Prevention And Detection Measures Against Cybercrimes Attack

**Muhammad Muhammad Suleiman
School of Computer Application, Lovely Professional University, Phagwara, India
(+91) 8264436830, muhddkd@gmail.com

Abubakar Abdurrahman Anas
Department of Local Government Studies, School of Rural Technology and Entrepreneurship Development, Rano, Kano State Polytechnic, Nigeria.

Aminu Jafaru
Department of Social Development, School of Rural Technology and Entrepreneurship Development, Rano, Kano State Polytechnic, Nigeria.

Abstract

Over the years, Information and Communication Technology (ICT) has changed our lives, which in the past was impossible, and more so it has become an integral part of one's existence. More than half the world's population is digitally linked, and the direction it is moving is going to grow more. In India, for example, a transition of ICT implementation in virtually all fields. Nevertheless, ICT not only offers benefits, but it also has pitfalls in the context of cybercrime, at the same time. Cybercrime is emerging globally as a big threat in cyberspace at present. It affects all actors including government departments, industry groups, NGOs, and even a person. ICT and other emerging tools are now a valuable resource for reacting to threats, participating in patrolling hotspots, investigating hate incidents, tracking the success of staff, and several other tasks. Technologies such as CCTV, data mining systems, heat sensors, biometric identification, GPS tracking systems, the internet and communication systems are used to prevent, detect, investigate and prosecute crime in the police forces and security sector. The text concluded that many approaches for the identification and avoidance of these cybercrime attacks among us could be implemented satisfactorily because of the usage of ICT-based resources such as social media platforms, social networking sites, electronic transactions, computer collaborations, etc.

***Keywords**: Cybercrime; Hackers; CCTV; Detection; Password; Cybersecurity.*

Introduction

With the increased use of Information and Communication Technology (ICT) in society, there emerges a new form of crime in cyberspace, which is called Cybercrime. The cybercrime is different from any other crime happening in society. The reason being, it has no geographical boundaries and cybercriminals are unknown. Therefore, in the present time, cybercrime emerges as an important challenge for all countries including India. It is affecting all the stakeholders from government, business to citizens alike. In India, in the last few years, cybercrime is increasing with increased usage of ICT. Therefore, this article tries to study and analyze the cybercrime happening in India (States/UTs-wise) in the last five years. Further, it discusses some important initiatives of the Government of India, to overcome cybercrime in the country (Bhatt and Pant 2011), (Kumar 2010).

The first recorded cybercrime is believed to have taken place in 1820. This can be true with the fact that computers have existed in India, China, and Japan since 3500 BC. The modern computer started with Charles Babbage's analytical engine.

(Prasanthi 2015). That is not shocking because the abacus, which is considered the oldest machine type, had been around since 3500 B.C. Japan, China, and India. Yet the advent of digital computers started with Charles Babbage's analytical machine. Joseph-Marie Jacquard, a textile fabricator in France, produced the loom in 1820. This system has required a set of steps to be replicated in the weaving of special fabrics. It contributed to a panic among Jacquard's workers that their conventional jobs and livelihoods were under attack. They committed acts of sabotage to discourage Jacquard from using the new technology any further. This is the very first computer crime registered! Computers have come a long way today, with neural networks and nano-computing aiming to transform any atom in a glass of water into a device capable of running one trillion operations per second. Cybercrime is a phenomenon that has its roots in the increasing reliance on computers in everyday life (Subha.C, Kaviarasu.S 2015).

ICT and other emerging tools are now a valuable resource for reacting to threats, participating in patrolling hotspots, investigating hate incidents, tracking the success of staff, and several other tasks. In law enforcement, technologies like video cameras, data mining systems, heat sensors, biometrics, GPS tracking, and Internet and telecommunication systems are used to detect, investigate, prosecute, and prevent crime. Technology, as it did in the middle of the 20th century, is beginning to change the nature of policing and affect the management and delivery of police services (Nunn, 2013). Emerging policing models in the 21st century need reliable real-time information for strategy preparation, crisis identification, tactical choices, neighborhood access, interagency coordination, transparency, hazard detection, and several other functions (Samoei 2018).

E-crimes rise in severity and do significant harm to states, companies, culture, and individuals (Broadhurst R. & Grabosky P., 2005). Also, cybercriminals are motivated in different ways, including (but not limited to) financial gains, emotional instability, societal norms, and a lack of legislation and punishment (Alansari, Aljazzaf, and Sarfraz 2019). There are numerous e-offenses titles like high-tech offenses, white-collar offenses, and cybercrimes (Majid, 2012). This year, e-crimes are on the rise as digital infrastructure and technological developments grow (Rekouche, 2011). Therefore, e-crimes have become very widespread and distributed by numerous strategies including malware applications that are specifically trained to hack into personal computers (PCs) or business networks to copy or delete sensitive information. Hacking, malware, Spamming, Cyber Stalking, Cyber perjury, Cyber Warfare and Malware (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, 2009) are the most popular of these techniques (Bhanu Sahu, Neeraj Sahu, Swatantra Kumar Sahu, and Priya Sahu, 2013) cited in (Alansari et al. 2019).

As a result, protection systems are the first step to protect the details and restrict entry to others. To secure their devices from hackers, too many individuals and companies have protection services (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, 2009). Several countries trying to enact e-crime laws present a threat to safety and individuals. This is attributed to the diffusion and production of Technology and the fast procurement of electronic appliances (Alansari et al. 2019).

Many security analysts identify cyber terrorism based upon an attack's impact. Included are actions where machines are attacked and the resultant results are damaging or harmful enough to elicit concern from a typical act of terrorism that is theoretically similar to this, even though it was perpetrated by offenders with no political intent (Agana 2015). Even computer assaults that are minimal which contribute to death, damage, prolonged power outages, aircraft collisions, water poisoning, or significant lack of faith for parts of the economy may even be called cyber warfare under this "impact" definition. Some observers argue that cyber terrorism can take the form of a physical attack that destroys computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the power grid, without ever touching a keyboard (Agana 2015), (Samoei 2018).

The Concept and Scope of Cybercrimes

What is Cybercrime or E-crime?

In the year 1995, Sussman and Heuston projected the word "cybercrime" in the first place. Cybercrime cannot be called a single definition; it is best understood as a group of acts or behaviors. These deeds are based on the material object of crime that disturbs data or structures on the computer. Those are the illegal activities where a computer interface or content structure is either a resource or a target, or a combination of both. The cybercrime is often known as e-offenses, computer-related offenses, elevation development crime, digital age crime, etc. (Bhatt and Pant 2011), (Shankar, Hemarj, and Panda 2014).

Clearly stated, "Cyber Crime" may be defined as a crime arising outside electronic messages or computer systems (Bhatt and Pant 2011), (Agana 2015), (Vinayak Pujari, Dr. R. B. Patil 2020), (Neha Mishr 2015). Such kinds of criminality are simply the forbidden behaviors under which a machine and a network become complicated. Thanks to the proliferation of the internet, the sizes of cybercrime happenings are now growing, as there is no longer a requirement for the criminal's physical appearance while linking a crime. The unusual aspect of cybercrime is that the victim and the perpetrator can never come into close communication. Cybercriminals sometimes chose to work from countries with no or poor cybercrime legislation to reduce the probability of detecting and prosecuting (Bhatt and Pant 2011), (Agana 2015), (Vinayak Pujari, Dr. R. B. Patil 2020), (Neha Mishr 2015).

Cybercrime or e-crime is an offense committed toward groups or individuals with a criminal motive that deliberately harms the victim's reputation, causes physical or mental harm, and causes money or information loss directly or indirectly through the use of the Internet and electronic devices (Johnson, 2013), (Broadhurst R. & Grabosky P., 2005), (Alex et al.) cited in (Alansari et al. 2019).

Cyber Law

Cyberlaw confiscated natal to turn over offenses committed to the internet or cyberspace, or by digital resources applications. Explanation of regulated problems connected with media or information technology applications may be known as Cyber Law (Bhatt and Pant 2011), (Vinayak Pujari, Dr. R. B. Patil 2020). Cyberlaw shows a very significant role in this modern technical age. This is relevant as it is concerned about virtually all aspects of doing and dealing that takes place on the internet or other networking tools. Whether we are alert or not, but each act and each response in Cyberspace has some legitimate and Cyber-entitled views (Bhatt and Pant 2011), (Vinayak Pujari, Dr. R. B. Patil 2020).

Nature of Cybercrime Acts

Cybercrime actions may be financially motivated activities, linked to information content, or against computer network security, credibility, and usability. The perceived danger and hazard can vary from one government to another to another. The human victimization of cybercrime is substantially higher than for 'conventional' types of crime, especially in countries with lower rates of growth, stressing the need to improve preventive measures in these countries. Private sector businesses in Europe record victimization rates varying from 2% to 16% for actions such as intrusion or phishing violation of records (Mittal and Singh 2012). There is a broad scope for digital tools of preference for such activities, such as botnets. In 2011 more than one million specific IP addresses functioned globally as botnets command and control servers (Mittal and Singh 2012).

- ✓ Includes child abuse and hate speech, but also slander and policy scrutiny, creating questions over civil rights in several situations.
- ✓ Several figures placed the total global proportion of Internet traffic suspected to be violating copyright at approximately 24%.

Cybercrime Case Study

A) **Parliament Attack Case -** Details about the incident:

a. The top cyber cases, including analyzing and retrieving information from the laptop recovered from terrorists, who attacked Parliament (Prasanthi 2015).

b. The laptop contained several pieces of evidence that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal (Prasanthi 2015).

c. The emblems (of the three lions) were carefully scanned and the seal was craftily made along with the residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop (Prasanthi 2015).

How to Recognize Cybercrimes

The movement to encourage all Americans to understand these three common cybercrimes and to take the simple steps below to defend themselves.

a) Identity theft is the illegal use of personal information about someone else to obtain money or credit. How do you realize you were a survivor of identity theft? You might be receiving bills for products or services you did not purchase. Your bank account may have withdrawals you did not expect or charges that were not authorized.

b) Phishing attacks use email to capture personal and financial data or spread malware and viruses on your computer. Cybercriminals use emails that appear genuine to enable users to click on a connection or open an attachment. The emails they submit that look as they come from an actual financial company, e-commerce platform, government department, or some other service or business.

c) Imposter schemes arise anytime you get an email or appear to be calling from a government agent, family member or relative telling you to send them money to cover taxes or fines or to support someone you care for. Cybercriminals use emails that appear genuine to allow people to send money or sensitive details to them.

Electronic Crimes Detection

Typically, one or more types of intrusion detection techniques detect electronic crimes. Such techniques Cn be a brief overview of each of these intrusion techniques follows as (Prasanthi 2015);

a. **Tripwires snooping:** They are software programs that take snapshots of key system characteristics that can be used to detect critical file changes. In this regard, tripwires provide evidence of electronic crimes because most of the intruding hackers make modifications when they install backdoor entry points or alter file systems and directory characteristics unknowingly while snooping (Prasanthi 2015).

b. **Configuration checking tools:** Configuration checking tools are also called as vulnerability assessment tools, referred to software programs used to detect insecure systems. Though configuration checking tools are primarily preventive, they use as monitoring devices can also provide evidence regarding electronic crimes. Specifically, configuration-checking tools can be particularly useful in detecting suspicious patterns of system misconfiguration that might be malicious. Admittedly further investigation will be necessary to determine if a system misconfiguration is an electronic crime (Prasanthi 2015).

c. **Honey pots**: Honey pots or Honey pot lures are employed to entrap and keep an electronic criminal occupied long enough to allow for identification and even apprehension of the preparatory. These lures can be bogus system administration accounts, fictitious product or client information, or a myriad of created files that appear to contain sensitive information. In addition to facilitating perpetrator identification, honey pots also store evidence of the electronic crime itself (Prasanthi 2015).

d. **Anomaly detection systems**: Anomaly detection system focus on unusual patterns of activity. In essence, anomaly detection systems develop and analyze user profiles, host and network activity, or system programs in hopes of discovering deviations from expected activity. Unusual keystroke intervals, abnormal commands, and unconventional program activities can provide evidence regarding the existence of an electronic crime (Prasanthi 2015).

e. **Operating system commands**: Intrusion detection is also possible with certain operating system commands, for example checking log files and comparing outputs of similar programs are among the numerous manual techniques involving operating system commands. Typically these commands are used on a daily bases by system administrators to search for evidence suggesting the possibility of electronic crimes (Prasanthi 2015).

Techniques used by Hackers

The following are some techniques used by blackheart hackers to attack your assets (Prasanthi 2015), (Pladna n.d.);

a) **Hackers and forensic experts use packet sniffing this**. Data travels in the form of packets and vary in size depending on the network bandwidth and amount of data. The intruder intercepts transmission between devices A and B. The IP address from one of the machines is what the hacker wants so all details can be taken. The data is not stolen because that is not what sniffers do. They extract the hex instead and convert it into original records. This is why it is hard for firewalls to detect this because they only provide application-level security (Pladna n.d.).

b) **Password Cracking**: A password is a form of authentication. The password is saved in memory before signing in. During this time, if a hacker has access to the computer, they may sift password through the memory. Another way to discover a secret is through "brute power," which is attempting to locate some combination of letter/number. These need a lot more time to find out (Pladna n.d.).

c) T**empest Attacks:** It is an acronym for normal Transient Electromagnetic Pulse Emanation. Data passing through circuitry and mechanical apparatus produces electromagnetic emanation. This helps hackers to monitor and position data from network cables. The intruder will stay beyond the range of the network cables so that they will be in a car park or nearby space in the building (Pladna n.d.).

d) **Buffer Overflow**: It is the most common method to hack through a machine. Buffers are designed for carrying a limited number of files. When it overflows, it enters adjacent buffers, which may cause overwriting of data. The extra data that contain instructions in buffer overload attacks, which cause different behavior. Such behavior will destroy files and/or change data (Pladna n.d.).

Forms of Cybercrimes Attacks

Specific modes of assault exploit various targets and require specific types of arms, although some could be within certain militant organizations' existing capability. Three specific methods of attack focused on the results found by the weapons used are (Alansari et al. 2019), (Agana 2015);

i. **Network Attack**: A computer network assault (CNA) typically includes malicious code used as a tool to hack adversary machines to manipulate a programming flaw, device setup, or an organization's or information user's computer protection habits. Other forms of CNA are enabled when an attacker enters restricted computer systems using stolen information.

ii. **Physical Attack**: A kinetic assault entails traditional arms or communication lines aimed towards a data facility; and

iii. **Electrical Attack**: An electrical attack (EA) includes the use of electromagnetic force as a tool, most generally as an electromagnetic pulse (EMP) to overwhelm device circuits but often in a less aggressive manner, to inject a stream of harmful software code directly through an enemy microwave radio transmission.

This review is focused on the first mode of the attack described above. Cybercrime is transmitted through computer networks (in fact, the Internet). When companies are increasingly reliant on information technology, even more entities have become susceptible to the effects of cybercrime. Many businesses are currently worried about the possibility of cyber abuse than with drug security, bribery, and robbery. Cybercrimes could endanger the protection and financial health of a nation (Alansari et al. 2019), (Agana 2015).

Manner of Cybercrimes

Cybercrime refers to all activities done with criminal intent in cyberspace. These fall into three different categories they are briefly described below (Agana 2015), (Shankar et al. 2014);

Against Individual Person:

a. **Harassment via e-mails**: Harassment through e-mails is not a new concept. It is very similar to harassing through letters (Subha.C, Kaviarasu.S 2015), (Mittal and Singh 2012).

b. **Cyber-stalking:** Cyberstalking involves following a person's movements across the internet by posting messages (Subha.C, Kaviarasu.S 2015), (Agana 2015).

c. **Email spoofing:** A mail that misrepresents its origin. It shows it's origin to be different from which it originates (Subha.C, Kaviarasu.S 2015) , (Agana 2015).

Against Government:

a. **Cyber Terrorism:** Terrorist attacks on the internet are by a distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. technology-savvy terrorists are using 512-bit encryption, which is impossible to decrypt. The recent example may be cited by- Osama Bin laden, the LTTE, and attack on America's army deployment system during the Iraq war (Subha.C, Kaviarasu.S 2015), (Agana 2015).

b. **Denial of service attack**: The computer is flooded with more requests than it can handle which it to crash. Distributed denial of service(DDOS) attack is an example (Subha.C, Kaviarasu.S 2015), (Agana 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

Against Assets:

a. **Computer Vandalism**: Damaging or destroying data rather than stealing or misusing them is called cyber vandalism. Damaging or destroying data rather than stealing or misusing them (as with cyber theft) is called cyber vandalism (Subha.C, Kaviarasu.S 2015). This can include a situation where network services are disrupted or stopped. This deprives the computer/network owners and authorized users (website visitors, employees) of the network itself and the data or information contained on the network. Examples (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020);

- Entering a network without permission and altering, destroying, or deleting data or files.

- Deliberately entering malicious code (viruses, rootkits, Trojans) into a computer network to monitor, follow, disrupt, stop, or perform any other action without the permission of the owner of the network.

- Attacking the server of the computer network (DDoS attack) so the server does not perform properly or prevents legitimate website visitors from accessing the network resources with the proper permissions (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

b. **Transmitting virus**: These programs attach themselves to a file and then circulate. They usually affect the data on a computer, either by altering or deleting it (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

c. **Email bombing**: It refers to sending large numbers of mail to the victim, which may be an Indi or a com by ultimately resulting in crashing (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

Types of Cybercrimes

The first step in developing an appropriate approach for the proofing of ICT goods is to develop a comprehensive information base of the crimes perpetrated and the relevant strategies to counter them. Thus, knowledge of current strategies for fighting crime and theft, as well as familiarizing oneself with the practice of crime prevention, will be useful for ICT protection professionals (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Brookson et al. 2007). This segment describes the forms of ICT violations and several of the possible countermeasures. Because of present ICT security concerns, there is a need for new strategies to combat advanced cyber-attacks. Governments all over the world are stepping up their efforts, both for offensive and defensive purposes (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Brookson et al. 2007), (Lysne 2016).

1) **Child Pornography**: The use of computer networks to create, distribute, or access materials that sexually use underage children

(Subha.C, Kaviarasu.S 2015), (Prakash, Baskar, and Sadawarti 2019).

2) **Cyber Contraband**: Transferring illegal items through the internet (such as encryption technology) that is barred in some locations (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Brookson et al. 2007), (Prakash et al. 2019).

3) **Cyber Laundering**: Electronic transfer of illegally-obtained money to hide its source and possibly its destination. In a tactic as old as banking itself, criminals have always used banks as a sure-fire way to launder money gained through internet communication (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Prakash et al. 2019).

4) **Cyber Stalking**: It is the use of the Internet or electronics to harass or stalk an individual, an organization, or a particular group. Cyber-stalking is a cybercrime in several respects. Cyberstalking may involve tracking someone's actions in real-time, even when they are on the computer or system now, even while they are offline, or not on the computer or mobile device. Cyberstalking is a felony because of persistent attacks, intimidation or surveillance of anyone with which the stalker has a connection or is no longer in touch (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Prakash et al. 2019), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

Cyberstalking may involve user abuse, accessing the victim's financial details, or bullying the victim to drive them off. A definition of cyberstalking may involve placing a tracking or surveillance system on a victim's machine or mobile to capture any keystroke they create so the stalker can get details. Another example would be the repeated posting on web pages or social media of derogatory or personal information about a victim, despite being warned not to. Cyberstalking holds the capacity for a jail term (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Prakash et al. 2019).

5) **Computer-based fraud**: Fraud is distinct from robbery, since the perpetrator voluntarily and intentionally offers the criminal money or goods, but would not have it if the criminal had not misrepresented himself or their deal. The fraud is a lie. When anyone leads you on or encourages you to think something incorrect to their favor, they are dishonest and that is theft. When you voluntarily surrender money or property based on their misrepresentation or lie you become a victim. Losing money from cybercrimes can be particularly devastating because it is often very hard to get back the money. Examples involve withdrawing criminal reports from a police department file, modifying ratings on a school database program, or eliminating speed violations from driving history, rather than overt scams (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Brookson et al. 2007).

6) **Fraud and Financial Crimes**: Data fraud is any deceptive misrepresentation of reality designed to encourage someone else to do something that causes harm or prevent them from doing anything. The fraud will, in this context, result in a benefit from the following (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Brookson et al. 2007), (Prakash et al. 2019);

a. Altering in an unauthorized way. It involves no technical knowledge and is a typical method of fraud by workers who change the data before entering or entering incorrect data, whether by inserting unauthorized orders by utilizing unauthorized processes;

b. Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;

c. Altering or deleting stored data;

Other forms of fraud can be facilitated by utilizing computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified data. Various internet scams, many based on phishing and social engineering, are aimed at consumers and companies (Subha.C, Kaviarasu.S 2015).

7) **Cyber-Warfare**: The US Department of Defense (DoD) states that cyberspace has arisen as a global problem through a series of recent geostrategic activities. The 2007 assault on Estonia’s network, reportedly by

Russian hackers, is among those mentioned. "In August 2008, Russia reportedly again carried out cyberattacks, this time in a concerted and orchestrated kinetic and non-kinetic assault against the country of Georgia. Fearing that such attacks might become the standard of future nation-state fighting, the idea of cyberspace operations would impact and be adopted in the future by military warfare commanders (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Brookson et al. 2007).

8) **Cyber- Extortion**: Cyber extortion happens when malicious hackers experience or assault a website, e-mail server, or computer network with periodic denial of service or other assaults. These hackers are seeking money in exchange for pledging to avoid the attacks and "secure" Cyber-extortionists are constantly targeting company websites and networks, disrupting their capacity to run, and seeking fees to resume their operation, according to the Federal Bureau of Investigation. About 20 incidents are registered to the FBI every month and several go unreported to hold the victim's identity out of the public domain. Perpetrators typically use a distributed denial-of-service attack (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Brookson et al. 2007).

9) **Mobile/Computer Viruses**: Mobile devices may become infected with viruses that spread through the cell phone network. Because cell phones have several various operating systems, these have become a minor hazard to date however when a small number of systems (such as Android and iOS) are popular, these viruses will propagate more broadly. They are similar to other computer viruses in any single way (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Neha Mishr 2015), (Brookson et al. 2007).

10) **Bluejacking**: This utilizes a feature initially designed to share contact details to transmit private, unwelcome messages to other users of cell phones or laptops activated via Bluetooth. In certain instances, this may be used to transmit offensive or threatening messages or pictures, and it may even be used to distribute malware (Brookson et al. 2007), (Neha Mishr 2015), (Subha.C, Kaviarasu.S 2015).

11) **Cyber Terrorism**: Terrorism threats on the internet go by Distributed Denial of Service (DDoS) assaults, hate websites and hate communications, threats on confidential computer networks, etc. Advanced hacker security utilizes 512-bit coding, and cannot be decrypted. The latest case of Osama Bin laden, the LTTE, and the assault on the mobilization network of the American army during the Iraq war (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Neha Mishr 2015), (Brookson et al. 2007), (Prakash et al. 2019).

Officials of the Cyber-Terrorism government and IT protection experts have reported a major spike in Internet issues and computer scans since early 2001. However, government authorities are deeply worried that these intrusions are part of an orchestrated attempt by cyberterrorists, international intelligence agencies, or other organizations to identify possible security vulnerabilities in sensor networks. A cyberterrorist is anyone who intimidates or coerces a government or organization to promote its political or social aims by initiating a computer-based assault on machines, networks or the information contained there (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Neha Mishr 2015), (Brookson et al. 2007).

Cybercrime Prevention Techniques

The following 25 strategies are a staple of Crime Proofing methodology (from the region known as 'situational' crime reduction, they originated more broadly in the world of crime prevention). Developed by Professor Ronald V Clarke over a quarter of a century, the methods aim to change facets of real crime-related circumstances in ways that minimize criminal opportunities (Brookson et al. 2007). The goal of the "25 tactics" is to solve unique and not general issues of crime. Identifying 'identity theft through email phishing' or 'identity theft via credit card fraud' is more useful than identifying identity fraud generally. That is since usually, various forms of identity fraud would need specific crime proofing strategies. The same goes for almost all forms of ICT-related criminality (Brookson et al. 2007).

Increase The Risks	Increase The Efforts	Reduce Provocations	Reduce The Rewards	Remove Excuses
Extend Guardship	Target Harden	Reduce Frustrations And Stress	Conceal Targets	Set Rules
Assist Natural Surveillance	Control Access	Avoid Disputes	Remove Targets	Post Instructions
Reduce Anonymity	Screen Exits	Reduce Emotional Arousal	Identify Property	Alert Conscience
Utilize Place Managers	Defect Offenders	Neutralize Peer Pressure	Disrupt Markets	Assist Compliance
Strengthen Formal Surveillance	Control Weapons/Tools	Discourage Imitations	Deny Benefits	Control Drugs And Alcohol

Figure 1: ICT Related Crime Prevention Techniques (Brookson et al. 2007).

The roots of the methods come from specific contexts than cybercrime. In what follows, some attempt is being made to adapt the techniques to ICT offenses, whilst recognizing that this is a pioneering experiment and the utility of the techniques should begin to develop as this research progresses. What has arisen is that a broad variety of such strategies may be adapted to different forms of criminality linked to online communication. The first step in finding innovative solutions to crime proofing is to recognize current common practice and to assess the possibilities for its wider use [8]. The probability of its existence can be determined by the real or potential amount of commitment or danger involved in the conduct of a crime. Similarly, decreasing the real or potential profit of committing a crime would decrease the risk of performing it (Subha.C, Kaviarasu.S 2015), (Brookson et al. 2007).

The 25 techniques are grouped into 5 main categories: each of these five categories contains five techniques that can be applied (Brookson et al. 2007).

a) The aim of the "25 techniques" is to solve uniquely, and not generally, criminal issues. This is more important to detect 'identity theft through email phishing' or 'identity theft through credit card fraud' than to recognize identity fraud in general. This is because typically different types of identity theft will require complex techniques for proving the crime. The same applies to nearly all aspects of crime related to ICT (Brookson et al. 2007).

b) Raise the chance of unlawful behavior. Danger includes the risk of being captured, the risk of defeat, the risk of resource depletion, and other threats. The likelihood of being identified in the conduct of a crime is enhanced by the possibility of GPS or other surveillance, for instance by monitoring on the phone, and most generally to other telecommunications devices. But, more generally, the danger is raised by surveillance and control that may be systematic (police and security) or that happens informally as part of daily practice. E.g., open platforms such as Linux promote universal inspection and effort to protect and develop its code, whereas a quiet street may have surveillance that decreases robbery (Brookson et al. 2007).

c) Reduce Provocation which might lead to the crime (Brookson et al. 2007).

d) Rising Crime Engagement Incentives. For example, mobile phone blacklisting does not make them any harder to steal. Instead, it works by reducing the rewards to steal them because if they don't work, they have a lower resale value

e) Remove Excuses that encourage people to 'justify' or 'require' a crime. This can be in the form of simple reminders of the illegal nature of certain types of offenses. Digital media players and computer applications also bear a sticker claiming that piracy of music or apps is fraud and a felony. This ensures individuals cannot validly say that they did not know that unauthorized copying was an offense (Brookson et al. 2007).

Electronic Identifications and Detection of Crimes

Through the ICT, identification of a person becomes very easy. Police can use several methods to trace a person to control the crime and maintain the law and order. Whatever method of electronic communication is used by a person it becomes an important means of electronic identification (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

As indicated previously, technology at the crime scene can also be used to real-time capture information relating to the crime at the point the crime is being committed. This information may relate to the crime itself, the victim, or the perpetrator (Mennell 2012). For example, consider the following examples (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020):

1) **Online Verification and Fingerprints Reader:** Biometric devices and fingerprint scanners are now helping to uphold the legislation and enhance the activities of the police. Biometric technology helps in the online verification and recognition of people from different geographical locations. This offers reliable details to the accused party and creates room for swift decision-making on relevant security concerns (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

2) **CCTV (Closed Circuit Television):** Used by a wide range of stakeholders, from police, transport providers and networks, city councils, businesses, householders, etc., to capture footage and images related to potential criminal activity and to facilitate the identification of the offender(s); and to act as a deterrent. We are all too well acquainted with the extent to which this technology has pervaded our work, social and community environments; and equally well acquainted with the 'mug shots' that have arisen, which have been circulated by the police or by charities such as Crime Stoppers, to the public via TV, web-sites or the press (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

3) **Electronic Transport (E-Transport)** Big transport-related operations can be done conveniently via mobile technologies. The E-Transport component includes a range of things such as registration of all forms of motor vehicles, issue of driving licenses, issue of permits for medium and heavy vehicles, recovery of taxes and costs through cash and bank coupons and emission management by inspections, etc. (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020)

4) **Mobile Phone:** There are already millions of cell phone users in the UK. Many owners also can record, intentionally or unknowingly, crime-related details; and they do have the opportunity to send such details (real-time), via social networking platforms such as Linked-in and Twitter, as well as through YouTube, etc. The captured information may include 'video' or photographic images taken as a crime, e.g. footage taken during the London riots that recorded the crimes being committed, or information stored on the phone that could be used to record a previous event, e.g. pictures showing the location of the crime, layout and 'contents' at a recorded (and verifiable) date and time (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020), (Brookson et al. 2007), (Kaur and Sharda 2014).

5) **Real-time Information Access**: In a large geographical area which is very hard to check and administer the Global Positioning System (GPS) and Geographical Information System (GIS) are used to track the information about a particular area and movement of suspected and terrorists etc. with the available data and video. The available information provides the ability to organize all the events for better tracking, recording, and taking action. This system allows police officers to take preventive measures. GPS is extremely helpful for monitoring a stolen car, allowing choices on traffic flow and reducing overcrowding, and offering intelligence about when police units are close to reacting to an incident (Kumar 2010), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020), (Quarshie and Mis 2014).

6) **RFID (Radio Frequency Identification)**: Recently, automated tracking methods have become popular in the provision of several services. They can have details on individuals, companies, and items. A technology uses radio waves to transmit data from an electronic tag or label attached to an object via a reader to identify and track the movement of material across the country. Police departments utilize such equipment so that transit networks may be checked to deter the transportation of illegal goods, which could affect public safety. The information on the tag is stored electronically. The precise position of each police officer could be more useful for the provision of police services. Such a device appears to be an effective resource for gathering and presenting details on the position of officers (Kumar 2010), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020), (Quarshie and Mis 2014).

Both of these instances represent the potential of a device customer to collect information or facts relevant to a crime now that it is conducted. Furthermore, it also greatly adds additional 'people' to the crime scene investigation, i.e. it is not just the crime scene detective who collects and reports information relevant to the incident. These agents, and the use of their technology, are introducing new functionality, new roles, and, of course, new challenges to the criminal investigation process, particularly in dealing with digital evidence resulting from their involvement in the crime scene (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

Safety Measures Against Cybercrimes

Cyber Security

Cybersecurity includes the defense of confidential individuals and company details by avoidance, monitoring, and reaction to numerous cyber-attacks. Cyber Security effectively protects your private information by responding, detecting, and preventing attacks (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020).

A) Protecting Your Privacy:

i. **Privacy policy**: Until sending your name, email address, or other personal details to the website, please check the Privacy Policy of the website.

ii. **Evidence that your information is being encrypted**: To protect attackers from hijacking your information, any personal information submitted online should be encrypted. Many sites use the SSL or secure socket layer to encrypt information (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020), (Quarshie and Mis 2014).

B) How Can We Protect?

i. **Keep software up to date**: If the seller releases patches for the software operating your device install them as soon as possible. Installing them will prevent attacked from being able to take advantage (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020), (Prasanthi 2015), (Quarshie and Mis 2014).

ii. **Use Strong passwords**: Select passwords that will be difficult for thieves to guess. Do not choose options that allow your computer to remember your passwords. It MUST be containing at least 8 digits and should not be dictionary words. They should combine upper and lower case characters (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020), (Prasanthi 2015), (Quarshie and Mis 2014).

iii. **Disable remote connectivity**: Some PDA's and phones are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use (Bhatt and Pant 2011), (Subha.C, Kaviarasu.S 2015), (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020), (Prasanthi 2015), (Quarshie and Mis 2014).

iv. Never give out your address, telephone number, hangout spots, or links to other websites or pages where this information is available (Prasanthi 2015).

v. Do not open a file attached to an e-mail unless you are expecting it or know what it contains. If you send an attachment, type a message explaining what it is. Never forward, any e-mail warning about a new virus. It may be a hoax and could be used to spread a virus (Prasanthi 2015).

vi. Confirm the site you are doing business with. Secure yourself against "Web-Spoofing". Do not go to websites from email links (Prasanthi 2015).

vii. Protect yourself from viruses by installing antivirus software and updating it regularly. You can download anti-virus software from the Web sites of software companies, or buy it in retail stores; the best recognize old and new viruses and update automatically(Subha.C, Kaviarasu.S 2015), (Prasanthi 2015).

C) The Changing Nature of Cybercrime

New trends in cybercrime are emerging all the time, with the global economy costing billions of dollars. In the past, cybercrime has been committed primarily by individuals or small groups (Bhatt and Pant 2011). Today, we see criminal groups collaborating with illegally inclined experts to conduct cybercrime, mostly to finance such illicit acts. Highly sophisticated, these cyber-crime networks put together people from across the world to conduct crimes to an unparalleled scale in real-time (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020), (Quarshie and Mis 2014).

Criminal organizations are rapidly moving to the Web to promote their operations and increase their income in the shortest period available. Crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, the sale of counterfeit medicines – but they are evolving in line with the opportunities presented online and are therefore becoming more widespread and harmful (Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu 2020)

Conclusion

Cybercrime is indeed getting the recognition it deserves. However, it is not going to restrict that easily. It is highly likely that cybercrime and its hackers will continue developing and upgrading to stay ahead of the law. So, to make us safer we must need cybersecurity. Cybersecurity solve cybercrime. There will always be new and unexpected challenges to stay ahead of cybercriminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and government. There is much we can do to ensure a safe, secure, and trustworthy computing environment. It is crucial not only to our national sense of well-being but also to our national security and economy.

Acknowledgment

We are grateful to our teachers and senior colleagues who help us in one way or another for making efforts during the creation of this piece of the manuscript. We acknowledged the supports by Kano State Polytechnic Management for their valuable financial supports.

References

Agana, Moses A. 2015. “Cyber Crime Detection and Control Using the Cyber User Identification Model.” 5(October):354–68.

Alansari, Mariam M. H., Zainab Aljazzaf, and Muhammad Sarfraz. 2019. *On Cyber Crimes and Cyber Security - Developments in Information Security and Cybernetic*.

Bhatt, Susheel, and Durgesh Pant. 2011. “Cyber Crime in India.” *International Journal of Advanced Research in Computer Science* 2(5).

Brookson, Charles, D. T. I. Uk, Graham Farrell, Jen Mailley, Shaun Whitehead, and Dionisio

Zumerle Etsi. 2007. "ICT Product Proofing Against Crime." *European Telecommunications Standards Institute F-06921 Sophia Antipolis Cedex, France* 5(1).

Kaur, Ramandeep, and Neeru Sharda. 2014. "Utilizing ICT to Fight against Crime : Emerging ICT Tools , Forms of Crime and Its Solutions." *International Journal of Computer Science and Information Technologies* 5(6):7452–57.

Kumar, B. 2010. "Role of Information and Communication Technology in the Indian Police." *Gian Jyoti E-Journal* 2(3):51–54.

Lysne, Janne Hagen and Olav. 2016. "Protecting the Digitized Society—the Challenge of Balancing Surveillance and Privacy - The Cyber Defense Review." *Spring. Army Cyber Institute Is Collaborating with JSTOR to Digitize, Preserve and Extend Access to The Cyber Defense Review* 1(1):75–90.

Mennell, Julie. 2012. "Technology Supporting Crime Detection - An Introduction." *Measurement and Control (United Kingdom)* 45(10):304–5.

Mittal, Saurabh, and Ashu Singh. 2012. "A Study of Cyber Crime and Perpetration of Cyber Crime in India." *Norton Cybercrime Report on Changing Face Of Cybercrime: Cybercrime Goes Social* 1–15.

Neha Mishr, Pooja Shelke. 2015. "Data Mining – A Necessity for Crime Detection." *International Journal on Recent and Innovation Trends in Computing and Communication* 3(2):291–94.

Pladna, Brett. n.d. "PREVENTING CYBER CRIME." *The Lack of Attention in the Prevention of Cyber Crime and How to Improve It , ICTN6883 East Carolina University* 1–28.

Prakash, Febin, Kala Baskar, and Harsh Sadawarti. 2019. "Cyber Crime: Challenges and Its Classification." Pp. 2–4 in *Proceedings for International Multi-disciplinary Academic Research Conference*.

Prasanthi, Ms M. Lakshmi. 2015. "Cyber Crime: Prevention & Detection." *International Journal of Advanced Research in Computer and Communication Engineering* 4(3):45–48.

Quarshie, Henry Osborn, and M. B. A. Mis. 2014. "Using ICT to Fight Crime - A Case of Africa." 5(1):21–24.

Samoei, Pamela Cherotich. 2018. "Role of Information Communication and Technology in Enhancing Security in Urban Areas in Kenya : A Literature Based Review Role of Information Communication and Technology in Enhancing Security in Urban Areas in Kenya : A Literature Based Review." *Stratford Peer Reviewed Journals and Book Publishing Journal of Information & Technology* 2(1):17–27.

Shankar, Yerra, Rao Hemarj, and Saini T. C. Panda. 2014. "Effect of Cyber Crime Indian Economy." *International Journal for Research in Technological Studies* 1(10):4–7.

Subha.C, Kaviarasu.S, Kavyapriya. G. .. 2015. "Cyber Crime – Attacks , Types and Protection." *International Journal of Trend in Research and Development* 2(5):351–55.

Suleiman Muhammad Muhammad, Kuliya Muhammed, Surajo Aminu Zubairu, Musa Jamilu. 2020. "ICT Is An Integral Strategy For Crimes Prevention And Detection." *Academic Leadership (Online Journal)* 21(06):249–57.

Vinayak Pujari, Dr. R. B. Patil, Rohit Dalvi. 2020. "Cyber Crime & Cyber Law's in India." *International Journal of Advance and Innovative Research* 7(1(VI)):62–66.