IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Crime "As A New Form of Business"

Shefali bajpai [1], Dr. Hardayveer[2]

Research scholar ,Head of department of law

P.K. University,Shivpuri (M.P.)

Abstract-

The internet is frequently hailed as a remarkable tool, an engaging platform, and a liberating experience. However, the question remains: for whom? As the online world expands, many of us are at risk of falling prey to sophisticated cybercriminals who expertly navigate the digital landscape. Cyberspace, often referred to as the web, is a dynamic and intangible environment.

This paper examines the emerging threat of cybercrime, a new breed of business and high-tech criminality. It provides an overview of cybercrimes, the perpetrators, and their motivations. A detailed discussion of various cybercrimes will be presented, along with the unique challenges and response issues that arise during prevention, detection, and investigation.

Additionally, this paper will outline the relevant sections of the IT Act 2000 of India and propose new provisions to enhance the legislation. The discussion will cover the complexities of cybercrime and the need for effective measures to combat this growing threat.

Key words –cyber crime ,laws ,threat ,internet, offence, remarkable tool

Introduction

The internet is a revolutionary force that transforms every aspect of our lives. It challenges traditional norms and conventions, reshaping governance, business operations, education, and even everyday activities like cooking. The internet disrupts our existing knowledge and perceptions of the world, others, and ourselves. This digital landscape is simultaneously empowering, thrilling, daunting, and intimidating. Despite its vast potential, the internet remains an enigma to many, evoking feelings of mystery, apprehension, and incomprehension. The rapid growth of the internet has led to an increase in cybercrime opportunities. As more people go online, crimes like hacking, extortion, and fraud have become more common. Lawmakers struggle to keep up with the fast-paced technological advancements, making it challenging to create effective laws. They must balance individual rights, such as privacy and free speech, with the need to protect networks and communities.

Cybercrime enforcement is further complicated by jurisdictional issues, requiring international cooperation to combat these crimes effectively. Law enforcement agencies worldwide are working together to develop new strategies and responses to ensure online safety and security.

This paper argues that cybercrime, particularly high-tech crime, requires a fundamental shift in policing approaches. The paper is structured as follows:

- Sections 2 and 3 provide an overview of cybercrimes and their perpetrators.

- Section 4 discusses different types of cybercrimes.

- Section 5 explores the challenges and response issues in preventing, detecting, and investigating cybercrimes.

- Sections 6 and 7 outline the IT Act 2000 of India's efforts to prevent and reduce cybercrime incidents.

- Section 8 proposes changes to the IT Act 2000.

- The paper concludes with a brief statement on the challenges posed by cybercrime.

2. **background**

Cybercrime refers to criminal activities that involve computers, networks, or the internet. There are different perspectives on what constitutes cybercrime. Some experts consider it to be traditional crimes committed using advanced technology, where the computer is either a tool, a target, or both. Others believe that cybercrime is a distinct category of crime that requires a new legal framework to address the unique challenges posed by emerging technologies, such as:

- Jurisdictional issues

- Need for international cooperation

- Difficulty in determining intent

- Challenges in identifying perpetrators

These differing views highlight the complexities of cybercrime and the need for a comprehensive approach to address its unique nature.

2.1 The Perpetrators – Hackers & Crackers

2.1.1 Hackers

A hacker is typically defined as an individual who attempts to gain unauthorized access to a computer system. According to Section 66 of the IT Act 2000, a person can be considered a hacker if they:

- Intend to cause or know that they are likely to cause wrongful loss or damage to the public or any person
- Destroy, delete, or alter information residing in a computer resource
- Diminish the value or utility of the information or affect it injuriously by any means

In essence, hacking involves unauthorized actions that compromise the integrity or security of computer systems or data.

2.1.2 Crackers

A cracker is a type of hacker who has malicious intentions. The term "cracker" is used to differentiate between hackers who engage in benign activities and those who cause harm to computer systems. Crackers are known for:

- Maliciously sabotaging computers

- Stealing sensitive information from secure systems

- Disrupting networks for personal or political gain

In essence, crackers use their technical expertise for nefarious purposes, compromising the security and integrity of computer systems and data.

3. Why People Hack?

Cybercrime is emerging as a "new form of business" that involves:- Novel forms of criminal activity, A wider scope and scale of offenses and victimization, The need for rapid response, Complex technical and legal challenges.

Hacking, a key aspect of cybercrime, can be driven by various motives, including:- Personal gain, Political agendas ,Professional interests

These factors highlight the evolving nature of cybercrime and the need for effective strategies to combat its growing threats.

3.1 Hactivism

In recent years, hacktivists have been launching business-motivated attacks on public web pages and email servers. These hacking groups and individuals:

- Overload email servers with massive amounts of emails to a single address (a technique known as email bombing or spamming)

- Hack into websites to display professional or business messages, often to promote a particular agenda or ideology

These types of attacks are typically used to disrupt or deface online platforms, and can have significant impacts on businesses and organizations.

3.2 Employees

Research has shown that disgruntled employees pose a significant threat to computer security. These individuals may:

- Steal confidential information and trade secrets for financial gain

- Use their insider knowledge to access and damage the system or steal sensitive data

According to the Cyber Crime Cell (CBI), insider threats are a major source of computer crimes. Insiders often have an advantage due to their familiarity with the system, which allows them to cause harm without requiring extensive technical knowledge.

3.3 Recreational Hacker

Recreational hackers break into computer networks primarily for the thrill of the challenge or to gain recognition within the hacking community. These individuals often:

- Download pre-existing attack scripts and protocols from the internet

- Launch these attacks against target sites without having in-depth knowledge of the systems they're targeting

Their actions are typically driven by personal satisfaction or to boost their reputation among peers, rather than for financial gain or malicious intent.

3.4 Web site Administrators and Web Pages

Websites also access a lot of hidden background information from the user. The remote website can determine the following important information about the visitor;

a. the IP address the user is accessing the web site from;
b. the number of prior visits to the web site, and the dates;
c. the URL of the page that contained the link to get the user to the web site;
d. the user‟s browser type and operating system and version;
e. the user‟s screen resolution;
f. whether JavaScript and VBScript are enabled on the user‟s computer;
g. how many web pages the user has visited in the current session;
h. the local time and date; and
i. FTP username and password, if there is one.

4. Types of Cyber Crime

Computers play a crucial role in almost all cybercrimes, serving as either the target, tool, or source of evidence. As more devices become internet-enabled, the opportunities for hackers to exploit them increase. The different uses of computers in cybercrime can be categorized into three main areas:

1. Computer as the target: The goal is to steal information from or cause damage to a computer, system, or network. Examples include:
   - Hacking
   - Cracking
   - Espionage
   - Cyberwarfare
   - Malicious computer viruses
2. Computer as the tool: Cybercriminals use computers to commit traditional crimes, such as:
   - Printing fake currency
   - Creating and distributing child pornography
   - Money laundering
3. Computer as evidence: Computers can contain crucial evidence of a crime, such as:
   - Child pornography
   - Financial records of money laundering operations

The role of computers in cybercrime highlights the need for effective laws and strategies to combat these evolving threats.

4.1 Malicious Code – Viruses, Worms and Trojans

Viruses - A computer virus is a program that modifies other computer programs, replicating itself and potentially causing harm. Viruses can spread through- Email attachments ,Infected disks, Execution of infected programs .A common method of virus execution is when a user is tricked into opening a malicious file, often disguised as a harmless program from a trusted source. A notable example is the Melissa virus, which: Spread through a Microsoft Word attachment, Activated a macro that emailed itself to 50 addresses in the victim's Microsoft Outlook, Caused an estimated $80 million in damages

Worms - A worm is a standalone program that replicates itself, spreading throughout a network without needing to attach to a file. Unlike viruses, worms can propagate independently. An example is the "I Love You" worm, which caused significant losses in 2001.

Trojan Horses - A Trojan horse is a seemingly innocent program that contains hidden malicious functions. These programs are often used to introduce viruses into computer systems. Once executed, the hidden sub-program performs unauthorized actions. An example is Back Orifice 2000, a program designed for misuse and attacks on other computers.

These types of malware highlight the importance of robust cybersecurity measures to prevent and mitigate the damage caused by such threats.

4.2 A Denial of Service

A Denial of Service (DoS) attack is a type of cyberattack where an attacker floods a computer or network with excessive traffic, preventing legitimate users from accessing it. The goal is not to breach the system or steal data, but rather to disrupt access to the network or website. DoS attacks can be motivated by:- Revenge ,Economic or political gain , Malicious intent

For example, in February 2000, a 15-year-old Canadian boy known as "MafiaBoy" allegedly launched a DoS attack that shut down popular websites such as:-Yahoo, Amazon, Buy abd other .This attack demonstrates the potential impact of DoS attacks on online services and the importance of robust cybersecurity measures to prevent and mitigate such threats.

Cyberstalking

Cyberstalking is a form of online harassment where an individual is pursued and monitored, often with their privacy invaded and every move watched. This can cause significant distress and fear for the victim. Cyberstalking can affect anyone, but it is more common among women and children. The anonymity of the internet can embolden stalkers, who may be strangers or individuals known to the victim.

Financial Crimes

Financial crimes in the cyber world include cheating, credit card fraud, and money laundering. An example of such a crime is a website offering goods at unusually low prices, only to exploit the trust of customers who provide their credit card numbers. The perpetrators would then misuse the credit card information for financial gain.

Cyber Pornography

Cyber pornography involves the distribution and sharing of pornographic content through the internet, including websites and online publications. There have been several incidents in India related to cyber pornography, such as:

- A student creating a website with morphed images of his classmates and teachers

- A couple forcing slum children to appear in obscene photographs, which were then uploaded to websites catering to pedophiles

These incidents highlight the need for awareness and action to prevent and address cybercrimes.

- **Sale of Illegal Articles**: This involves selling prohibited items like narcotics, weapons, or wildlife through online platforms, auction sites, or email communications. For instance, some auction sites in India might be selling cocaine disguised as 'honey'.

- **Online Gambling**: Millions of websites offer online gambling, often hosted on foreign servers. Some of these sites might be fronts for money laundering.

- **Intellectual Property Crimes**: These include software piracy, copyright infringement, trademark violations, and theft of computer source code.

- **Email Spoofing**: This occurs when someone sends emails that appear to originate from a different source. For example, if someone spoofs Pooja's email (pooja@asianlaws.org) and sends obscene messages to her acquaintances, it could damage her relationships and reputation.

- **Forgery**: Counterfeit currency notes, postage stamps, mark sheets, and certificates can be forged using advanced computers and printers. In India, some student gangs sell fake mark sheets and certificates to students.

- **Cyber Defamation:** This happens when defamation occurs through computers or the internet. Examples include publishing defamatory content about someone on a website or sending defamatory emails to their friends.

5.unique challenges

Investigating cybercrime comes with a unique set of challenges. Some of the key difficulties include:

1. Jurisdictional issues: Cybercrimes often cross multiple jurisdictions, making it hard to determine which laws apply and which authorities should handle the investigation.

2. Evidence preservation: Digital evidence can be easily altered, deleted, or encrypted, making it crucial to preserve it properly.

3. Decoding encryption: Encrypted data can be difficult to access, and investigators may need specialized tools and expertise to crack the encryption.

4. Proving identity: It can be challenging to determine the identity of cybercriminals, as they often use pseudonyms, VPNs, and other methods to hide their tracks.

5. Finding evidence: Investigators need to know where to look for digital evidence, which can be scattered across various devices, networks, and online platforms.

6. Staying up-to-date with technology: Cybercriminals are constantly evolving their tools and techniques, so investigators need to stay current with the latest technology and trends.

7. Real-time response: Cybercrimes often require a rapid response to prevent further damage and preserve evidence.

8. Coordination and collaboration: Effective investigations often involve multiple agencies and stakeholders, requiring strong coordination and collaboration.

9. Training and expertise: Investigators need specialized training and expertise to handle complex cybercrime cases.

10. Strategic partnerships: Building partnerships with other agencies, organizations, and industry experts can help investigators stay ahead of cybercriminals.

11. Reporting and information sharing: Encouraging reporting and sharing information about cybercrimes can help identify patterns and trends.

12. Attracting and retaining talent: Investigative agencies need to attract and retain skilled professionals with expertise in cybersecurity and digital forensics.

13. Avoiding tech-lag: Agencies need to stay up-to-date with the latest technology and tools to effectively investigate cybercrimes.

By understanding these challenges, investigators and agencies can develop strategies to overcome them and effectively combat cybercrime.

6.Cyber Laws in India: In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses

and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Information Technology Act, 2000 is a crucial piece of legislation that provides the legal framework for e-commerce in India. The Act aims to:

- Provide legal recognition to electronic records and digital signatures

- Facilitate e-governance and e-commerce

- Regulate certifying authorities and digital signature certificates

- Prescribe penalties for cyber offenses

Key Provisions of the IT Act

Some of the key provisions of the IT Act include**:- Digital Signatures:** The Act allows subscribers to authenticate electronic records using digital signatures, which can be verified using public keys.

- **Electronic Governance:** The Act provides for the use of electronic records and digital signatures in government transactions, and recognizes the legal validity of digital signatures.

- **Regulation of Certifying Authorities:** The Act establishes a Controller of Certifying Authorities to oversee the activities of certifying authorities and specify standards and conditions for issuing digital signature certificates.

- **Secure Electronic Records and Digital Signatures:** The Act provides for the use of secure electronic records and digital signatures to ensure the authenticity and integrity of electronic transactions.

- **Penalties and Adjudication:** The Act prescribes penalties for various cyber offenses, including damage to computer systems and hacking, and establishes an adjudicating officer to investigate and impose penalties.

- **Cyber Appellate Tribunal:** The Act establishes a Cyber Appellate Tribunal to hear appeals against orders passed by adjudicating officers.

Impact of the IT Act

The IT Act has a significant impact on e-businesses and the new economy in India, as it provides a legal framework for electronic transactions and digital signatures. The Act aims to promote e-commerce and e-governance, while also protecting against cyber threats and offenses.

7.Advantages of Cyber Laws

The Information Technology Act, 2000 provides a legal framework for electronic transactions and digital signatures, offering several benefits, including:

- Legal validity of electronic records: The Act recognizes electronic records as a valid and enforceable form of communication, which can be used in court proceedings.

- Digital signatures: The Act gives legal validity to digital signatures, enabling secure and authenticated electronic transactions.

- E-commerce growth: The Act provides a legal infrastructure for e-commerce, allowing companies to carry out electronic transactions with confidence.

- E-governance: The Act enables government departments to accept and process electronic documents, promoting e-governance and efficient public services.

- Certifying Authorities: The Act allows corporate companies to become Certifying Authorities, issuing Digital Signature Certificates and promoting the use of digital signatures.

- Security: The Act addresses security concerns by defining secure digital signatures and providing a framework for protecting electronic transactions.

- Remedies for cyber crimes: The Act provides statutory remedies for companies that suffer damages or data theft due to unauthorized access to their computer systems or networks.

By providing a clear and comprehensive framework for cyber laws, the IT Act, 2000 promotes trust and confidence in electronic transactions, supporting the growth of e-commerce and e-governance in India.

8.Proposed Changes to the IT Act, 2000

To address emerging challenges in cybercrime investigations, the following changes are proposed:

1. Trap and Trace Orders: The new legislation should enable cyber investigators to obtain a single "trap and trace" order to track the origin of online communications, including IP packets, across multiple jurisdictions. This would facilitate the investigation of cybercrimes such as hacking, DoS attacks, and virus outbreaks.

2. Age of Criminal Responsibility: The proposed legislation should consider lowering the age of criminal responsibility for serious computer crimes to 15 years, acknowledging the increasing involvement of young individuals in cybercrime.

3. Regulation of Cyber Cafes and Computer Training Centers: The proposed legislation should incorporate cyber cafes, computer training centers, and other institutions that use computers as a mode of training under a specific act. This would ensure that these establishments maintain adequate records, implement security measures, and cooperate with law enforcement agencies during investigations.

These proposed changes aim to enhance the effectiveness of cybercrime investigations, promote accountability, and ensure that the legislation keeps pace with the evolving nature of cyber threats.

9.Conclusion

Cybercrime poses a significant challenge to law enforcement agencies globally, including India. As technology advances and becomes more pervasive, electronic crime will increasingly feature in various forms of criminal behavior, including traditional offenses. Digital evidence will become more common, and law enforcement agencies must be prepared to address this new challenge.

To combat cybercrime, agencies worldwide are developing new partnerships, forensic methodologies, and responses. This requires new skills, technologies, and investigative techniques applied in a global context. The scope and scale of cybercrime demand timely responses and pose technical and legal complexities.

Innovative solutions, such as "cybercops," "cybercourts," and "cyberjudges," may be necessary to overcome jurisdictional issues and effectively address cybercrime. By working together and developing new strategies, law enforcement agencies can ensure safety and security on the internet.

Reference

1. Legard, D (2001), Hackers Hit Government Sites, Computer World, Vol 24 No. 26, 29 Jan, p.12.

2. Russell G. Smith, Peter Grabosky and Grgor Urbas, 0521840473 – Cyber Criminals on Trial, Cambridge University Press.

3. Seamus O Clardhuanin (2004), An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Summer 2004, Vol 3, Issue 1

4. International crime and Cyber Terrorism, http://www.dfait-maeci.gc.ca/internationalcrime/cybercrime-en.asp. 15. Visited www.cbi.nic.in