IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

To Study on Cyber Crime Burgeoning in India and Crucial Actions Need for Every Cybercrime Victim

Kirti Saneja[1] and Dr. Ajit Kumar[2]
Research Scholar, Department of Computer Science[1]
Research Guide, Department of Computer Science[2]
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India

Abstract: *India is facing a great deal of challenges due to the rapid digitalization and broad adoption of technology in many different areas. One such concern is cybercrime. In this paper explores the nature, scope, and impact of cybercrime in the Indian context. The rising ubiquity of internet usage has rendered people, companies, and governmental organizations more susceptible to a range of cyber threats, such as identity theft, financial fraud, data breaches, and cyber harassment. Despite developments in cyber security protection, the lack of awareness and poor regulatory frameworks has aggravated the situation. To address these issues, the Indian government has put in place a number of efforts, including the National Cyber Security Policy and the Information Technology Act, 2000. But enforcement is still patchy, and a lot of crimes go unreported or ignored. The problem has been made worse by insufficient regulatory frameworks and a lack of knowledge, even in spite of advances in cyber security measures. But enforcement is still patchy, and a lot of crimes go unreported or ignored. This research paper emphasizes India's cybercrime victims have several legal options, the need for a multimodal strategy that includes improved cyber security infrastructure, better legislative frameworks and greater public awareness in order to tackle cybercrime. In light of the transnational character of cyber threats, it also highlights the significance of international cooperation. In the end, a thorough plan is necessary to protect India's digital environment and guarantee the security and safety of its people in a world that is becoming more interconnected by the day*

Keywords: Cyber Security, Threats, Digital Environment, Policy

I. INTRODUCTION

To put it simply, cybercrime refers to illegal activities in which a computer is used as a tool, a target, or both. Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The Information Technology Act of 2000 addresses a variety of new age offenses that have been brought about by computer abuse.There are two ways that we can group cybercrimes.

- **Computer as a Target**: attacking other computers using a computer. Such as DOS attacks,hacking, and virus/worm, attacks.
- **Computer as a weapon**: utilizing a computer to carry out illegal actions in the real world.Such as pornography, credit card fraud, EFT fraud, IPR violations, and cyber terrorism.

Cybercrime include illicit actions such as ransomware, cyber bullying, online fraud, and hacking. Hackers, con artists, or fraudsters are those who engage in cybercrime or other related acts. Financial loss results from cybercrime for those who become victims of it. Cybercrime frequently violates an individual's privacy by taking their private information, such as private messages, images, and sensitive data, which can then be utilized for malevolent purposes or blackmail.
Numerous governmental and non-governmental entities are operational. To combat cybercrime by educating the public, providing cyber security training, putting strong security measures in place, and passing legislation that specifically address cybercrime.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

- **Identity Theft:** When personal data is taken, it is utilized fraudulently. Social engineering or data breaches may be the cause of this.
- **Cyber bullying:** Intimidation or harassment through the use of internet platforms, especially directed at children.
- **Hacking:** Unauthorized access to systems with the intention of stealing or altering data; typically directed at businesses or government organizations.

1.2 Problems on hand

India's cybercrime problem is becoming worse, and the public and government need to keep paying attention to it. Strong legal frameworks, awareness campaigns, and education are necessary to properly counter this ever-evolving menace.

The usage of online services, digital transformation, and greater internet penetration has all contributed to an upsurge in cybercrime in India in recent years. The following are some major causes of this issue:

- **Rise in Internet Use:** The number of people using the internet has increased, especially since the pandemic, which has greatly increased the attack surface for cybercriminals
- **Lack of Awareness**: Users are more vulnerable to malware, phishing, and scams since many are not completely aware of cyber security best practices.
- **Inadequate Cyber security Infrastructure**: Many small and medium-sized firms lack the resources required to implement robust cyber security procedures, despite the fact that some companies are stepping up their security measures.
- **Sophistication of Attacks**: More advanced techniques that are more difficult to identify and stop, such ransomware and social engineering are being used by cybercriminals.
- **Regulatory Challenges**: The implementation of cyber laws may exhibit heterogeneity, and numerous incidents remain unreported or unresolved owing to inadequate legal frameworks or resources.
- **Financial Crimes**: Financial crimes such as credit card fraud and online banking fraud are on the rise, impacting both individuals and companies.
- **Data Privacy Concerns**: As data breaches proliferate, the protection of personal and sensitive information remains a serious worry, leading to increasing distrust in digital platforms.

Malicious software with the potential to steal data or lock files and routinely demand payment in order to be unlocked is called ransomware, also referred to as malware.

II. LITERATURE REVIEW

Researching cybercrime in India involves a comprehensive approach that includes various methodologies to understand its nature, prevalence, impacts, and responses.

Bansal & Arora (2012): Cybercrime, as described by is any illegal activity that involves computers and the internet, with a focus on crimes like online fraud, phishing, identity theft, and hacking. They contended that as more people have access to the internet, cybercrimes have skyrocketed in India.

Saini & Saini (2014): highlighted how the country of India's increasing digitization, e-governance programs, and growing smartphone usage are all factors in the rise in cybercrime. India is susceptible because of the growth of digital platforms without commensurate advancements in cyber security.

Saxena (2015): stated that cybercrime comprises both the technological component (virus, hacking) and the social aspects (fraud, exploitation, privacy violation). He pointed out that new developments in technology are bringing about trends like ransomware and social engineering attacks.

Gupta (2016): To classify cybercrimes into other categories, including cyber terrorism (attacks on vital infrastructure), cyber bullying, and financial crimes (phishing, credit card fraud). An essential framework for comprehending the state of cybercrime in India was supplied by Gupta's research.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

Kumar & Mittal (2018): Emphasized how cybercrimes are distributed geographically and demographically. Major cities like Bangalore, Delhi, and Mumbai are the hubs of cybercrime activity, according to their research. Increased internet usage and technical developments in these fields are partially to blame for this.

Banerjee (2022) urged the continuation of empirical studies that examined the psychological characteristics of Indian cybercriminals. Better preventive measures, he added, might result from an understanding of the motivations behind cybercrimes.

2.1 Objectives

- To study on main causes and types of cybercrime in India.
- To demonstrate the States with the most Number of Crimes in India.
- To focus on have a number of legal options and actions of every Cybercrime Victim need to stay safe and secure.
- To describe the government agencies in India that tackle cybercrime, along with their roles and responsibilities:

2.2 Research Methodology

Quantitative Research

Surveys:

- Design questionnaires targeting various demographics (e.g., general public, businesses, and law enforcement).
- Use online platforms to distribute surveys widely.

Data Analysis:

- Analyse crime statistics from government agencies (e.g., NCRB) and private cyber security firms.
- Analysis on what crucial actions every cybercrime victim needs.
- Analysis on top most states of India where increasing the cyber-crime day by day.

Qualitative Research

- Interviews: Hold semi-structured interviews with relevant parties, including victims of cybercrime, law enforcement officers, and cyber security specialists.
- Case Studies: Examine individual cybercrime instances in India to comprehend the background, strategies, and reactions.

Policy Analysis-Assess government initiatives and policies aimed at tackling cyber-crime.

2.3 Data Collection-Primary data and Secondary data.

- **Government Reports**: Agencies like the Ministry of Home Affairs (MHA) and the National Cyber Crime Reporting Portal (NCRP) provide annual reports on cybercrime statistics.
- **Law Enforcement Agencies**: The Cyber Crime Cells of various state police departments collect and report data on cybercrime incidents.
- **Research Organizations**: NGOs, think tanks, and academic institutions often conduct studies and publish findings on cybercrime trends and impacts.

III. INDIA'S ADOPTION OF DIGITAL TECHNOLOGIES

India's adoption of digital technologies will only increase the difficulty of cybercrime. To properly tackle this issue, on-going legislative measures, law enforcement training, and public awareness campaigns are crucial. India is facing a serious problem with the rise of cybercrime, one that calls for coordinated actions from the public and commercial sectors. Recent years have witnessed a notable surge in cybercrime in India, primarily due to factors such as higher internet usage, the growth of digital payments, and an increased dependence on online services. Here are some key points:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

- **Types of Cybercrime**: Phishing, identity theft, ransomware attacks, online fraud, and cyber bullying are examples of common kinds. The proliferation of digital banking and e-commerce has led to a notable increase in financial fraud.
- **Effect of the Pandemic**: The COVID-19 pandemic hastened the adoption of digital technology, increasing the susceptibility of people and companies to online dangers.
- **Government Response**: The Indian government has implemented various measures, including the introduction of laws like the Information Technology Act and initiatives like the Cyber Crime Coordination Centre to combat cybercrime.
- **Public Awareness**: There is an on-going need for public education regarding safe online practices, as many cybercrimes exploit human vulnerabilities rather than just technical flaws.
- **Emerging Threats**: As technology evolves, new threats like deep fakes, AI-driven attacks, and more sophisticated scams are becoming prevalent.
- Addressing cybercrime requires a multifaceted approach, including better law enforcement training, international cooperation, and public awareness campaigns.India is facing a serious problem with the rise of cybercrime, one that calls for coordinated actions from the public and commercial sectors. The main causes of cybercrime in India are:
- **Rapid Digitalization:** More people and businesses are utilizing digital services as a result of the Digital India project. Cyber security precautions, though, haven't always kept up with this expansion.

Insufficient Cyber security Awareness: A lot of people, particularly in remote or less tech-savvy areas, don't know the basics of cyber security, which leaves them open to fraud.

- **Weak Legal Framework**: India's legal system is not very strong, and even though legislation like the Information Technology Act of 2000 have been revised to handle cybercrimes, there are frequent delays in the courts.
- **Increasing Use of Mobile and Online Payment Systems**: Fraud and cyber-attacks targeting financial data have increased in tandem with the explosive expansion of digital payments, particularly through UPI and mobile wallets.
- **Increase in Internet Users:** India is now the nation with the second-highest percentage of internet users. Since many of these users are new to the platform, there is a higher chance that they will become victims of cybercrimes.

3.1 Challenges

- **Issues with underreporting:** Many victims are humiliated or mistrustful of the legal system, which makes them hesitant to report cybercrimes.
- **Skill Gap**: Law enforcement does not have enough skilled personnel to successfully combat cybercrimes. **Rapid technical advancement** usually means that cybercriminals are able to seize new opportunities before law enforcement can react appropriately.

3.2 Government Initiatives

The government has launched a number of programs to combat cybercrime, such as:

- The Cyber Crime Prevention against Women and Children (CCPWC) scheme
- The Emergency Response Support System (ERSS)-112
- Safe City Projects
- Strengthening State Forensic Science Laboratories (SFSLs)
- Integration of Women Helpline (WHL)-181 with ERSS
- The Indian Cyber Crime Coordination Centre (I4C)

State wise crime rate all kinds of crimes are registered with the Government of India's National Crime Records Bureau (NCRB). For its annual report, the NCRB receives data from the State Crime Records Bureau (SCRB) and the District Crime Records Bureau (DCRB) each year. There is also data from megacities (cities with a million people or more).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

This information is given individually by district and is grouped by different sections of the Indian Penal Code (IPC). India's crime rate dropped from 487.8 incidences per 100,000 people in 2020 to 445.9 in 2021, according to the NCRB. States and types of crimes have different incidence and rates of crime. Comprehending this data is essential for preparing for the UPSC since it offers insights into the trends and patterns of crime in India. Go here to read more:
Summarizing key government agencies in India that tackle cyber-crime, along with their roles and responsibilities:

Sr. No.	Agency	Role
1	Ministry of Home Affairs	Formulates policies and guidelines for cyber security; coordinates with state agencies.
2	Indian Computer Emergency Response Team (CERT-In)	Responds to cyber security incidents; provides alerts and advisories on cyber threats.
3	Cyber Crime Cell (CCCs)	Specialized units in various states; investigate cybercrimes, gather intelligence.
4	Central Bureau of Investigation (CBI)	Investigates serious cyber-crimes; coordinates with other agencies for complex cases.
5	National Cyber Security Coordinator	Oversees national cyber security strategies; ensures collaboration among agencies.
6	Enforcement Directorate (ED)	Investigates financial crimes, including those involving cyber elements (like money laundering).
7	Intelligence Bureau (IB)	Gathers intelligence on cyber threats to national security; works on preventive measures.
8	Police Departments	Local law enforcement units handle basic cybercrime cases and awareness programs.
9	Digital India Initiative	Promotes digital literacy and cyber security awareness among citizens.

Table-1 Government Agencies in India that Tackle Cyber Crime

3.3 States with the most Number of Crimes

According to the most recent data from the National Crime Records Bureau (NCRB), India's 2024 Latest Crime Rate Report was 445.9 per 100,000 people. Theft was found to be the most common crime, followed by robbery and assault. It was determined that the states with the highest rates of crime in the nation were Uttar Pradesh, Kerala, Maharashtra, Delhi, and Bihar. The report also showed an alarming increase in domestic abuse cases and cybercrimes, which reflected the evolving nature of criminal activity in the nation.

- **Uttar Pradesh**: The rate of crime per person in the state is 7.4. Uttar Pradesh has the highest crime rate, according to the National Crime Records Bureau, suggesting that it is not a safe area to travel alone.
- **Arunachal Pradesh**: Because of its high rate of crime and other problems, the state is ranked second in terms of danger. Traveling by yourself after dark is prohibited in several areas of Arunachal Pradesh. The crime rate, which is 5.8, is rising in tandem with an increase in crimes.
- **Jharkhand:** Jharkhand is another state whose risk factor shouldn't be disregarded. The public's safety has not received much attention. A significant portion of criminal incidents are not even recorded in police reports.
- **Meghalaya**: Meghalaya comes in fourth place for both crime and security. There are rumoured to be dangerous and off-limits travel spots in Meghalaya. According to current reports, the state is regarded as one of the most hazardous in India, with a reported 5.1 crimes per capita.
- **Delhi:** Despite Delhi's fifth-place position, the state has five crimes per 1,000 residents, according to the crime bureau. Regretfully, despite the state's political might controlling the scene, not much has been done to guarantee the state's safety

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

EFFECT AND CAUSES OF CYBERCRIME CASES IN INDIA

Sr. No	Year	Cybercrime Cases in India	Effect and Causes
1	2017	**44,546 cases**	There was a noticeable rise in cases due to increased internet usage and digital financial transactions.
2	**2018**	**27,248 cases**	Many cases involved fraud, followed by sexual exploitation and attempts to cause disrepute (defamation).
3	**2019**	**44,546 cases**	The sharp increase from 2018 is attributed to better reporting mechanisms and rising cyber threats.
4	**2020**	**50,035 cases**	The COVID-19 pandemic saw a rise in online fraud, phishing attacks, and exploitation due to increased online activities.
5	**2021**	**52,974 cases**	Increased awareness of cyber security threats led to more reports, with financial fraud being the leading category.
6	2022	60,000 (estimated)	Online fraud, phishing attacks
7	2023	70,000 (estimated)	Online fraud, phishing attacks sexual exploitation and attempts to cause disrepute

Table-2 (Effect and Causes of Cybercrime Cases in India)

Chart Analysis:

- **Steady Increase**: The number of cybercrime cases reported has increased significantly from 2015 to 2023.
- **Notable Jumps**: The largest jumps are observed between 2016-2017 and 2018-2019, potentially linked to digital transformation initiatives and increased internet penetration.
- **Pandemic Impact**: There was a notable increase during the COVID-19 pandemic, as remote working led to more cyber threats.

3.4 Latest Crime Rate Report of India 2024

- **Overall Crime Rate**: For every 100,000 individuals in India in 2024, there were 445.9 recorded crimes.
- **Common Crimes**: Robbery and assault are the next most common crimes, after theft.
- **High Crime States**: The states with the highest rates of crime include Uttar Pradesh, Kerala, Maharashtra, Delhi, and Bihar.
- **Urban vs. Rural**: Urban areas have greater crime rates than rural ones.
- **Causes of the Decline:** More police presence, improved law enforcement, and greater public awareness of crime have all contributed to a decline in the overall crime rate.
- **Obstacles to Come**: Even with these advancements, there are still issues, such as the requirement for increased funding for law enforcement and improved training for police officers.

3.5 Security of the System

The process of safeguarding information systems against unwanted access, alteration, or destruction is known as system security. It aids businesses in thwarting cyber-attacks and safeguarding sensitive data.Using free antivirus Online 35%, Using Paid antivirus 25%,Security and provided by browser 10%.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

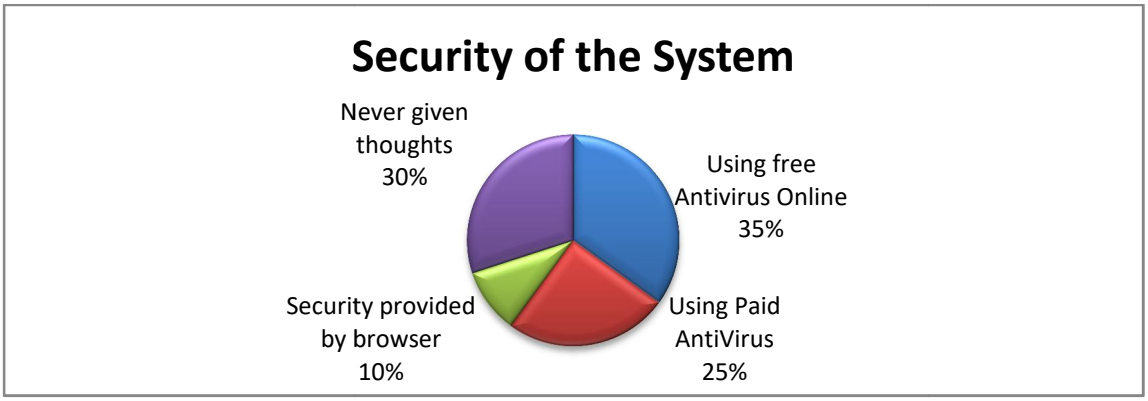

Figure 1(Security of the System

3.5.1 Cybercrime victims in India have a number of legal options:

- **Making a grievance** -Using the National Cyber Crime Reporting Portal, submit a complaint online. Users can anonymously report cybercrime on this law enforcement agency-managed platform. In addition, users can follow the development of their case and upload evidence.
- **Going to a cyber-cell** -Submit a complaint to the cyber cell located closest to your residence or to one in your city.
- **Looking for different ways to resolve disputes** -Think about mediation or arbitration, which can be less expensive and speedier than traditional litigation.
- **Making a claim with insurance -**you can submit a claim to get your damages reimbursed if you have cyber insurance.
- **Preventive actions** -Put cyber security safeguards into place, carry out security audits, and increase public knowledge of cyber dangers.

3.5.2 Crucial Actions for Every Cybercrime Victim Needs To Take

The number of cybercrime cases recorded in India* has increased by 350%. All forms of theft, from simple phishing emails to advanced malware assaults, aim to obtain personal information or interfere with your systems' ability to access it. Consumers becoming victims of cybercriminals is frequently caused by elements including high-speed internet connectivity, the rise in smartphone usage, and a lack of knowledge about Internet security. As vital as it is to stay safe and secure, it's also critical to know what to do if you fall victim to cybercrime.

The following actions are recommended to help reduce the risk.

- **Cut off and separate**-The best course of action to stop more data loss in the event of a continuing attack on your computer or IT infrastructure is to disconnect the device from the Internet. Before taking legal action in cases of cyber bullying or cyber stalking, the victim should only turn away from the screen.
- **File a lawsuit**-Even while you are attempting to lessen the bad effects of the cybercrime, do not disregard it, delay the procedure, and file a lawsuit. To lodge a formal complaint against the cybercriminals, get in touch with your neighbourhood Cybercrime Investigation Cell. Give thorough details regarding: The type of offense committed, the degree of the harm Documents, statistics, and more pertinent information pertaining to the compliance.
- **Inform your Contacts-** Cybercriminals may exploit the theft of your virtual identity to obtain personal information and data from all of your online acquaintances. To get the word out about the occurrence, use social media. By taking one easy step, you may reduce the chance that someone will exploit your identity to commit new crimes and raise awareness of cybercrime among your friends and family.
- **Make Future Preventive Measures -** Install authorized antivirus software, create a secure password with a mix of alphanumeric and alpha characters, and never give out your banking information to third parties.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

3.6 Limitation

India lacks effective international agreements and methods to effectively handle cybercrime across borders.
Study only on Cyber-crime in India.
Reporting cybercrimes can be difficult for victims, especially businesses, because they worry about losing their good name, losing the faith of their clients, or possibly incurring negative consequences.

3.7 Result and discussion

Even in the face of an increase in cybercrime instances in India, most people are still generally ignorant of basic cyber security procedures, which make them easy targets and these all are handled by to take important steps that every cyber -crime victim must take for safeguarding.

Government Initiatives

- **National Cyber Security Policy**: Launched to strengthen the country's cyber security framework.
- **Public Awareness Campaigns**: Initiatives aimed at educating the public about safe online practices.
- **Capacity Building**: Training law enforcement and cyber security professionals to better handle cybercrime cases.
- **National Database of Cybercrime**: By tracking incidences, investigations, and convictions related to cybercrime, a centralized database would be useful for identifying patterns and developing more effective preventative measures.
- **Research Institutions for Cybercrime**: Setting up centres for research on cyber security and cybercrime will aid in the development of cutting-edge tactics and technologies that will help organizations remain ahead of ever-evolving threats. Specialized cybercrime units have been established by the government inside law enforcement authorities. The purpose of the Cyber Crime Cells is to manage complaints and look into violations; they frequently work in tandem with foreign authorities.

IV. CONCLUSION

This research explained the effects and causes of cybercrimes on several societal levels in India and how to increase day by day.In India, the main law addressing cybercrime is the Information Technology Act, 2000. Despite the modifications, the act still does not provide a thorough coverage of new cyber threats, including deep fakes, crimes involving crypto currencies, and attacks powered by artificial intelligence.In addition to focusing on understanding cybercrimes and way of protection from cyber threats.It is imperative that we all keep in mind that the benefits of constantly evolving technologies have left us with a shared legacy of cyberspace, which we have inherited throughout our lives. Given that cyberspace is the lifeline of the entire universe and that it is here to stay, it is the responsibility of every netizen to work toward keeping it free of criminal activity and other problems.

REFERENCES

[1]Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672 (2019).
[2]Floyd, D.H., Shelton, J.W., Bush, J.E.: Systems and methods for detecting a security breach in an aircraft network. In. Google Patents, (2018)
[3]Ron, M.: Situational Status of Global Cybersecurity and Cyber Defense According to Global Indicators. Adaptation of a Model for Ecuador. In: Developments and Advances in Defense and Security: Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018) 2018, p. 12. Springer
[4]Taha, A.F., Qi, J., Wang, J., Panchal, J.H.: Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. IEEE Transactions on Smart Grid 9(2), 886-899 (2018).
[5]Taylor, R.W., Fritsch, E.J., Liederbach, J., Saylor, M.R., Tafoya, W.L.: Cyber Crime and Cyber Terrorism. (2019).
[6]Valeriano, B., Maness, R.C.: International Relations Theory and Cyber Security. The Oxford Handbook of International Political Theory, 259 (2018).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

[7] von Solms, B., von Solms, R.: Cybersecurity and information security–what goes where? Information & Computer Security 26(1), 2-9 (2018).
[8]http://www.cyberlawsindia.net/cyber-india.html
[9]https://en.wikipedia.org/wiki/Information_Technolo gy_Act,_2000
[10]http://www.cyberlawsindia.net/cyber-india.html
[11]https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
[12]https://www.ijarcsse.com/docs/papers/Volume_5/8_ August2015/V5I8-0156.pdf
[13]https://cybercrime.gov.in/webform/Crime_NodalGrivanceList.aspx