Journal of Namibian Studies, 33 (2023) : 1060-1071 ISSN: 2197-5523 (online)

Special Issue On Multidisciplinary Research

Study Of Cybercrime- Impact On Government & Its Prevention Mechanism

Himani

Ph.D Scholar, Jayoti Vidyapeeth Women's University, Jaipur

Abstract:

Cybercrime has become a major threat to global business and society. As the economy becomes more digital, India has become a prime target for cybercriminals. This research paper aims to examine the impact of cybercrime on the Indian economy and society. It explores the different types of cybercrime prevalent in India, their occurrence, and the steps taken by the government and other stakeholders to combat this menace. The study also highlights the challenges faced in combating cybercrime and suggests potential strategies to mitigate its negative impact.

Introduction

Background & Significance:

In recent years, the rapid development of information technology and the widespread use of the internet have brought about changes in every aspect of society and business. While these developments have brought many benefits, they have also created new challenges, especially cybercrime. Cybercrime refers to crimes committed against individuals, organizations, and even governments through computer systems or communication. The country's large population, increasing internet penetration, and expanding digital infrastructure provide fertile ground for cybercrime activities. Therefore, understanding the impact of cybercrime on the Indian economy and society has become an important issue.

Objectives

The main objective of this research paper is to identify and assess the impact of cybercrime on the economy and society of India. The study specifically aims to achieve the following objectives:

1. Identify and analyze the various types of cybercrime present in India, including hacking, identity theft, financial fraud, data breaches, and online crimes.
2. Assess the economic impact of cybercrime in India, including financial loss, business disruption, privacy theft, and increased cybersecurity spending.
3. Engineering and destruction of public faith. Explore initiatives taken by the Indian government and other stakeholders to combat cybercrime, including cybersecurity policies, laws, and enforcement.
4. Understand the challenges India faces in combating cybercrime, such as rapid evolution of cyber threats, lack of cybersecurity awareness, and inadequate capacity.
5. Recommend mitigation strategies and recommendations to policymakers and stakeholders to improve cybersecurity measures and reduce the negative impact of cybercrime on the Indian economy and society.

Definition of cybercrime:

Cybercrime includes a variety of crimes that use computers, computer networks, or the internet. These criminals use vulnerabilities in digital systems to gain unauthorized access, steal sensitive information, disrupt services, or harm individuals, organizations, or governments.

Some common types of cybercrime include

Hacking: Allow access to a computer or network for the purpose of stealing, altering, or destroying information, disrupting service, or conducting other attacks.

Identity Theft: They may engage in fraud, disrupt systems, and steal information or extort money. Violation of privacy, such as personal information or trade secrets, or resulting in tort.

Phishing & Social Engineering: where illegal agencies or hackers gain authorized access to sensitive information or disrupt government operations.

Malware Attacks: Distribute malware such as viruses, worms, or ransomware to disrupt systems and steal data or steal money.

Financial Fraud: Engaging in online fraud, credit card fraud, or cryptocurrency crime for criminal financial gain.

Data Breaches: Unauthorized access to or disclosure of sensitive information (such as personal information or trade secrets) leads to compromise of privacy or potential misuse.

Cyberbullying & Harrassment: Use digital platforms, often via social media or text messaging, to threaten, intimidate, or harm people.

Cyber Espionage: State-sponsored organizations or hackers operate illegally to gain illicit access to sensitive information or disrupt government operations.

Global Trends in Cybercrime:

Cybercrime has become a global phenomenon that transcends regional borders and affects countries around the world. Some of the major global changes in cybercrime include:

Increasing Sophistication: Cybercriminals continue to evolve their methods using advanced techniques and techniques to carry out more attacks and attack schemes.

Dark web Activities: The dark web provides a hidden place for crimes, including the sale of stolen goods, stolen property, drugs and weapons.

Supply Chain Attacks: Cybercriminals target vulnerabilities in devices to obtain critical information or compromise trust.

Ransomware Attacks: Ransomeware has become a threat as cybercriminals encrypt victims' data and demand ransom for it. Hacking tools, drugs, and weapons.

IoT Vulnerabilities: The increase in the number of connected devices has created new ways for cybercriminals to exploit vulnerabilities and obtain illegal information.

Government-backed means: The government seeks to gain political advantage or add interest to the country.

Economic Impact of Cybercrime in India

A. Financial Losses & Damages:

Cybercrimes cause significant economic losses and damages to people, businesses and the entire Indian economy. The financial impact of cybercrime includes:

i. **Direct financial loss**: Cybercrime activities cause direct financial loss through fraud, theft, or unauthorized access to the bank. Individuals and businesses bear the brunt of financial theft resulting in huge financial losses.
ii. **Indirect financial loss**: Cybercrime issues often have indirect economic impacts, such as reputational damage, reduced consumer confidence, and reduced business trust. These factors impact business, customer acquisition, and overall business growth.
iii. **Legal & Regulatory Cost**: Organizations affected by cybercrime will often incur costs related to litigation, investigations, and compliance. These costs compound the financial impact.

B. Business Disruption & Activity Losses:

Cybercrimes disrupt business operations and cause loss of productivity, disrupting the entire business. The consequences include:

i. **Downtime & Disruption Services**: Cyberattacks such as Distributed Denial of Service (DDoS) attacks can render websites, online services, or critical systems inaccessible, leading to lost revenue, customer dissatisfaction, and reduced productivity.
ii. **Operational Delays**: Organizations affected by a cyber incident may experience delays in daily operations, including production, supply chain management or delivery. This disrupts the flow of goods and services, making the business inefficient.
iii. **Business Continuity Cost**: To protect against cyber threats, businesses invest in backup systems, disaster recovery plans, and cyber measures. These additional costs include the full economic impact of cybercrime.

C. Intellectual Property Theft and Economic Espionage:

Cybercriminals often target valuable intellectual property (IP) and engage in business surveillance, causing serious harm to innovation and financial competitiveness.

i. **IP Theft**: Cybercriminals use cyber espionage to steal trade secrets, research, and proprietary information, causing business losses. This reduces competitive advantage and disrupts business.
ii. **Counterfeit Goods & Piracy**: Online platforms can cause revenue losses in industries such as software, entertainment and pharmaceuticals by allowing counterfeit goods and pirated digital content to be sold and distributed.
iii. **Economic Impacts on Industries:** Private theft and commercial espionage affect the growth, investment and operations of certain businesses. Activities such as technology, R&D and creative industries are affected by this type of cybercrime.

D. Increased Costs of Cybersecurity:

The growing threat of cybercrime requires greater investment in cybersecurity measures, resulting in additional costs for businesses and industries.

i. **Cybersecurity Infrastructure**: Organizations must invest in a secure cybersecurity infrastructure that includes firewalls, intrusion detection systems, encryption, and security software. These investments increase operating costs.
ii. **Workforce & Expertise**: Building a skilled cybersecurity workforce and hiring outside experts to combat cyber threats requires significant financial resources. Hiring cybersecurity experts and training personnel comes with a high price tag.
iii. **Compliance & Regulation**: Regulatory and business standards require compliance with cybersecurity best practices, increasing compliance costs for organizations. Failure to comply may result in a fine or damage to your reputation.

Social Impact of Cybercrime in India

A. Privacy and Data Crime:

Cybercrime has had a major impact on privacy and data breaches in India, wreaking havoc on personal data and sensitive information of individuals and organizations. The social benefits include:

i. **Access to Privacy:** Data breaches and unauthorized access to personal information undermine an individual's right to privacy. Cybercriminals can gain access to sensitive information, including financial details, medical information, or personal photographs, leading to malicious and uncontrolled attacks

ii. **Trusted online platforms**: On e-commerce websites, government portals, users may refuse to provide personal information or participate in online activities, which can affect digital usage and connectivity. This can lead to psychological and emotional distress and poor online security for victims.

iii. **Cyberstalking & Harrassment**: Personal information obtained through cybercrime can be used for cyberstalking, harassment or blackmail. This can cause psychological and emotional harm to victims and undermine online security.

B. **Identity Theft & Fraud:** Cybercrime cases in India mostly involve identity theft and various types of fraud and cause serious social disruption:

i. **Financial loss**: Victims of identity theft may suffer financial loss due to fraud, unauthorized use of credit cards, or loan sharking. This can lead to financial instability and depression for the victim.

ii. **Reputation Damage:** Internet incidents in India frequently involve identity theft and various forms of fraud, leading to social unrest.

iii. **Impersonation & Social Impact:** Identity theft allows cybercriminals to impersonate someone online, causing trust issues in relationships and communities. This can lead

to conflict, misunderstandings, and relationship breakdowns.

C. Impact on Public Trust and Confidence:

The social impact of cybercrime affects public trust and confidence in digital systems, government institutions, and online services:

i. **Confidence in E-governance:** Cybercrime incidents, such as data breaches or hacking of government institutions, can undermine public trust in government electronic measures. This can impact public participation, use of online services, and the digitization of government processes.

ii. **Online Commerce & transactions**: Cybercrime is undermining trust in online shopping, digital payments and e-commerce platforms. Consumers may be reluctant to engage in online transactions due to concerns about fraud, data compromise or identity theft.

iii. **Trust in Online Communication**: Cybercrime undermines trust in online communications, including email, messaging apps or social media platforms. People may be concerned about privacy breaches, social media attacks or unauthorized access to their private conversations.

The societal impact of cybercrime in India highlights the importance of promoting a safe digital environment, increasing cybersecurity awareness, implementing strong privacy protection measures and ensuring public trust in the digital ecosystem.

D. Government Initiatives & Legal Framework:

i. **Cybersecurity Policy & Legislation**: The Indian government has recognized the need to combat cybercrime and has implemented cybersecurity policies and laws to counter this threat. These Includes:

ii. **Information Technology (IT) Act:** The IT Act, 2000 was enacted to address the issue of cybercrime and provide a legal framework for electronic

commerce, data protection and prosecution of cybercrime.

iii. **National Cyber Security Policy:** The National Cyber Security Policy was formulated in 2013 with the aim of developing cybersecurity capabilities, raising awareness and ensuring the security of important information.

iv. **Data Protection Laws**: The personal Data Protection Bill, 2019 was introduced to store and process personal information while ensuring data protection and confidentiality.

E. International Cooperation & Partnership:

i. **International Coorperation Agreements**: India has signed bilateral and multilateral agreements with various countries to promote cooperation in combating cybercrime, sharing information and theft.

ii. **Collaboration with International Organization:** Interpol, the United Nations Office on Drugs and Crime (UNODC) and the International Multilateral Partnership Against Cyber Threats (IMPACT) work together to strengthen cybersecurity capabilities and share information with other countries to share best practices, improve skills and promote international cooperation in preventing cybercrime. However, there are still challenges to effectively combating cybercrime.

iii. **Joint Exercises & workshops**: The government plans joint cybersecurity exercises, seminars and knowledge-sharing platforms with other countries to share best practices, improve skills and promote international cooperation in defence bloc cybercrime.

F. **Challenges in combating Cyber crime**:

Despite the efforts of the Indian government and other stakeholders, several challenges remain in combating cybercrime:

i. **Rapid evolution of cyber threats**: Cyber threats are evolving rapidly and cybercriminals are adapting their strategies. These high levels of cybercrime pose challenges to law enforcement agencies and require continuous

improvement of cybersecurity strategies and technologies.

ii. **Huge disparity among government agencies**: Users are vulnerable to cybercrime due to lack of knowledge about cyber threats and protection. There is also a shortage of professional cybersecurity experts to effectively combat cyber threats.

iii. **Inadequate Infrastructure and Technological Incapabilities**: India's expanding digital ecosystem requires secure cybersecurity infrastructure and capabilities. However, challenges remain, including outdated systems, inadequate investment in cybersecurity infrastructure, and the need to develop capabilities to deal with complex cyber threats.

iv. **Support research and development**: Support cybersecurity, data protection and new technologies to stay ahead of cyber threats and drive innovation in this area. Assess the long-term impact of cybercrime on the Indian economy, including its impact on direct foreign trade, economic competitiveness, and economic growth. Impact and Effect of Cyber Threats Develop more effective strategies to effectively respond to cyber threats.

Cybercrime Laws in India:

Information Technology Act, 2000:

Due to the increase in cybercrimes in India, there is a need to create a special organization to combat cybercrimes. The Information Technology Bill is the first bill to be approved by the Parliament to provide legal certainty to all transactions conducted through electronic exchange of information against cybercrimes. In addition, it amended the Indian Evidence Act, 1972, the Bankers' Books Evidence Act, 1934, the Reserve Bank of India Act and the Indian Penal Code, 1860.

Section 43: This Section of the IT act connected to those cybercriminals who have harmed the computer of the other person alluded to as casualty without consent will be liable for the recompense of the harm.

Section 66: This section spells out the punishment which may extend to 3 years and fine which may extend to Rs 5 lakh, imposed on an offender under Section 43 of the Act.

Section 66B: This section explains that counterfeiting a stolen communication device or computer is punishable with imprisonment up to 3 years and a fine up to Rs.1 lakh.

Section 66C: This section explains that cyber criminals who commit identity theft by stealing passwords or forging digital signatures will be punished with imprisonment of up to 3 years and a fine of up to Rs 1Lakh.

Section 66E: This section describes the crime of taking private photographs without a person's consent and publishing them, which is punishable by up to 3 years in prison or a fine of up to 2 Lakh

Section 66F: This section describes cybercrimes related to cyber terrorism

Section 67: The section explains that publishing substandard electronics is punishable with imprisonment of up to 5 years and a fine of up to Rs 10 Lakh.

Indian Penal Code, 1860

Section 292: This section covers cybercrimes related to the sale of obscenity. All internet crimes related to the publication of obscene and sexual crimes against children fall under this section and are punishable by up to 2 years in prison and a fine of Rs.2,000 - Repeat offenders are sentenced to a maximum of 5 years in prison and a maximum fine of Rs.5,000/-

Section 354C: The Section describes publishing photos or recording video of a woman without her consent, for example: photos of her private parts. This section is broad enough to include voyeurism, which includes watching women have sex without their consent.

Section 379: This section covers theft and theft of electronic devices with stolen data or stolen computers, which can result in sentences of up to 3 years in prison in addition to fines.

Section 420: This section deals with fraud by internet fraud, creating fake websites and using fraudulent means to deliver private goods and is punishable by up to 7 years in prison and a higher fine.

Section 465: This section explains the crime of fraud, which is punishable by up to 2 years in prison under the law.

Companies Act, 2013:

The Companies Act, 2013 was enacted to regulate the day-to-day operations and legal liabilities of companies. Investigate and prosecute serious crimes, including fraud, committed by Indian authorities and Indian companies.

International Cybercrime Laws:

The United States of America: The most common cybercrime law in the United States is the Fraud and Abuse Act, which prohibits computer fraud and abuse and protects state banks and Internet connections from all kinds of threats, abuse, scams, etc. that can come from homes and the world of cybercriminals.

Canada: The Canadian Cybercrime Act operates as a special information policy to curb cybercrime in Canada, combined with the Privacy Act and the Electronic Documents Act to introduce two important cybersecurity measures for Canadian private sector organizations.

European Union: There are many laws, but the general and unified cyber law is the General Data Protection Regulation Act. The law applies to all companies operating in the EU, was established in 2018 and has a particular impact on foreign companies doing business in the EU & provides compensation for victims of cybercrime.

China: China's cyber law is the Information Security Law its main purpose is to protect and secure all important and confidential government information which is important for public interest and this is important to influence the country’s security.

United Kingdom: Cyber laws apply to the UK's Computer Misuse Act 2013, which imposes criminal penalties on criminals who use technology to gain permission to use a computer.

Conclusion:

Cybercrime, with its widespread use and motivation, has penetrated into the heart of government electronic systems. These attacks have serious consequences because they undermine the integrity of public services and threaten the foundations of democratic institutions. The most important effect is the loss of public trust in government. This is therefore the purpose of e-government because it does not use technology to fully engage people and provide good services. Privacy and electronic government. Its impact extends far beyond the digital world because it undermines the integrity of public services, undermines public trust in government and costs money. However, by using a protective cyber security approach, international cooperation, and a commitment to data protection, the government can protect the confidentiality of public information and strengthen their electronic use within the government. Our common mission is to deliver on the promise of e-government and deliver effective, secure and transparent public services while adhering to the principles of freedom and good governance.

References:

1. https://lexpeeps.in/the-impact-of-cybercrime-on-the-indian-economy-and-society/
2. https://www.academia.edu/23704589/Effect_of_cyber_crime_in_Indian_Economy
3. https://www.legalserviceindia.com/legal/article-11766-the-impact-of-cybercrime-on-theindian-economy-and-society.html