# Use of Force Doctrine: How the League of Nations Forged the Modern Interpretation of Use of Force?

*Sourodip Nandy, Symbiosis Law School.*

## ABSTRACT :

*The objectives include:*

*1. To drive home the need for today's networked organizations to support the notion that the professional practice of computer forensics and knowledge of relevant laws is essential.*

*2. To help stakeholders consider how technology forensics blends into overall corporate computer security as a strategic feature.*

*3. To enlighten the mass on issues associated with computer forensics.*

*4. To embark on a product awareness and campaign to leverage cybercrime.*

## RESEARCH METHODOLOGY

*The researcher has adopted the doctrinal study as the information of policy decisions and analysis of precedents and its implications have already been made available through journals, research papers and other scholarly works in circulation. The doctrinal study aids the researcher in presenting a practical and real-world view of the method in which investigations for cybercrime are being carried out in the country in the present scenario. The present research can be called as doctrinal as it is an examination which has been finished on an honest to goodness social word by strategy for exploring present statutory courses of action as well as going through various precedents and examining the operation of the concerned statutes in real life scenarios.*

## RESEARCH QUESTIONS

1. *Whether the present statutory provisions regarding investigation are achieving their desired objectives?*
2. *Whether our current laws and investigative mechanisms are sufficiently equipped to deal with burgeoning volume of cyber-crimes in the post-covid era?*
3. *Whether the current strength of investigating officers and cyber crime cells are adequate to ensure proper investigation?*
4. *Whether there is a need to undertake training of officers and upgradation of technology to keep pace with the rapidly involving ways in which cybercrime is committed?*

## LITERATURE REVIEW

### 1. Divya Mukta Martolia, Types of Cybercrime in India and Its Detection, (2020).

This study talks about the recent trends and patterns of cybercrime that has been committed in India. It presents a case study of the prominent incidents of cybercrime and also the responses formulated by the authorities to ensure that such patterns are detected at an earlier stage in the future. The author has critically analyzed the trends and incidents and presented them in a chronological manner. However, the lacunae in this work is that the views of the judiciary while adjudicating on the issue have not been presented. The observations of the Court are important to delve into the mind of the judges.

### 2. Sesha Kethineni, *Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms*, (2020).

This study presents a brief overview of the mechanisms and regulations that have been put into place to curb the threats of cybercrime in India. In the context of cybercrime investigation, the author talks about the existing mechanisms such as statutory mechanisms and the functioning of the cyber cells which have been set up in order to distribute and ease the workload of the investigating agencies. However, the study fails to touch upon the challenges faced by the existing infrastructure in the face of evolving challenges of cybercrimes.

3. **Juneed Iqbal & Bilal Maqbool Beigh, Cybercrime in India: trends and challenges, (2017).**

The work talks about the challenges faced by Indian executive agencies in terms of the advancement and rising sophistication of cybercrimes being committed. The safest systems of the world are not safe and are vulnerable to attacks by hackers. In this context, it is imperative for India to quickly guard itself against this by taking the required steps to protect itself.

4. **Vineet Kandpal & R. K. Singh, *Latest face of cybercrime and its prevention in India***

The authors talk about the latest patterns and types of cybercrime being committed in India. It also highlights the steps taken by the authorities to seek out the parties responsible and to administer justice. In the context of investigation, the authors detail the challenges faced by the authorities in tracing, locating, evidence gathering and finally nabbing the accused in the face of paucity of evidence to support the investigation. The lacunae of this work is that there is not adequate analysis available to highlight the role played by the judiciary in highlighting the importance of investigation in solving cyber-crimes.

5. **V. K. Agarwal et al., *Cyber Crime Investigations in India: Rendering Knowledge from the Past to Address the Future***

The authors have derived this research from contextual viewpoints that have affected the actions of disadvantaged groups that have been subjected to high rates of cybercrime. Cyber-crimes are growing over the years, but aimed at a particular age demographic. The resulting policy perspective is intended to create public awareness programs in the coming years.

6. **Paul Hunton, *Managing the technical resource capability of cybercrime investigation: a UK law enforcement perspective***

This report addresses the obstacles faced by law enforcement authorities in the investigation of cybercrime. The author describes the specialized research functions required for the cybercrime police in the resource capacity matrix incorporating a standard resource capacity structure through the broader law enforcement sector would help to improve shared strategies and practices and increase the productivity and efficacy of cybercrime investigations in a declining global economy.

## CHAPTERIZATION

This study is divided into the following chapters:

**Chapter I: Investigation machinery in cybercrime**

This chapter seeks to elucidate the existing machineries involved in cybercrime investigation and analyze the workings of the machineries.

**Chapter II: Evidence procurement and admissibility of cybercrime offences**

This chapter lists the provisions from various legislations which deals with the procurement and appreciation of digital evidence used for cybercrime investigations. It also analyzes the procedure in which such data is gathered.

**Chapter III: Issues and Recommendations**

A summary of the findings is drawn and steps to address the issues highlighted in the preceding chapters are provided by the author.

# CHAPTER-I

# INVESTIGATION MACHINERY IN CYBERCRIME

The investigation methods followed in our country are still following the conventional methods put in place years ago. This is the reason for low conviction rates in our country. However, in 1980 there were some measures taken to address this deficiency. There was an attempt to shift the keeping of records and create a national database among various police branches in order to facilitate the pooling of case records, case history and case information to make them widely available to the officers irrespective of geographical location. This was the intention behind the creation of the 'Common Integrated Police Application' and the 'Crime Criminal Information System'.

## Common Integrated Police Application [CIPA]

It involves the setting up of basic machinery and substructure for crime investigation and information system and aims at creation of a standard database across police networks of the country. The Implementation is to be carried out by the National Crime Records Bureau with help from the Home Ministry, National Institute of Criminology and Forensic Science and with the cooperation of the states. Training is given to police officers with regards to operation of the database and the data entry to be carried out as well as trouble-shooting in case any issue arises.

## Crime Criminal Information System [CCIS]

This system enables the police to save and retrieve the crime records and store incidents of crime in order to increase efficiency and recognize the patterns in which a crime is committed. Under the National E-Governance Plan (NeGP) of Govt, CCTNS is a mission mode project in India. The CCTNS aimed to create an integrated and robust framework to enhance police accountability and effectiveness by implementing an e-Governance principle and developing a national IT-enabled state-of-the-art network infrastructure to measure 'Crime Investigation and Criminal Detection.'[1]

## **Investigation in Cyber-Crime**

The implementation of the law is dependent on the executive in the Indian context. However, the current cybercrime investigation agencies and machineries have not been able to correct the low conviction rate and speed up the process of cybercrime investigations. The legislature and the judiciary also have to keep pace with the changes in contemporary society while framing laws and adjudicating on matters of cybercrimes. The major reason for low cybercrime conviction rates is the lack of awareness among the public regarding reporting the same. When matters are reported, the quality of investigation carried out does not lead to good evidence and as a result cases do not reach the trial stage in court. The absence of scientific evidence, proper evidence processing knowledge and poor cybercrime investigation have collectively resulted in low conviction rates. In the case of *Dilipkumar Tulsidas Shah v. UOI*[2], a PIL was filed bringing to the Court's attention the lack of procedural safeguards available to victims of cybercrime. Harassment by police, negligence by investigation agencies and the apathy displayed towards the victims are commonplace in Indian cybercrime investigation.

With the advent of technology, cybercrimes have become sophisticated and advanced. The modus operandi of these crimes can easily fool the conventional and traditional methods currently used for cybercrime investigation. Informational technology offers criminal offenders the possibility to commit traditional crimes such as fraud, fraud, card frauds, misappropriation of bank deposits, industrial and political espionage, cyber terrorism, etc. while helping to commit crimes such as attacks against the safety of critical infrastructure and other non-traditional and IT-related crimes.[3] The distinctive characteristic of cybercrime is the archaicity and ineffectiveness of standard procedural rules. The issues are not related to the trial process but rather to the extent of research

[1] Crime and Criminal Tracking Network & Systems (CCTNS) | National Crime Records Bureau, https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns (last visited May 1, 2021).

[2] W.P. (C) 97/2013

[3] Juneed Iqbal & Bilal Maqbool Beigh, *Cybercrime in India: trends and challenges*, 6 INTERNATIONAL JOURNAL OF INNOVATIONS & ADVANCEMENT IN COMPUTER SCIENCE 187–196 (2017).

and evidence gathering. In cyber-criminal investigations, standard investigation rules and protocols and evidence gathering are also of little use. In one country and to the next, and in several other nations, a criminal offense is committed. The pace and precision are both fast and fine. The cybercrime features have posed a number of questions and implications in the pre-trial cybercrime inquiry. The superior police offices conduct cybercrime investigations in India. The IT Act 2000 established a special protocol for investigating and continuing cybercrime as laid out in the IT Act, 2000, which slowed the prosecution of cybercrime. The inspector must prosecute computer fraud according to section 78 of the Act. Before the IT Act 2008 was amended, the Deputy Superintendent of Police was issued the investigative authority, which aims to mainstream cyber-crime as a traditional offense. This amendment authorizes the inspector to report the cyber fraud and to prosecute it as another crime. These changes are altering the scope of cybercrime research dramatically. Different problems and minute procedures are required for cybercrime investigations. In the computer crime investigation, no single proceeding can be established.

## **The challenge of jurisdiction in cyber-crime investigation**

The legal concept of competence serves to establish the authority and govern situations, persons and property of the State. This power of competence gives the state legal authority to render legislation a constitutional authority, enforce law means the enforcement and award means the judicial authority. Jurisdiction is an essential factor, since the investigative body cannot exercise the authority to prosecute the subject without possessing legitimate jurisdiction. The investigating department must do different tasks in its investigation, such as search and seizure and detention among other activities. Since territorial borders actually vanish as certain cyber offences are considered, jurisdiction is another difficult matter. Countries vary in standards of civil and criminal offences, constitutional and administrative legislation, data storage and maintenance procedures, and other evidence and legal considerations. Furthermore, the responsibility for addressing a specific case or conducting an inquiry or how to work effectively through extradition and mutual aid policies is often unclear. This is not only at a global level, but also within countries including various branches of law enforcement. Internet messages slash through state lines establishing a virtual human sphere and undermining the authority of local frontier law enforcement. This current world is threatening to some territorially dependent legislators and law enforcement agencies. A State is territorial, although the Internet does not have a strict reference to its territorial limits.

Anybody (with access to a computer and modem), for example, can view a website at any time in any part of the world. This attempts to decrease the position of the site yet to broaden the geographical area of a company.

Taking into account the issue of jurisdiction, at the time of passage of the Act 2000 on information technology that has given the jurisdiction the Criminal Procedure Code and the IPC was modified. Chapter XIII includes sections 178-186 and 188 to broaden the scope of the 'local jurisdiction,' which can include investigation or prosecution of the offenses. 66 In addition to dealing with the offenses committed in India, Section 4 IPC, containing the expansion of IPC to extraterritorial offenses, also supplements Cr.PC If the computing resource concerned is located in India, the amended section shall grant the Indian Court jurisdiction. As provided for in Section 188 Cr. P.C. and I T Law section 2, the protocol to be followed is (I). The combined laws laid down in this section illustrate the legal right of a sovereign state not only to its citizens but also to any other country outside their own countries. Thus, the amendment elsewhere tries to grant competence, but without the other state's co-operation the implementation of this section is still impossible. International cooperation is thus the urgent need in case of cybercrime investigation to resolve the issue of jurisdiction.

# CHAPTER-II

## EVIDENCE PROCUREMENT AND ADMISSIBILITY IN CYBERCRIME OFFENCES

Evidence is the method of determining facts relating to a person's guilt or conviction during a trial. All such materials in electronic or digital media are electronic proof. You should save it or pass it on. The format of disk files, transmissions, records, metadata, or network data may be used. Digital forensics focuses on retrieving material that may have an evidence significance, which is also unreliable and potentially polluted. Forensic strategy consists of creating "bit for bit" backups of saved and lost documents, "write block" to ensure that the originals are not modified, and "hash" cryptogram files or digital signatures that show information changes.

Civil and criminal proceedings are governed by Indian Evidence Act. Proof, like electronic or visual evidence, can be of any kind of cybercrime. Digital documentation is any material that a claimant to the case can use in the proceedings stored or distributed in digital form. Whenever digital evidence is presented to the courts before it is accepted, the Court shall decide if the evidence is valid or admissible. The Court shall also decide whether a copy is appropriate or original. The Evidence Act of 1872 provides a preview of the electronic document. In order to cover all records, including the electronic record created for court review, the concept of photographic evidence has been modified.[4] Section 3 of Indian Evidence Act 1872 distinguishes evidence, whereby evidence refers to (1) all the statements which a court authorized or required to submit to the court in relation to an investigated matter of fact; such statements shall be considered oral evidence; These papers are referred to as historical evidence.

In order to be able to admit electronic documents in 2000, amendments to the Indian Evidence Act include some new provisions as Sections 65A and 65B, which allow for proof to be made in the courts of law of the contents of electronic records. Therefore, whether it is cybercrimes or traditional crime, Indian Evidence Act, which applies to conventional crime and cybercrime, takes

[4] Tejas Karia, Akhil Anand & Bahaar Dhawan, *The Supreme Court of India re-defines admissibility of electronic evidence in India*, 12 DIGITAL EVIDENCE & ELEC. SIGNATURE L. REV. 33 (2015).

the same account. The laws of proof only have to be changed because of the digital quality of the evidence. Section 17 of the Indian Evidence Act on entry now has an electronic declaration suggesting an indication of facts and relevance. This modification is made solely to make the digital proof true. In order to include the relevance of oral testimony with respect to the electronic record contents, new Section 22A is incorporated into Indian Evidence Act (1872). It provides that, since the genuineness of electronic records provided is at issue, oral admissions to the contents of electronic records are not applicable. As a result, these two Sections 65A and 65B in the Indian Evidence Act are concerned with the relevancy of electronic proof in a court case with regard to Digital Evidence. Section 65A specifies, in conformity with the rules of Section 65B, that electronic document contents can be proven.[5] Section 65B specifies that, regardless of what is said in the Indian Evidence Act, 1872 is considered a text and is admissible as evidence without proof of its production, providing that the provision laid down in section 65B is fulfilled.[6]

Wherever proof of cyber-crime is necessary, investigative devices can prove this by using evidence such as e-mail copies, e-mail header copies, which should include the date in the hh:mm:ss format, or I P address owner's detail. When needed, you can use cyber coffee, ISP, email services log companies. Even CCTV and video cameras are registered. In addition, if required or if a server log or other details can be used, the electric signature or signature detail can also be used. In general, the means of correspondence is e-mail in the age of information technology, and this e-mail is often used for cybercrime purposes. The e-mail is also used as testimony in cyber-crime courts. When cybercrime is perpetrated via e-mail, including illegal harassment, computer robbery, defamation, threat or fear, it is an important piece of evidence. The evidence worth in e-mail is then also the important issue in the courts.

Section 88A of the Evidence Act, 1872, as incorporated in the IT Act, 2000. It gives the court authority to assume for an electronic massage the originator passes on to the massage corresponding persons feed into his computer transmission through an electronic mail server. Section 88A explained that no person who submitted such an electronic massage shall be presumed by the court. The statute also recognizes that the electronic communication is vulnerable.

[5] Ashwini Vaidialingam, *Authenticating Electronic Evidence: Sec. 65B, Indian Evidence Act, 1872*, 8 NUJS L. REV. 43 (2015).
[6] *Id.*

The digital data was also covered by the various provisions of the Evidence Act and the invention of Information Media is the definition of digital evidence. The technology of information therefore impedes the development of information technologies in all aspects and the system of criminal laws. Changes in illegal activity and the way they commit crime impair the age-old practice of data gathering and evidence.

While deciding the charges against accused persons in a corruption case, the Hon'ble High Court in *Sanjaysinh Ramrao Chavan Vs. Dattatray Gulabrao Palke*[7] noted that the evidence for the audio and video CDs concerned is clearly unacceptable, the trial court had erroneously relied on them to find that there were strong suspicions about petitioners conspiring criminally with the concentration of the accused. There is also no evidence from which one can very reasonably say that in the commission of the offense concerned there is a clear presumption of the guilt of the petitioners. The Hon'ble High Court in *Ankur Chawla Vs. CBI*[8] held in its decision on the e-mail admissibility that an e-mail from the person's e-mail account downloaded and printed could be demonstrated in the context of Section 65B, in accordance with Section 88A of the Evidence Act. To prove the electronic contact, the testimony of the witness to carry out the process to download and print the same.

In this substantial decision, the Supreme Court in *Anwar PV vs PK Basheer And Others*[9] resolved the controversy around the admissibility of the electronic evidence emanating from the numerous contradictory decisions and the practices adopted by the many high courts and the courts. The Court has read Sections 22A, 45A, 59, 65A & 65B of the Evidence Act, and held that, unless certificates U/s 65B (4) of Evidence Act, secondary data on the CD/DVD/Pen Drive are not permitted. It was explained that the electronic proof without U/s 65B certificate cannot be proven by oral proof and it was not appropriate to use expert U/s 45A Evidence Act opinion.

[7] [MANU/SC/0040/2015]
[8] [MANU/DE/2923/2014]
[9] [MANU/WB/0828/2014]

## Procurement of Electronic evidence

## Investigation and Forensics tool

This is an effective method for discovering the facts. It provides the investigator with an effective way to explore the subject by using new technology along with the advancement of technologies. The use of forensic instruments is becoming an effective way to carry out technical crime investigations. This science is now on the brink of being used only in different crimes. Forensics is a major division that is needed today so people use this technology for violence because of developments in civilization, it was a valuable tool to track the facts.

## Computer Forensics

The study of information science where it concerns the law is computer forensics. The purpose of the forensic method is to get as much information as possible about criminals. This indicates in general that the system is analyzed by various forensic instruments and procedures and that the perpetrators are investigated. For each device examined, the actual forensics procedure is different. 80 The art and technology in the use of computer science to support the judicial process is computer forensics. Thanks to the dramatic transition in advanced technologies, it soon became more than just an art, and now you do have the possibility to graduate in cyber forensics in this field. The technologies will demonstrate cybercrime, but in investigation the authenticity of the digital proof is the most critical issue. The digital documentation collection is not the work of a legal professor, but rather the technical expert. Taking into account the issue of reorganizing digital facts, the new addition to the IT Act, as referred to in the Evidence Act, 1872, in Section 45-A. The evidence in this section is entrusted to a digital specialist. The management and retention of records and information before it has reached the Court requires additional care and safeguards.

## Stages followed in Digital Evidence Search

All these precautions have to be taken by Forensic Investigator so that no misinformation will ruin an organization's credibility.

1. The company staff appeal for legal counsel to the business counsel.

2. A first response to proceedings (FRP) is prepared by a forensic investigator

3. The criminal investigator seizes and transfers samples to the forensic lab in the crime scene.

4. Bit-steam pictures are prepared and the forensic researchers build an MD5 # of the files.

5. Before the search ends, the criminal detective investigates signs of a crime and draws up a report.

6. The report is given to the client and it is up to the client to press charges or not.

# CHAPTER-III

## CURRENT ISSUES AND SOLUTIONS

The Indian police system and criminal prosecution remain in the old forms in which a confession of the suspects is collected and they are beaten up. The police department is totally untrained in new forensic investigative procedures and is not primed to collect scientific facts to present a stubborn legal argument. This is why the disparity between police reports, the detention of a suspect and the conviction of the convicted persists.

### Issues in Investigation

Police are the subject of a State and the police force's numbers and qualities vary from one State to another. The majority of the recruits on the entrance level have a purely schooling experience, which has affected their education through their faith, caste, community, and economic status, which generally clash when it comes to police urban areas and where their social mentality differs from those of those in which they have grown up. In police matters relating to women's rights and the educated part of society, this ethnic distinction is very obvious. Furthermore, lack of education prevents the police from solving any crime scientifically. The teaching is confined to basic policing and is not exposed to advanced criminal investigation methods. Even the departments that are to be prepared with scientific research methods are normally saddled with outdated technologies and techniques.

In addition, data gathered and reported for crimes differ from State to State in their process and substance. In the lack of the exchange of criminal evidence and coordination, cross-border violence also poses a threat to the State police. It is therefore essential to improve the operating methods of the police machinery. State shall have technical training in cybercrime investigation. The state has put in place separate wings to investigate cybercrime since IT Act 2000, but the workforce and manpower in certain special branches or branches are much lower and the specialized training that these wings can get is much less, given current needs. Consequently, the offences will not be prosecuted in a necessary way and the outcome will be acquittals. In the conventional criminal investigation in India, however, crime usually involves property and people, in particular, means against the human body, in a particularly strict way in traditional crime. Proof of such crimes shall be physically preserved by the police until the evidence is obtained by the court until such time that such evidence has been presented before the court. When obtained, these data can be safely preserved. For cybercrime, this type of crime is generally in breach of the right to privacy, but it causes fraud or property loss, but in general the evidence for cybercrime is not physically as in the traditional way. Then it is very difficult to retrieve, even though once the police collect it, another problem is how to protect it before the court submission. Since India's police have little technical expertise, research institutions in India are normally less scientific professional, so the Indian police often usually prosecute cyber criminals equally, so the convictions in cybercrimes are much lower.[10]

In order to redress this problem, the Government of India had set up the National Cyber Security Policy[11]. The important deliberations of this policy are:

a) Foster cooperation between government entities and developers of private cyber protection technologies to refine and secure vital government initiatives

b) The policy is a cyber-security route map and it ensures a computing environment which can encourage customer trust in an electronic purchase.

c) At the macro level, cyber security intelligence would become easier to prevent threats, making them an essential element and rapidly adopting counter-actions.

These measures demonstrate that when the government somewhere agrees to use the assistant of private cyber security engineers to shape cyber policies, research machines enable private cyber security intelligence to investigate the technological cybercrime. The Indian investigation machinery faces these types of problems because of the lack of technological expertise and facilities. In India each crime will be investigated on a single formula of the state jacket, and even in the case of traditional crime, multiple loopholes exist, which means that the conviction rate in India is very limited. There is no difference between the issues of the inquiry into classical and cybercrime, but it is only likely that the investigation machine requires specific know-how during the investigation. Therefore, only the crop authorities can track the actual suspect along with

[10] Iqbal and Beigh, *supra* note 6.
[11] National Cyber Security Policy-2013 | Ministry of Electronics and Information Technology, Government of India, http://meity.gov.in/content/national-cyber-security-policy-2013-1 (last visited May 1, 2021).

successful facts to bring it to justice, so the state must provide the necessary instruction in such a manner.

## Quality of Investigation and documentation

Police are much disabled in carrying out a successful operation in case of lack of modern devices like scanners, recording equipment, etc. Forensic science labs are small and there is no laboratory that can help the Police investigate quickly, except at district level. In addition, the lack of forensic and cyber specialists in police offices in different States is common knowledge. Instead of focusing on scientific and circumstantial facts, the police are therefore relying heavily on oral evidence. There is no sufficient care and attention to examine and document witnesses' claims. In addition, the timeliness is desirable in this respect.

The registered declarations/FIRs/reports are neither automatically forwarded to the machine because there is no computer network or because there is no professional staff or because explicit orders are required. There is not much consideration and time to draft the final reports. Defective charge sheets are recorded as being very normal which appear to prolong prosecutions without mentioning all the pertinent evidence and charge sheets unaccompanied by annexes. The Station House Officer would not thoroughly review this vital paper, which is usually written by a "Writer" at the Police Station. Heavy police stations have overworked the 'Writer' who can barely waste much time.

The images of a convicted person (not to mention witnesses) are not attached to the indictment sheet/arrest memos etc. nor are even markings indicated that make it impossible to locate the accused or to locate the absconding defendant during the trial. The pictures (not to talk of witnesses) of the accused are neither attached to the charging sheets/arrest memos nor even to identity signs, which make it impossible to locate or pinpoint the accused during the process of the trial.

# CONCLUSION

The 2008 amendment to the IT law altered the essence of cyber law in India dramatically. In the preview in the general investigation process, it implemented numerous new provisions which were cybercrime, but they are not adequate to stop cybercrime without successful execution and well-trained investigation machinery. These are the issues before the investigative machinery, given that it is impossible to inquire about the technological crime or even cybercrime by the investigating agencies. The fundamental practice in research must then be changed. The attempt made by the Indian administration to enforce different laws and rules to address cybercrime and its regulation cannot be denied, but merely new rules and legislation cannot address the problem unless adequate and empirical research on cybercrime investigation and occurrence is carried out.

# REFERENCES

1. Vivek Dhupdale, *Cyber Crime and Challenges Ahead*, 2 IN THE INDIAN JOURNAL OF LAW AND JUSTICE, DEPARTMENT OF LAW, UNIVERSITY OF NORTH BENGAL, DARJEELING, WEST BENGAL 102–114 (2011).
2. V. K. Agarwal et al., *Cyber Crime Investigations in India: Rendering Knowledge from the Past to Address the Future*, *in* ICT AND CRITICAL INFRASTRUCTURE: PROCEEDINGS OF THE 48TH ANNUAL CONVENTION OF COMPUTER SOCIETY OF INDIA- VOL II 593–600 (Suresh Chandra Satapathy et al. eds., 2014).
3. AKSHAT MEHTA, "CYBER POLICING AND CYBER CRIME INVESTIGATION" - AN E-CONTENT DEVELOPED UNDER THE UNIVERSITY GRANTS COMMISSION (UGC) OF INDIA'S E-PG PATHSHALA PROGRAMME. THE CONTENT WAS DEVELOPED FOR THE DISCIPLINE OF CRIMINOLOGY AND SPECIFICALLY FOR THE PAPER - 'CYBER CRIMINOLOGY & CYBER FORENSICS'. (2018).
4. Nir Kshetri, *Cybercrime and cybersecurity in India*, *in* CYBERCRIME AND CYBERSECURITY IN THE GLOBAL SOUTH 101–118 (2013).
5. Nir Kshetri, *Cybercrime and cybersecurity in India: causes, consequences and implications for the future*, 66 CRIME, LAW AND SOCIAL CHANGE 313–338 (2016).
6. Sesha Kethineni, *Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms*, THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE 305–326 (2020).
7. Vineet Kandpal & R. K. Singh, *Latest face of cybercrime and its prevention in india*, 2 INTERNATIONAL JOURNAL OF BASIC AND APPLIED SCIENCES 150–156 (2013).