Title : To study the changing face of crime caused due to Cyber Security

Aayush Kumar, Jenim Shah

BBA (IB) Sem-III, Swarrnim Startup and Innovation University

Dr.Pushpalata S.Patil

Associate Prof. Swarrnim Startup and Innovation University

## ***Abstract***

The aim of the paper is to bring to light the changing pattern of crime due to emerging technology and how this technology is being misused by criminals for their own benefit and affecting the peace and security of society. In today's fast-paced world, advancements in technology are essential. Technology is developing at a faster pace. As with digital crimes such as hacking, the crime is committed without using violence and depriving the victim of her property. Online social networks such as Facebook, blogs, online games, and online dating sites have opened up a virtual encyclopaedia of personal information. This information is used by criminals to commit fraud. Current laws are not very effective in preventing these crimes. The latest technology should be adopted to prevent crimes, for example, police departments should be equipped with modern technology, using smart phone apps and the web to report crime, smart security systems at various locations and implementing effective surveillance systems.

## ***Introduction***

In today's fast-growing world, technological progress is necessary. Computer technology is developing at a rapid pace, but the gap between computer security and computer technology is widening. Advances in technology have created new opportunities in the area of crime. A cybercriminal hacks websites and portals, implants viruses, commits online fraud, accesses extremely confidential and sensitive information and commits other crimes on the Internet.

The defines mechanism of states appears futile when it comes to advanced technologies and cyberspace. The notion of jurisdiction loses all its meaning when an individual's only identity is an address on a computer network. The legal communities' lack of preparedness and law enforcement in the face of crime in cyberspace continues to grow. In this day and age, the law must go hand in hand with technological progress and contribute to public safety. There needs to be a balance between crime control and the interests of citizens. Technology can be defined as the application of soft or hard scientific knowledge, materials and methods to the practice of arts and skills. Technology continues to advance rapidly while organizations and individuals are not agile enough to recognize the risks involved. New technologies designed to gain a competitive advantage may include trade secrets. As criminals compete with security officials for technological advantage, crime is constantly complex, policing and security lead to quite confusing and thus unmanageable threats to the public. with society. 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. What constitutes a crime in one country may not be a crime in another.

## ***Type of crime***

I. Ordinary crime: - Conventional crime is conventional. Therefore, these crimes can be easily detected and prevented. For example, theft, burglary and robbery are common crimes because they can be easily detected.

II. Adaptive crime: - Technological variations in common crime are called adaptive crimes. These crimes involve one or more existing forms of security threats or criminal activity. Adaptive crimes can be prosecuted using existing legal instruments.

III. 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.

When new crimes are discovered, they cause public violence, disbelief, and public shock. These crimes are not easy to detect because they are not initially defined as crimes and therefore are not considered crimes at the initial stage. It may not be impossible, but taking legal action against these crimes is very difficult. For example, the September 11, 20011 suicide bombings of terrorist aircraft could be considered a new crime because crime.

## ***Technology and changing the pattern of crime***

Due to advances in technology, there has been a great change in the nature of crime and the various crime control techniques used around the world. Advances in technology have greatly contributed to changing the nature of crime and crime control throughout this century. Activities that could not be conceptualized until recently, such as online fraud or the online exchange of child pornography, are now a major problem for crime control agencies. Technology not only facilitates the processing of many existing forms of illegal behaviour, but also provides a target for some new forms of illegality for technological products and services themselves.

Some technological changes have created entirely new types of crime. The increasing prevalence of new and miniature information technology devices such as cell phones, palms and laptops will make these devices attractive targets for thieves who will steal not only the hardware but also the information contained in these devices. One of the main fears associated with technology and crime is the much wider accessibility of contact and therefore the pool of victims available, possibly through the use of the latest telecommunications and internet technologies. Such technologies have also increased the potential for networks of communications and illegal criminal activity on a global basis, posing significant challenges for the transnational policing of crime.

EFTPOS technologies very quickly became targets for illegal interference and exchange of funds. We can identify three categories of computer or computer crime. The first is the use of computers or communication technologies to commit a traditional crime. These traditional crimes are fraud, forgery, intellectual property crime, extortion. Second, the use of technology to support other criminal activities.

Third, crimes against the technologies and their users, such as unauthorized access to computers and systems, unauthorized use of computer systems, creating or spreading hostile programs such as "I love you" affecting 45 million computers and costing $7-$. 10 billion2. When we look at crimes involving electronic crime, online stalking, identity theft, online gambling, dissemination of objectionable materials, criminal abuse of pension systems, drug development, violence from exclusion, modern forms of slavery, new reproductive technologies, body parts trafficking and human cloning are important areas. We can detect changes.

## ***Types of cybercrime: Evolving with technology***

### HACKING

Hacking as a cybercrime is very dangerous for the internet as it has the effect of eroding the credibility of the internet.

## VIRUSES

The growth of these types of computer crimes has become much more visible over the past decade. The greatest threat facing the computer world, today, is the threat of corruption and damage to digital information induced by a human agent using various types of programs. There was a stage of progress where pornography was not an integral part of human progress.

## CYBER TERRORISM

Internet bomb threats, Internet harassment and technological crimes, such as targeted virus attacks, are the next waves of crime that the world will face in the coming days.

## ***Landmark cybercrime incidents:***

### RED CASE IN INDIA

A terrorist attack happened on the Red Fort of Delhi in December 2000. Steganography is the science and art of communicating in a way, concealing the existence of communication. In the case of Red Fort, investigations further revealed that the masterminds were sending messages to their accomplices embedded behind pornographic materials Other cybercrimes included email bombings, fakes forgery, digital signatures, forgery, online gambling, online money laundering, cyber fraud and cyber fraud.

### 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.

## ***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.

## ***RESPONSE TOWARDS NEW CRIMES***

Due to technological innovations, the pattern of crime is changing. This poses a challenge to traditional crime prevention techniques. There are different types of approaches to combat emerging crime such as public awareness, situational crime prevention, international cooperation, etc. People should have confidence and trust in our democratic system and legal institutions. Technological innovations have helped in the fight against crime. These include improvements to locks and alarm systems, locating devices, identification and tracking, limiting individuals who pose a risk to themselves and society. All these methods help in crime control. Less attractive products can also reduce crimes such as robberies to some extent. Currently, there are many anti-theft measures such as car alarms, ink or electronic tags on retail commodities, security code requirements, etc. Many new innovations are emerging gradually. If a deviation from the set profile is detected, the phone will be blocked if no personal identification number is entered. Installing electronic tracking devices in trucks that could wipe out organized truck theft. Security changes can be introduced into law. Many such restrictions have been imposed. For example, New York imposed restrictions on international calling options at the bus terminal in Manhattan. These restrictions have helped New York eliminate multi-million-dollar fraud. Similarly, in Britain, credit card companies have made several security changes that have prevented millions of pounds in fraud. The private sector is more effective in fighting transnational crimes such as smuggling, extortion.

## ***Conclusion***

“Don't shrink from a new technology just because it could be abused by criminals. » These traditional crime prevention techniques are not effective in controlling criminals using emerging techniques to commit new crimes making them difficult to detect. The purpose of this study was to investigate the impact of technology on crime and how it has contributed to the development of new techniques in crime investigation and law enforcement. The use of new technology to commit crimes is not a new phenomenon and all the advancements in technology are always providing offenders with new ways to engage in illegal activities. Due to the anonymous nature of the internet, it is possible to engage in various criminal activities with impunity. Smart people have been brutally abusing this aspect of the internet to spread criminal activities on the internet. Internet privacy is another debated issue in cyberspace. We should look to the future and find new techniques for crime prevention. The changing environment makes a big contribution to criminal activities, but it also creates new opportunities for crime prevention. The new challenge ahead is the use of new techniques in crime control.

## ***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)