ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

Volume 11, Issue 2, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

IMPACT FACTOR: 7.583

| www.ijarasem.com | ijarasem@gmail.com | +91-9940572462 |

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 11, Issue 2, March 2024 |

Cyber Laws- Advantages and Significance

Vijayant Sinha

Faculty of Law, Dept. of Law, Chanakya National Law University, Patna, Bihar, India

ABSTRACT: Cyber law, also known as internet law or digital law, signifies the legal regulations and frameworks governing digital activities. It covers a large range of issues, including online communication, e-commerce, digital privacy, and the prevention and prosecution of cybercrimes. As the internet has become a fundamental part of our daily lives, cyber law has become crucial in ensuring digital space's orderly and secure functioning.
KEYWORDS-cyber law, crime, security, internet, digital

I.INTRODUCTION

The significance of cyber law lies in its capacity to navigate and regulate the intricate challenges that arise from the pervasive use of technology. Cyberlaw provides a framework for protecting individuals and organizations from cyber threats, ensuring the privacy and security of digital transactions, and establishing guidelines for ethical and legal conduct in cyberspace. As the digital world evolves, the importance of cyber law becomes more pronounced, serving as a cornerstone for the responsible and lawful utilization of digital resources.

Advantages of Cyber Law

- Protection Against Cybercrimes:

Cyber laws act as a deterrent by offering legal recourse and prescribing penalties for various cybercrimes. This proactive approach helps curb illegal online activities and provides a safer digital environment for individuals and businesses alike.[1,2,3]

- Data Privacy:

Safeguarding individuals' digital information is a paramount concern addressed by cyber laws. These regulations ensure that organizations handle personal data responsibly, establishing a foundation of trust in digital transactions and interactions.

- E-commerce Regulation:

The legal framework provided by cyber laws is crucial for the regulation of e-commerce. It defines rules for online transactions, contracts, and consumer protection, thereby fostering a fair and secure online marketplace.

- Intellectual Property Protection:

Cyber laws play a pivotal role in protecting intellectual property rights in the vast digital domain. These laws prevent the unauthorized use and distribution of digital content, encouraging innovation and creativity by safeguarding the fruits of intellectual labor.

- Cybersecurity Standards:

Cyber laws contribute significantly to the establishment of cybersecurity standards. By mandating organizations to implement measures for the protection of their networks and systems, these laws address the evolving landscape of cyber threats.

Types of Cybercrime

- Phishing:

Phishing involves deceptive attempts to obtain sensitive information, like passwords or credit card details, by posing as a trustworthy entity. Cyber laws play a crucial role in prosecuting individuals engaged in phishing activities.

- Hacking:

Unapproved access to computer systems or networks to gather, alter, or destroy data constitutes hacking. Cyber laws define and penalize such activities, ensuring legal consequences for those who breach digital security.

- Identity Theft:

Illegally acquiring and using someone else's personal information for fraudulent activities falls under the purview of cyber laws. The legal framework addresses identity theft, protecting individuals whose identities may be compromised.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 11, Issue 2, March 2024 |

- Ransomware:

Ransomware involves the use of malicious software to encrypt files, demanding payment for their release. Cyber laws aim to prevent and prosecute individuals involved in orchestrating ransomware attacks.

- Online Scams:

Cyber laws address fraudulent schemes conducted over the internet to deceive individuals for financial gain. These laws provide legal recourse for victims and impose penalties on perpetrators.

- PUPs (Potentially Unwanted Programs):

Cyber laws address software that may harm a computer or its user, often installed without the user's knowledge. This helps regulate the distribution of potentially harmful programs and protects users.[4,5,6]

- Denial of Service Attack:

Overloading a system, network, or website to make it unavailable to users constitutes a denial of service attack. Cyber laws define and penalize such attacks, discouraging individuals from engaging in disruptive online activities.

- Cyberstalking:

Cyber laws are made to tackle ongoing online harassment or stalking carried out through electronic methods. These laws recognize the seriousness of cyberstalking and provide legal avenues for victims to seek protection.

II.DISCUSSION

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes 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 abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways

- The Computer as a Target :-using a computer to attack other computers.
  e.g. Hacking, Virus/Worm attacks, DOS attack etc.
- computer as a weapon :-using a computer to commit real world crimes.
  e.g. Cyber Terrorism, IPR violations,Credit card frauds, EFT frauds, Pornography etc.

Cyber law (also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. Yes, Cyberlaw does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails , to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyberlaw for your own benefit.

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 11, Issue 2, March 2024 |

the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.[7,8,9]

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

III.RESULTS

Cyber laws that everyone using the internet must be aware of
Internet is just like life. It is interesting and we spend a lot of time doing amusing things here, but it comes with its fair share of trouble. With the technology boom and easy Internet access across the country, cyber crime, too, has become a pretty common occurrence. From hacking into computers to making fraudulent transactions online, there are many ways in which we can become a victim of illegal cyber activities.

To regulate such activities that violate the rights of an Internet user, the Indian government has the Information Technology Act, 2000, in place. Here are some of its sections that empower Internet users and attempt to safeguard the cyberspace.

Section 65 – Tampering with computer Source Documents
A person who intentionally conceals, destroys or alters any computer source code (such as programmes, computer commands, design and layout), when it is required to be maintained by law commits an offence and can be punished with 3 years' imprisonment or a fine of 2 Lakhs INR or both

Section 66 - Using password of another person
If a person fraudulently uses the password, digital signature or other unique identification of another person, he/she can face imprisonment up to 3 years or/and a fine of 1 Lakh INR.

Section 66D - Cheating Using computer resource
If a person cheats someone using a computer resource or a communication device, he/she could face imprisonment up to 3 years or/and fine up to 1 Lakh INR

Section 66E - Publishing private Images of Others
If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge, the person is entitled to imprisonment up to 3 years of fine up to 2 Lakhs INR or both[10,11,12]

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 11, Issue 2, March 2024 |

Section 66F - Acts of cyber Terrorism
A person can face life imprisonment if he/she denies an authorized person the access to the computer resource or attempts to penetrate/access a computer resource without authorization, with an aim to threaten the unity, integrity, security or sovereignty of the nation. This is a non-bailable offence.

Section 67 - Publishing Child Porn or predating children online
If a person captures, publishes or transmits images of a child in a sexually explicit act or induces anyone under the age of 18 into a sexual act, then the person can face imprisonment up to 7 years or fine up to 10 lakhs INR or both

Section 69 - Govt.'s Power to block websites
If the government feel it necessary in the interest of sovereignty and integrity of India, it can intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. The power is subject to compliance of procedure. Under section 69A, the central government can also block any information from public access.

Section 43A - Data protection at Corporate level

If a body corporate is negligent in implementing reasonable security practices which causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages to the affection person.
“The Cyber Law & Data Governance Division, operating under the Ministry of Electronics and Information Technology (MeitY), assumes a pivotal role in shaping India's digital landscape. Since the inception of the Information Technology Act in 2000, this division has been at the forefront, fostering electronic transactions, providing legal validation for e-commerce, facilitating e-governance, preventing computer-based crimes, and implementing robust security measures.
A notable recent addition to the division’s initiatives is the Digital Personal Data Protection Act of 2023, a landmark legislation that adeptly balances individual privacy rights with the imperative to process digital personal data for lawful purposes. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 further showcase the division's commitment to regulating social media intermediaries, online gaming, and safeguarding digital citizens. The establishment of a Grievance Appellate Committee reflects the division's dedication to resolving social media grievances where grievance officers couldn't provide relief to the social media users in India.

Moreover, the division actively pioneers frameworks for data governance and protection, crucial for establishing an open, safe, trusted, accountable, and adaptable cyberspace. Acknowledging data protection as a fundamental right for Indian citizens, the division formulates policies to safeguard these rights. Furthermore, the division delves into the legal implications of cutting-edge technologies such as IoT, Blockchain, and Artificial Intelligence, while also addressing aspects of Competition Law, Company Law, Copyright Act, and Intellectual Property Rights (IPR) protection within the domain of information technology. In essence, the division operates as a guardian of digital rights, ensuring a secure cyberspace that is indispensable for the nation's digital economy growth.”[13,14,15]

Significance of Cyber Law
Cyber laws are formed to punish people who perform any illegal activities online. They are important to punish related to these types of issues such as online harassment, attacking another website or individual, data theft, disrupting the online workflow of any enterprise and other illegal activities.
If anyone breaks a cyber law, the action would be taken against that person on the basis of the type of cyberlaw he broke, where he lives, and where he broke the law. It is most important to punish the criminals or to bring them to behind bars, as most of the cybercrimes cross the limit of crime that cannot be considered as a common crime.
These crimes may be very harmful for losing the reliability and confidentiality of personal information or a nation. Therefore, these issues must be handled according to the laws.

- When users apply transactions on the Internet, cyber law covers every transaction and protect them.
- It touches every reaction and action in cyberspace.
- It captures all activities on the Internet.

Areas involving in Cyber Laws
These laws deal with multiple activities and areas that occur online and serve several purposes. Some laws are formed to describe the policies for using the Internet and the computer in an organization, and some are formed to offer people security from unauthorized users and malicious activities. There are various broad categories that come under cyber laws; some are as follows:

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 11, Issue 2, March 2024 |

Fraud
Cyber laws are formed to prevent financial crimes such as identity theft, credit card theft and other that occurring online. A person may face confederate or state criminal charges if he commits any type of identity theft. These laws have explained strict policies to prosecute and defend against allegations of using the internet.

Copyrighting Issues
The Internet is the source that contains different types of data, which can be accessed anytime, anywhere. But it is the authority of anyone to copy the content of any other person. The strict rules are defined in the cyber laws if anyone goes against copyright that protects the creative work of individuals and companies.
Scam/ Treachery
There are different frauds and scams available on the Internet that can be personally harmful to any company or an individual. Cyber laws offer many ways to protect people and prevent any identity theft and financial crimes that happen online.[16,17,18]

IV.CONCLUSON

Online Insults and Character Degradation
There are multiple online social media platforms that are the best resources to share your mind with anyone freely. But there are some rules in cyber laws if you speak and defaming someone online. Cyber laws address and deal with many issues, such as racism, online insults, gender targets to protect a person's reputation. People using the internet depends on cyber laws and policies to protect their personal information. Companies or organizations are also relying on cyber laws to protect the data of their users as well as maintain the confidentiality of their data.
Contracts and Employment Law
When you are visiting a website, you click a button that gives a message to ask you to agree for terms and conditions; if you agree with it, that ensures you have used cyber law. For every website, there are terms and conditions available that are associated with privacy concerns.
Trade Secrets
There are many organizations that are doing online businesses, which are often relying on cyber laws to protect their trade secrets. For example, online search engines like Google spend much time to develop the algorithms that generate a search result. They also spend lots of time developing other features such as intelligent assistance, flight search services, to name a few and maps. Cyber laws help these organizations to perform legal action by describing necessary legal laws for protecting their trade secrets.[19]
How to protect yourself on the Internet
Although the Internet is a resource that contains multiple different types of content, there are many hackers or unauthorized users that may be harmful to you in order to thief your personal information. Below are given all of the steps that may help you to keep your personal information and computers safe while using the Internet. All of the given steps or suggestions can be beneficial for all computer users, even if what type of computer, device, or operating system they are using.

Verify data is encrypted
When you are sending any confidential information, such as debit card numbers, credit card numbers, usernames, or passwords, send these types of information securely. In Internet browsers, look for a small lock (Internet browser security lock) to verify this; an icon will be shown in the right corner of the bottom of the browser address bar or browser Window. If you see the icon, it should be in a locked condition and not in an unlocked position.
If the lock icon is in the locked position and data is intercepted, the data is encrypted that helps to keep secure your data and prevent others to understand it. The data can be read by anyone if the lock is in the unlocked position or no lock is visible because all information will be in the form of plain text. For example, an online forum is not secure, use a password, but you will not use the password with protected sites like an online banking website.

Use a safe password
Like online bank site or other websites that contain confidential information, need to use very strong passwords, it is also recommended; you must use the different and strong password for all websites that require login id and password. You could use a password manager if you required help to remember your password.

Keep your software and operating system up-to-date

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 11, Issue 2, March 2024 |

To protect yourself on the Internet, it is better to update your software installed on your computer and operating system regularly. It is necessary because many updates are released by the developers of the operating system that are related to computer security-related issues. Therefore, you should update your system when the latest updates are released.

When available always enable two-factor authentication

You can use the two-factor authentication feature to make more secure your accounts, like Gmail or others that require a login and contain your private data. It offers advanced protection by adding an additional step in verifying you at the time of login. If you enable two-factor authentication and the service does not verify your computer or other devices after authenticating your password, it sends a text message with a verification code on your cell phone. It includes more powerful security; for example, if someone knows your password of any account and tries to access your account, but he does not have your phone, he cannot access your account even with a valid password.

Always be cautious of e-mail links and attachments

The email attachments and hyperlinks sent through email are the most common resources to spread viruses and malware. It is recommended to always be extremely cautious to open any attachments and hyperlinks, which you have received through email from others, even if they have sent by friend or family.

Be aware of phishing scams

There are many phishing scams and techniques that can be more harmful in respect to losing your secret information. Therefore, it is necessary to familiarize yourself with these types of techniques. Hackers mainly target websites that need a login, such as PayPal, eBay, Amazon, online banking sites, and other popular sites.

E-mail is not encrypted

If you send any confidential information through email, it can be read or understood by unauthorized users as email is not encrypted. Therefore, confidential data like debit card information, credit card information, password and more should not be transmitted over e-mail.

Use an alternative browser

For protecting your systems, Internet browsers also play an important role. For example, earlier versions of Internet Explorer are not more secure. If you are using a lass secure browser in terms of your browser like Internet Explorer, you should switch to another browser like Mozilla Firefox or Google Chrome. Also, if you are using Microsoft Windows 10 operating system on your computer and want to stay to use a Microsoft Internet browser, you can switch to the Microsoft Edge rather than Internet Explorer that is more secure in terms of protecting your systems.

Use caution when accepting or agreeing to prompts

When you are indicated to install an add-on or any program, before clicking on the Ok button, you need to read and understand the agreement carefully. If you do not understand the agreement or feel it is not necessary to install, you should not install this kind of program, cancel or close the window, which may be harmful for you.

Also, when you are installing an add-on or any program, you need to care about any check box that asks if this third-party program will be ok to install. These often cause more issues and leave these boxes unchecked because these are never required.

Be cautious where you are logging in from

Business

If you are working in any organization, your place of work can monitor your computer by installing key loggers or use other methods. In this case, someone can collect usernames and passwords and read these logs if he has access to this information. It can be more harmful to lose your personal information. Additionally, if your computer is shared with other co-workers, do not store any passwords in your browser.

Wireless network

When you are using a wireless network, you must be careful that all the information sent from your computer and to your computer can be read and intercepted by any unauthorized person. You can log in to the network securely with the help of using WPA or WEP and prevent losing your secret information. Furthermore, make sure the network is secure if it is a home wireless network.

Friend's house

Sometimes, you may use your friend's computer and log in to your account on that computer, which may not be fully secure. Intentionally or unintentionally, you can enter your username and password on your friend's computer or the computer with whom you are not familiar. Finally, never save the password information on your friend's computer browser when you are logging into any site on a friend's computer.

Always think before you share something

There are many social media sites, such as Instagram, Facebook, that enable you to make online friends and connect with them. The networking sites are also the best place to share your personal information with your friends, family or others.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 11, Issue 2, March 2024 |

When you share something on social networking sites or the Internet, make sure you are not sending any information that can be harmful to you if everyone sees it. The sent information on the social network or the Internet should be public. Also, make sure you are sharing such something that will not offend anyone or embarrass you, and you must not be uploaded on the Internet.

Update Internet browser plugins

You should update Internet browser plugins or install the latest plugins to protect yourself while online on the computer. Due to browser plugins like Adobe Flash, attackers may find some easiness or security vulnerabilities to hack any system. Therefore, you need to check out regularly that all your installed Internet plug-ins are up-to-date.

Be aware of those around you

If you are working on the computer at any public area, school, library and more, make sure anyone is not looking at your screen, as there will be many people around you. On the other hand, it can be cautious if anyone is looking at your system screen that is called shoulder surfing. If you are required to system screen private, you can use a privacy filter for the display.

Secure saved passwords

There are many users that are habitual to save login information and password on the system, but it can be insecure. Therefore, make sure you are storing your personal details, such as credit card detail and account passwords, in a secure area. It is recommended for everyone to use a password manager to save your passwords.

A password manager is a software that holds all securely encrypts and login information, and password protects that information. If you save a password in a browser and anyone has access to your Internet browser, the password information may be seen by that person. For instance, in the Firefox Internet browser, anyone can see all stored passwords if you do not set up a master password.

Do not always trust what you read online

You should be aware about that it is possible for anyone to publish a website on the Internet. There are various creators who may have intention for creating a site only for malicious purposes. For instance, a website can be created to gain unauthorized access and spread fear, lies, or malware[20]

REFERENCES

1. A Murray, Information Technology Law: The Law and Society (3rd edn 2016)
2. ^ Computer Law: Drafting and Negotiating Forms and Agreements, by Richard Raysman and Peter Brown. Law Journal Press, 1999–2008. ISBN 978-1-58852-024-1
3. ^ "Everything You Need to Know About the California Privacy Rights Act". spark. 2022-10-13. Retrieved 2023-02-09.
4. ^ "How Europe's new digital law will change the internet". The Economist. ISSN 0013-0613. Retrieved 2023-12-16.
5. ^ Leuf, Bo (2002). Peer to Peer: Collaboration and Sharing Over the Internet. Addison-Wesley. ISBN 9780201767322.
6. ^ Barlow, John P. (20 January 2016). "A Declaration of the Independence of Cyberspace".
7. ^ "Revision history of "An Introduction to Cybersecession" - Cybersecession". editthis.info. Retrieved 2023-12-16.
8. ^ "An Introduction to Cybersecession".
9. ^ Trout, B. (2007). "Cyber Law: A Legal Arsenal For Online Business", New York: World Audience, Inc.
10. ^ Emerging Technologies and the Law: Forms and Analysis, by Richard Raysman, Peter Brown, Jeffrey D. Neuburger and William E. Bandon III. Law Journal Press, 2002–2008. ISBN 1-58852-107-9
11. ^ "The EU copyright legislation | Shaping Europe's digital future". digital-strategy.ec.europa.eu. 2023-12-15. Retrieved 2023-12-16.
12. ^ "Law and Borders – The Rise of Law in Cyberspace". Cli.org. Archived from the original on 2008-05-07. Retrieved 2013-11-05.
13. ^ Autoriteit Consument & Markt. "Netneutraliteit". www.acm.nl (in Dutch). Retrieved 2023-12-16.
14. ^ Bundeszentrale für politische Bildung (2020-07-17). "SPACE NET – Netzneutralität". bpb.de (in German). Retrieved 2023-12-16.
15. ^ "Universal Declaration of Human Rights - English". OHCHR.org | United Nations Department of Public Information, NY.
16. ^ Zittrain, Jonathan (2003). "Be Careful What You Ask For: Reconciling a Global Internet and Local Law". SSRN 395300.
17. ^ Gibson, Owen (March 23, 2006). "Warning to chatroom users after libel award for man labelled a Nazi". The Guardian.
18. ^ Myers KS (Fall 2006). "Wikimmunity: Fitting the Communications Decency Act to Wikipedia". Harvard Journal of Law & Technology. 20: 163. SSRN 916529.
19. ^ "opennetinitiative.net". opennetinitiative.net. Retrieved 2012-01-17.
20. ^ "Home | OpenNet Initiative". opennet.net. Retrieved 2023-12-16.

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |