Research Paper

Integrating Artificial Intelligence into Cybercrime Investigation: Challenges and Future Directions

Vibhor Kumar Awasthi[*1] and Abhishek Mishra[2]

[1]-*LL.M - final year 4th semester, Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India.*
[2]-*Associate Professor Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India.*

ARTICLE DETAILS	ABSTRACT
Corresponding Author: Vibhor Kumar Awasthi *Key words:* Artificial Intelligence, Cybercrime Investigation, Cybercrime.	Computer and social networking whereby criminals use the Internet to propagate criminal activities are some of the major challenges faced by existing policing strategies. Modern-day crimes include hacking into computer systems and stealing money from consumers, ransomware, identity theft cases, and hacking. All of which use the dark web and encryption. In this regard, artificial intelligence (AI) is the most efficient solution for improving the manner of cybercrime investigation. This paper also analyses how Al technologies such as machine learning natural language processing, and deep learning can be incorporated in cybercrime investigations and how they can assist in dealing with difficulties concerning data volume, complexity, and encryption. The advantages of utilizing Al are numerous from pattern recognition to repetitive tasks cutting down the investigation time. However, the paper recognizes that applying Al in business brings legal, technical, and ethical concerns including; privacy, bias, and legal constrictions. This research analyses existing legal frameworks of India, the EU, and the United States while looking at how it would be possible to incorporate Al into cybercrime investigations without violating the rights of a citizen. Further, it reveals infringement and possible bias, as well as unlawful use for violations, and recounts drawbacks related to the lack of resources and expertise that police departments confront. In the final section of the paper, directions for future research focusing on the use of Al in the fight against cybercrime are given in addition to that, the practice of cooperation with different countries, legal regulation of such activities, protection of ethical issues, and training of personnel are described. They are useful in making sure that the levels of artificial intelligence benefits are achieved fully without compromising security and the basic rights of an individual.

1. Introduction

Cybercrime has emerged and grown stiff through the enhancement of information technology and the enhanced popularity of the internet and this has facilitated crimes such as financial fraud and cyber theft, identity theft, ransomware attacks, hacking, and cyber espionage. These threats have advanced greatly in terms of their usage of the dark web, cryptocurrencies, and conjunction and mastering concealment mechanisms, which is why the traditional approach to law enforcement could not potentially chase them. Another strategy that has come to light in the process of supporting the performance of conventional police functions in the fight against cyber criminality is Artificial Intelligence (AI). Advanced Al technologies, including machine learning, natural language processing, and deep learning, can search datasets containing large volumes of information, identify outliers, and find patterns that may be hard even for detectives to notice. Therefore, to curb incidences of cybercrime and the procedures involved AI becomes a crucial tool in handling digital evidence, especially in cases where data is encrypted. The main research question in this study is, what are the issues of incorporating Artificial Intelligence in

cybercriminal investigations in the future, especially within the Indian context The usage of Al in such a domain has both benefits and risks including the following concerning the existing privacy laws and due process rights as expressed by the seven-judge bench of the Supreme Court of India in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India. The involvement of Al in cybercrime investigation, issues associated with its implementation, and ways to make its usage legal and ethical will be investigated. Thus, the current legal regimes in India, the US, and the EU will be compared to determine the current state of regulation alongside the implementation of Al without underestimating the fundamental rights.

2. Understanding cyber crimes and investigative needs

Computer crime, or cybercrime, as it is more commonly known, is a criminal act that employs the computer or uses it as an object or goal. The increase in the use of technology has made cybercrimes expand into different categories and now offer different activities like hacking, identity theft, phishing and ransomware. Virulent computer crimes, for example, hacking, entail breaking into computer systems to acquire, alter, or manipulate information. This form of cybercrime is therefore a real concern to people and organizations, as the S.S. Lotus, France v. Turkey Showed that when an organization's data is hacked, it stands to lose a lot of money. Likewise, identity theft, which is a situation where somebody embezzles personal information like credit card details or social security details, is still a major concern for the police.

3. Year-wise Trend of Cyber Crime Cases in India (2017-2022

Phishing is also a very popular type of cybercrime, where attackers attempt to deceive individuals by accessing the personal
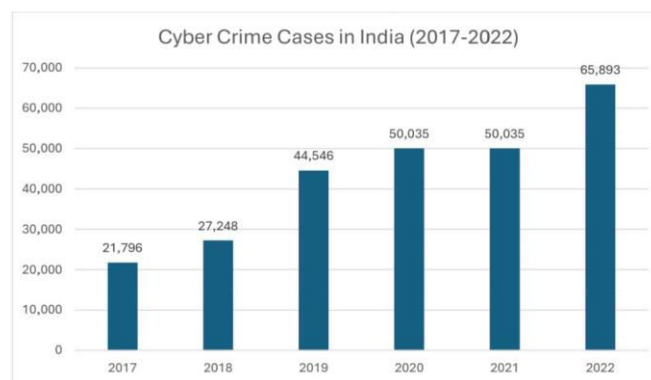
and organizational information of a user through ordinary email or fake websites. Ransomware-malware that encrypts a victim's files and demands a ransom for the release of the files-is also on the rise. The most recent and large-scale manifestation of this type of cybercrime is described by the WannaCry ransomware attack in the year 2017, which impacted hundreds of thousands of organizations across the world, inclusive of healthcare services, making a clear manifestation of key infrastructure ill-prepared for this type of cyber threat. The range of possible cybercrimes is vast, and it requires a particular approach to investigation, mainly because of the different types of obfuscation used by the criminals. These crimes are mostly transnational, which poses problems in determining the accuracy of jurisdiction and common coordination between various agencies. In the process, traditional forms of detective work often fail to work because, as new. Technologies are developed, so are new strategies, schemes, and tactics by the wrongdoers. This has made it necessary to deploy newer forms of technology, such as artificial intelligence (AI), to handle the modern challenges of efficient cybercriminal investigations.".

4. Challenges in traditional cybercrime investigation

The primary problem with traditional cybercrime investigation approaches is that they contain numerous difficulties, especially about the constantly growing number and level of complexity of cyber threats. Another drawback of using manual approaches for threat assessment is the impossibility of tracking rapid and multiple threats simultaneously. Due to the large amount of information that can be collected during a cybercrime investigation, including a fairly large amount of information from different sources, the analysis takes a lot of time, and it is practically impossible to be conducted by humans without using technical means. For instance, when analyzing the recent high-profile hacking case where investigators look for the source of the data leak, it might take weeks or even months to search through terabytes of data, which has a high probability of giving incorrect results."A second challenge is that there is no current protocol for retrieving and analyzing digital evidence. Digital data can be tampered with easily, and this is especially important for a prosecution where digital evidence forms the premise of the case. In addition, such heinous crimes know no bounds and are ever-evolving. Creating a need for law enforcement agencies to adapt to effectively deal with the ever-evolving threats, a thing that the legal and procedural mechanisms are unable to do, hence the ineffectiveness of traditional investigation as a method of dealing with cybercrime. Section 65B of the Indian Evidence Act of 1872, which deals with electronic records, talks about proper procedures needed, and the procedure of handling the records still presents some challenges because where manual methods are used, they are not efficient and reliable. The issue of ample volumes of data in law enforcement agencies is the second major challenge identified below. Criminal activities online include the examination of logs, metadata, encrypted communications, and other evidence forms that need technical prowess or tools to understand. In cross-borderinvestigations, there are basic issues of

jurisdiction and cooperation with other agencies, further compounding the difficulty of the process. Realizing the drawbacks of the conventional approaches and the growing complexity of the cyber threat landscape, different technological approaches have been considered more suitable for contemporary investigating practices, and Al is selected as one of the viable approaches to assist cybercrime investigators.

5. AI as a Solution for Cybercrime Investigation

Al provides an effective approach to solving the issues encountered in ordinary cyberspace crime investigations. Thus, the strong and diverse areas of AI, which can include the analysis of large volumes of data as well as pattern recognition and automation capabilities, provide a revolutionary step change in how cybercrime may be identified and combatted. Where manual investigations fail due to the slow pace and possible inaccuracies that come with sifting through a myriad of papers, records, and electronic data, Al enhances investigations by making quick work of the same due to its capabilities to sort through and analyze large amounts of data in a relatively short period. Through the use of machine learning, large databases can be scanned, weaknesses detected, and possibly future threats assessed, thus enabling the investigators to concentrate on certain areas. "Pattern recognition is another important function carried out by artificial intelligence to identify cyber-crimes. Al systems can be taught to identify the manners of operation of known hackers, so once such hackers engage in similar activities in different networks and systems, they can be nabbed by law enforcement. For instance, it is possible to pick the phishing emails and analyze the linguistic feature or structure similarity of the email message before using it in an attack. These advanced features are further expanded by deep learning, a subfield of AI: the recognition of faces and voices, as well as chain connections linking various data containing the specifications of cybercriminals."

Automation also has its contribution to improving the effectiveness of cybercrime investigations. Cognitive automation tools in Al can do simple, tedious work like scanning logs, obtaining digital evidence, and preparing reports, thus easing work for human investigators. This in turn makes it possible for police officers to focus on more core and constructive tasks in any investigation. "Al also plays a role in improving the aspects of digital investigation, which is an important factor in the collection of proofs in cybercrime-related court trials. Data may be either deleted, and forensic tools created using Al are capable of searching for it, encrypted, or encrypted in such a way that the Al-based instrument used in the cybercriminal's case is also capable of breaking the encryption. On the other hand, it is important that all use of Al is legal and has regard to relevant protected rights, such as the contemporary right to privacy.

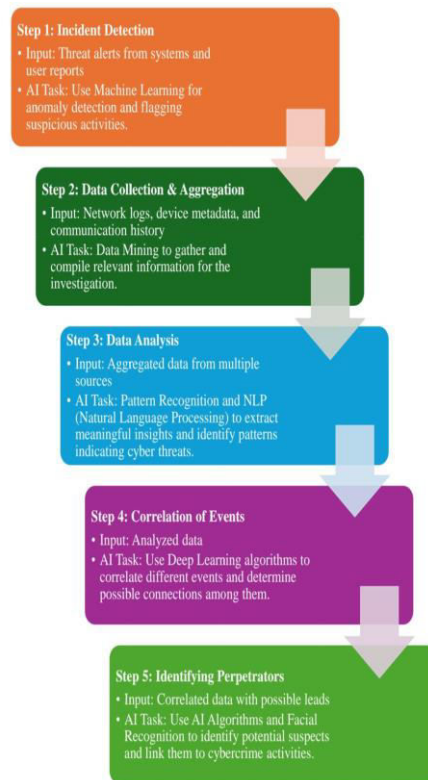## 6. AI Integration in Cybercrime Investigation: A Step-by-Step Approach

6.1 Role of artificial intelligence in cyber crime investigation ÷

Al can adopt different technologies in its process of supporting law enforcement agencies to fight cyber-crimes for the following reasons: Currently, one of the most used Al technologies in cyber investigations is machine learning. First, it is the ability to analyze huge amounts of data, identify already existing patterns, and learn new ones-an essential function for fighting cybercrime. These algorithms are capable of detecting anomalies, raising an alarm, or even outlining possible cyberattacks using prior data. Another important Al technology applied in cyber investigation is natural language processing (NLP). NLP is useful in making reflections and translations of textual communications, and that is how it can be used by investigators to decode messages from coded and distinct types and recognize disguised threats in communicated messages. They are particularly useful in surveillance of social media, email, and instant messengers for signs of a cybercriminal. For instance, in a phishing ring, NLPs were used to help the investigators make a discovery on the most used linguistic features in emails, hence leading to the arrest of the ring leaders. Another important nugget of Al is that the predictive analytics ability assists the law enforcement agency in avoiding cybercrimes. The relative analysis of trends and patterns in previous cyber-attacks is useful in the development of models of predicted future threats and possible countermeasures. The subcategory of ML is known as deep learning and is used to make a model that can work for comprehending intricate representations such as images, audio, or video streams. This technology is helpful when it comes to some jobs, such as the identification of criminals (Hackers) through a camera or an image captured during an investigation, such as facial recognition. He also learned that deep learning models have powered efforts to crack codes used by criminals through an encryption system, something that has been used in cases of ransomware attacks in which Al makes it possible to identify the key encryption patterns. Altogether, these AI technologies form a set of tools that can be used effectively for a variety of tasks important for a law enforcement agency to effectively confront diverse and challenging aspects of modern computer crime investigation.

6.2 Applications of AI in Investigation

There is a myriad of ways in which Al is currently used in the context of cybercrime investigation, from malware detection to behavioral analysis and automated data mining. One of the main uses is the identification of viruses, with which hackers break into Internet resources and steal information. Traditional antivirus programs are not able to cope with the dynamic growth of malware while using behavior-based techniques, Al-based systems can react to new types of malware. Another crucial area that can benefit from Al in the combating of cybercrime includes the identification of fraud. Scams and cyber theft on financial accounts have been on the rise, with the common ones being credit card fraud and identity theft, and through learning transaction patterns and tendencies of customers, Al can detect the fakes in real time. Using Al technology has become the norm in banks and other financial institutions since it can be used to recognize fraudulent transactions and alert the

management before great loss occurs. Another crucial approach is based on behavioral analysis, the work of which is aimed at assessing user actions and applying the results to identify cyber threats. Al can easily detect anomalous trends, which, if unusual in normal usage, could be a sign of violation, thus allowing investigators to act quickly towards threats,

Data mining is one of the most important applications of artificial intelligence, and this is an excellent feature for increasing

Step 1: Incident Detection
- Input: Threat alerts from systems and user reports
- AI Task: Use Machine Learning for anomaly detection and flagging suspicious activities.

Step 2: Data Collection & Aggregation
- Input: Network logs, device metadata, and communication history
- AI Task: Data Mining to gather and compile relevant information for the investigation.

Step 3: Data Analysis
- Input: Aggregated data from multiple sources
- AI Task: Pattern Recognition and NLP (Natural Language Processing) to extract meaningful insights and identify patterns indicating cyber threats.

Step 4: Correlation of Events
- Input: Analyzed data
- AI Task: Use Deep Learning algorithms to correlate different events and determine possible connections among them.

Step 5: Identifying Perpetrators
- Input: Correlated data with possible leads
- AI Task: Use AI Algorithms and Facial Recognition to identify potential suspects and link them to cybercrime activities.

the efficiency of the investigation of cybercrimes. The police require retrieving information from digital storage media, including mobile phones, computers, or servers, to prosecute individuals suspected of cybercrime. When the process is handled manually, it can at times be a tiresome and very time-consuming affair. Data mining using artificial intelligence makes it easy and fast to search through large data packages to look for evidence and sort the data into bins for further examination. For instance, in the arrest of a hacking group that specializes in attacking financial institutions, Al systems could be used to interpret data obtained from gadgets seized from the group members to unravel the communication threads and the core members of the group, 14

7. Legal framework for ai in cyber crime investigation

Technology advancements concerning artificial intelligence Al in cybercrime investigations reflect a research duality of Al applications and the laws that regulate them. National and global legal systems affecting data privacy place constraints on the use of AI in these investigations. At the international level, the EU's General Data Protection Regulation, or GDPR, acts as a reference regulation with strict conditions governing data processing, privacy, and consent, among others. GPDR continues to be a significant law for Al-driven cyber investigations with strict detail on the legal and authorized process to be followed when processing any personal data. According to the GDPR, DPIAs are required before implementing an artificial intelligence process on data, which are considered special categories of personal data, and this increases the accountability of law enforcement agencies utilizing artificial intelligence tools in combating cyber-crimes. This regulation acts as a model that has an impact on other legislation in other countries outside the EU. 1 Another and especially relevant international instrument is the Budapest Convention on Cybercrime, or more officially, the Convention on Cybercrime is the first of its kind treaty designed on internet and computer crime by pulling together national laws, improving investigation tools, and increasing international cooperation. The Convention brings a focus to human rights and freedoms-again, when it comes to Al used in cyber investigations, privacy and other human rights have to be protected. While India has not ratified the Budapest Convention, it has displayed a positive approach towards accustoming the nation's laws to international standards, leaning specifically towards the Budapest Convention in areas of cybercrime and data protection. Nationally, the Digital Personal Data Protection Act, 2023 (DPDP Act) in India is for legal regulation of data protection". This intends to control the handling of personal information by government and private players through setting standards in the collection, storage, and processing of data. The DPDP Act has consequences for the use of Al in the investigation of cybercrimes since police forces will be expected to guarantee compliance with data minimization and purpose limitation principles in the utilization of Al. It Also lays rules on data localization that may hamper cross-border investigations involving any artificial intelligence technologies. Also, Section 69 of the Information Technology Act of 2000 provides the power to any authorities to intercept, monitor, or decrypt

information in the interest of the sovereignty and integrity of India and the security of the state. However, the application of such power has to be 18 contingent on privacy compliance, and in the case of applying Al for surveillance mechanisms, there has to be legal backing explaining why and how it is applied to prevent bad actors from exploiting such platforms.

8. Challenges with Legal Compliance
The incorporation of Al in cybercrime investigation is a complex process in terms of compliance with the existing law regarding data acquisition, retention, and processing. The first is the issue of processing the data timely while dealing with requirements provided under current applicable privacy laws. Artificial intelligence technologies use data feeds for their teaching and operation, and data feeds usually entail information concerning individuals. However, provincial or national legislation like the DPDP Act in India and the GDPR in Europe sets certain standard requirements for the collection, storage, and use of the data. Police agencies and forces need to tread on these legal issues very carefully because if there is a violation by the police, then all the evidence gathered can be thrown out of court. Another huge task is the management of the collected data during cybercrime investigations in a way that minimizes the risk of it being accessed by anyone who has no business with it. Given that Al models are applied in investigations, the data on which they are trained must be relevant, adequate, and do not exceed the data necessary for its processing. It corresponds to the concepts of data minimization and purpose limitation contained in data protection statutes. Nevertheless, the ways of adhering to these principles are not always clear, as cybercriminal activity investigations presuppose the accumulation of a great deal of information that can be irrelevant at first sight. 19 Furthermore, cross-border data transfers have a concern of legalities enhanced by cross-border electronic crime investigations, which require the exchange of data between jurisdictions. The GDPR has put barriers to the transfer of data to non-EU countries, and India's proposed data localization standards pose legal and procedural challenges to effectively implementing Al in transnational cybercrime analytics. It, however, means that efficient and effective Al-based investigations need to be carried out while, at the same time, compliance with such regulations is achieved through the negotiation of international data-sharing agreements and other legal compliance measures. Noncompliance with these requirements results in legal responsibilities, inability to investigate, and infringement of the legal rights of individuals.

9. Ethical Considerations in Using AI
The application of artificial intelligence in cybercrime investigations also brings out several ethical issues, especially about the conflict between the Privacy Act and the Crime Prevention Act. On the one hand, AI technologies bring much value in improving the speed and quality of cyber investigations; on the other hand, they are concerning for personal data privacy. Hyping alarm concerns regarding the state's extent of intrusive powers, surveillance, and data gathering. Al systems are capable of amassing substantial amounts of personal data. The second one is that bias is very likely to show up in Al algorithms. Like all human creations, Al systems are designed by humans with the use of specific sets of data, and if this set of data has pre-existingData mining is one of the most important applications of artificial intelligence, and this is an excellent feature for increasing the efficiency of the investigation of cybercrimes. The police require retrieving information from digital storage media, including mobile phones, computers, or servers, to prosecute individuals suspected of cybercrime. When the process is handled manually, it can at times be a tiresome and very time-consuming affair. Data mining using artificial intelligence makes it easy and fast to search through large data packages to look for evidence and sort the data into bins for further examination. For instance, in the arrest of a hacking group that specializes in attacking financial institutions, Al systems could be used to interpret data obtained from gadgets seized from the group members to unravel the communication threads and the core members of the group.

10. Legal framework for AI in cyber crime investigation
Technology advancements concerning artificial intelligence Al in cybercrime investigations reflect a research duality of Al applications and the laws that regulate them. National and global legal systems affecting data privacy place constraints on the use of Al in these investigations. At the international level, the EU's General Data Protection Regulation, or GDPR, acts as a reference regulation with strict conditions governing data processing, privacy, and consent, among others. GPDR continues to be a significant law for Al-driven cyber investigations with strict detail on the legal and authorized process to be followed when processing any personal data. According to the GDPR, DPIAs are required before implementing an artificial intelligence process on data, which are considered special categories of personal data, and this increases the accountability of law enforcement agencies utilizing artificial intelligence tools in combating cyber-crimes. This regulation acts as a model that has an impact on other legislation in other countries outside the EU. Another and especially relevant international instrument is the Budapest Convention on Cybercrime, or more officially, the Convention on Cybercrime is the first of its kind treaty designed on internet and computer crime by pulling together national laws, improving investigation tools, and increasing international cooperation. The Convention brings a focus to human rights and freedoms-again, when it comes to AI used in cyber investigations, privacy and other human rights have to be protected. While India has not ratified the Budapest Convention, it has displayed a positive approach towards accustoming the nation's laws to international standards, leaning specifically towards the Budapest Convention in areas of cybercrime and data protection. Nationally, the Digital Personal Data Protection Act, 2023 (DPDP Act) in India is for legal regulation of data protection". This intends to control the handling of personal information by government and private players through setting standards in the collection, storage, and processing

of data. The DPDP Act has consequences for the use of Al in the investigation of cybercrimes since police forces will be expected to guarantee compliance with data minimization and purpose limitation principles in the utilization of Al. It

11. Challenges with Legal Compliance

The incorporation of AI in cybercrime investigation is a complex process in terms of compliance with the existing law regarding data acquisition, retention, and processing. The first is the issue of processing the data timely while dealing with requirements provided under current applicable privacy laws. Artificial intelligence technologies use data feeds for their teaching and operation, and data feeds usually entail information concerning individuals. However, provincial or national legislation like the DPDP Act in India and the GDPR in Europe sets certain standard requirements for the collection, storage, and use of the data. Police agencies and forces need to tread on these legal issues very carefully because if there is a violation By the police, then all the evidence gathered can be thrown out of court.

12. Ethical Considerations in Using AI

The application of artificial intelligence in cybercrime investigations also brings out several ethical issues, especially about the conflict between the Privacy Act and the Crime Prevention Act. On the one hand, Al technologies bring much value in improving the speed and quality of cyber investigations; on the other hand, they are concerning for personal data privacy. Hyping alarm concerns regarding the state's extent of intrusive powers, surveillance, and data gathering. Al systems are capable of amassing substantial amounts of personal data.

13. Conclusion

Artificial Intelligence is believed to have a lot of potential in terms of improving the given operational environment, given the availability of intelligent tools applicable to the investigation of cybercrime, something that current methods cannot deal with in terms of their broad scope. Sub-technologies of artificial intelligence belonging to machine learning, natural language processing, and deep learning classes can help detect and investigate cybercrime more effectively since they work with big data and perform data analysis, as well as recognize patterns and automate routine tasks. These capabilities are essential to preventing phishing schemes, ransomware, and other criminal activities, to allow the police to prevent such criminal activities in cyberspace. On the use of artificial intelligence in solving cybercrime: Challenges. Traditional methods prove disadvantageous by addressing the problem of big data and. encrypted processes in cyber surveillance. Al though effective comes with some challenges including: privacy, bias, and regulation. The application of Al requires prudential measures to be taken, namely in non-unfair discrimination and the prevention of over-surveillance, which is intrusive of a person's rights. Furthermore, laws such as the GDPR in the European Union and the DPDP Act in India contain harsh requirements for the use of data, which is needed to protect the citizens' rights but, at the same time, will allow Al technologies to effectively contribute to investigations. The use of Al in the investigation of cybercrime: the legal systems of countries have crucial importance in the integration of the use of Al in the investigation of cybercrime. This paper emphasizes recognizing certain effective guidelines that would enforce the proper ethical and legal use of AI Technologies. Such regulations should help make the use of Al in the police service easily explainable, and devoid of any prejudice. That is why countries have to join to introduce international conventions and memoranda that can help exchange information on cyber representatives and coordinate their activities. This collaboration will be important in dealing with the transnational character of cybercrimes and ensuring that AI can work properly and to optimum results. Therefore, the following recommendations can be made to improve Al in cybercrime investigations in the future. This is the kind of support governments and law enforcement agencies should direct on the development of various advanced forms of Al models that would handle the encryption or the various other aspects of it so that the utilization of the cloud as well as open source, which they have been advocating as the cost-saving measures, can be stepped up while at the same time improving on the Al's of investigations so that they are more efficient and faster. Education for law enforcement personnel in terms of the new Al technology as well as issues of public-private partnerships is also essential in developing the necessary stock. In conclusion, Al holds great significant value regarding the solution to those threats that modern cyber security faces, but the incorporation of Al into the processes of investigation of cybercrime has to be done carefully to avoid violation of individuals' and groups' rights to privacy, ethical values, and the overall requirement of community and governmental trust. Policing through artificial means is a great concern for the future as long as it is done in a balanced fashion where the ability to harness Al as a tool for law enforcement will not infringe on such basic rights for citizens. The most important condition for the prevention and further fight against contemporary cyber threats will be the constant progress of the Al technologies used, as well as the existence of an efficient legal and ethical foundation to contrast the cybersecurity threat and fight against cybercrime, while at the same time preserving crucial civil rights and liberties.

Literature Cited

Anderson, R., & Moore, T. (2006). *The economics of information security*. *International Journal of Electronic Commerce*, 10(3), 15-44..

Chio, C., & Freeman, D. (2018). *Machine learning and cyber security: A survey of applications and future research directions*. *Computers & Security*, 73, 97-112.

Ghorbani, A. A., & Lu, W. (2007). *A survey of machine learning techniques for cyber security*. *Journal of Computer Science and Technology*, 22(6), 850-867.

He, Z., & Yao, L. (2019). *Artificial intelligence in the detection and prevention of cybercrimes: A systematic review*. *Journal of Information Security and Applications*, 48, 1-14.

Kumar, A., & Ravi, V. (2020). *Cybercrime detection and prevention using artificial intelligence: Trends and challenges*. *International Journal of Advanced Computer Science and Applications*, 11(4), 71-77.

Liao, X., & Zhang, Y. (2020). *Artificial intelligence for cybercrime investigation: Frameworks and case studies*. *Proceedings of the 2020 IEEE International Conference on Cyber Intelligence and Information Retrieval*, 32-39.

Liu, B., & Wei, X. (2019). *AI-based systems in cybercrime investigation: Current status and future prospects*. *Artificial Intelligence Review*, 52(2), 965-990.

Moustafa, N., & Slay, J. (2015). *The use of machine learning in cybercrime detection and prevention*. *Cyber Security and Privacy*, 10(3), 213-226.