Ethical Issues In Combating Cyber-Crime

Introduction:

As we go deeper into the world of innovation and technology, our reliance on the World Wide Web grows with each passing day. Using these enormous networks and technology has both advantages and disadvantages to consider. As the internet becomes more widely used for personal purposes, education, ecommerce, banking and entertainment, the hazards that exist in this virtual world intensify every day. As cyber-attacks on individuals and groups become more common, users must be more cautious and responsible while clicking, accessing links, or visiting websites. There is enough content on the internet to ruin people's minds or destroy their lives. Moreover, having potential benefits for education, creativity, and media literacy, the Internet also contains a number of risks that can negatively affect children's psychological and physical well-being such as cyber bullying, access to sexual and violent content, etc.

The dramatic rise of cyberspace has also fostered immoral practices by those who seek to exploit others through the use of technology. Cyber-attacks involve the exploitation of cyberspace for illicit purposes, including access to unauthorized or secure information, spying, disabling networks, and stealing both data and money or to manipulate mindsets of the vulnerable. The goal of a cyber attack is to steal or hack personal, organizational, or government information. (*IEEE Xplore,* 2003)

Younger generations are becoming increasingly immersed in newer technology and as a result of the increased use of social media and virtual entertainment, Youth spend their days and nights on these devices for the sake of education and amusement, and leading to immature mistakes in their real lives that impact themselves and others.

According to the national poll, a significant number of young people are subjected to sexual solicitations for which they did not volunteer, sexual material for which they certainly didn't ask, and are intimidated and harassed in various ways. Several teenagers have reported experiencing increased stress and despair as a result of situations they learned about on the internet. Additionally, one out of every thirty-three youngsters experienced aggressive sexual solicitation from a solicitor who sought to meet them someplace, called them, or gave them mail, money, or presents. Furthermore, only 17% of adolescents and about 10% of parents could name a specific authority to whom they may report, such as the FBI, CyberTipline, or an Internet service provider, while more indicated they had "heard of" such institutions. There are a lot of offensive episodes experienced by youth, some of which are distressing and most of which are unreported. To combat this phenomenon, a comprehensive strategy would seek to reduce the occurrence of offensive behaviour, enhance protection for young people from its occurrence, increase the reporting of incidents, and provide more support to young people and families. (*IEEE Xplore ,* 2017)

Strategies:

Cyber cells and local officials must take substantial measures to ensure a safe online environment for the young and vulnerable in order to combat the problem of online exploitation of youths. To detect and eradicate the threats, online surveillance of suspicious activity and suspicious users must be done at all times. Age limits on these websites and online content must also be double-checked.

Social media platforms have been severely compromised by malicious actors such as Twitter bots, Wikipedia vandals, fake Facebook accounts, trolls, and spammers on Twitter, Slashdot, etc. As the number of young people using social media sites such as Instagram, Snapchat, Twitter, and others has skyrocketed, so has their use of these platforms. Users spend several hours each day on these social media platforms creating, researching, and trading material, which leads to interactions with strangers on this virtual platform. Furthermore, cybercriminals also known as bad actors frequently distort and extrapolate information from young and immature internet users in order to harm them and their friends and families. These are the types of account which on the social media platforms which distributes misinformation and often causes confrontation. Hence, to terminate the online crimes, Maryland State Police have adopted several strategies to overcome this barrier.

1. Police officers have created fake profiles on many popular social media sites to look for bad actors.
2. The Maryland State Police have decided to employ several “ethical hackers” to access known social media forums, platforms and websites which have been proven to host inappropriate content and allow for the victimization of individuals.
3. the Maryland State Police has also asked for foreign intelligence services to access U.S. servers without judicial authorization to provide data in the search of online predators.

4. the Maryland State Police has hired a local university to have its graduate data science students build an artificial intelligence application to further help find online criminals using the data it has collected.

   (*SAGE Journals: Your Gateway to World-Class Research Journals*, 2013)

Ethical Issues:

Ethics is a set of moral principles at its most foundational sense. They have an influence on how individuals make choices and live their lives. Ethics, generally known as moral philosophy, is concerned with what is beneficial for individuals and community If ethical theories are to be relevant in practice, they will have an impact on how individuals act. An individual's ethics define himself or herself, his or her behavior, and his or her personality and character. Consequently, an individual's or organization's ethics have an impact on their decision-making and life choices as well. (*Practical Ethics,* 2017)

In every aspect of society, ethics must be respected. Global reliance on the internet has expanded dramatically in this rapidly evolving technological age, specifically in the age of pandemics beginning in 2020 due to novel coronavirus. Multinational corporations have begun to operate remotely, data transmission has intensified over the internet, and internet use for educational and entertainment purposes has flourished. As a result, Online Ethics has become increasingly significant part of the society. Online ethics refers to online conduct patterns which have been guided by both law and personal philosophy. Because of this communication medium's vast capabilities, it has the ability to do immense harm, cruelty, and even crime. The protection of private information, the boundaries of an assumed freedom of expression, and libel difficulties are all major concerns in the subject of online ethics. The prevalence and influence of online bullying is another key topic in online ethics. With social networking sites becoming such a huge component of many people's online lifestyle, a whole new way of bullying or manipulating individuals has emerged. In one of the most well-known news stories of the online ethics era, grieving parents tried to charge an adult female with contributing to the suicide of a 13-year-old girl. According to news sources, the woman befriended and then cut off communication with the youngster using a false name on a social media network, presumably to earn her trust and then hurt her feelings.

Maryland State Police are implementing the tactics stated above to counter the growth in cyber-crime targeting underage and innocent children in recent years. However, the question remains whether these theories can be confirmed ethically without compromising or invading personal data. Even if the Maryland State Police and Officials have examined various approaches to address the issue of cyber-crime, the user's and data's confidentiality must not be jeopardized. All official procedures must strive to eradicate online danger and provide a safe working environment for children and teenagers on the internet.

Possible Ethical Issues With the Strategies Of Maryland Police Department:

Cybercrime has been on the minds of Maryland Police Department officers for some time. For the sake of tackling this issue, they will have to consider reading all the data that floats around on the internet and flagging the explicit content that threatens to harm people's mind-sets. In order to do so, officials may have to engage in hacking and gaining backdoor access to encrypted and secured data. The officials of Maryland may find themselves in a situation where they are not doing anything illegal, but acting unethically. In many instances, things that are unethical aren't necessarily illegal. Moreover, Also, the distinction between what is illegal and what is unethical is not always obvious (Stephan, 2002). When it comes to cyber activities, there are a lot of questions that come up. Here are some of the issues that must be addressed:

1. What information about a person or a group must be brought to light?
2. What data pertaining these cyber operations must be stored, and how safe is the data once it has been collected?
3. How should data piracy and privacy be dealt with in this circumstances?
4. Who has access to the data, and who has the authority to change or analyse it?
5. What procedures can be done to ensure that only verified and authorised individuals or organizations have access to the information?

   (*Cybercrime and Shifts in Opportunities during COVID-19: A Preliminary Analysis in the UK*, 2020)

Basically, dealing with this situation, there are a few ethical issues that might arise namely:

1. Privacy of an individual’s data: When an Internet user exchanges data over the internet, the data must be sent from the source to the destination without being tampered with or accessed by any unauthorized body. The Maryland Police Department's strategies may have an impact on data privacy, regardless of whether the data is in flight or resting in storage. Access rights to the data being analysed and traced.

2. Access rights of the data: In databases, data must be securely kept and protected. There must be no unauthorised users or access to the data. Data security has become a significant priority in today's world. As the number of break-in attacks has increased in recent years, users have found it difficult to protect their systems with the highest level of security to prevent illicit data access. Hence the Maryland State Police strategies must hiring foreign intelligence to deal with the in-state issue of cyber activities might lead to invasion of privacy and leaking the data or personal information.
3. Loss or Damage of the Data: Harmful action in the context of computer ethics refers to any action that causes harm or has negative repercussions, such as unintended loss of data, property loss, property damage, or unintended environmental implications. This concept forbids the use of computing technology in ways that affect users, the general public, employees, or employers in any way. Intentional destruction or modification of files and programs, which results in a significant loss of resources or an excessive expenditure of human resources, such as the time and effort required to clean systems of "computer viruses," are examples of harmful activities. Therefore this can be a serious ethical issues faced by the cyber cell of Maryland State.

Implementation of Ethical Theories In Cyber Security:

Ethical Theories are attempts to provide a coherent, unambiguous understanding of our ethical responsibilities. Ethical theories describe what a person should do while making decisions or taking actions. Ethical theories are used to guide decision-making by highlighting parts of an ethical dilemma that are essential to them and leading them to the most ethically proper resolution based on the ethical theory's standards. {Link :

Some of the Ethical theories that are frequently used and applied in the day to day conduct are as follow:

1. **Utilitarianism**: Utilitarianism states that in any scenario, the action or decision to be taken must be based on the outcome and repercussions of the action. Every choice made in accordance with this ethical principle must be analysed and evaluated in order to maximize the net benefit to the individuals engaged or affected.

   Furthermore, the strategies determined by Maryland State city leaders can be used. As they will eventually be aiding in the elimination of online risks or traps designed for children who are using internet. Providing foreign intelligence with access to databases and personal information, on the other hand, may not be a good idea, as Maryland State police may end up compromising personal files and information about everyone who uses the internet, as foreign intelligence will be working under their own laws and legislation, which may differ from those of the United States. Thus, leading to a much bigger sacrifice and compromise. (*Beyond Utilitarianism and Deontology: Ethics in Economics*, 2007)

2. **Kantianism:** Kantian ethics are a set of universal moral principles that apply to all mankind, independent of context or circumstance. Kant believed that moral principles should guide people's conduct, and that these moral laws should be universal. He believed that any highest moral norm must be based on reason in order to apply to all rational beings.

   Hence, according to the Kantianism theory of Ethics, Creating fake profiles on the internet or collecting the information from the users without their knowledge or consent is also a wrong doing irrespective of the outcome of the situation. Therefore, If following the Kantianism theory to tackle this problem, It will be considered as unethical. (Baron, 2018)
3. **Social Contract Theory:** We should consider what ethical principles reasonable humans would agree to in a "ideal" decision-making circumstances in order to figure out what ethical norms to follow. In a civilized society, everyone has implicitly agreed to two things: (1) the formation of a system of moral rules to govern citizen relations, and (2) a government capable of enforcing these rules. According to this argument, giving foreign intelligence services access to U.S. servers without judicial authorisation is unethical. This actions might leak the files of personal as well as government organisations.
4. **Virtue Theory:** The virtue ethics approach of Aristotle examines if an actor is using his or her virtues, which can be thought of as abilities or talents, to conduct a morally good action. This morality based on character assumes that we learn virtue via practice. A person's honourable and moral character is developed by practice being honest, brave, just, generous, and so on. Rather than substituting a distinct sort of reasoning, virtue ethics seeks to better the reasoning we all share.

   In light of the Maryland State Police's tactics for combating cybercrime, hiring ethical hackers is the appropriate thing to do in order to track down and destroy online threats, as according to them, hacking with consent is a virtuous work.

References:

- Quinn, M. (2016). *Ethics for the Information Age* (7th ed.). Pearson.
- *IEEE Xplore Temporarily Unavailable*. (2003). Advances in Internet Congestion Control. https://ieeexplore.ieee.org/abstract/document/5342228?casa_token=bUKbp_usMbIAAAAA:ii0eSfT7bZEJpgfwxvNFxhEQ3DDYM8zba8YQjoRX2BcHSoaz2-53Wek_3_m9GMyqPoySy1izewo
- *IEEE Xplore Temporarily Unavailable*. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. https://ieeexplore.ieee.org/abstract/document/7955906?casa_token=BlUMUXEoI0UAAAAA:-VPny9SY5gEXCHKbrtFokEjaeyxFaGlboZOnttRnrLz2Sbvaep-Oli4FsVoS4W6Erv1fkZJH9-w
- *SAGE Journals: Your gateway to world-class research journals*. (2013, November). SAGE Journals. https://journals.sagepub.com/action/cookieAbsent?casa_token=gla-bLGDmbAAAAAA%3AjaNkiB16vlqBvql_HlYpNvjPtenvb7FUt2RoCCTwoMYZKzhOoGfAus3_Uz4BdWZTzyPTJKOeGmErvQ
- *Practical Ethics*. (2017). Practical Ethics. https://books.google.nl/books?hl=en&lr=&id=lNgnV0eDtM0C&oi=fnd&pg=PR7&dq=what+are+ethics&ots=N3Bfc-1mpB&q=what+are+ethics&redir_esc=y
- *Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK*. (2020). Taylor & Francis. https://www.tandfonline.com/doi/full/10.1080/14616696.2020.1804973

- *Beyond Utilitarianism and Deontology: Ethics in Economics*. (2007). Beyond Utilitarianism and Deontology: Ethics in Economics. https://www.tandfonline.com/doi/abs/10.1080/09538250601080776
- Baron, M. W. (2018, October 18). *Kantian Ethics Almost without Apology*. De Gruyter. https://www.degruyter.com/document/doi/10.7591/9781501720895/html
-