ISSN:0975-9646

Utilizing ICT to Fight against Crime: Emerging ICT Tools, Forms of Crime and Its Solutions

Ramandeep Kaur, Neeru Sharda

D.A.V College,
Jalandhar

Abstract-Malefaction, policing and security are enabled by and co-evolve with technologies that make them possible. As malefactors compete with security and policing officials for technological advantage perpetually intricate malefaction, policing and security results in relatively perplexing and therefore unmanageable threats to society. Incipient, adaptive and mundane malefactions emerge over time to engender technology malefaction waves, the magnitude of which can theoretically be quantified, compared and presaged. These principles underscore an incipient theory of technology-enabled malefaction, policing and security pertinent for understanding contemporary threats posed by emerging forms of cybercrime, transnational malefaction and terrorism networks that defy traditional methods malefactor equity and security measures for averting and controlling malefaction. The exordium of Information and Communication Technologies (ICTs) are rapidly transmuting the way of public interact not only with each other but withal with private businesses, regime institutions. ICT in policing make possible the accumulation, storage and rapid dissemination of information, it upgrades public safety and reduces malefaction. This research paper is an attempt to focus shadow on the various forms of crime and assess the ICT tools available to law enforcement. These technologies work as force multipliers that amend efficiency, efficacy, and officer safety in a variety of ways.

Keywords: **ICT, Crime, Policing and Security**

I. INTRODUCTION

The global nature of the Internet has sanctioned malefactors to commit virtually any illicit activity anywhere in the world, making it necessary for all countries to habituate their domestic offline controls to cover malefactions carried out in cyberspace[1]. The utilization of the Internet by bomber, particularly for recruitment and the incitement of radicalization, poses an earnest threat to national and international security.

More and more malefactors are exploiting the speed, accommodation and anonymity that modern technologies offer in order to commit a diverse range of malefactor activities. These include attacks against computer data and systems, identity larceny, the distribution of child sexual wrong images, internet auction fraud, the penetration of online financial accommodations. The following figure [2] illustrates this concept. These considerations must be borne in mind along with the aforementioned cost and malefaction risk assessment issues so that the engenderment and selling of a malefaction-proof product remains feasible and provides a viable business model.

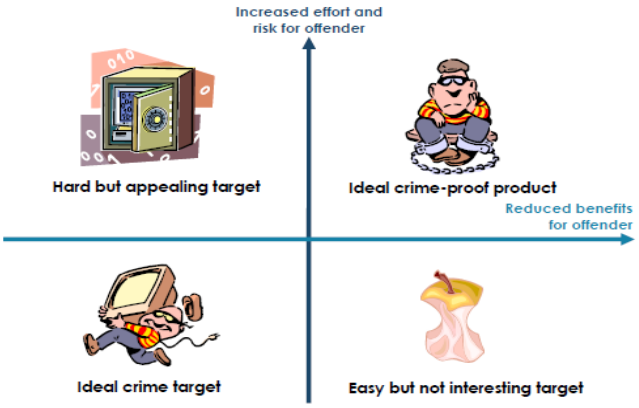

Figure 1 Crime Proofing

The objective of this paper is to assess the ICT implements available to law enforcement institution to fighting malefaction. The study revealed that, Africa is yet to capitalize on this everyday technology such as CCTV technology, tracking technology, gregarious media and mobile phone. The malefactors have gone high tech, and the solution is a coordinated approach in utilizing ICT to fight malefaction.

II. TECHNOLOGY AS CRIME, POLICING AND SECURITY

Cunning malefactors have always capitalized on incipient technologies often as the result of learning how to do so from other people including fellow malefactors. Periodically they experiment with subsisting implements or techniques in order to develop a copacetic modus operandi with which they are comfortable and believe gives them plausible advantages over the security technologies of aimed targets, as well as police who may be tramp about physical and cyber environments for denotements of malefaction.

Malefaction as gregarious technology will virtually always involve utilization of physical technologies (i.e., implements), albeit rape, assault, and murder committed without the utilization of weapons or other instruments such as those used to penetrate body cavities are eminent exceptions[3]. Conceiving of malefaction as social technology incorporating utilization of physical technologies sanctions for construction of a matrix, differentiating as depicted in the following figure: (1) simple malefaction committed utilizing simple implements; (2) simple malefaction committed utilizing intricate implements; (3) intricate malefaction committed utilizing simple implements; and (4) intricate malefaction committed utilizing intricate implements.

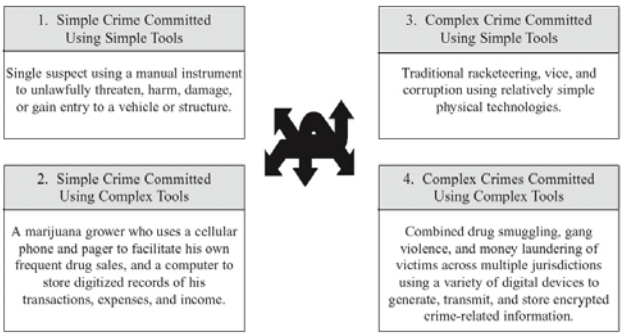

Figure 2 Simple-to-complex crimes committed with simple-to-complex tools

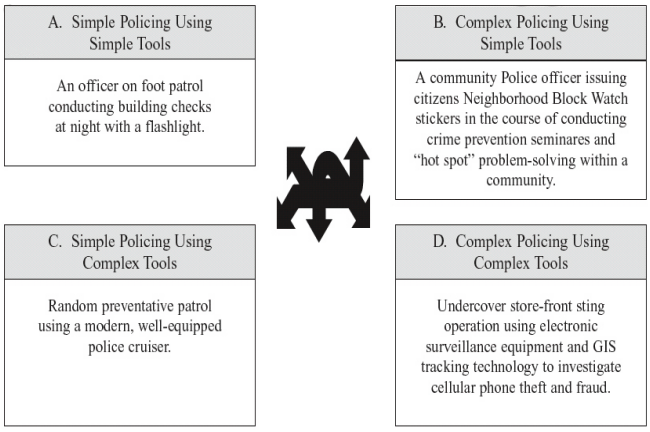

Figure 3 Categories, interplay, and examples of simple-to-complex policing methods and physical technology

Community policing emphasizes problem-solving in partnership with community members to enhance crime prevention methods may be conceptualized as a social technology[2]. Obviously security and policing technologies are also physical and range from being relatively simple to complex. Thus, akin to crime as technology, the give-and-take of simple-to-complex policing or security methods and tools such as described by the examples in Figure 2 are also social technologies that are bound only by human ingenuity.

Figures 1 and 2[3] represent conceptual analogues of malefaction and policing/security which coalesce implements and techniques (or methods) into practical functions that are subject to transmute as incipient technologies. For example, a sniper might first learn to shoplift utilizing her purse for concealment, and later graduate to purloining from multiple victims utilizing a computer. Thus, and in reference to Figure 2, a Category 1 malefaction might evolve into Category 2, then into Category 3, and finally Category 4 malefactions with corresponding increases in technological intricacy.

Thus, Malefaction and policing/security are technologically competitive enterprises that are inextricable, dynamic and co-evolving. Malefactor innovations drive policing and security innovations, and by expansion each perpetually co-evolves the other throughout time and society. Malefaction and methods for obviating it via security and policing evolve together as a function of these factors plus human ingenuity. But as long as the security officials and police are winning the complete game, there is relatively little cause for alarm. Yet, when it comes to keep a safe, secure and orderly society, security and police forces utilizing their technological capabilities must ultimately triumph over malefactors.

III. TYPES OF ICT CRIME

The first step towards achieving an efficacious ICT product proofing methodology is to acquire an exhaustive cognizance base of the malefactions committed, and of the techniques available to combat them. Thus cognizance of the subsisting techniques of combating malefaction and fraud, as well as becoming habituated with the discipline of malefaction aversion, would be subsidiary for ICT security professionals. This segment presents types of ICT malefaction and some of the countermeasures adopted.

I. Fixed Line Telephones

1. DISA (Direct Inward System Access) Fraud

Where the fraudster obtains information (for example a password) that is mundanely used legitimately by telecommunications workers, in consideration to make frugal calls via their Private Branch Exchange (PBX) connection **[2].**

Solutions:

- Enable automatic logging of calls if available.
- Customarily check the log records for reiterated short duration calls to the same number. This could be a designation of an endeavor to assail the system.
- Personal Identification Numbers (PINs), if enabled, be activated and transmuted customarily.
- If possible engineering entry should only be approved on a 'call back' substructure; this will obviate unauthorized access to this privileged account.

2. Premium Rate Service (PRS) Fraud

In some instances a fraudster can endeavor to make utilization of the accommodation without paying for it. In other cases the PRS numbers may be dialled willfully, in a fraudulent manner, by the same person that established the PRS reconciliation. The aforementioned is a rather facile form of fraud since often the acquiescent between the operator and PRS provider states that a quota of the earnings will be due to the PRS provider, whether or not the operator is able to amass from the caller. This is because the PRS accommodation provider is unable to ascertain that all callers are legitimate **[4].**

3. Clip-on Fraud

Where the fraudster taps into a subsisting telephone line and can therefore communicate without being charged**[4]**

4. Calling Card Fraud

The swindler accesses the calling card details from the victim by a variety of betokens. They then utilize those card details to make their own calls **[4].** An apparent solution is for the caller to eschew displaying their calling card details.

II. Mobile Phones

1. Subscription Fraud

Subscription and surfing fraud are sometimes identified as the most prevalent types of fraud relating to telecommunications **[5].**

Subscription fraud occurs when a fraudster utilizes a mendacious or fake identity to gain access to an electronic accommodation, for example to obtain a subscription to a mobile phone. Since bogus identification documentation is utilized to establish the account, the bill efficaciously peregrinates to no-one and will never be paid, being absorbed instead by the company supplying the phone. The intention is to make costly phone calls, either for personal use or to engender income from a cognate Premium Rate Accommodation

Solutions:

- Credit worthiness checking software
- Cross-checks to external databases
- Biometric subscriber verification (voice apperception would be suited to this
- example)
- "ProFile", an intercarrier database of accounts-receivable, indite-offs and accommodation shut-offs that provides on-line pre-screening of potentially fraudulent applicants. Helps identify applicants with a history of lamentable debt.
- "InSight", a customer database that carriers scan for anteriorly qualified applicants to eradicate the re-qualification process.

Surfing fraud is where a service is utilized and charged to the account of an unsuspecting payee who has an account. In this scenario the body does exist and so they get the bill for the services utilized by the fraudster.

2. Roaming fraud

Running up bills outside the home network (while 'roaming') with no intention of paying.

International roaming fraud is arduous to detect. Subscription fraud can be put into action to obtain mobile phones in one country, and then to dispatch them for use elsewhere. In the alternative countries, the telephones may run up high rate and premium rate roaming call charges, and the authority of a phone can be more arduous to check when it is utilized in a country far from its home network. As a result, such misconduct is estimated to run into billions of Euros.

Solution:

- Fraud Information Gathering System (FIGS) sanctions the network that roaming subscribers are entering to amass information about their action. The network then sends this data info back to the home network of the subscriber, which can later clear certain kind of calls and avert fraudulent utilization of the system [6].
- Computer systems which speed the cross-checking system utilizing neural network-predicated detection algorithms have the potential to expedite the checks, detect and deter such fraud. In some cases it has been noted that detection system speeds detection time by 50% and reduces fraudulent losses by 50% [7].

3. Cloning

Mobile phone cloning involves facsimileing the identity of a mobile phone into another mobile phone, so that any calls made by the clone are billed to the account of the facsimiled phone.

Solutions: *Smart cards*

4. Theft of sensitive data

The malefaction in this case is self-informative. Sensitive data may comprise location information, identity-cognate information and the like.

Solutions:

- GSM and UMTS provide anonymity by utilizing ad interim identifiers when the feature is activated. When a utilizer first switches on the mobile contrivance, the authentic identity is utilized and an ad interim identifier is then issued. From then on, the ad interim identifier is utilized, until the network requests the authentic identity again. Only by tracking the utilizer is it possible to determine the ephemeral identity being utilized.
- For authentication and signalling aegis ETSI has developed three security algorithms for GSM. The A3 and A8 algorithms are concrete to the operator and are preserved on the SIM card and in the authentication centre. A5 is preserved in the mobile equipment and sanctions for data encryption and decryption over the air interface. Verification is performed by a challenge and replication mechanism.

5. Mobile Phone Theft

The crime in this case is self-informative.

Solutions: The GSM standards engendered by ETSI include the definition of a system (additionally adopted in UMTS) to obviate handset larceny predicated on a handset identity number called the International Mobile Equipment Identity. This is a unique number attributed during handset manufacturing, certified by the Mobile Network Operator and held electronically on the mobile phone. MNOs may utilize the IMEI to blacklist mobile equipment that is reported purloined.

6. Accounting Fraud

A more conventional fraud, often involving insiders, where charges are reduced or discounts fraudulently claimed for mobile phone accommodations. This malefaction is applied to mobile technology, but does not compulsorily utilize the technology as an instrument.

Solutions:

- Use audit authenticates the systems
- Separation of obligations for employees
- Job rotation of employees to evade collusion

III. Internet

1. Hacking

A hacking attack can be defined as [8]: "a series of intentional steps taken by an assailer to achieve an unauthorized result".

S.No.	Types of Attack	Attack Variation
1.	**Denial of Service**	• Local process degradation • Local disk space exhaustion • Network client side aimed at a particular product • Network client side aimed at a particular service
2.	**Information Leakage**	• Service information leakage e.g. via error messages • Protocol information leakage e.g. via a system query command • Leaky by design e.g. SNMP • Inherently leaky e.g. some web design tools
3.	**Regular File Access**	• Changes of permission • Symbolic link attacks
4.	**MisInformation**	• Create conflicting entries • Malicious kernel modules
5.	**Special File/Database Acess**	• Special files such as Run As in Windows 2000 can allow unauthorized users to log on as someone else. • Data base files: attack through Web interfaces, inherent database software vulnerabilities and weaknesses in permission regimes
6.	**Remote Arbitrary Code Execution**	• Usually prefaced by information gathering attack, uses automated tools to gain local administrative access
7.	**Elevation of Priviliges**	• Remote unprivileged access through, for example, Web interfaces • Remote privilege access exploiting operating system weaknesses

Table 1 Various forms of Hacking [8]

2. Cyberstalking

In cyberstalking, the victim is hassled and threatened by unwanted e-mail and messages posted on bulletin board accommodations by people with whom they have interacted on the Internet [9].

3. Content Theft

Content larceny relates to file sharing networks for music and video; facsimileing, sharing of software; ripping CDs and DVDs liberatingly available via the Internet.

Solutions:

- Encryption obviates intercepted content from being used or resold without the key.
- DRM (Digital Rights Management) sanctions only the purchaser of the content to view it, and averts copies being made.

IV. ICT TOOLS

From an ICT perspective ICT implements in fighting malefaction, is simple and has been implemented many times. Most malfunctions are not caught by things so out of the norm, most potential assailers and larcenists are fended off or caught by everyday technology utilized by everyday people.

1. CCTV Technology

Countries should install Closed circuit television (CCTV) cameras on public highways and in shopping malls and arcades. CCTV cameras can perpetually monitor what people do. CCTV is additionally utilized by the police to monitor road traffic[10]. These types of CCTV operations are acclimated to remotely monitor premises without having to have police officers engaged in long term operational surveillance. It can be utilized in emergence replication, patrol management, individual and conveyance tracking and gunshot detection. The Following figure3 illustrate the use of CCTV technology.

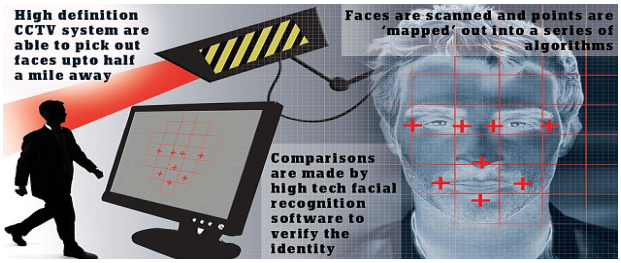

Figure 4 This graphic shows how the advanced CCTV technology works[11]

CCTV alone cannot reduce or detect the malefaction, but utilized in conjunction with other methods it can avail in the detection of offenders. The assets of CCTV are as under:

- Track the forms of kineticism of malefactors
- Locate victims of malefaction
- Identify potential witnesses
- Identify any suspects
- Provide corroboration for evidence
- Prove or deprecate alibis
- Help to determine the earnestness and context of any misdeed, particularly in court cases
- Monitor public order perturbances
- Cater surveillance of critical locations

2. Tracking Technology

In the past, GPS contrivances were immensely colossal, unwieldy and expensive. As a result, minority of the law enforcement agencies have access to them. Today, GPS contrivances can be engendered in minute packages that can be facilely concealed in a suspect's conveyance. Armed with these GPS contrivances, law enforcement agents can track suspects and utilize their locations as potential evidence. In additament, cell phones perpetually communicate with cell towers, and detailed logs can concede where particular individuals were located during particular periods of time. This information can be subpoenaed and utilized as evidence against alleged malefactors. Thanks to this technology, more malefactors are behind bars where they cannot commit further malefactions in many developed countries.

3. **Radio Frequency Identification:**
Radio Frequency Identification (RFID) is a gift of modern technology, which incorporates the utilization of electromagnetic or electrostatic, coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal, or person. This technology is utilized by the police ascendant entities so that conveyance systems can be verified to obviate kineticism of unauthorized materials which can affect the public safety[10].

Figure 5 Flow of Radio Frequency Identification

4. **Electronic Transport:**
The major activities cognate with the convey system can be handled facilely with the electronic contrivances. E-Convey aspect covers number of activities such as: registration of all types of motor transferences, Issue of driving certificate, Issue of Permits for the light and heftily ponderous communication, Tax and fee amassment through cash and bank challans and control of pollution through checking etc. Thus, electronically preserved data will be subsidiary for the efficacious traffic management.
5. **E-Identification:**
The Electronic Identity Card is a regime-issued identity card for online and offline identification. Apart from online authentication many EIDs additionally give users the option to sign electronic documents with a digital signature[12]. The EID has the format of a customary bankcard, with printed identity information on the surface as well as an embedded microchip. Police can find any person expeditiously to maintain security in the society with EID.
6. **Online Verification and Fingerprints Reader:**
A biometric check can identify an individual or authenticate identity. Identification has the capabilty to locate somebody in one-to-many probing. Authentication approaches to be more of a one-to-one application to substantiate that you are in fact the person who you represent yourself to be. Both of these terms apply to law enforcement applications. Police can authenticate the arrestee‟s identity and determine if that person has a malefactor record. A biometrics-predicated identification search may be obligatory if the arrestee has dissimulated his or her identity[12].
7. **Photo Enforcement Systems**
Photo enforcement systems automatically engender red light breaches and/or speeding summons and as a result greatly ameliorate safety for the motoring public. There are a number of trustworthy hawkers of photo enforcement systems available to communities. The IACP first endorsed the utilization of photo enforcement systems a decade ago. The essentials for establishing a photo enforcement system include good engineering practices, public edification, community involution, and program management.
8. **Automatic License Plate Recognition**
Technology now enables officers to check thousands of license plates per shift to determine if conveyances are glommed, if registered holders are wanted, or if there are constraints on registered owners' driver's licenses. The automatic license plate apperception (ALPR) system is an integrated camera-database technology. The system takes a image of the car license plate and then processes the numbers and letters utilizing optical character apperception software against a kenned database. Suspected "hits" are relayed to users either visually or verbally. This technology can be deployed in a fine-tuned position or as a mobile system. These can be mounted in patrol conveyances and used while moving. Mobile systems are often utilized in conveyance larceny interdiction, but as more databases are linked through ALPR systems, the data accessible from the systems will expand to include more information on conveyances and their owners.
9. **Diagramming Systems**
Thanks to amendments in computer technology, malefaction scenes and collisions can now be diagrammed in a matter of minutes, as distinguished with hours just a few years ago. The systems that make this feasible are highly precise and facile to utilize, and they engender astronomically professional-looking images for use in court or for further analysis.
The high terminus of diagramming technology is the state-of-the-art forensic three-dimensional scanner that utilizes a high-speed laser and a built-in digital camera to photograph and quantify rapidly a scene in the exact state in which the first responder secured it.
10. **Social Media**
It is a great way to distribute information, and news of malefaction can expeditiously spread across these networks. By distributing a surveillance camera image on gregarious media, law enforcement agents may be able to get tips as to the identity of the perpetrator. Convivial media can withal be a great place to apportion tips for eschewing perilous areas and tips for keeping safe against malefaction.
11. **Mobile Phones**
Modern systems can be accessed through astute phones and other mobile contrivances, which sanctions homeowners to get instant alerts about potential

property malefactions[3]. Another advantage of modern systems is that they can automatically vigilant law enforcement agents. Because of this, homeowners may not require to call the cops after a larceny has transpired; police officers may be able to respond while the malefaction is in progress.

V. CONCLUSION

The fight against malefaction requires a cohesive and coordinated approach fortified by vigorous ICT security system. In additament, the security agencies require support in the form of vigorous licit framework, vigorous base of cyber security experts with expertise in system administration, information security, penetration testing, security audit, forensic investigation, network administration and software development to deal with the future challenges of both conventional and cybercrime.

Today the battle against malefaction perpetuates, and law enforcement agents have more implements at their disposal than ever afore. To meet the authoritative ordinances of investigation as well as prosecution, the research recommends the utilization of these every technology (CCTV technology, tracking technology, gregarious media and mobile phone) which are not implements expensive to purchase, install and operate. Accordingly, this article did not fixate on why malefaction occurs, but rather how it may occur with deference to innovative utilization of technology. These issues are germane for assessing the technological nature, extent and potential threats posed by malefaction and terrorism, and likely for allocating resources for deterring, obviating, interdicting, displacing or otherwise controlling these convivially undesirable demeanors.

Malefaction today is borderless in nature and this makes malefactor investigations more perplexed for law enforcement ascendant entities. To efficaciously tackle malefaction, bellwethers of the countries need to learn from the steps taking by most developed countries in utilizing ICT combat malefaction.

REFERENCES

1. Balbir Kumar, "Role of Information and Communication Technology in Indian Police", *Gyan Jyoti E-Journal*, Vol 1, Issue 1, January-March 2012.
2. Charles Brookson, Graham Farrell, Jen Mailley, Shaun Whitehead and Dionisio Zumerle, "ICT Product Proofing Against Crime", *European Telecommunications Standards Institute,* February 2007.
3. Sam McQuade, "Technology-enabled crime, Policing and Security", *The Journal of Technology Studies,*August 14, 2014.
4. Walker, Wall.D.S. "Policing the internet: maintaining order and law on the cyber-beat", *The Internet, Law and Society*, London: Longman.
5. Bolton, R.J. and D.J. Hand, "Statistical fraud detection: A review", *Statistical Sciences*, Vol. 17, Issue 3, pp. 235-255, 2002.
6. C. Brookson and D.Zumerle, "Information Security Standardization – the ETSI Perspective", *Securing Electronic Business Processes,* 2006.
7. D.Lloyd, "International Roaming Fraud: Trends and Prevention Techniques", *Fair Isaac Corporation*, December 17, 2003
8. G. R. Newman and R.V. Clarke, "Superhighway Robbery: Preventing Ecommerce Crime", *Cullompton: Willan publishing*, 2006
9. H. Tavani and F. Grodzinsky, "Cyberstalking, personal privacy, and moral responsibility", *Ethics and Information Technology*, Vol. 4, Issue 2, pp. 123-132, June 2002
10. Vikesh Sethi, "Role of ICT in Police Force in India", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol 3, Issue 11, pp. 778-781, November 2013.
11. Anthony Bond, *http://www.dailymail.co.uk/news/article-2212051/Powerful-CCTV-cameras-track-faces-half-mile-away-breach-human-rights-laws.html[*Online], October 03,2012.
12. Henry Osborn Quarshie, " Using ICT to Fight Crime - A Case of Africa", *Journal of Emerging Trends in Computing and Information Sciences*, Vol 5, Issue 1, pp. 21-24, January 2014.
13. Alana Northrop, "Police Use of Computers", *Center for Research on Information Technology and OrganizationsUniversity of California, Irvine*
14. Gopal K. N. Chowdhary, "Emerging Challenges in Policing", *The Indian Police Journal*, October-December 2009
15. Hale, C, "Cybercrime: Facts & Figures Concerning the Global Dilemma", *Crime and Justice International*, 2002.
16. Henry Osborn Quarshie and Alex Martin Odoom, "Fighting Cyber crime in Africa", *Scientific and Academic publishing, Computer Science and Engineering*, Vol.2, Issue 6, October 2012