The Impact of Technological Advancement on Policing Driven by the Sophistication of Crime

Shashidhar S. Galimath
Assistant Professor in Hurakadli Ajja Law College, Dharwad, Research Scholar in P.G. Department of Studies in Law, Karnatak University Dharwad, Karnataka, India

Abstract

Police is bound to maintain law and order. It is responsible for the protection of citizens life, personal liberty, dignity and public property. To fulfil these duties Indian police has his authority from Indian Police Act, 1861, Indian Penal Code, 1860, Criminal Procedure Code, 1973, Indian Evidence Act, 1872 and many more legislations passed by State and Central legislations with the framework of Indian Constitution. The Information Technological (IT) Revolution brought tremendous negative changes where crimes and criminals become more sophisticated but unfortunately, the Indian Police administration remains woefully technologically inadequate, failing to adopt the same IT related sophistication to the Indian Policing System.

KEYWORDS: Information Technology, Indian Policing System, Traditional Crimes, Cyber Crimes, Digital Policing, Forensic Scientific.

Traditionally,police is a government agency responsible for maintaining law and order. It is responsible for the protection of citizens life, personal liberty, dignity and public property.As an executive body of the government it maintains internal security by minimising crimes, booking and investigatingthose committed, and keeping concerned authorities informed. In addition, the police force has the authority to take necessary measures to avoid future crimes.The police is responsible for the protection of private and public property including roads, canals, wells, bridges, different establishments and basic institutions like hospitals, schools, government offices and more from internal aggressions or terrorist activities. Maintaining and creating communal harmony and a feeling of security in the community are basic responsibilities. To fulfil these duties Indian police has his authority from Indian Police Act, 1861, Indian Penal Code, 1860, Criminal Procedure Code, 1973, Indian Evidence Act, 1872 and many more legislations passed by State and Central legislations with the framework of Indian Constitution.

Indian Penal Code, is the main criminal code drafted in 1860. This code classifies crimes in to different category such as cognizable non-cognizable, bailable, non-bailable, offences against State, offences again individual, offences against property, offences against human body along with intention or without intention, and in some cases mere preparation is also amounts to fine. Accordingly, police have to take action against the accused person and file complaint, start investigation and file a charge sheet as prescribed under Criminal Procedure Code.While prosecuting he has to submit Evidence as prescribed under Indian Evidence Act. This process describes how the police administration generally functions in India, and has been doing so for the last ten to fifteen decades with very few modifications.

As stated by Alvin Toffler,[1] "Change is the process by which the future invades our life." Changes in technology invaded police functioning when the British introduced, railway, postal, telegraph and telephone facilities in India. These services were under the control of the British rulers and used effectively to repress the 1857 Sepoys Mutiny. These technologies helped the British administration rule efficiently for long time.

Similarly, after gaining independence, India is began to move purposefully towards globalization. The Information Technology (IT) Revolution has parallelly brought tremendous changes as well. While most changes were positive, an alarming development was the increase in sophistication of crimes. Unfortunately, the Indian Police administration remains woefully technologically inadequate, failing to adopt thesame IT related sophistication to the policing system.

The Indian police is trained to deal with low-tech, rudimentary crimes, but today, crime is pushing the boundaries of our legislations, demanding the modification of definition and the laws that are responsible for policing. Simply implementing new laws, writing new definitions, or expanding the scope of words is not sufficient.The executive machinery need reform to enable the Police to deal with more technologically crimes.

In today's connected world people are more reliant on mobile connected device. Our day to day activities are closely connected and administered by computers, and the use of internet. This creates new challenges in the form of cyber-crimes: an emerging threat that the current Indian police system is not equipped to adequately handle. In today's world, "Traditional Crimes" and "Organized Crimes" combined with IT become aneven more dangerous threatto law and order, life and liberty of individuals and society at large.

Traditionally, homicide means one person kills another physically. Now, under the umbrella of cyber homicide,additional manners of crimes are emerging. Criminals can use fictitious names in social networking sites to befriend and harm victims.[2] Internet mediated homicide also includes Internet suicide, as the example Blue Whale Challenge game that tookmany lives in India showed[3]. Hacker criminals have also been known to modify patients' medical protocol, resulting in patient death.[4]For example, cyber homicide can be committed by hacking a pacemaker to kill a man.[5]As technology changes, and criminals continue to have access to it, crimes will be committed in more manner than we can even imagine today. The Police need to be adequately prepared and equipped to handle such advancement in criminal activity.

Recording and storing data is an important aspect of developing IT. Storing information in a legal manner is important. Using stored personal information for any illegal purposes or gaining access to stored personal information database through hacking for the intent of committing illegal activities are classified as cybercrimes. Such crimes violate individual right to privacy which is protected under Article 21 of Indian Constitution, and can also be described as identity theft. In cybercrime terminology "Date theft", expands the previous definition of 'Theft', which was limited only to movable property and data.[6]Previously, unauthorized acts with date were not considered theft to deal with such acts and this requires certain provisions to be made in Indian Penal Code, 1860, Information Technology Act, 2000 and The Copy Right Act, 1957. These Acts define crimes and modes of punishing those crimes but

unfortunately, the system does not support adequate training for the police authorities that would enable them prevent such offenses in India.

Like theft, traditional crimes such of Robbery, andblackmail are also reforming under cybercrime and can be re-branched as Identification theft.[7] Ransomware attack[8], Hacking[9], Spamming[10], Email Scams/fraud[11], Phishing Scams[12], Malwares development[13], Email Bombing[14], Virus Dissemination[15] and more. Often, these are different modes to commit Financial crime.

Electronic Money Laundering[16], is another recent mode of cybercrime where money generated in large volumes by illegal activities must be "laundered," or made to look legitimate, before it can be freely spent or invested; otherwise, it may be seized by law enforcement and forfeited to the government. Transferring funds by electronic messages between banks "wire transfer" is one way to swiftly move illegal profits beyond the easy reach of law enforcement agents and at the same time begin to launder the funds by confusing the audit trail.[17]

Cyber piracy is the illegal copying, distribution, or use of software, books, movies, songs and other forms of copyrighted data or media.

Defamation was defined and punishable under section 499, 469, 503 of Indian penal code but when such defamation takes place with the help of social media it can be redefined as cyber defamation. In this manner, there are countless types of emerging cybercrimes that will need to be redefined under Indian penal code, including theft, fraud, cheating, trespassing, criminal breach of trust, infliction of bodily harm, culpable homicide, even when not amounting to murder, criminal conspiracy and many more.

Another threat to the working process of the Indian Police administration is the exploding use of mobile connected devices by minors. Downloading and transferring songs, movies, photos, software, games, and other media is a popular and growing trend. Minors take part in such activities without being aware of its illegality. Similarly, social media platforms such as Facebook, Twitter, Orkut, Instagram, YouTube, WhatsApp, are used by the minors extensively.This leads the vulnerable minor population open to exploitation. Media that minors have access to can also be inappropriate (sexually or physically violent) for their age. Policing access and protecting minors is a challenging issue for the Indian Police today.

The Information Technology Act, 2000 which came in to force on 17th October, 2000 was written to equip the administration for cybercrime. The Information Technology Act deals with hacking, or tampering electronic documents, e-publishing of obscene information, child pornography and breach of confidentiality & privacy.Cybercrime other than those mentioned under the IT Act include cyber stalking, cybersquatting, data diddling, cyber defamation, Trojan attacks, forgery, financial crimes, internet time theft, virus/worm attack, E-mail spoofing, Email bombing, salami attack and web jacking and many more.

Under the Information Technology (Amendment) Act, 2008 offences were included under civil prosecution and criminal prosecution. The Act also punishes a network service provider or an intermediary if theycan be held liable for known misuse of third party information or for not exercising due diligence to prevent the offence. Therefore, Indian companies may be liable as a network service provider as they receive and transmit data. The Information Technology Act 2000 is transborder, and applicable to offences committed outside India,

irrespective of the nationality of an offenders while the computer system or network is physically located within India's geopolitical borders.

The Copyright Act 1957 was enacted to protect the interest of Intellectual Property Rights of a person which includes rights in literary, dramatic, musical, artistic and cinematographic works. Therefore, copying and distributing a database amounts to a breach of copyright for which civil and criminal remedies can be initiated.

Across cybercrimes, one commonality is that offenders are well educated, with working knowledge of science and technology. However, the Indian police lacks such technological competency, or systems of training to reach such competency. The few officers with such knowledge work in higher ranks, and the working knowledge they have is often outdated.They are also unlikely to have gotten financial or technical support from the government to gain their tech-competency. Expecting the police system to respond appropriately to cybercrimes without the funding to support resources or training to do so, amounts to tyranny.

Cybercrime is a global threat. The criminal and victim need not even be in same country. With differing jurisdiction across borders, crimes in one country may not be classified as crimes in another. This inconsistencies in law provide loopholes for the cyber offenders to escape punishment. Another hurdle in dealing with cybercrimes is detection and prosecution.Some criminals can hide behind technologically advanced firewalls built with finesse and a high level of expertise.[18]Such technological walls and boarders can be stronger than physical ones and though, police may locate the physical computer or the device from which crimes were committed, it is incredibly difficult to determine the individual responsible for the crime. Prosecuting and collecting evidence against the criminal to prove beyond all the reasonable doubtthat he is responsible is next to impossible task in the current Indian adverbial system. The prosecution is still not fully ready to deal with cybercrimes, and hesitate to accept electronically based evidence due to concerns around, quality of forensic labs, efficient preparation and delivery by qualified persons, accurate tracking of data, admissibility of such reports in court, less stringent data analysis and statistics amongst others.[19] Therefore, for effective handling of cybercrimes, policing requires active cooperation at an international level from all countries with uniform globallaws. These laws should build a system and process that is nimble and responsive to the fast-developing world of IT.

Mobile connected devices are no longer considered luxuries. So, to monitor crimes taking place that use such devices, the police system needs to modernize as well. Indian Policing cannot be improved until modern technology is widely adapted across the police organizations. Modern technologies not only facilitate better management, supervision, control, accountability but also provide better professional, democratic Policing which is a dire need for India and the Indian police image.

The National Crime Record Bureau's Report of 2016 shows that there are more than 17 lakh cases registered in Indian in 2016 alone, with respect to crimes falling under IPC[20]. Section 154 of Criminal Procedure Code authorizes the Indian police to receive a First Information Report about a cognizable offence at a police Station. This First information report is the basic requirement to initiate police functioning. This involves six basic issues: What is the nature of incident, Where and When did the incident happen.Who is reporting and

against Whom and Why did the incident occur.[21] These basic six **W**'s initiate police investigation, and every police station in India has a police constable in charge who will write the complaint as stated by the victim or otherrelevant person. This registration of FIR takes near about 15 to 90 minutes depending upon the nature of the crime. The recording of FIR is mechanical and easily be computerized, minimizing human interaction.Using an unbiased software system would allow more accurate, less manipulatedinformation to be collected from the victim or a concerned person. The individual may be more open to providing situation details as needed in a private environment, as opposed to verbally reporting to a stranger. This additionally, reduce the time and resources required for manual entry in paper work. Though literacy and comfort with computers is widespread, a small population of rural users may find this system less preferable than reporting to a physical constable.

With this in mind, the India government initiated a "Digital Police Force" where any person can file a criminal case and provide associated information such as property stolen / recovered, missing persons, recovered / unidentified dead bodies and so on. This information would help expedite Police investigations to solve crime as well as to provide antecedent verification services to citizens. Today Government of India started "www.digitalpolice.gov.in" web site to initiate digitalizing and computerizing the police system in India.Following this initiative different State governments launched similar websites. (examples include Bangalore: www.bcp.gov.in, Mumbai: www. mumbaipolice.com) While these are noble initiatives, their usability remains unclear. Working computer knowledge of police personnel, availability of staff, availability of working computers, access to electricity and Internet connection, availability of printers and related paraphernalia are challenging operational and implementation issues for the Indian police. As stated by Dr. Arvind Kumar, a former IPS officer, in his book, "The Indian Police, A Critical Evaluation,""there is not even one single police station that is completely computerized"as of 2018 "and to this day almost all data management in the police organization is manual." There are a number of villages in India where there are no police stations at all. There several police stations where police authorities do not have vehicles for patrolling, and if they do, they may not be operational, and if they are operational, they may not contain fuel due to lack of funding or availability. Many stations do not have connected, working, telephones and across India, there are often challenges regarding scarcity of police staff.

After registration of FIR police have to start investigation where police collect, information from the witnesses, informants, citizens, law enforcement individuals and other professionals. Furthermore, information obtained from physical objects like weapons, clothes, bodily fluids, and other particulars are significant pieces of evidence vital to the success of the case. A diary is kept that records the stages of the investigation and all the collected evidences.This record can easily become 45-50 pages. Thus, even a single criminal case generates vast amounts of data. In addition to the primary stage of information collection, there are citizen complaints, general information and material objects brought to and from the police stations. All these involve additional record keeping ranging from the station diary entries to *malkhana* (Seized or recovered property) registers. For the proper supervision and functioning of the police station these records must be up to date. All these records are also inter-

connected and each has related entries that indicate corresponding information in other record books. All these records are to be kept at the station for a long period of the time, at least until theresolution of a case which may take 10-15 years.[22] In such cases, computerized documentation would be space efficient, protected from natural disasters and easily searchable and cross referenced. Software built specification for police authorities could enable efficient record keeping and updating, saving time and labour cost. However, this either requires the use of the services of a specialized, third party software company, or internal specialised police labour force development, the latter of which is impractical under the current system set-up for hiring, training and developing police personnel. The software system built would need to be capable of connecting across station and departments, using the internet for the safe and efficient transfer of information: for example, within a station- between departments, from stations to headquarters, from stations to court and vice versa. These tasks are currently handled manually leaving them open to interception, delay, and loss of information. The use of IT can reduce the time and labour burden of paper work, relieve the responsibility of maintaining voluminous records and save on mail distribution duty. The police department has numerous periodical reports, inspection report and statistical data analyses which have to be sent to superiors, the Government or other agencies like Courts, Legislature, State and National Human Rights Commission, etc. Every district prepares a monthly crime and administration report. At least five officers and staff at each police Station, and Sub Divisional Police Offices remain busy for the first ten days of every month with these reports. The District Crime Records Bureau uses 6 to 10 officers and staff (depending up on the crime workload) for the next one week for compiling, verifying and consolidating the report. Yet human error cannot be eliminated and the SCRB finds it difficult to reconcile the data received from the police districts and Commissioner's. Use of IT can certainly expedite this process.

Innovative ways of reducing workload in the police Department through digitalization will be cost effective in the long term, after initial set-up costs are absorbed. Costs aside, the system would enable the improved effectiveness of the police force. As IT changes all of India, the Indian Police cannot afford to fall behind the progress of the nation. Computer literacy will be the first step towards digitalizing the Indian Police, and bringing them into the 21st century.

As discussed, the collection and analysis of vast amount of data is integral to police work, their efficiency and their performance. The force could be considered and institution for an information generation, processing and dissemination. Information recorded pertaining to criminal violation, order maintenance, conflicts of various nature and citizen police interactionscan be overwhelming. All these factors play vital roles in crime mapping. Crime mapping is used by analysts in law enforcement agencies to map, visualize, and analyse crime incident patterns. It is a key component of crime analysis and the CompStat policing strategy[23]. Mapping crime, using Geographic Information Systems (GIS), allows crime analysts to identify crime hot spots, along with other trends and patterns.[24]These maps have generally served the purpose of showing, at a glance which areas have been affected and where serious crimes are taking place. In addition, crime maps have been useful in planning preventive measures to combat crime.

Surveillance is one of the most important techniques in criminal investigation wherein police asks questions to the people connected with the suspects or follow the physical movement of a specific person.While performing police duties and during investigation, police officials have to remain vigilant of their surroundings. However, at the end of the day, the police official is a human being, prone to distraction, negligence and human error. For those reasons, technological developments to assist with surveillance are particularly useful. Surveillance during investigation includes monitoring of behaviour, and can utilised for influencing, managing, directing, or protecting people. Examples of such technologies includes Electronic message (e-mail) monitoring, wiretapping, use of Closed Circuit Television (CCTV) Camera, Drones, GPS, License Plate Readers, Mobile Phones tracking, fax tracking, and tapping of telephonic communications with the prior permission of appropriate legal authorities with in the frame work of the law. Using such techniques may reduce the risk of life of undercover officers. At the same time this may help the police dependency on the witness.

In 2016 alone, there were around 5 lakh cases registered with respect to motor vehicles theft. Surveillance using previously mentioned technologies can help police maintain traffic monitor areas prone to vehicle theft, prevent crimes from occurring, or effectively nab criminals.

Technological innovations develop daily and numerous examples are not mentioned here. The implementation of mentioned technologies and the future adoption of those yet to be developed can transform the effectiveness of the Indian Police. There are several advanced forensic scientific methods including, biometrics, fingerprints, DNA research, facial recognition, speech recognition, social media policing, ShotSpotter detection system, high-performance liquid chromatography (HPLC), mass spectrometry for partial detection, 3-D computer recreation and imaging, ballistic photography, brain Fingerprinting, Narco-Analysis and many more.

Compared to other countries, the rate of adoption and use of scientific and technologically advanced techniques for the purposes of law enforcement in India are low. This negatively affects the administration of criminal justice. There is a dire need for reform. The government needs to see this need for technology in everyday police operations, and encourage the incorporation of such innovations, even if not for efficiency improvement, but for the sole purpose of simple functioning of the Indian police system in the 21st Century.

References:

[1] Alvin Toffler (October 3, 1928 – June 27, 2016) was an American writer and futurist, known for his works discussing the digital revolution, communications revolution, corporate revolution and technological singularity.

[2]https://www.lifedeathprizes.com/real-life-crime/killers-who-met-their-victims-online-internet-murder-52318 (Visited on 24th August 2018 at 6.31 P.M.)

[3]https://indianexpress.com/article/india/blue-whale-challenge-these-are-the-suspected-cases-india-4798745/(Visited on 21th August 2018 at 9.31 P.M.)

[4]https://www.wired.com/2013/04/charles-cullen-hospital-hack/(Visited on 2nd June 2018 at 11.31 A.M.)

[5]https://www.computerworld.com/article/2981527/cybercrime-hacking/researchers-hack-a-pacemaker-kill-a-man-nequin.html(Visited on 9th July 2018 at 10.31 A.M.)

[6]Section 3 of The General Clauses Act, 1897 defines Movable Property and Immovable Property as, "Movable property" mean property of every description, except immovable property. And "Immovable property" shall include land, benefits to arise out of land, and things attached to the earth, or permanently fastened to anything attached to the earth.

[7]Identity theft is one of the most common types of cybercrime. The main reason identity theft occurs is with the view of creating fraud for financial gains. Criminals usually steal identity information of others such as credit card information, addresses, email addresses and more. With this information they can pretend to be someone for financial or monetary gain. This includers your id, password, finger prints, or any kinds or unique identification date.

[8] Ransomware attack is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called crypto viral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

[9] Hacking generally refers to unauthorized intrusion or a tress pass into a computer or a network by identifying weakness in the computer system. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.

[10] Electronic spamming is the use of electronic messaging systems (E-mails, advertisements etc) to send an unsolicited message (spam), and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. The term spamming is also applied to other media like in internet forums, instant messaging, and mobile text messaging, social networking spam, junk fax transmissions, television advertising and sharing network spam.

[11] Email scam or fraud is the intentional deception made for personal gain or to damage another individual through email. It is an unsolicited email that claims the prospect of a bargain or something for nothing. Some scam messages ask for business, others invite victims to a website with a detailed pitch. Such emails usually targets naive individuals who put their confidence in get-rich-quick schemes such as 'too good to be true' investments or offers to sell popular items at 'impossibly low' prices. Many people have lost their life savings due to fraud.

[12] Phishing scams are attempts by scammers to trick victims into giving out their personal information such as bank account numbers, passwords and credit card numbers. These scammers will contact victims out of the blue, via email, text message, phone call or even through social media, pretending to be a legitimate business such as their bank, telephone company or even internet provider. The scammer may ask them to update them on their details so they can refresh their systems, they may even ask to fill out a survey as victim have the chance to win a prize at the end. But here is where the scammer can get access to email address, phone number and more. Another way these scammers get hold victims information by tell that ‘unauthorised or suspicious activity has been happening in their account’, and they will then ask there information so they can “sort it out”. This is nothing but the modes of identity theft.

[13] Malware is a piece of software written with the intent of causing harm to data and devices. Malware is the overarching name for different types of viruses such as a 'trojan' and 'spyware'. it often done through a range of viruses that will get into the computer to cause havoc, by damaging computer, tablet, phone; so the culprits can steal credit card details and other personal information.

[14] Email bombing is an overload of emails directed to one email address, this will cause the person receiving the emails server to become sluggish or even crash. They may not necessarily be stealing anything from you but having a sluggish server can be a real pain and hard work to fix.

[15] This is particularly sneaky form of cybercrime. It not only gets a piece of malware (a virus of some sort) onto one part of the victim's system, but it spreads across other pieces of software.

[16]It is nothing but digitalizing money laundering.

[17]https://www.memresearch.org/grabbe/02ch1.pdf(Visited on 9th August 2018 at 1.31 P.M.)

[18] Just for an example "Data protection" and "Database protection" under the copyright Act., are different issues because, Data protection is aimed at protecting the information privacy of individuals, while database protection has an entirely different function, namely to protect of the creativity and investment put into the compilation, verification and presentation of databases.

[19] Gerald L. Kovacich, William C. Boni, *High-technology-crime Investigator's Handbook: Working in the Global Information Environment*, (Butterworth Heinemann Boston Oxford, USA, 2000, First Edition) p-xiii.

[20]http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf(Visited on 9th August 2018 at 1.31 A.M.)

[21]https://www.thehindu.com/features/the-yin-thing/all-you-must-know-about-the-fir/article5260951.ece(Visited on 4th May 2018 at 12.31 A.M.)

[22]Arvind Verma, *The Indian Police A Critical Evaluation*, (Regency Publications, New Delhi, 2005, First Edition), p-229

[23]COMPSTAT stands for Compare Statistics, which was the computer file name of the original program) is a combination of management, philosophy, and organizational management tools for police departments.

[24]https://en.wikipedia.org/wiki/Crime_mapping. (Visited on 19th April 2018 at 7.31 A.M.)