|LAW AUDIENCE JOURNAL™|

|VOLUME 1 & ISSUE 2|

|DECEMBER 2018|

|ISSN (O): 2581-6705|

EDITED BY:

LAW AUDIENCE JOURNAL'S

EDITORIAL BOARD

Law Audience Journal,

Mr. Varun Kumar, V.P.O. Gagret, Ward No.5, Tehsil. Ghanari, District. Una, Himachal Pradesh, Pincode: 177201,

Phone: +91-8351033361,

Email: lawjournal@lawaudience.com, info@lawaudience.com,

Website: www.lawaudience.com,

Contact Timings: 10:00 AM to 9:00 PM.

DISCLAIMER:

Law Audience Journal (ISSN (O): 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in Volume 1 & Issue 2 are the original work of the authors.

Views or Opinions or Suggestions, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work. All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

TECHNOLOGY, CRIME AND ITS CHANGING PATTERNS.

AUTHORED BY: MS. DEEKSHA SHARMA & CO-AUTHORED BY: MR. MANIK DHINGRA, LLOYD LAW COLLEGE, GREATER NOIDA.

I. ABSTRACT:

The focus of the paper is to bring to the knowledge the changing pattern in crime due to emerging technologies and how the technology is misused by the criminals for their own benefit and affecting the peace and security of the society. In today's fast growing world, advancement in technology is necessary. Technology is emerging at a faster pace. But everything which has a positive impact also has its dark side as well. Its negative impact is that it has a major contribution in growing crime which is a matter of concern. Earlier the major crimes involved physical injury but due to the latest technology a number of cybercrimes are reported which has posed a major risk on the privacy of the people.

Like in digital crimes such as hacking offence is committed without the involvement of violence and depriving the victim of his property. Online social networking sites such as Facebook, blogs, online gaming and online dating have opened a virtual encyclopedia of personal information. This information is used by criminals for committing frauds. Because of which people suffer the loss of personal financial resources and subsequent emotional damages. New techniques designed for the purpose of curing diseases can be used to modify viruses like H5N1 influenza which impose a threat to the lives of people at large. Terrorists also use technology to hack private information about countries.

The research was carried with the main objective to have a better understanding about the topic, to have knowledge about the developments in technology and its impact on growing crime and its changing pattern, the methods used by criminals to bring into action their evil plans targeting innocent people, how it is affecting the society and different law policies made to prevent such crimes and the use of technology in criminal analysis.

Developments in law policies are not at pace with technological advancement. The existing laws are not much effective to prevent these crimes. Latest technology should be adopted to prevent crimes like police departments should be equipped with modern technology, using smartphone apps and web for reporting crime, smart security systems at different places and establishing effective oversight systems.

Keywords: technological advancement, cybercrime, crime analysis, preventive measures, hacking.

II. INTRODUCTION:

"Change is the law of nature". In today's fast growing world, advancement in technology is necessary. It has changed the way we live and will continue to change in future. As a result, everything is emerging at a faster pace. But everything which has a positive impact also has its dark side as well. Its negative impact is that it has a major contribution in growing crime which is a matter of concern. Computer technology is growing at a fast pace but the gap between computer security and computer technology is becoming wider. Technological advancements have generated new opportunities in crime. It has modified the scope and area for criminal operation. Technology brings legal challenges. Because of the internet all the information is just a click away. Criminals always take advantage of this information available over the internet to commit illegal acts. Most of the time victims are not aware of the extent to which they got victimized.

Cybercrime is emerging and new types of crimes in cyberspace are coming to the front line. A cybercriminal hack websites and portals, implant viruses, commit online frauds, gain access to extremely confidential and sensitive information and commit other crimes over the internet. Nothing is completely secure in the cyber world. The defence mechanism of the states appears futile when it comes to advanced technology and cyberspace. The concept of jurisdiction becomes meaningless when an individual has only an address on a computer network as an identity. Unpreparedness for legal and law implementation communities for cyberspace crime is increasing constantly. Cybercrime has become a matter of concern for every nation in the past few years. Because of the lack of clarity and enforcement of laws it is difficult to determine a criminal act which had made the criminal activity common, easier to commit and harder to detect.

The major issues which have arisen are:

- Whether the form of crimes committed today is the same as that of earlier?
- How much is the crime prevention techniques successful in preventing new crimes?
- How much modern technology has helped in making new policies for preventing new crimes?

- Are the organizations effective in dealing with such crimes and whether the traditional techniques can be applied to these crimes?

New technologies are being misused for illicit purposes but are also used for security purposes and making new policies. Crime, policing and security co-evolve with technologies that make them possible. In this era, the law has to go hand in hand with technological advancement and contribute to public security. There should be a balance between crime control and interests of citizens.

Technology can be defined as the application of soft or hard science knowledge, materials and methods to practice arts and skills. Technology continues to advance quickly while the organizations and individuals are not quick enough to recognize the risks involved. New technologies are designed to achieve competitive advantage which may consist of trade-related secrets. These secrets can be misused by criminals for an illicit purpose.

As criminals compete with security officials for technological advantage continuously complex crime, policing and security results quite confusing and therefore unmanageable threats to society.

In today's world, everything is dependent on software. All information can be found on the internet such as information related to the manufacturing of drugs, how to commit suicide etc. Availability of such information so easily poses a risk to the world. Risks of plagiarism, forgery and other offences related to intellectual property have been increased significantly because of digital technology. Cases of piracy are growing and the government is not capable enough to control such crimes. The increase in electronic funds transfer systems will boost the risk that these transactions may be interrupted and diverted. The major question is that how to ensure the security of commercial trade along with competitive advantage.

Telecommunication services can be used for committing fraud or criminal conspiracy. Because of the global nature of information technology criminal activity has become transnational. A person sitting in one country can commit a crime in another country. This raises the problem of jurisdiction. It becomes difficult to identify where the offence has occurred. There is no uniformity of laws in the countries. What constitutes a crime in one country may not be a crime in another country. The degree of punishment also differs with countries.

III. TYPES OF CRIME:

Crime changes with technology and becomes complex with time and distance depending upon the resources available such as money or culture.

There are three types of crime:

a) ORDINARY CRIME:

Ordinary crimes are conventional. These crimes can be recognized and their variations can be understood and they occur in many places. Therefore these crimes can be easily detected and prevented. Whether a crime is ordinary or not is determined by the existence of statutes which define criminal behaviour and security recordkeeping systems or police which keep a track on the crimes. For example theft, burglary, and robbery are ordinary crimes because they can be easily detected.

b) ADAPTIVE CRIMES:

The technological variations in ordinary crime are called adaptive crimes. They are indicated through incremental as well as innovative use of technology. These crimes include one or more existing forms of security threats or crime. They occur frequently even though the criminal behaviour is not legally defined in the statute. Adaptive crimes can be prosecuted with the help of existing legal tools.

c) NEW CRIMES:

These forms of crimes are committed using absolute innovative technology which may not be illegal at the first instance of its occurrence.

Opportunities for new crimes are generated by:

- Demographic change
- Economic reform
- Globalization
- Technological advancement

These crimes happen rarely and are not detected easily. Initially, police and security officials may not be able to detect these types of crimes because they do not have much knowledge or experience regarding such crimes. Therefore they are not able to understand these crimes. They remain complex and mysterious to government officials, media and public because of the following reasons:

1. They involve the use of complicated technologies
2. There are many suspects and victims and there is a significant amount of loss or harm
3. Contain various forms of adaptive or ordinary crime
4. As it may not be justifiable by one investigative expert to other investigative experts across long distance or time adequately to formulate control as well as prevention strategies.
5. Creates intensity in the form of public violence not only against the act and its offenders but also against police officers or security officials for not responding effectively towards these forms of crime or security threat.

Once new crimes are discovered they cause public violence, disbelief and shock to the general public. These crimes are not easy to detect because initially they are not defined as a criminal act and so at the first instance they are not considered a crime. It may not be impossible but it is very difficult to take legal action against these crimes.

For example, suicidal terrorist airliner bombings of September 11, 2001[1], can be considered as a new crime because even though the crime i.e., murder, was in existence previously also, the technological means i.e., crashing hijacked airliners into buildings, involved complete new innovation. It was not easy to understand the nature of the terrorist attack and at that time there was no specific law against hijacking an aircraft in order to simultaneously commit suicide, mass murder and large amounts of property damage for political or religious purposes.

IV. TECHNOLOGY AND THE CHANGING PATTERN OF CRIME:

Because of the advancements in the technology there has been a great change in the nature of crime and various crime control techniques used throughout the world. Advances in technology have contributed a great deal in changing the nature of crime and crime control throughout this century. Activities such as online fraud or the online exchange of child pornography, which could not even be conceptualized until recently, are now a significant problem for crime control agencies. Recent technological developments have formed a wide range of novel approaches by which individuals may break down the law. Technology not only facilitates the commission of many existing forms of illegal conduct but also presents a

[1] Dr. Assaf Moghadam, "Top-Down and Bottom-Up Innovation in Terrorism: The Case of the 9/11 Attacks" (2013).

target for some new forms of illegality which are directed at technological products and services themselves. Some technological changes have created entirely new types of crime. The increasing prevalence of new and miniaturized information technology devices such as mobile phones, and palmtop and laptop computers, will make them attractive targets for thieves who will steal not only the hardware but also the information contained within these devices.

One of the main fears regarding technology and crime is the much wider accessibility of contact, and the hence available pool of sufferers, which is likely through the use of recent telecommunication and internet technologies. Such technologies have also increased the potential for communication and illegal networks of criminal activity on a global basis, posing significant difficulties for transnational policing of crime. Most of the technological developments are related directly to computers and telecommunications. It is probably no coincidence that these are the two technologies most easily accessed by ordinary persons. Personal computers have already been used to commit crimes of fraud, data manipulation, such as counterfeiting, and software piracy.

Technology and crime are bigger than computers and telecommunications. Technology has also been important in the drug trade in the sense that new drugs can be developed with the help of technology, can be easily manufactured in large quantities, information is easily available on the internet on how to produce drugs, on what drugs to take for what kind of effect etc. Development in telecommunication increases opportunities for theft and misuse of such services. Frauds which use the telephone such as telemarketing frauds and other forms of false advertising have already been well documented. Existing systems such as ATMs and EFTPOS technologies very quickly became targets for the illicit intervention and alteration of funds. Home banking and online shopping are also vulnerable targets. Technology has also allowed individuals involved in criminal actions to conduct such activities with reduced chances of detection. The technologies also facilitate the production, storage and retrieval as well as transmission of material very rapidly and unremarkably. Encryption software is becoming more and more sophisticated but at the same time also increasingly user-friendly.

We can identify three categories of computer or computer crime.

First, the use of computers or communications technologies to commit a conventional crime. These conventional crimes are fraud, forgery, intellectual property crime, extortion.

Secondly, the use of technology to support other criminal activity. These offer criminals the same advantage as they offer legitimate businesses. It can be used for rapid global communications, encryption, mobile phones and drug dealing, money laundering, communicating across borders in new ways with other criminals

Third, crimes committed against the technologies and their users like gaining unauthorized access to computers and systems, unauthorized use of computer systems, creating or propagating hostile programs for example viruses such as 'I love you' which affected 45 million computers and cost $7-10 billion[2].

Many countries, in which there is high computer usage, access and reliance, consider computer and telecommunications networks and their supporting infrastructure as the most likely potential targets for terrorism.

As we look at areas of electronic crime, internet stalking, identity theft, internet gambling, the dissemination of objectionable materials, criminal exploitation of pension systems, the development of drugs, violence borne of exclusion, modern forms of slavery, crimes involving new reproductive technologies trade in body parts and human cloning, we can identify significant changes.

a) CYBER-CRIME:

It has become a major threat. The term cybercrime includes any criminal act committed by using computer systems or network. These crimes are generally committed by non-professional, business rivals, computer programmers, students, individuals having knowledge of internet and criminals. Because of the anonymous characteristic of cybercrime they usually are not noticed and go undetected and unreported. Characteristics of cybercrime are, it is silent in nature, global in character, the non-existence of physical evidence, creates high impact, high potential and easy to penetrate. Many countries have established complex IT infrastructures to manage electricity generation and supply, banking, air traffic control, oil and gas and other information based civic amenities which could become easy targets of cyber-attack. The internet makes this system within the reach of hostile persons anywhere in the world. It can be against a nation, corporate or an individual. At individual level cybercrime could be committed for revenge, financial gain, mischief, blackmail or for some other darker motives. At corporate level it is committed for the purpose of theft of secrets,

[2] Dr. Amit Verma, "Cyber Crimes and Law", Central law publications (2009).

releasing the secrets that can damage the company in such a way that its survival is at stake. Cybercrime has become a major threat for the country. Young minds are attracted and misled by the internet. These crimes are increasing gradually. Nothing is entirely secured in this era of the internet unless there is upright cybersecurity. India is concerned about cybersecurity and has taken various steps in this regard.

"Rajnath Singh in 'Ground Zero Summit-2015' said efforts must be made to guarantee that the country's systems and networks were updated accurately. He said that the government will set up a cybercrime coordination centre constituting an expert committee which will provide suggestions in this regard. A cyber-control hub amounting Rs 400 cores called 'Indian Cyber Crime Coordination Centre' will be set up to control cybercrime which will include online abuse and child pornography as suggested by the committee. Its main objective is to check the attempts made by intruders trying to penetrate the Indian government's official communication network and hack them. Its other objective is to act as an early warning system for law enforcement agencies by proper cybercrime monitoring. Victims can raise the complaints regarding cybercrime by setting up an open platform along with rules for resolving online crime reporting, to manage and support investigations of cybercrime and assist the law agencies in investigating the criminal cases. It would assist CBI as well as state police on all the issues related to cybercrime.[3]"

b) TYPES OF CYBERCRIME: EVOLVING WITH TECHNOLOGY:

1. HACKING:

Hacking is either a successful or unsuccessful attempt to gain unauthorized use or access to a computer system. Hacking as cybercrime is very dangerous for the internet because it has the effect of eroding the credibility of the internet.

2. VIRUSES:

The growth of these kinds of computer crimes has become far more visible over the past decade. The largest threat faced by the world of computers, today, is the threat of corruption and damage of digital information induced by a human agent with the help of various types of programs. These programs include- Virus, Worms, Logic Bombs, and Trojan horse.

[3] 'Cybercrime has become a big threat", Times of India, November 5, 2015.

3. CYBER PORNOGRAPHY/CHILD PORNOGRAPHY:

The electronic revolution has made pornography more accessible, bringing immoral and hard-to-get images into the home. Pornography has also evolved from ancient caves to modern day fastest means i.e. internet and has been keeping pace with development in technology. There has been any stage of the progress where pornography has not been an integral part of human progress.

4. CYBER STALKING AND CYBER HARASSMENT:

Women are more exposed to the new 21st Century computer era abuse, cybernetic harassment and cyber violence such as cyber-stalking, etc., with no safeguards under the international law and even the national legislation in India to provide protection against such a modern violation of their human rights.

5. CYBER TERRORISM:

Cyber terrorism means the use of cyber tools to shut down critical national infrastructures such as transportation, energy and communication and compel government into submission. Internet bomb threats, internet harassment and technology-driven crimes, such as focused virus strikes are the next waves of crime that the world has to face in the fore coming days.

V. LANDMARK CYBERCRIME INCIDENTS:

a) THE RED FORT CASE IN INDIA:

A terrorist attack took place on Delhi's Red Fort in December 2000. Investigation of the crime revealed that the terrorists were using steganography as a means for communicating the terrorist designs online. Steganography is the science and art of communicating in a way, which hide the existence of communication. In comparison to cryptography, where the rival is allowed to detect, intercept and transform messages without even being able to violate confident security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages within other inoffensive messages in a manner that does not allow any enemy to even detect that there is a second hidden file in the computer information. In the Red Fort case, the investigations further revealed that the conspirators were sending messages to their accomplices embedded behind pornography materials[4].

[4] Miller T.M., "Crime scene investigation", CRC Press, 2001.
Cybercrimes & cyber law– The Indian Perspective, 2018.

Other cybercrimes include E-mail bombing, spoofing, digital signatures, forgery, cyber gambling, cyber money laundering, cyber fraud and cyber cheating.

b) MRS. SONIA GANDHI- MAIL THREAT CASE:

In the last week of March 2002, Mrs. Sonia Gandhi received threatening emails apparently from victims of the 1984 riots in Delhi, following the assassination of Mrs. Indira Gandhi. As reported by the media, she received five emails. In all the emails, the 1984 riot victims reportedly accused Mrs. Sonia Gandhi of acting against their interests and have threatened revenge. One of the emails received stated: "We will take revenge for what you did to us in 1984". Investigation of the case revealed that the emails were sent to the two accounts that Mrs. Sonia maintains as the Head of the Congress Party and as MP. These emails were sent via Hotmail account[5].

VI. TECHNOLOGY AND CRIME INVESTIGATION:

In 1879, the first scientific system of personal identification was devised in which a series of body measurements were applied to identify criminals. It was a good method to identify criminals for a few decades. Later it was overthrown by fingerprinting. Until 1900 it was not possible to identify whether the blood sample was of a human or an animal. So in 1915, the blood group technique was brought in a criminal investigation by Dr. Leone Letter. After 1st world-war, Albert S. Osborn was able to convince some of the countries to build police laboratory. Today, Federal Bureau of Investigation (FBI) is the biggest laboratory in the world which analyzes almost one million cases every year.

a) CRIME LABORATORY FOR CRIMINAL INVESTIGATION:

Crime laboratories are generally developed by those agencies whose main purpose is to investigate the crime. New technology helps forensic scientists who possess various skills to face active involvement in the criminal justice system. Forensic laboratories provide two key services viz. basic and optional services.

1. In basic services:

   First, the physical science unit examines the principle of geology, physic and chemistry to catch hold of the criminal with the help of evidence available at the

[5] www.cyberlawclinic.org.

crime scene such as explosives, soil, drugs, paint; glass etc. microscope was very helpful in identifying these kinds of physical evidences. It has a major contribution to the history of forensic science in investigating the crime.

Second, the biological unit is basically responsible for DNA Profiling. DNA is taken from various sources such as saliva, skin, hair, blood and other sources which help to arrest the actual criminal. DNA verification is widely recognized as a forensic technology for criminal investigations. It has become the most powerful tool in forensic science. Third, firearms unit examines the arms that have been used for committing the crime. Then documents examine unit, analyses handwriting, the relationship between ink and paper.

Lastly, the photography unit uses new techniques such as digital and ultraviolet photography, X-Ray to new evidences which are not visible with naked eye.

2. Other than these services, operational services include Latent fingerprinting unit, voiceprint analysis unit, toxicology unit, polygraph unit and crime scene investigation.

The two more vital additions in the field of criminal investigation are computer forensic and internet. They provide a faster response in identifying the criminal. Computer forensic is concerned with storing data, gaining data and explanation of the data. This data is stored in devices such as smart card, camera, memory stick and various other storage devices. Further internet is a core source of communication these days; anyone can obtain billions of information on the internet. Every week a lot of information is uploaded about forensic science. There is no aspect which is left untouched by the internet, including forensic science. As such we can have a lot of information on the internet. Apart from this, all forensic science agencies over the world exchange their information through the help of internet.

VII. TECHNOLOGY AND CRIME PREVENTION:

Technological innovations play a major role in law reforms, policy-making and crime prevention. There are two types of technological innovations that are information based innovation and material based innovation. The most commonly acquired technologies vary from agency to agency such as record management systems (RMS), mobile data centres (MDCs) or laptops, personal computers, followed by automated field reporting systems (AFRS), Automated Fingerprint Identification Systems (AFIS) and Computer-Aided Dispatch (CAD) Systems. Technological Innovations in criminal justice can be divided into

two categories: hard technology and soft technology. Hard technology innovations include new materials, devices, and equipment that can be used to either commit a crime or prevent and control crime. Examples are CCTV cameras, metal detectors in schools, baggage screening at airports, bulletproof teller windows at banks, and security systems at homes and businesses, personal protection devices and ignition interlock systems with alcohol-sensor devices to prevent an individual from starting a car while intoxicated.

VIII. RESPONSE TOWARDS NEW CRIMES:

Because of the technological innovations, the pattern of crime is changing. This poses a challenge for the traditional crime prevention techniques. Today's requirement is to develop new techniques in the criminal investigation. There are various types of approaches to counter the emerging crime these are public awareness, situational crime prevention, international cooperation etc. people should have trust and confidence in our democratic system and legal institutions. Technological innovations have helped to tackle crimes. These developments are improvements in locks and alarm systems, locating devices, identification and surveillance, restraining individuals who pose a risk to themselves as well as to the society. These all methods help in crime control. Biometric devices and passwords also ensure safety. They prevent unauthorized access to some extent. Protective measures can be incorporated into the products either at the time when they are manufactured or can be added later. This will help in preventing some of the products from becoming the targets of the criminal. Less attractive products can also reduce crimes such as robbery to an extent.

Nowadays there are many theft countermeasures like car alarms, ink or electronic tags on retail commodities, security code requirements etc. Many new innovations are gradually emerging. For example, programs to track portable computers can be embedded in the machine's hard drive. The software regularly handles into a monitoring centre when the device is linked to the internet, supplying identification information and the telephone number of its calling location. Mobile phones are protected through monitoring patterns based on the time of day, duration and numbers called. If a deviation from the established profile is detected, the telephone is locked unless a personal identification number is entered. The installation of electronic tracking devices in trucks, which could wipe out organized thefts of trucks. Security changes can be introduced in the law. Many such restrictions were imposed. For example, New York imposed restrictions on international calling capabilities in

Manhattan Bus Terminal. These restrictions helped New York to eliminate multimillion-dollar fraud business. Similarly, in Britain, credit card companies made several security changes which avoided millions of pound fraud. The private sector is more effective in fighting against transnational crimes like smuggling, extortion.

Most of the illicit acts related to the computer are beyond the control of law enforcement and regulatory agencies. Therefore cyberspace security depends widely on self-help measures or on the efforts of institutions. Uniform international laws can help in preventing transnational crimes so that the criminals will not be able to target the country with the least controls. There should be uniform business practices so that it becomes difficult to commit economic crimes but easier to detect such crimes. Other conventions and treaties are required to be adopted to deal with cybercrime. U.S. and Canada formed a multi-agency international task force to deal with the rising problem of smuggling.

IX. CONCLUSION:

"Don't shrink from a new technology just because it may be subject to criminal abuse. Exploit its strengths, while controlling its weaknesses." This is the method by which we can survive in this world full of competition. Technology is changing but the methods used in crime prevention are traditional techniques. These traditional crime prevention techniques are not effective in controlling the criminals who use emerging techniques to commit new crimes which make them difficult to detect.

The aim of this research was to study the impact of technology on crime and how it has contributed in developing new techniques in the criminal investigation and law enforcement. As previously acknowledged, new technologies are adopted for illegitimate purposes as well as countervailing policing and security purposes.

The quest for new and innovative ideas has made it possible to have the tremendous progress in every sphere of life. The use of new technology to commit crimes is not a new phenomenon and all advancements in technology have always provided wrongdoers new ways for engaging in illegal conduct.

Due to the anonymous nature of the internet, it is possible to engage in a variety of criminal activities with impunity. People with intelligence have been grossly misusing this aspect of

the internet to disseminate criminal activities on the internet. Cybercrime is the noxious endemic confronting our world in this millennium. Privacy on the internet is another debated issue in cyberspace. Cybercrime has developed as a major source of concern for governments across the world. Since cybercrime is relatively a very recent phenomenon, the judicial response in terms of interpretation of various statues of cyberlaw assumes vast significance. The enforcement agencies in India are not much aware of the technical issues involved in cybercrime and this turn makes the task of an investigation into cybercrime rather difficult.

Technology has also contributed in crime prevention techniques though not at the same pace at which it has contributed in creating crime opportunities. Earlier it was very difficult to identify the criminal. But because of the DNA Profiling and computer forensic, it has become a little bit easier to identify the actual criminal. The internet also has a major contribution in the criminal investigation. We should look at the future and find new techniques for crime prevention. Regulatory controls should work effectively and efficiently in preventing and detecting crimes. The changing environment has a major contribution in criminal activities but it has also generated new opportunities for crime prevention. The new challenge ahead is to use the new techniques in controlling the crime.

➢ References:

1. Dr. Assaf Moghadam, "Top-Down and Bottom-Up Innovation in Terrorism: The Case of the 9/11 Attacks" (2013).
2. 'Cybercrime has become a big threat", Times of India, November 5, 2015.
3. Dr. AmitVerma, "Cyber Crimes and Law", Central law publications (2009).
4. Pepper L.K., 'Crime scene investigation: Method and procedures", Maidenhead: Open University.
5. Miller T.M., "Crime scene investigation", CRC Press, 2001.
6. Dr. Adam Graycar, "New Crime or New Responses: Australian Institute of Criminology" (2001).
7. Heath J. Grant and Karen J.Terry, "Law Enforcement in the 21st Century" (2005).
8. D. Geoffrey Cowper QC, "A Criminal Justice System in 21st Century, BC Justice Reform Initiative" (2012).
9. James Byrne and Gary Marx, "Technological Innovations in Crime Prevention and Policing: A Review of the Research on Implementation and Impact" (2013).
10. BYRNE, J. and REBOVICH, D., "The New technology of Crime, Law and Social Control Monsey", NY: Criminal Justice Press (2007).
11. CHAN, J., "The Technology game: How information technology is transforming police practice", Journal of Criminal Justice (2001).
12. NUNN, "Police technology in cities: Changes and challenges" (2001).