cation
net.

both government owned web-sites & those set up by Indian companies.

4.1% is rate of cyber criminals increased per week

→ Section 80 of an IT Act 200

• 80 Power of police office & other officers to enter, search etc

- Any police office, not below the rank of an deputy Superintendent of police, or any other officer of central government or a state government authorized by the central government in this behalf may enter any public place & and arrest and search without warrent any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this act. (in such public place)

- The person arrested under sub-section (1) by an officer other that a police ~~pol~~ officer, such police officer shall, without unnecessary delay take or send person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station

—

Page No.
Date

Ingredients of sub-section(1) of section 80
- The power to enter any public place & search & arrest without warrant any person found therein is vested only in a police officer not below the rank of DSP (as all listed backside)
- The power can be exercised only in 'public place' which as per section 80 includes any hotel, shop or any other place accessible to public
- [ ] box, can be exercised only on the ground that such person is reasonably suspected of having committed or of committing or of being about to commit any offense under the IT act, 2000.

9. Restricting the power of arrest without warrant only from a public place, section 80 becomes vulnerable for being defeated luxuriously
eg 1 → If person has committed the of offense of hacking under section 66 of the IT Act from his house. After committing the offence, he goes to a hotel. As per section 80, Person can be arrested without warrant from the hotel which is a public place. But if a person remains in his house, he cannot be arrested without warrant as per section 80.

eg 2 → If person is committing the offence of hacking under the It Act from cyber cafe, he can arrested without warrant under section 80 only if he is found in the cyber cafe itself or in some public place, but he goes home & stays there then he cannot be arrested without warrant.

-Before the victim even realize that he has been hit by a cyber crime, the criminal would be far away from a public place.
-The power of arrest without warrent can only be exercised effectively where crimes under the It act are committed from work-places, which are public places, by those who work there & thus have to visit there regularly

1) Section 80 in its present form is anomalous. the power of arrest without warrant only from a public place should be scrapped
2) The power of arrest without ~~arrest~~ warrant should be without any such limitation, this would firstly remove the anomalies in section 80, in its present form.
3) Section 80 would become an effective weapon to counter various cyber crimes under the IT Act.
4) The power of arrest without warrant from any place (public or not) is justified & necessary also, because otherwise there would be a premium on cyber criminality and a penalty upon the victims of offences under the IT Act.

In cognizable offence

- Every information relating to the commission of a cognizable is given to officer-in-charge of police station. That info should be read in front of informant & signed by informant.
- A copy of the informat" as recorded under sub-sectio (1) shall be given forthwith, free of cost, to the informant
- If police-in-charge refused to record information a person may send the substance of such information in writing and by post to DSP, DSP shall either investigate himself or direct an investigation to be made by any police officer
- As per section 156 of code of criminal procedure, any office-in-charge of Police station may, without the order of a magistrate, investigate any cognizable case falling within the jurisdiction of such police station
- If information provided by informant is a cognizable offence then investigation starts. Investigation not start if case is not of serious nature
- Investigating officer has power during investigation, to require the attendance of persons who appear to be acquinted (known) with the facts & circumstances of the case, for recording their statements.
- After completing the investigation, the police is required to file a charge sheet / Challan / Report Against the accused before the criminal court.
- After charge-sheet has been filed, other stages occured like prosecution evidence, defense evidence, final arguments and judgement.

- Non-cognizable offences
  - In non-cognizable offences the substantial burden of prosecution has been cast upon the complainant and in appropriate cases the court has the power to direct the police to investigate such cases.

- In IT Act
  - If the accused is in a public place, he can be arrested without warrant event if the IT Act offence is not serious.
  - Even if the offence is serious, the accused can not be arrested without warrant, if he is not in a public place

- Obtaining an order of the court for investigation by the police in a non-cognizable offence would further delay the investigation of a case, which ~~would~~ would further delay the investigat^{n} of a case, which would be fatal in most cases of ~~cyber~~ cyber crimes.

- The offences under the IT Act, 2000 which should be expeditiously (rapidly) investigated and which can be done effectively by the police only under the FIR procedure, have been correctly classified as cognizable offences and others as non-cognizable.

- Checks and balance against arbitrary arrests
  - The safeguards provided by the legislature in section 80 are
    a) The power of arrest without warrant, has been vested in high-ranking police officer i.e not below the rank of DSP or any other officer authorized by the central government.

b) The basis of arrest must be reasonable suspicion entertained by the said officer against the accused of having committed or of committing or of being about to commit any offence under the IT Act, 2000.
- In the author's opinion though the grant of power without warrant to a high-ranked police officer relatively enhance credibility when compared to the exercise of the same power to any junior officer
- In the context of cyber criminality it is not a reasonable safeguard against arbitrary arrests & certain other safeguards are also necessary.
- As the technology is improving, cyber crime is also progressing ∴ In the opinion of the author, the law of IT must mandate that police officer (not below a DSP) or any other authorized Government officer must be assisted by an expert from the field of information technology.
- Investigative skills of a high-ranking police officer (not below DSP) coupled with the technological expertise of an IT professional would be an ideal combination to effectively investigates crimes under the IT Act and to prevent arbitrary arrests of innocents as well.
- Cyber crimes under laws other than the IT Act, would continue to be governed by the respective statutes and the criminal procedure code, 1973.
- Cyber crimes which are not mensioned in It Act should be investigated by high-ranking police officer with assistance of IT experts.
- IT engineers and experts help can be taken in cyber crime investigation.

- The word 'reasonably suspected' in section 80 of the IT Act are loose, subjective & hence vulnerable for misuse.
- Reasonable suspicious implies that there has to be some credible basis or material
- Since police officer (not below A DSP) may not be competent to entertain reasonable suspicion due to lack of understanding of advanced technology, it is all the more necessary to take the assistance of IT experts in cyber crime investigations, as sugested by the author.

- Arrest for 'About to commit' an offence under the IT Act: A Tribute to DRACO
- The word 'about' according to Black's law dictionary means:
  a) Near in time, quantity, number, quality, or degree.
  b) substantially, approximately.
- In the context in which the words "about to commit" are used in section 80, they imply a preperation to commit any offence under the IT Act, 2000
- In opinion of author this component of section 80 is wide open for misuse. Innocents can easily be put behind bars on the 'ground' of being about to commit an offence under the IT Act, 2000.
- There is wide scope for erroneous appliation even though the said power is sought to be exercised honestly.
- As the world is also new to cyber crime so this act misapplied in many cases.
eg. Person visits a web-sites which gives ideas on models of hacking systems, he can be arrested on the allegation

of being about to commit hacking under section 66 although he may be just viewing the site casually for fun.

- Arrest, but no punishment

→ -Section 80 covers 3 grounds of arrest when it says "reasonably suspected of having committed or of committing or being about to commit any offense under This Act.

-Three grounds are
  * of having committed or
  * of committing or
  * of being about to commit

- 'having committed' → situation where the offence has been concluded, various offences in the IT Act, 2000 only refer to this situation

- "of committing" → situation where person is caught in the process of commission of an offence which has not yet concluded

- 'about to commit' → Refers to stage of preparation

-In opinion of author rather than having this 3 categories, section 80 should have used the words 'reasonably suspected of being concerned'

-Without prejudice in any event, the grounds of arrest namely 'of committing' and 'of being about to commit' in section 80 are not harmonious with other provisions of the IT Act, 2000.

-eg. If a person is about to commit hacking of a computer system or is committing it he can only be arrested under section 80, but cannot be punished under section 66 for the offence of hacking

because it does not cover either 'of commiting' or 'of being about to commit' within its ambit.
- section 70 of IT act out of all the offences speaks of attempt and thus indirectly covers the situation 'of committing' referred to in section 80.

- IT Act 2000
- The information technology Act, 2000 is an Indian legislation that was enacted to provide legal recognition for electronic transactions and to faciliate electronic governance.
- Objectives
  a) Ensure the security and confidentiality of electronic transactions
  b) Grant legal recognition to electronic documents and digital signatures.
  c) Faciliate electronic filing of documents with government agencies.
  d) Provide legal measures to combat cybercrime and unauthorized access to computer systems.
- Offence includes
  a) Unauthorized Access and Hacking (section 66)
  It covers unauthorized access to computer systems & hacking.
  b) Damage to computer system
  c) Theft of computer system
  d) Virus/worms attack
  e) Trojan attacks
  f) Email bombing
  g) Denial of service attacks.

IPC - Indian Penal Code

Cyber Crime & Criminal Justice

Chapter 2 : Penalties, Adjudication & Appeals Under the IT Act, 2000

- Concept of "CYBER CRIME"

- The information Technology Act, 2000 does not explicitly define the term 'cybercrime' but outlines specific offences & punishments related to electronic transaction & cyber activities

- Narrowly defined, cybercrime under the IT Act, 2000 include offences such as tampering with computer source code, cyber pornography, hacking, email abuse.

- Broadly defined, cybercrime encompasses any illegal act committed through or with the help of internet, whether directly or indirectly connected, as long as it is prohibited by law.

- Cyber crimes classified as

a) old crimes → committed on or through the new medium of the internet eg. cheating, fraud. These crimes are old but their plate of operat° is new i.e. internet. Crimes on internet

b) New crimes :- created with internet itself such as hacking, IPR Thefts. Crimes of internet

- Computer crimes also been classified by the nature of usage of computers.

a) Crimes where computer & network are essential for the commission of offence eg. hacking

b) Crimes where computer are assisted eg. cyber pornography

c) Crimes where computer is only incidental for commission eg. cyber fraud

Page No.
Date

- Hacking

-A person who enjoys exploring the details of programmable systems and how to stretch their capabilities as opposed to most users who prefer to learn only the minimum necessary or one who programmes enthusiastically (even obsessively) described as hacker

- hacking refers to breaking into computer systems

-Hacker's classified as

a) Code Hackers → Are those who have knowledge of the intricacies of computer systems & their operations.

b) Phreakers → Are those have knowledge of the Internet and telecommunication systems.

c) Cyber-Punks → specialize in cryptography.

d) Crackers → Who are the breakers into computer security systems

- Out of all cyber crimes, criminal hacking is amongst the biggest threats to the Internet & e-commerce.

- hacking has the effect of eroding the credibility of the Internet.

- It creates a perception in the minds of netizens that the Internet is vulnerable & weak.

- Hacking makes e-commerce costlier because of huge investments required to install system to guard against hackers.

- Hacking is performed today

a) For fun as a hobby, mostly by teenagers obsessed with internet

b) To damage the business of competitors

c) For intension of fraud

-IT Act 2000 defines & punishes 'hacking' as

- CYBER fraud and cyber cheating
-Internet fraud & forgery have increased by a substantial 29% over the past year
-cyber frauds profitability is directly linked with the growth of e-commerce
-Major areas of fraud & cheating on the internet include misuse of credit cards by obtaining passwords by hacking, non-delivery of goods purchased from online auctions & websites, mis appropriation & tranfer of funds etc.
-As per IPC 1860 a person is said to do a thing fraudulently if he does that thing with the intent to defraud but not otherwise.
-Defination of 'fraud' under contract law.
a) Making a promise without any intension of fulfilling it.
b) Engaging in any act intended to deceive
c) Actively hiding a fact by someone who has knowledge or belief of that fact.
d) Suggesting as a fact something that is not true