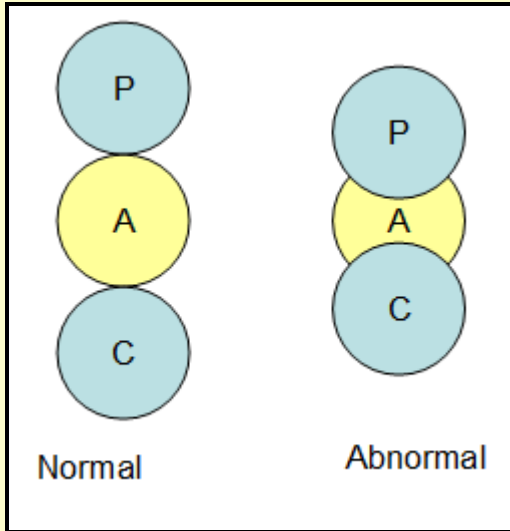
This is an area of research and the assessment may give raise to interesting observations of people. There may be the “Silent Killers” who appear to be loners, attend to work once assigned but otherwise remain idle, inquisitive about unrelated work and showing keen interest particularly in the security issues. There may people who display “Systematized Absenteeism” such as being absent on specific days of the week or month, and leaving without trace. There may be people who display abnormalities in how they get motivated for work. People with high greed quotient have long been tagged as potential fraud risks and they continue to be terror risks as they are amenable to act as “mules” and carry out malicious instructions from others without knowing the real implications.

There are two major strategies that a security professional should consider implementation. First is the “Whistleblower Policy” with appropriate confidentiality, witness protection and filter to avoid victimization. Key to a successful Whistle blowing policy is to appoint an external ombudsman rather than relying on an internal official.

The second strategy is to devise appropriate HR programmes map the deviant behavioural tendencies through well established behavioural science approaches.

...Contd

### Eric Berne's Ego Gram Approach



Eric Berne introduced the theory of “Transaction Analysis” according to which he suggested that people appear to transact from three types of ego states called Parent, Adult and Child ego states.

By observing the behavioural patterns of people in different circumstances real and imaginary, it is possible to draw a rough ego-gram of a person to identify the relative development of the different ego states of a person and to identify which ego state dominates his behaviour.

Typically the ego gram of a deviant person would display an unbalanced development of the ego states.

I am Not OK You're OK	I am Not OK, You're Not OK
I am OK, You're OK	I am OK, You are not OK

Similarly, Eric Berne also propounded a theory of “Scripts” that drive a human being to a type of behaviour during his life. He classified the scripts into 4 types, I am OK-You are OK being the idealistic position to I am OK –You re Not OK or I am Not OK, You are Not OK as scripts driving criminal tendencies.

Identifying such script maps individuals in an organization is a task that precedes the next corrective step.

Mapping the ego grams or Scripts of individuals identified as potential or probable threats is achieved through not only game situations but also through extensive data mining techniques using Natural Language Processing Techniques, Artificial Intelligence through CCTV analysis, monitoring of behaviour in social networking sites etc.

Additionally, basic steps such as Ethical training, obtaining of ethical declaration etc need to be used appropriately.

The human de-risking process in an organization is a complex exercise but one which is essential. In the current rage amongst HR managers for a “no Holds Barred Recruitment”, some of these strategies may appear impractical. Only time will tell if they are critical to the survival of organizations in a terror filled world around us.

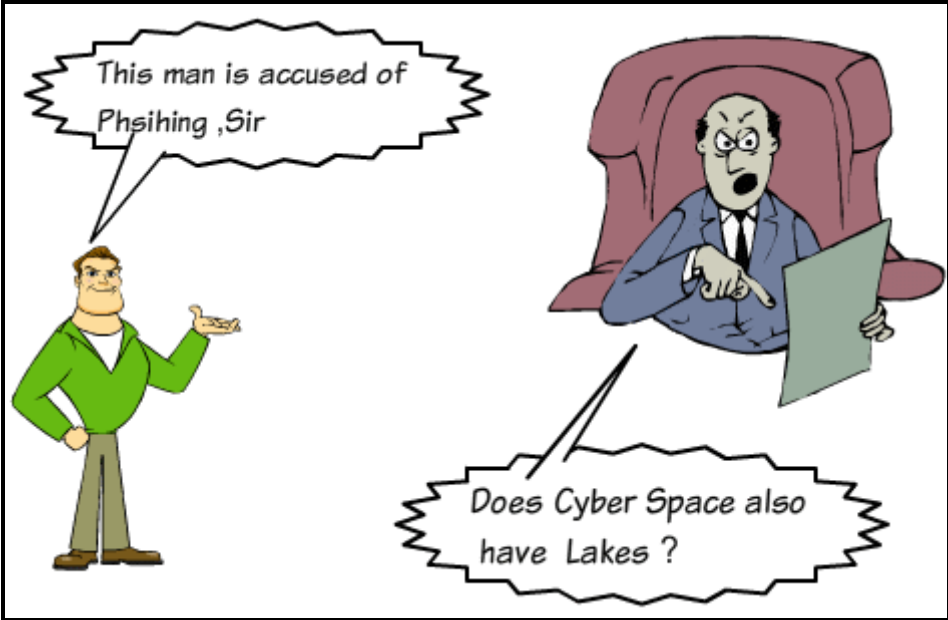
Naavi



Laugh and Learn



*Naavi: If Terror is created in a section of society through Hacking, Virus or Denial of access, with the intention of causing harm to the country, it could be a Sec 66F offence.*



*Naavi: “Phishing” today is not “Fishing”. However, as the “Second life” concept develops in future, there could be Cyber Lakes in the virtual world where “Cyber Fishing” is prohibited and violation could be punishable.*

### **Section 66F Analysed**

The Amendments passed to ITA 2000 through the ITA 2000 amendment Act 2008 which have become effective since October 27, 2009, has introduced a new section 66F into the 10 year old Act (now referred to as ITA 2008). This section covers what in India can be constituted as a definition of “Cyber Terrorism” and its consequences. It states as under

#### **Sec 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 authorised to access computer resource;  
or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised 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 authorised 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 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’.

If we closely analyse the Section 66F provisions, we recognize that the offence under this section is recognized under two sets of conditions represented by sub sections 1(A) and 1(B).

**..contd**

## Knowledge ++...

Sub Section 1(A) requires three conditions to be met to constitute an offence as “Cyber Terrorism”.

The first condition to be satisfied is that “There should be an intention to threaten the unity, integrity, security or sovereignty of India” or to “Strike Terror in the people or any section of the people by certain activities”.

The activities that need to be committed for the purpose of “Striking Terror” could be

- i) denying or causing denial of access
- ii) Unauthorised access to a computer resource
- iii) Introducing a computer contaminant

Finally by means of such intentional act, death or injuries to person or damage to property disruption of critical services essential to the life of the community etc should have been caused or is likely to be caused.

Since the above requirement includes “destruction of property” and “Information” is considered as “Property”, any damage to information which falls under Section 66 or 65 of ITA 2008 also qualifies for invoking Section 66F if the malicious intent is to “threaten the unity of India” or to strike “Terror” in a section of people.

The second subsection of 66F can be invoked “information restricted for access for reasons of security” is accessed again with the intention of affecting the integrity of the nation etc. Here, the emphasis is classification of information as “Restricted”. It is not clear if this can be invoked only in case of information held by the Government or may also be invoked in case of information at the hands of private sector. Companies engaged in providing services to defense sector could be holding such restricted data and need to take steps to classify the data appropriately if they need to use the protection provided by this section.

The section however raises doubts as to whether it applies to “indirect offences” where the offensive action itself does not directly satisfy one of the above conditions but is used to support the activities leading to a threat to the integrity of the nation.

Hence when a network of “Phishing” is established to raise money for terrorism or “Logistics Network” is established to fund the traveling of terrorists, though the offence easily qualifies under Section 66, additional evidence may have to support its escalation to Section 66F.

The punishment prescribed under the section is “Life Imprisonment” and hence a correct application of the conditions has to be ensured to prevent misapplication of law.

At the same time, it would have been better if the section had clarified at least through an explanation that “Intent to threaten under this section includes intention to provide any support to such activity by means of funding or otherwise”. This would have clarified the meaning of “indirect intent to threaten the unity and integrity of the country”.

Naavi

## Questions and Answers

We intend using this section of the news letter to answer the Cyber Law related queries raised by our readers. This being a special issue on Digital Signatures we are using this space to explain some of the basic concept of Digital signatures.

We appreciate if queries are raised by persons indicating their Name, Occupation and Contact details. We however don't want to restrain the readers from raising questions without revealing their identity. Such readers may therefore send the questions as "Anonymous" in which case even their e-mail ID would not be provided on the news letter.

All questions may however be sent by e-mail to [naavi@in.com](mailto:naavi@in.com) by e-mail with the subject line containing "Cyber Laws for CxOs".

### What Constitutes a Cyber Terrorism?

According to FBI,

"Cyber Terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."

U.S. National Infrastructure Protection Center defines "Cyber Terrorism" as

"A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda"

These definitions essentially mean that "Terrorism committed with the use of Cyber Tools is recognized as Cyber Terrorism". This definition is however dependent on the damage to the physical society and does not fully address the instances where the damage is restricted to the Cyber Space. We may however extend the definition to Cyber Space attacks since they anyway create uncertainty in the given population.

The Indian Legal definition is contained in the 2008 version of Information Technology Act 2000 which is analyzed in greater detail elsewhere in this news letter. Under Section 66F of the amended Act, destruction of property is covered as one of the requirements for constituting an offence as "Cyber Terrorism" and this may include "Cyber Property". A few other conditions are also to be fulfilled for a "Cyber Crime" to be escalated as "Cyber Terrorism".

## Questions and Answers

### **Cyber Terrorism and Cyber Crimes.. How related?**

Cyber Crimes are committed for individual gains. Cyber Terrorism is committed for a cause. However, since Cyber terrorism includes rising of funds and also destabilizing of the normal activities of the society, Cyber Terrorists look at “Cyber Crimes” as helping in their cause. Hence Cyber Terrorists encourage Cyber Crimes. They also try to harness the proceeds of Cyber Crimes to fund the terrorist activities. Hence Cyber terrorists try to establish, maintain and develop an underground economy for Cyber Crimes.

A large part of “Phishing Frauds” raise funds which eventually reach terrorist organizations. To proliferate Phishing, Cyber Terrorists need to maintain the support infrastructure which includes spamming, rogue ISPs etc. Cyber Terrorists may also indulge in “Cyber Extortionist” activities by exploiting the security vulnerabilities in organizations.

Counter Cyber terror strategies therefore include Cyber Crime mitigation.

### **A Government Website is hacked and defaced. It carries some messages promoting terrorist cause. Is it Cyber Terrorism?**

This has created “damage” to Government property through unauthorized access. If the message displayed can be called as promoting enmity, spreading disharmony etc, the act can be considered as Cyber Terrorism.

### **I have received a mail stating that “Bombs will be placed in a few Government Offices and set to explode some time next week”. Is it Cyber Terrorism?**

It is a threat likely to cause physical damage and loss of life. It would create terror in a section of the society. Hence it may be covered under Cyber Terrorism

### **A Hacker obtains the e-mail addresses of several Government functionaries including those working in the defense department. Is it Cyber Terrorism?**

Could be. Since the information can be further used to access classified information and used against the interest of the sovereignty and integrity of the nation.

## Questions and Answers

**I have received a mail stating that the popular Chief Minister who died in a Helicopter crash was actually murdered by some religious fanatics who created a malfunction in the helicopter deliberately. The message has been sent to many and riots have started in the street. Is it Cyber Terrorism?**

Spreading rumours which are likely to cause unrest and incites commission of offences, damages public order could qualify as Cyber Terrorism under Section 66F of ITA 2008

**A suspected Naxal sympathizer sends an SMS message to a State Government that if all trains to the Capital city should be stopped ..Otherwise they will be blasted. Is it Cyber Terrorism?**

Yes. Cyber Terrorism is also recognized when internal disturbances are caused by the residents or citizens of the country. Even Naxal activities in Cyber Space may come under Section 66F of ITA 2008

### **Indian Banks are US Patriot Act Compliant !**

When we observe that some of the Indian Banks state on their website that the Bank has taken steps to comply with “US Patriot Act”, one feels that the Banks have come of age to recognize the risks of Cyber Terrorism to the extent that they are scanning International laws and diligently complying with them.

However, the Indian Banks have not recognized that they need to comply with the Indian ITA 2008 which interalia requires compliance of other associated security guidelines including AML which is extremely important to avoid the Banking industry being used for funding Cyber Terrorist activities.

Taking steps to prevent commission of offences which may be classified as “Cyber Terrorism” is part of the due diligence of any organization including Companies. IT and IT Services companies are more liable in this regard and need to establish a suitable Counter Terrorism strategy as part of their Information Security program. This requires classification of information as “Section 66F critical” besides avoiding purchase of hardware and software without appropriate safeguards. Further the HR policies need to be suitably structured to ensure that potential threats in the form of people are properly addressed.

Probably the exercise has to start with the CEO is being trained in “Counter Cyber Terrorism”. It is necessary for our Management Education System to also introduce “Information Security” as one of the necessary subjects to be studied by students before they graduate out of premier management schools.

## Reader's Questions

*One of the main objectives of starting this e-News letter was to disseminate Cyber Law information to the Corporate sector. In order to sustain a momentum for this news letter, it is very important that Readers should raise their doubts on various relevant issues. I am therefore looking forward to such questions flowing in from all of you.*

*I do appreciate that the mailing list of this newsletter consists of many persons in Government, Banks, and Companies and perhaps even in Police and Judiciary. Some of them may be not comfortable to reveal their identity. We however assure you that unless the readers want, we would not publish their names or even the e-mail address.*

*We have picked one such question here from a reader sent as "Anonymous" and others may also send their queries similarly. We recognize our responsibility as a "Journal" and ensure that the identity of the person would not be revealed.*

*Naavi*

### **Question from Mr Anonymous:**

I just wanted to know details regarding 'deletion of an e-mail without authorized access to the system by a third party, with regards to cyber law and Information technology Act 2008.

*This offence attracts multiple sections of ITA 2008. "Unauthorized Access" invokes Section 66 along with the civil provisions of Section 43.*

*"Deletion" also attracts Section 66 and Section 43.*

*It may be necessary to prove that the deletion was done with intention to create a wrongful harm to any person.*

*The punishment is a possible imprisonment of upto 3 years. If any financial loss is suffered, damages may be claimed to the extent of the loss and related costs.*

*The complaint for claiming damages should be made to the Adjudication officer of the relevant State upto a damage claim of Rs 5 crores.*

*The difficult part is to gather necessary evidence which may be possible only if a complaint is filed with the Police and they initiate investigation.*

*If the victim remains silent when such an offence has been committed, it may harm his interests when he wants to take action against the same person for a similar act on a later day.*

*It is therefore recommended that the victim files a complaint and registers an FIR even if the chances of a successful investigation are not bright.*

*Naavi*

*P.S: Views expressed here may be considered as suggestive and other experts may have differing opinions.  
Answers given here are for academic clarification and debate and do not constitute legal advice.*

## **Building the Digital Security Consortium in India**

With increasing dependence of the society on Cyber Space and Digital Documents, Digital Security is a matter of concern for all. It is no longer possible for individuals to conduct Banking or Stock Market activities or even certain Citizen to Government activities without using the Cyber Environment and exposing oneself to the risks of Cyber Space.

With the launching of the Unique ID System, every individual in India will soon have his basic identity linked to the Digital Data called the UID.

In the coming days we will not have exclusive Citizens or exclusive Netizens. Every one of us would be Cinezens with our UID in cyber space and existence in physical space. We will have assets both in Physical and Cyber Space and some physical assets such as Bank funds being held in digital form.

Under these circumstances, it has become critical that the security of digital space is the key determinant of the society. Lack of digital security would throw the life of future citizens of the country.

It is therefore considered necessary for all those who are interested in the wellbeing of the society to come together and work for the common goal of a “Secure Digital Society”.

Since the task before us requires action on several fronts and in several places, Naavi.org has undertaken a task to build a “Digital Security Consortium” in India which proposes to bring together all likeminded organizations working in the Cyber Security space in India under a common umbrella banner of “Digital Security Consortium”.

The objectives of the Consortium would be to work towards Digital Security in all its dimensions.

Naavi invites all interested persons or organizations to come together in this initiative. Naavi also invites Corporates to join in this initiative as part of their CSR initiatives to support the activity of creating a “Secure Digital Society” in India.

Interested persons may contact [naavi@in.com](mailto:naavi@in.com) with necessary information.

*Na. Vijayashankar*  
(Naavi)

**Be A Part of the ADR Revolution in India**

**Use online arbitration for lower costs and greater convenience**

**At**

**[www.arbitration.in](http://www.arbitration.in)**

## Disclosure

This is an e-news letter published by Ujvala Consultants Pvt Ltd, No 37, “Ujvala” 20<sup>th</sup> Main, B S K Stage I, Bangalore 560050. (Ph: 080 26603490).

Web: [www.ujvala.com](http://www.ujvala.com). E Mail: [ujvala@md2.vsnl.net.in](mailto:ujvala@md2.vsnl.net.in)

The news letter is being edited by Naavi, Na.Vijayashankar, no 37/5, “Ujvala”, 20<sup>th</sup> Main, B S K Stage I, Bangalore 560050.

Web: [www.naavi.org](http://www.naavi.org). E Mail: [naavi@in.com](mailto:naavi@in.com)

A copy of the news letter is also being hosted on the website <http://www.cyberlaws4cxo.com>. In future the news letter may be reproduced in any other website owned by the same management or its assignees.

The views expressed in the news letter and the hosting website would be considered as belonging to the respective authors and provided for educative purpose and are not considered as legal advice. Kindly check with a qualified advocate if any legal action is contemplated.

Any comments and complaints if any may be sent to the editor at [naavi@in.com](mailto:naavi@in.com) for resolution.

Contents of this news letter may be reproduced only on specific permission from the editor and with due credit.

Copyright in respect of any contributions from authors published in the news letter will be deemed to have been transferred to the publisher at the time the article is submitted for publication. In the event an author intends to publish the same article in any other publication, he shall inform the publisher of Cyber Laws For CxO the name of such other publication and also add a note “First submitted for publication with Cyber Laws For CxO” in the other publication.

Any dispute arising out of the publication shall be settled through arbitration through the virtual arbitration center <http://www.arbitration.in> as per the terms of the Indian Arbitration and Conciliation Act 1996.

---

For Subscription: Visit [www.cyberlaws4cxo.com](http://www.cyberlaws4cxo.com)