Cyber Security, Laws & Policy: A Study

ANUPAMA MISHRA[1], AVADHESH KUMAR GUPTA [2]
[1]Department of Computer Science & Information Himalayan School of Science & Technology, Swami Rama Himalayan University, India (e-mail: (tiwari.anupama@gmail.com)
[2]Karnavati University, Gandi Nagar, India (e-mail: dr.avadheshgupta@gmail.com)

ABSTRACT
Today's digital era promotes e-commerce, communication, and more. Everything has pros and downsides, like a coin. Cyber-crime refers to crimes conducted through the internet using communication devices and channels such as laptops, mobiles, desktops, etc. Maintaining law and order prevents such crimes. Cyberattacks are a top five global risk. With the rise of online shopping, internet banking, and other transactions, people should know how to protect themselves and the cyber laws. Cyber rules enable victims act responsibly in event of a catastrophe. This article describes prevalent cyber-crimes, cyber laws, and the necessity for reforming cyber legal framework

KEYWORDS Cyber Crime; Cyber Attacks; E-commerce; Cyber Policies

I. INTRODUCTION
Today we have become slaves to the technology we master. If we look back in time, no one had ever imagined that technology would become a necessity for each and every human [1]. Gathering information just by a click of mouse, buying and selling products, connecting through video calls were once just a nightmare for all of us. The invention of internet has made it much easier and convenient for humans to achieve things which were once unimaginable. Initially people were unaware about the powers of internet, so mostly the usage of internet was primarily done for legal activities and specific purposes [2-4]. But, with time as internet gained popularity there was a drastic change in the statistics of misuse of internet. In 2019, a significant jump that is around 44.5 thousand cyber-crimes were reported. As of 2020, the number of internet users are around 696.77 million out of which 7.5\% people become victims of cyber-crime quarterly [5-9]. Most common cyber-crimes include phishing in which the criminal attempts to lure individual's personal information, banking details or passwords by impersonating him or herself as a reliable entity, Online harassment is another major crime that is very popular mainly among the teenagers, in which the victim is being harassed by the criminal who attempts to stalk his/her social lifestyle by using popular social media platforms, which may also lead to cyber bullying. Surfing on internet has become unsafe due to invasion of privacy crime, in which the criminal attempts to intrude someone's personal life which includes hacking the victim's computer or monitoring the online activities that the victim performs without letting the victim know about it [10-13]. There a huge variety of these types of cyber-crimes, so one should install and update a trustworthy antivirus program. But the question that arises is that can an antivirus program be trusted blindly and will there be any hundred percent guarantee that it would protect you against cyber-crimes? So, there are certain laws to make sure that one thinks before attempting a cyber-crime and the criminals should be penalised as per the intensity of the crime and the damage caused to the victim[14,15].

II. CLASSIFICATION OF CYBER CRIMES
We can define "Cyber Crime" as any malefactor or other offences where electronic communications or information systems, including any device or the Internet or both or more of them are involved [16-18].

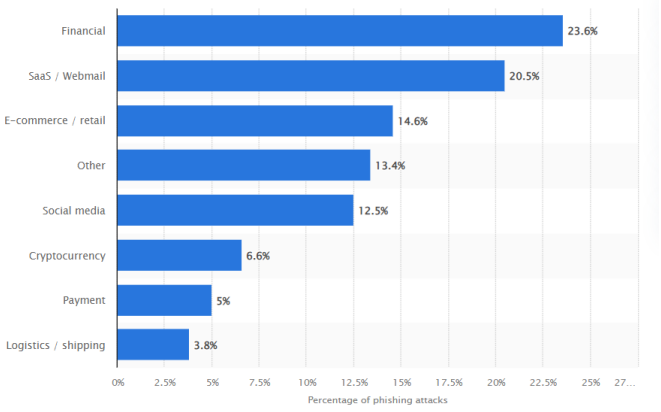

FIGURE 1: Percentage of Phishing Attacks

Cybercrimes can broadly be classified as follows [19]:

1) Crime against the Individuals
2) Crimes against Property
3) Crime against Organization
4) Crime against Society

A. CRIME AGAINST THE INDIVIDUALS

Crimes committed against any individual or a person by the cyber criminals. Some of the cybercrimes against the individual are [20-22]

- Harassment & Cyber stalking: Cyber Stalking can be defined as an act of keeping a check on the activities of an individual over internet or other electronic mean to intimidate, harass or defame the victim. Cyber Stalking can eventually lead to harassment. It is mainly executed by using various social media platforms, e-mails, etc.[23]
- Cyber defamation: Cyber Defamation is an act of deliberately publishing false and unauthorized information over the internet. The primary aim is to defame, insult or offend the target[24].
- Phishing: Phishing is a cyber-crime in which the attacker impersonates as a recognized institution tempting the individual to provide sensitive data like password, credit/debit card details, etc. which can be further misused by the attacker[25].
- Spoofing: Spoofing is a specific type of cyber-crime in which attacker masquerades as a trusted source with an objective of accessing recipient personal details or trying to get control over their system. This type of attack is usually carried out via emails[26].
- Spamming: Spamming refers to sending a bunch of unsolicited messages to a huge number of receivers usually to achieve the purpose of commercial advertisement[27].

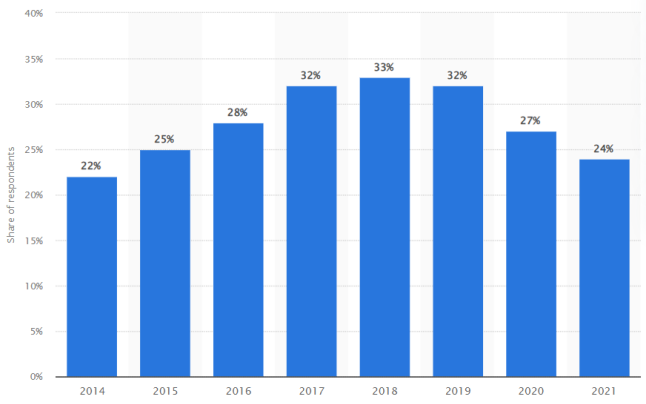

FIGURE 2: Share of Respondents

B. CRIME AGAINST PROPERTY

In this type of crime the attacker focuses on damaging/harming physical property of the victim such as computer, mobile phones, etc. Some of the cyber-crimes against property are [28-29]

- Internet time theft: It is one of the major cyber-crime that is occurring globally. It takes place in such a way that the internet hours paid by the victim is used by an unauthorized user without the victim being aware of the theft[30].
- Credit card fraud: In this the fraudsters try to fetch the payment card details of the card holder by illegal means. For example: one uses a fake website which pretends to be the authenticated (official) website and ask the user to enter the confidential details i.e. card number, password, CVV, etc [31].
- Computer Vandalism: Computer Vandalism is a cybercrime that is executed using malware (executable programs) which can damage the whole system or can steal the user data.

There is also an Intellectual property crime that includes:

- Software piracy: It refers to the illegally making duplicate copies of the original software and making profit by selling them to the end user without having any legal rights from the organization to which the software belongs[32].
- Copyright infringement: It refers to the usage of the copyright-protected content without the permission of the copyright holder. For example: using copyrighted photos/images for commercial/professional work[33].
- Trademark infringement: It refers to the unauthorized usage of the trademark or service mark by breeching the policies of the related organization [34].

C. CRIME AGAINST ORGANIZATION

- Cyber-crime in which a particular firm is targeted by the attacker in order to threaten the organization via internet [35].
- DOS attack: The Denial-of-service attack aims to flood the servers of the target with bogus requests consistently in an attempt to make it inaccessible for the intended users. For example: In 2020, AWS servers were attack by sending approximately 2.3 tbps of traffic [36].
- Email bombing: It is a type of cyber-crime in which attacker sends emails in bulk by training botnet to overflow the mailbox of the recipient which may leads to server crashing [37].
- Data diddling: Data diddling refers to altering the information either during data entry or by making changes in the database. It can be done often by a virus or a data entry clerk [38].
- Salami attack: Salami attack consist of series of small attack (salami slicing) that will add up to larger attack, which remains unnoticeable due to the nature of the attack. For example: the criminal tries to access the customer's bank details, credit/debit card details through database and deduces very small amount from each account which turns into a massive collection [39].
- Unauthorized accessing of computer: The criminal tries to access the computer of an organization over the internet without even being an authorized user. If an attacker somehow manages to gain access to the computer he/she can harm the system mainly in two ways40]:

- Changing/deleting data: Unauthorized changing or deleting of data.
- Computer voyeur: The confidential information is copied or read by the attacker but the information remain intact as no changes are made.

D. CRIME AGAINST SOCIETY

The type of crime that affects the whole society at a time is known as crime against society[41].

- Online gambling: It refers to a cyber-crime which is conducted over the internet. Online gambling may include sports betting, online casinos & poker which involves the transaction of currency.
- Forgery: Forgery involves generation or altering of legal documents or instruments such as making counterfeit money, stamps, signature, etc. It is done using computers having high quality devices like printers and scanners.
- Web jacking: Web jacking is somewhat similar to hijacking, in this typeof cyber-crime the attacker takes control over the website by illegal means. In this a fake website is created by the attacker which may appear genuine and the attacker places a malicious link on the victim's website, which when clicked redirect the victim to the cloned website which makes the victim lose complete access to the his/her website.
- Cyber trafficking: Cyber trafficking is a type of trafficking which takes place using the internet. It refer to the recruitment, advertisement of victim for the purpose of attracting clients. The term "virtual trafficking" can also be used in place of cyber trafficking.

III. CLASSIFICATION OF CYBER LAWS

Cyber laws deal with the crimes committed via internet. It refers to the illustration of laws related to the usage of internet [42].

Meddling with computer Source Documents: If a person commits a crime of intentionally hiding, modifying or destroying any computers source code when it is needed., can be either penalized with a few years of imprisonment or a fine.

Using password of another person:if the password, digital signature or any other unique identification is fraudulently misused by a person, then an imprisonment and fine can be imposed on the culprit.

Cheating Using computer resource: If a person is being cheated upon by someone by the use of computer resources, or a communication devices then the culprit could face an imprisonment and fine.

Publishing private Images of Others: Capturing, publishing or transmitting pictures of someone's private parts without the knowledge or permission of the concerned person is considered to be a heinous act, for which the culprit can be imprisoned for upto 3 years or can be charged a heavy fine of INR 2 lakhs or both.

Acts of Cyber Terrorism: Any person with the purpose of threatening the integrity, sovereignty or unity of the nation by attempting to access a computer resource without authorization or denying access of the computer resource to an authorized person is entitled to face life imprisonment and fine in some country.

Publishing Child Porn or predating children online: A person who attempts to capture or broadcast obscene images of a child under the age of 18 which are inappropriate can face an imprisonment and fine.

Govt.'s Power to block websites: The government can seize, decrypt or keep a check on any information generated, transmitted or stored in a computer resource which according to the government harms the integrity and sovereignty of the nation. Any information can also be blocked by the government.

Data protection at Corporate level: If a corporate body is unmindful while implementing required security practices which may lead to wrongful loss or gain to any person, such an organization shall be liable to pay damages to the affected person.

IV. CONCLUSIONS

The Internet has become advance into a complex medium over the few decades that enables the users to circulate information rapidly and inexpensively to a billion individuals world-wide. The advantage of the Internet over other communication and commerce methods is that it give access to a much wider audience, even a world-wide. Physical distance and International borders are inconsequential to the deployment of an Internet business, numerous are designed for expanding sales across borders. Thus, dispute of law are likely to arise in cyber-space, the location and cause of an occurrence of the dispute is never certain, where conflicting laws are basically created by ideological differences, and where laws are made not only by country and their representatives, but also by transnational and sub-national institutions.

The conclusion that arrives is that implementation of the conventional principles of jurisdiction in cybercrime may result to growing concurring jurisdictional claims. And no guiding principle determining the scope of applicability resides under International or National law. The principle thus become very personalized and have a case to case basis of application. Accordingly nations may apply several theories essentially, nationality, universality, protection and territoriality justifying their exercising jurisdiction to forbid and examine the application of dictatorial law to particular types of unusual criminal activity, The essential is that a nation's movement of jurisdiction either to forbid or to examine must also be "sensible/reasonable" i.e. Having some connection with the delinquent, the crime, or the sufferer and must be sensible with reference to adjudication

REFERENCES

[1] Mishra, A. et al. (2011, September). A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques. In 2011 European Intelligence and Security Informatics Conference (pp. 286-289). IEEE.

[2] Jain, A. K. et al. (2018). PHISH-SAFE: URL features-based phishing detection system using machine learning. In Cyber Security (pp. 467-474). Springer, Singapore.

[3] Kumar, N. et al. (2021). A novel framework for risk assessment and resilience of critical infrastructure towards climate change. Technological Forecasting and Social Change, 165, 120532.

[4] Tewari, A. et al. (2017). A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. International Journal of Advanced Intelligence Paradigms, 9(2-3), 111-121.

[5] Zou, L. et al. (2019). A novel coverless information hiding method based on the average pixel value of the sub-images. Multimedia tools and applications, 78(7), 7965-7980.

[6] Gupta, B. B. et al. (2011, July). On estimating strength of a DDoS attack using polynomial regression model. In International Conference on Advances in Computing and Communications (pp. 244-249). Springer, Berlin, Heidelberg.

[7] Mishra, A., & Gupta, N. (2019, October). Analysis of cloud computing vulnerability against DDoS. In 2019 international conference on innovative sustainable computational technologies (CISCT) (pp. 1-6). IEEE.

[8] Mishra, A. et al. C. H. (2021, January). Classification based machine learning for detection of ddos attack in cloud computing. In 2021 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-4). IEEE.

[9] Kaur, M., et al. (2021). Secure and energy efficient-based E-health care framework for green internet of things. IEEE Transactions on Green Communications and Networking, 5(3), 1223-1231.

[10] Gupta, B. B. et al. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. IEEE/CAA Journal of Automatica Sinica, 8(12), 1877-1890.

[11] Tewari, A. et al. (2020). Secure timestamp-based mutual authentication protocol for iot devices using rfid tags. International Journal on Semantic Web and Information Systems (IJSWIS), 16(3), 20-34.

[12] Sahoo, S. R., et al. (2019). Hybrid approach for detection of malicious profiles in twitter. Computers & Electrical Engineering, 76, 65-81.

[13] Gupta, B. B. et al. (2018). Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimedia Tools and Applications, 77(7), 9203-9208.

[14] Stergiou, C. L. et al. (2020). Secure machine learning scenario from big data in cloud computing via internet of things network. In Handbook of computer networks and cyber security (pp. 525-554). Springer, Cham.

[15] Alieyan, K. et al. (2021). DNS rule-based schema to botnet detection. Enterprise Information Systems, 15(4), 545-564.

[16] Dahiya, A., & Gupta, B. B. (2021). A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Generation Computer Systems, 117, 193-204.

[17] Bhatti, M. H. et al. (2019). Soft computing-based EEG classification by optimal feature selection and neural networks. IEEE Transactions on Industrial Informatics, 15(10), 5747-5754.

[18] Hammad, M. et al. (2022). Myocardial infarction detection based on deep neural network on imbalanced data. Multimedia Systems, 28(4), 1373-1385.

[19] Quamara, M. (2020) et al. Decentralised control-based interaction framework for secure data transmission in internet of automated vehicles. International Journal of Embedded Systems, 12(4), 414-423.

[20] Gupta, B. B., & Ali, S. T. (2019). Dynamic policy attribute based encryption and its application in generic construction of multi-keyword search. International Journal of E-Services and Mobile Applications (IJESMA), 11(4), 16-38.

[21] Sahoo, S. R. et al. (2018). Security Issues and Challenges in Online Social Networks (Osns) Based on User Perspective. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, 591–606.

[22] Ahmed, E. et al. (2018). Recent advances in fog and mobile edge computing. Transactions on Emerging Telecommunications Technologies, 29(4), e3307.

[23] Gupta, B. B., & Gupta, A. (2018). Assessment of honeypots: Issues, challenges and future directions. International Journal of Cloud Applications and Computing (IJCAC), 8(1), 21-54.

[24] Deveci, M. et al. (2022). Personal mobility in metaverse with autonomous vehicles using Q-rung orthopair fuzzy sets based OPA-RAFSI model. IEEE Transactions on Intelligent Transportation Systems.

[25] Chui, K. T., et al. (2022). An MRI scans-based Alzheimer's disease detection via convolutional neural network and transfer learning. Diagnostics, 12(7), 1531.

[26] Tewari, A., et al. (2018, January). A mutual authentication protocol for IoT devices using elliptic curve cryptography. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 716-720). IEEE.

[27] N. A. Khan, et al., "Ten deadly cyber security threats amid covid-19 pandemic," 2020.

[28] B. B. Gupta and Q. Z. Sheng, Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.

[29] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, pp. 65–88, 2015.

[30] A. Khan, et al., "Future scope of machine learning and ai in 2022," Future, 2021.

[31] K. Yadav, "Blockchain for iot security," 2021.

[32] P. Negi, et al., "Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment," arXiv preprint arXiv:1304.7073, 2013.

[33] A. M. Manasrah, et al., "An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment," Cluster Computing, vol. 22, no. 1, pp. 1639–1653, 2019.

[34] P. Chaudhary, et al., "Shielding smart home iot devices against adverse effects of xss using ai model," in 2021 IEEE International Conference on Consumer Electronics (ICCE). IEEE,2021, pp. 1–5.

[35] S. Tripathi, et al., "Hadoop based defense solution to handle distributed denial of service (ddos) attacks," 2013.

[36] M. Zwilling, et al., "Cyber security awareness, knowledge and behavior: A comparative study," Journal of Computer Information Systems, vol. 62, no. 1, pp.82–97, 2022.

[37] I. A. Elgendy, et al., "Joint computation offloading and task caching for multi-user and multi-task mec systems: reinforcement learning-based algorithms," Wireless Networks, vol. 27, no. 3, pp. 2023–2038, 2021.

[38] G. Tsochev, et al., "Analysis of threats to a university network using open source technologies," in 2021 International Conference Automatics and Informatics (ICAI). IEEE, pp. 366–369.

[39] A. Bhardwaj and K. Kaushik, "Predictive analytics-based cybersecurity framework for cloud infrastructure," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–20, 2022.

[40] A. Gaurav, et al., "Security of cloud-based medical internet of things (miots): A survey," International Journal of Software Science and Computational Intelligence (IJSSCI), vol. 14, no. 1, pp. 1–16, 2022.

[41] J. Lu, et al. "Blockchain-based secure data storage protocol for sensors in the industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 5422–5431, 2021.

[42] Z. Zhou, et al., "Coverless information hiding based on probability graph learning for secure communication in iot environment," IEEE Internet of Things Journal, 2021.