UDC: 342.738.037:341.24(4-672ЕУ)
343.9:004]:004.8(4-672ЕУ)

PREVENTION OF CYBERCRIME IN THE AGE OF ARTIFICIAL INTELLIGENCE (AI) WITHIN THE EUROPEAN UNION

Trajkovska Elena
PhD candidate, Faculty of Law, Goce Delcev University, Stip
trajkovskae23@yahoo.com

Del Becaro Tommaso
Master student, Faculty of Political Science, University of Pisa, Pisa
t.delbecaro@studenti.unipi.it

Mijalkov Bogoljub
Master student, Faculty of Law, Goce Delcev University, Stip
bogoljub.mijalkov@ugd.edu.mk

Abstract

The significant technological development experienced between the late 20th and early 21st centuries has raised a series of fundamental questions regarding the protection of civil, political, and social rights. The exploitation of new technologies by governments and international organizations, as well as private companies and individuals, opens up enormous possibilities for development on one hand, while posing serious risks to the aforementioned rights on the other. In recent decades, cybercrime has represented a crucial challenge for global actors and continues to evolve thanks to the availability of increasingly advanced technologies. What mechanisms do countries around the world use to protect themselves and their citizens? Is full legal protection even possible? These are questions that constantly arise and are gaining more and more significance.

The European Union, especially in the past 10 years, has taken legal measures to create a safe space for its institutions and member countries. Among the most interesting technologies is artificial intelligence (AI), which has captured global attention on the subject in recent years, especially after the public exploitation of generative AI systems. Since AI technologies mainly rely on machine learning systems that exploit data, European regulation of these tools, pending the full implementation of the AI Act, primarily depends on data protection laws. In this regard, the adoption of the General Data Protection Regulation (GDPR) in 2016 represented a milestone for data protection and the right to privacy within the European Union context; on the subject, reference is also made to the "Convention 108+" of 2018.

The second part of this contribution will focus on the definition and taxonomy of cybercrimes. These crimes, facilitated by the development of new technologies, are expected to undergo a significant acceleration thanks to the development of AI technologies. Also for this reason, the approval of the risk-based Artificial Intelligence Act has been one of the top priorities for the EU, in order to promote trust in artificial intelligence technologies, and at the same time to ensure that it does not jeopardize fundamental rights guaranteed by EU treaties and acts.

Keywords: *cybercrime, artificial intelligence, EU, GDPR, fundamental rights*

1.Introduction

Artificial intelligence can be used as both a tool and a target in the cybercrime domain, enhancing the capabilities of both attackers and defenders. The ongoing development of artificial intelligence technologies requires continuous adaptation and innovation in cybersecurity strategies to address evolving threats. When it comes to Artificial Intelligence (AI), it is probably the technology that sparks the most curiosity and excitement today, but at the same time, it brings about uncertainties and fears. The regulation of new tools, such as those of generative AI, which currently dominate the discourse on the legislative approach to emerging technologies, involves both national and international discussions. This type of technology, capable of generating profits in the order of billions of euros, promises to exponentially increase the global GDP in the coming years, as highlighted by the Goldman Sachs report of June 2023 (Briggs & Kodnani; Goldman Sachs; 26th March 2023) and by various analysts. However, the enormous economic benefits potentially brought by these tools are contrasted by the aforementioned fears, leading to ongoing analyses of various issues, including ethical, privacy, and non-discrimination concerns. The strength of these new technologies lies in their multifunctionality, with virtually infinite sectors of application: from education to health, from security to copyright law (Lane, 2022:932-933).

The second part of this contribution will focus on the definition and taxonomy of cybercrimes. These crimes, facilitated by the development of new technologies, are expected to undergo a significant acceleration thanks to the development of AI technologies. Cybercrime can range from financial crime to identity theft and cyber extortion which is constantly evolving and expanding. Policymakers need to know the cost of cybercrime, even approximately, so that they can allocate priorities more effectively, but cybercrime not only has financial costs, but also social impacts. (Wright and Kumar, 2023) Cybersecurity and threat intelligence analysts agree that cybercriminal activity is increasing exponentially. What needs to be done is to realize the approach of techniques and indicators for the detection of cybercrime with the help of more complex investigations carried out by intelligence and engineering activities. In this paper, we systematically analyze the current state of cybercrime from a security perspective in the age of artificial intelligence. For the purpose of this paper, it is provided (i) an overview of legal acts and conventions adopted by the EU in relation to AI and cybercrime (ii) an overview of cybercriminal activities that can be detected, namely types of cybercrime and (iii) an overview of possible solutions in the future.

2. The EU fundamental data protection laws: GDPR and 'Convention 108+'

The technical basis of these tools is mostly characterized by the collection and exploitation of a large amount of data, especially for AI systems developed through machine learning (Gloria González Fuster, 2020, p.21). Therefore, data protection is paramount in this context (and not only this context), and it is certainly no coincidence that the first legislations capable of influencing the development and deployment of AI are precisely those concerning this topic, with data protection being at the forefront of the link between AI and law (Sartor & Lagioia, 2020, p.1).

'The world has changed from one in which physical risks were at the centre of attention to today's increasingly abstract risks where intangible values such as dignity and privacy are the targets of protection' (J. Chamberlain, 2023, pp.5-6)

Regarding the European framework, which is the focus of this contribution, Regulation (EU) 2016/679, better known as the General Data Protection Regulation (GDPR), represents a milestone in the regulation of the use of personal data. In line with the EU Charter of Fundamental Rights (Article 8) and the Treaties (Article 16 TFEU), where the right to personal data protection has been recognized as an EU fundamental right (González Fuster, 2020, p.14). From a legal standpoint, it is one of the few

examples of binding instruments until recently applicable in the field of AI, although it is a regulation generally related to data processing activities (Lottie Lane, 2022, p.931). In this context, in addition to the GDPR of 2016, it is worth mentioning the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' ('Convention 108') of the Council of Europe, enacted in 2018 and revised in 2019, now known as 'Convention 108+' (González Fuster, 2020, p.13). Convention 108 as an international agreement is legally binding for the member states of the Council of Europe to protect the right to privacy of individuals. In fact, the process of creating the convention for the protection of personal data of individuals began in 1950[1] with the adoption of the European Convention on Human Rights[2] which laid the foundations of the right to privacy by providing individuals with the right to respect for their "private and family life, their home and their correspondence".[3] However, these rights are not absolute, subject to certain limitations that are "in accordance with the law" and "necessary in a democratic society".(Ragan, 2022)

The absence of the right to data protection was evident in the European Convention on Human Rights. Years later after the adoption of the ECHR, it has become increasingly clear that systematic and specific changes are needed to ensure effective protection of individuals' personal data. Almost in parallel, the advent of computers combined with telecommunication tools opened up new possibilities for data processing from a global point of view. To this end, internationally binding international norms have become increasingly necessary. Since its adoption, Convention 108 has undergone several amendments and updates. An additional protocol was adopted in 2001 to harmonize Convention 108 with the Data Protection Directive[4]. The Convention was again updated in 2018 to comply with GDPR in what is known as Convention 108+. The update to Convention 108+ incorporates the core principles of the GDPR, meaning that countries that adopt Convention 108+ are closely aligned with the regulation (ibid).

2.1.1. The lack of binding instruments

This trend of not adopting binding instruments seems to have been extremely common for a long time, favoring a whole series of non-binding initiatives capable of covering a good part of the field of human rights and leaving the obligation of laws 'almost exclusively' in the field of privacy and data protection (Lane, 2022, p.941). Indeed, as highlighted by Lane in 2022, both at the national and supranational levels, the concentration of binding instruments seems to have been mainly based on these two aspects, adding that the theme of non-discrimination has also played, and continues to play, a very important role (ibid., pp.942-943). Moreover, according to the EU Fundamental Rights Agency, 'direct or indirect discrimination through the use of algorithms using big data is increasingly considered as one of the most pressing challenges of the use of new technologies' (EU FRA, 2018, 3). However, despite understanding the rationale behind this initial attitude, Lane emphasizes how binding initiatives should have been extended to other human rights otherwise insufficiently protected (2022, pp.942-943).

2.1.2. The Artificial Intelligence Act (AIA)

In this direction, the Artificial Intelligence Act (AI Act) of the European Commission, proposed in 2021 and approved by the European Parliament on March 13, 2024, and then by the Council of the European Union on May 21, will enter into full force 24 months after final approval. It sets a new

[2]The European Convention on Human Rights is a legal instrument of the Council of Europe, signed in 1950, which entered into force in 1953, it is a binding act for all signatory countries to the convention.
[2] See more. https://www.echr.coe.int/documents/d/echr/convention_ENG.Accessed on 17.05.2024.
[3] Article 8, Parapraph 1. European Convention on Human Rights (1950). Council of Europe.
[4] See more. https://eur-lex.europa.eu/eli/dir/1995/46/oj. Accesseed on 17.05.2024.

objective for the European Union, which is " to protect fundamental rights, democracy, the rule of law and environmental sustainability from high-risk AI, while boosting innovation and establishing Europe as a leader in the field" (European Parliament Press Office, March 13, 2024), representing 'the key exception' in the discourse on the lack (identified at the time) of binding instruments (Lane, 2022, p.941). This is a very important initiative that could provide greater certainty to the various stakeholders involved: from the 'victims of human rights abuses caused by reliance on AI systems, to State entities and private businesses developing and/or deploying AI' (ibid., pp.919-920).

Based on the indications provided by initiatives within the EU such as the European Commission's 'White Paper on Artificial Intelligence' (COM(2020) 65 final), and Parliamentary Resolutions and recommendations on topics related to AI, with the AI Act, the European Union decided to choose 'to understand trustworthiness of AI in terms of the acceptability of its risks' (J. Laux et al., 2023, p.3). The idea of 'trustworthy AI' is based on giving greater importance to the credibility that these technologies must assume in the eyes of the population, in order to encourage users to exploit them more, unlocking their economic and social potential (ibid). This is not a new concept: in 2019, the High-Level Expert Group on Artificial Intelligence (AI HLEG) in its Ethics Guidelines for Trustworthy AI identified 'trust' as the 'prerequisite for people and societies to develop' (Ethics Guidelines for Trustworthy AI, p.4); then, in 2020, the aforementioned European Commission's White Paper on Artificial intelligence 'explicitly states that trustworthiness is a 'prerequisite' for AI's uptake in Europe (J. Laux et al., 2023, p.6).

2.1.3. The AI ACT risk-based approach

The AI Act focuses on a risk-based approach, with the construction of a "pyramid of criticality" divided into four categories: minimal risk, limited risk, high risk, and unacceptable risk (J. Chamberlain, 2023, p.1). Risk is therefore the protagonist of this instrument, although it is not a well-established legal concept, but rather much debated (ibid). According to Chamberlain, 'a risk-based approach may become the global norm for regulating AI' (ibid, p.5). This kind of approach depends on the notion of acceptability: the unacceptable risks are prohibited (J. Laux et al., 2023, p.6). The "unacceptable risks" are indicated in Article 5 of the regulation and are those that violate the Union's values, such as infringements of human rights, practices capable of manipulating people, social scoring by public authorities, and the use of real-time remote biometric identification systems in public spaces (in this case, there are limited exceptions based principally on people's security matters) (J. Chamberlain, 2023, p.5).

The 'high risk' systems are the ones discussed in the most articles, from Article 6 to 51. These are the systems that represent a menace to EU values, so the EU legislator performed a 'balancing act' (ibid, p.6). The third level, represented by the 'limited risks', has been regulated in Article 52, which indicates that people 'must be informed when they are interacting with AI systems' (ibid). At the lowest level of this pyramid of criticality are the 'minimal risk' systems, represented, for example, by spam filters, computer games, or chatbots (ibid, p.7).

2.2. Binding EU Measures for Cybersecurity and Cybercrime Prevention

The European Union (EU) has established several binding legal instruments to prevent cybercrime and enhance cybersecurity across its member states. These instruments set out obligations for member states to adopt and implement specific measures aimed at protecting networks, systems, and data from cyber threats. The next binding instruments collectively contribute to the EU's comprehensive approach to preventing cybercrime, ensuring robust cybersecurity measures, and

fostering international cooperation in the fight against cyber threats. Here are some of the key binding EU instruments:

- *Regulation (EU) 2019/881;*

Cybersecurity Act[5] is adopted on April 17, 2019, and the goal is to strengthen the cybersecurity framework within the EU and enhance the role of the EU Agency for Cybersecurity (ENISA). Key provisions of the Cybersecurity Act are: 1. Establishment of a cybersecurity certification framework for ICT products, services, and processes; 2. Reinforcement of ENISA's mandate, providing it with more resources and responsibilities to support member states in improving their cybersecurity capabilities.

- *Regulation (EU) 2016/679;*

General Data Protection Regulation (GDPR)[6] is adopted on April 27, 2016, to protect personal data and privacy of EU citizens and to harmonize data protection laws across the EU. Key provisions of the GDPR are**:** Requirements for data controllers and processors to implement appropriate technical and organizational measures to ensure data security; Mandatory breach notification to supervisory authorities and affected individuals in the event of a data breach; and Significant fines for non-compliance with data protection and security obligations.

- *Directive 2013/40/EU on Attacks Against Information Systems;*

Directive on Attacks Against Information Systems[7] is adopted on August 12, 2013, со цел To combat large-scale cyber-attacks and strengthen the security of information systems. Some of key provisions are: Criminalization of the illegal access to information systems, illegal system interference, illegal data interference, and illegal interception; Establishment of penalties for natural and legal persons involved in cyber-attacks, and Enhanced cooperation among member states through the designation of contact points available 24/7 to support investigations.

- *Directive (EU) 2019/1937 on the Protection of Persons Who Report Breaches of Union Law;*

Whistleblower Protection Directive[8] is adopted on October 23, 2019, with a goal to provide protection for whistleblowers who report breaches of EU law, including those related to cybersecurity. As key provisions we do have: Establishment of secure reporting channels for whistleblowers and Protection against retaliation for individuals who report breaches.

- *Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive)*

NIS Directive[9] is adopted on July 6, 2016, to ensure a high common level of network and information security across the EU. Key provisions of the directive are considered: the Obligations for member states to develop national cybersecurity strategies; Requirements for operators of essential services and digital service providers to take appropriate security measures and notify significant

[5] See more. https://eur-lex.europa.eu/eli/reg/2019/881/oj Accesseed on 25.05.2024.
[6] See more. https://eur-lex.europa.eu/eli/reg/2016/679/oj Accesseed on 25.05.2024.
[7] See more. https://eur-lex.europa.eu/eli/dir/2013/40/oj Accesseed on 25.05.2024.
[8] See more. https://eur-lex.europa.eu/eli/dir/2019/1937/oj Accesseed on 25.05.2024.
[9] See more. https://eur-lex.europa.eu/eli/dir/2016/1148/oj Accesseed on 25.05.2024.

incidents to the relevant national authorities; and Establishment of Computer Security Incident Response Teams (CSIRTs) and a cooperation group to facilitate strategic cooperation and information sharing among member states.

- *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive);*

Last but not least, NIS2 Directive[10] is Adopted on November 14, 2022 which actually replaced the NIS Directive and further strengthen cybersecurity resilience and incident response capabilities across the EU. Key Provisions of NIS2 Directive are: 1. Broader scope covering more sectors and entities critical to the economy and society; 2. Stricter security requirements and more detailed incident reporting obligations; and 3. Enhanced cooperation and information sharing among member states and EU institutions.

3. Phenomenon of the 21st century: Cybercrime

Cybercrime is a challenge that is undeniably growing in the world of technology every day. It is considered a form of behavior that is against the law, although in addition to this term, others appear such as: internet crime, e-crime, high technology crime, network crime, etc. (Babovic, 2004) Europol defines cyber crime as criminal activity that either targets or uses a computer, a computer network or a networked device. A cybercriminal can use a device to access a user's personal information, confidential business information, government information, or disable a device. Computer crime represents a special type of criminal acts that differ from other illegal acts, and a particularly significant feature that is recognized is the use of the computer as a means of committing a crime.

It is important, to not confuse cybercrime with cyber security. Both cyber threats are different in motive, intent, purpose, scope, consequences, as well as the parties involved in preventing and mitigating the threats. In practice, cybercrime varies from spam and phishing emails, internet fraud and impersonation, to prohibited offensive and illegal content, identity theft and online child sexual abuse material. The main motivation behind acts of cybercrime, as is the case with "traditional" crime, is generally financial gain. Cybercriminals are essentially hackers with malicious intent.

Computers and networks can be main target or to be used as a tool for commiting crimes. When it comes to computers and networks as main target, few of the most commonly used tools are malicious software such as viruses, trojans, adware and spyware to gain access to systems, monitor activities and collect data; bot networks (botnets), or hijacked computers that perform tasks remotely without the knowledge of their users; and Denial of Service (DoS) attacks that aim to exhaust available resources in a network, application, or service, to prevent users from accessing them (Klopfer et al.). And in such cases, the effects of these attacks are numerous. Individuals can suffer financial losses, or be victims of theft of personal and sensitive information. When it comes to companies, they can be victims of cybercriminal attacks facing potential financial losses, the risk of losing sensitive business information, in the last case, patent data or personal data of their customers and users, which can indirectly led to serious reputational consequences. On the other hand, public institutions and non-profit organizations can become victims of extortion or theft of the personal data of the users of their services (ibid.)

When computers are used as tools to commit crimes, they can spread in cyberspace, including illicit trafficking in drugs, weapons and sensitive data and information, human trafficking, and other forms of violence. Generally such contracts take place on the so-called darknet where users act

[10] See more. https://eur-lex.europa.eu/eli/dir/2022/2555/oj Accesseed on 25.05.2024.

completely anonymously. By using the darknet, individuals and criminal organizations use encrypted messaging services and crypto-currencies to conduct financial transactions, making tracking and identification extremely difficult. Criminals with technical knowledge or technical experts hired by criminals, also known as black hat experts, also use the potential of the darknet by exploiting weak points they have discovered in software and anonymously selling them to anyone looking for ways to abuse specific systems, a practice that has been increasing over time (ibid.)

Regardless of everything, wherever the internet is, there are also cybercriminals who represent an inevitable threat from individuals to public institutions, companies and corporations. Hackers or also known as cybercriminals can be classified into several groups:

Organized Hackers - This type of hackers are usually organized together to accomplish a specific goal. The reason may be to fulfill their political bias, fundamentalism etc. The Chinese are said to be some of the best hackers in the world. They publicly target the locations of other governments in order to fulfill political objectives. (Brigadier General Md. Khurshid Alam)

Professional Hackers/Crackers - Such hacking stuffs are motivated by money and mostly used to hack rivals site and get reliable, secure and valuable information. Furthermore they are used to hack the employer's system basically as a measure to make it more secure by exposing loopholes in the law. (Ibid.)

Dissatisfied Employees - This group includes those people who have either been fired by their employer or are dissatisfied with their employer. Traditionally, insider attacks have been the biggest threat to computer networks, accounting for about 70 percent of all intrusion attempts. (Ibid.)

Different documents classify types of cybercrime in different ways. Also, in the material for the "workshop" on online crime, the UN's 10th annual report states that there are two subcategories of online crime: Cyber crime in the narrower sense - any undetected attack aimed at the electronic operations of the security of computer systems and data, which is being tackled cyber crime in the broader sense - any undetected attack related to or connected to a computer system and network, including such crimes as is an independent provider of information, services and distribution through computer systems and networks (Шемерикић К., 2019).

The European Convention on Cybercrime[11] foresees 4 groups of acts:

a) acts against the confidentiality, integrity and accessibility of computer data and systems - such as unauthorized access, interception, interference in data or systems, connecting devices (retrieval, distribution, sale), programs, passwords;

b) acts related to computers - counterfeiting and theft are the most typical forms of attack;

c) acts related to the content - child pornography is the most common content that is published in the this group, including the creation, distribution, transmission, storage or sharing of accessible and accessible materials, including reproduction for the purpose of distribution and processing in a computer system or on a data storage device;

d) works related to the violation of copyright and related rights include the reproduction and distribution of unauthorized copies of the work by computer systems (ibid).

3.1. Categories of Cyber Crime

There are several categories of computer crime, but for the purposes of this paper, the following will be singled out:

Data Crime - The modification of data and the theft of data are also called as data crime. An attacker monitors the flow of data to or from a target in order to gather information. This attack can be

[11] Also known as Budapest Convention. See more https://rm.coe.int/1680081561 Accessed on 29.05.2024.

undertaken to gather information to support a later attack or allow the collected data to be the ultimate goal of the attack. This attack usually involves snooping or sniffing network traffic, but may involve observing other types of data streams. In most types of this attack, the attacker is passive and simply observes regular communication, but in some variants the attacker may attempt to initiate the establishment of data flow or influence the nature of the transmitted data. Most often, information that is susceptible to cybercrime is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Since this information was obtained illegally, when the individual who stole this information is considered to have committed a crime and will be held accountable before the law (Nayak, October 2013)

Cybercrime - Unauthorized access and spreading of viruses is called cybercrime. "Unauthorized Access" is called An Insider's Look at the Computer Hacker Underground. This type of cybercrime has been observed across the United States, the Netherlands and Germany. "Unauthorized Access" looks at the people behind the computer screens and aims to separate the media's reporting of the "renegade hacker" from reality (Arya, G., 2020). Performance analysis of arithmetic logic unit with reversible logic. International Journal of Advanced Trends in Computer Science and Engineering,]. Malware that attaches to other software. Such as virus, worm, trojan horse, time bomb, logic bomb, rabbit and bacteria are examples of malware that destroys the victim's network system. (Virus Glossary (2006), 2012)

Related Crimes - Aiding and abetting cyber crime, computer forgery and fraud and content related crimes are called Related Crimes. There are three elements to most aiding and abetting charges against an individual.

- Another person committed the crime;
- The individual had knowledge of the crime;
- The individual provided some assistance to the perpetrator of the criminal act (Goni et al., 2022).

4. The Role of AI in Offensive Cyber Tactics

AI has significantly altered the landscape of offensive cyber tactics, empowering cybercriminals with advanced capabilities to launch more sophisticated and targeted attacks. Recent trends indicate a growing reliance on AI-driven techniques, enabling adversaries to exploit vulnerabilities, evade detection, and maximize the impact of their malicious activities (Johnson, 2019). One prominent area where AI plays a pivotal role in offensive cyber operations is in the development and deployment of malware. AI algorithms can generate highly sophisticated malware variants that are specifically designed to bypass traditional cybersecurity defenses. These AI-powered malware strains are capable of adapting their behavior in real-time, making them extremely challenging to detect and mitigate. Recent statistics reveal a significant increase in the number of AI-enhanced malware variants, highlighting the effectiveness of this approach in evading detection. Additionally, AI is instrumental in automating and optimizing the process of launching cyberattacks. For example, AI-driven tools can automate the reconnaissance phase of an attack by scanning networks and systems to identify potential vulnerabilities.

Moreover, AI algorithms can analyze vast amounts of data to identify high-value targets and craft tailored attack strategies, significantly increasing the success rate of offensive operations (Whyte, 2020). Recent trends show a rise in AI-driven reconnaissance activities, reflecting cybercriminals' increasing sophistication in targeting and exploiting vulnerabilities. Spear-phishing, a tactic commonly used by cybercriminals to trick individuals into divulging sensitive information or installing malware, has also been transformed by AI. AI-powered spear-phishing campaigns can generate highly

personalized and convincing messages by analyzing large datasets to craft targeted content. These AI-driven phishing attacks have seen a significant increase in recent years, with cybercriminals leveraging AI to bypass email security filters and improve the success rate of their campaigns (Guembe, 2022). Furthermore, AI is employed to enhance the effectiveness of brute force attacks and passwordguessing techniques. By leveraging machine learning algorithms, cybercriminals can accelerate the process of cracking passwords by predicting likely combinations based on patterns observed in previous breaches. This AI-driven approach significantly reduces the time and effort required to compromise accounts and gain unauthorized access to sensitive information. Recent statistics indicate a rise in AI-assisted brute force attacks, underscoring the growing prevalence of this tactic in offensive cyber operations.

5. AI Powered Cyber Threat Detection and Response Mechanisms

The integration of AI into cybersecurity has revolutionized the detection and response to cyber threats, addressing the increasingly sophisticated and fast-evolving cyber threat landscape. AI-powered systems leverage advanced algorithms, machine learning models, and real-time data processing to identify, analyze, and mitigate cyber risks more effectively than traditional methods. A key advantage of AI in cybersecurity is its ability to process and analyze vast amounts of data at unprecedented speeds. Traditional cybersecurity measures often struggle to keep up with the volume of data generated by modern digital activities. In contrast, AI systems can shift through massive datasets, identifying patterns and anomalies that may indicate potential threats. Machine learning algorithms learn from historical data, enabling them to recognize known threats and predict new, emerging ones. This predictive capability is crucial for proactive threat mitigation.

AI-powered threat detection systems utilize various techniques to identify malicious activities. For instance, anomaly detection algorithms monitor network traffic and user behavior to spot deviations from established norms, which may indicate a cyber-attack. These systems can detect unusual login attempts, abnormal data transfers, and other suspicious activities in real time, enabling faster incident response (Dwivedi, 2021). Additionally, AI can enhance endpoint security by continuously monitoring and analyzing device behavior, identifying potential threats before they can cause significant damage. Deep learning, a subset of machine learning, plays a crucial role in enhancing the accuracy of threat detection. Deep learning models can analyze complex data structures, such as images, text, and network traffic patterns, to identify subtle indicators of cyber threats. For example, deep learning can be used to detect advanced persistent threats (APTs), which are sophisticated, long-term cyber-attacks often aimed at stealing sensitive information. By identifying the subtle patterns associated with APTs, deep learning models can provide early warnings, allowing organizations to take pre-emptive action.

AI also significantly improves incident response capabilities. Automated response systems, powered by AI, can quickly contain and mitigate cyber threats, reducing the time between detection and response. For example, AI-driven security orchestration, automation, and response (SOAR) platforms can execute predefined response actions, such as isolating infected systems, blocking malicious IP addresses, and applying patches (Carsten Stahl, 2021). This automation reduces the burden on cybersecurity teams, allowing them to focus on more strategic tasks. Another emerging trend is the use of AI in threat intelligence. AI can analyze vast amounts of threat data from various sources, including dark web forums, threat feeds, and social media, to identify emerging threats and vulnerabilities. This intelligence can be used to update threat databases, refine detection algorithms, and inform proactive defense strategies. In 2023, IBM reported that its AI-powered threat intelligence platform, IBM X-Force, identified over 150 new threats and vulnerabilities within a year, demonstrating the effectiveness of AI in enhancing threat intelligence. AI-powered cyber threat detection and response mechanisms are transforming the cybersecurity landscape. By leveraging advanced algorithms,

machine learning, and deep learning, these systems offer enhanced capabilities for identifying, analyzing, and mitigating cyber threats. As AI technology continues to evolve, it will play an increasingly vital role in safeguarding digital assets and maintaining cybersecurity in an ever-changing threat environment (Bai & Fang, 2022).

6. Future of AI in Cybersecurity

The future of AI in cybersecurity is set to revolutionize how we detect, prevent, and respond to cyber threats. AI's ability to process vast amounts of data quickly allows it to identify patterns and anomalies that indicate potential threats. Machine learning algorithms learn from previous attacks, continuously improving their detection capabilities (Juneja et al., 2021). This predictive power enables AI-driven systems to anticipate attacks, providing pre-emptive defenses and minimizing damage. AI enables the creation of adaptive cybersecurity systems that adjust strategies based on threat nature. These systems deploy real-time countermeasures, offering dynamic defenses that static systems cannot match (Morel, 2011). This adaptability is crucial for responding to new, unknown threats. Automation of routine tasks is another significant advantage of AI in cybersecurity.

Technologies like robotic process automation (RPA) will handle repetitive tasks, freeing cybersecurity professionals to focus on complex, strategic issues. Automated systems can manage patch management, log analysis, and compliance monitoring efficiently, reducing human error. AI also enhances incident response by quickly analyzing attack scope and impact, recommending remediation steps, and even executing some autonomously. This rapid response capability is critical for minimizing damage and restoring operations swiftly. In user authentication, AI will play a crucial role. Biometric systems powered by AI will provide higher security levels compared to traditional passwords, analyzing fingerprints, facial recognition, and behavioural patterns for accurate identity verification (Kaur et al, 2023). AI will enhance threat intelligence by aggregating and analyzing data from various sources to identify emerging threats.

Predictive analytics will enable proactive vulnerability management. This forward-looking approach is essential to stay ahead of cyber adversaries. The future will see a symbiotic relationship between AI and human experts (Patel, 2023). AI handles data-intensive tasks, while human intuition interprets insights and makes strategic decisions. Collaborative platforms leveraging both AI and human judgment will become standard. However, integrating AI into cybersecurity raises ethical and legal considerations (Sarker et al, 2021). Ensuring ethical AI use, protecting privacy, and developing regulatory frameworks are essential. Transparency and accountability in AI decision-making will maintain trust.

Conclusion

The AI technologies have led the EU to adopt the AI Act, which will be fully implemented within the next two years. In the meantime, these data-based technologies have been regulated in some of their components by existing data protection laws, such as the GDPR and the "Convention 108+". The need for regulation of these tools becomes even more evident when considering the issues related to various types of cybercrimes mentioned: from data crimes to the development of malware, and the search for information useful to criminals to commit related crimes, exploiting the functionalities allowed by these tools.

A comprehensive and diverse strategy that makes use of legal frameworks, international cooperation, and technical breakthroughs is required to prevent cybercrime within the European Union (EU) in the era of artificial intelligence (AI). AI offers cybersecurity both tremendous benefits and formidable difficulties as it develops. With its automated threat detection, smart response mechanisms, and predictive analytics, AI technology can greatly improve cybersecurity measures. With real-time

threat detection and mitigation capabilities, these products shorten response times and lessen the effect of cyberattacks. AI-driven systems offer a dynamic defense against ever-more-sophisticated cybercriminal operations by adapting to new and developing threats. There are hazards associated with integrating AI into cybersecurity, though. Cybercriminals may target AI systems directly, and they may also use AI technology to create more sophisticated and potent attack plans. Because AI has two sides, it needs a strong governance structure to make sure that its applications in cybersecurity are transparent, ethical, and safe.

To keep ahead of cyberthreats, the EU has to invest more money in AI-driven cybersecurity research and development. This involves providing funds for creative initiatives, encouraging public-private collaborations, and offering rewards for the creation of cutting-edge cybersecurity products. The EU should also encourage a culture of ongoing learning and adaptation to make sure cybersecurity experts have the most up-to-date information and abilities to meet new threats. Frameworks for laws and regulations are essential for preventing cybercrime. The EU needs to make sure that its laws are up to date with the latest developments in technology and offer precise rules for the creation and application of AI in cybersecurity. This entails dealing with concerns like accountability, algorithmic transparency, and data privacy. Although the General Data Protection Regulation (GDPR) is a good starting point, other steps would be required to handle the particular difficulties that artificial intelligence presents. Combating cybercrime also requires international cooperation. Because cyber hazards are worldwide in scope, they cannot be addressed by one nation or area alone. To exchange intelligence, plan responses, and create best practices for AI-driven cybersecurity, the EU should further up its cooperation with other nations, international organizations, and the commercial sector. This entails taking part in international projects, encouraging collaboration across borders, and endorsing global cybersecurity norms. Education and public awareness campaigns are essential parts of a thorough cybersecurity plan. The EU needs to fund campaigns that educate people about cyberthreats and advance safe online behavior. This contains resources for people and organizations to improve their cybersecurity posture, as well as focused campaigns and educational initiatives. In conclusion, preventing cybercrime in the era of artificial intelligence inside the European Union necessitates a proactive and well-balanced strategy that incorporates public awareness, international cooperation, regulatory frameworks, and technological innovation. The EU can create a robust digital ecosystem that shields its people, companies, and vital infrastructure from the always changing threat of cybercrime by utilizing AI's potential while managing its hazards.

REFERENCES

Wright D., Kumar R. (2023) Assessing the socio-economic impacts of cybercrime. Societal Impacts. https://doi.org/10.1016/j.socimp.2023.100013.

Cascavilla G., Tamburri D. A., Van Den Heuvel W-J (2021) Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security. https://doi.org/10.1016/j.cose.2021.102258.

European Convention on Human Rights (1950). Council of Europe.

Ragan S. (2022). What is "Convention 108"?.

Babovic M (2004). "Kompjuterska prevara I Internet prevara", Clanak objavljen u zbirci, Symorg.

Klopfer F. et al. Вовед во управувањето со Сајбер Безбедност – Прирачник за пратеници. Geneva Center for Security Sector. Pg 8.

Шемерикић К. (2019). Последице сајбер криминала у Републици Србији. Универзитет у Београду - Тероризам, организовани криминал и безбедност. Pg. 11.

Goni O., Ali H., Alam M., (2022) The Basic Concept of Cyber Crime. Journal of Technology Innovations and Energy, https://doi.org/10.5281/zenodo.6499991.

Johnson J., (2019). The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability. 4 Journal of Cyber Policy. Pg 442.

Whyte C., (2020). Problems of Poison: New Paradigms and "Agreed" Competition in the Era of AI-Enabled Cyber Operations, 1300 in 2020 12th International Conference on Cyber Conflict (CyCon). Pg 215.

Guembe et al., (2022) The Emerging Threat of Ai-Driven Cyber Attacks: A Review, 36 Applied Artificial Intelligence. https://doi.org/10.1080/08839514.2022.2037254.

Dwivedi et al., (2021) Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy, 57 International Journal of Information Management. https://doi.org/10.1016/j.ijinfomgt.2019.08.002.

Stahl B. C., (2021) Artificial Intelligence for a Better Future: An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies. Springer Cham.

Bai M., Fang X., (2022) Cybersecurity Analytics: AI's Role in Big Data Threat Detection, 11 Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal. Pg 392 (2022).

Juneja A. et al., (2021). Artificial Intelligence and Cybersecurity: Current Trends and Future Prospects, in The Smart Cyber Ecosystem for Sustainable Development. Pg 431.

Morel B., (2011) Artificial Intelligence and the Future of Cybersecurity. In Proceedings of the 4th ACM workshop on Security and artificial intelligence. Pg 93.

Kaur R., Gabrijelčič D., Klobučar T. (2023). Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. Information Fusion. Pg 97.

Patel H. (2023), The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning (ML). doi:10.20944/preprints202301.0115.v1

Sarker I. H., Furhad M. H., Nowrozy R., (2021) AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions, Vol.:(0123456789)SN Computer Science (2021) 2:173. https://doi.org/10.1007/s42979-021-00557-0.

Briggs, M., & Kodnani, N. (2023, March 26). The potentially large effects of artificial intelligence on economic growth. Goldman Sachs. Retrieved from https://www.gspublishing.com/content/research/en/reports/2023/03/27/d64e052b-0f6e-45d7-967b-d7be35fabd16.html

Chamberlain, J. (2023). The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective. European Journal of Risk Regulation, 14, 1–13. https://doi.org/10.1017/err.2022.38

European Commission. (2020, February 19). White Paper on Artificial Intelligence - A European approach to excellence and trust (COM/2020/65 final). Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065

European Parliament Press Office. (2024, March 13). Artificial intelligence: MEPs adopt landmark law. Retrieved from https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

European Parliament, Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

European Union Agency for Fundamental Rights (EU FRA). (2018a). #BigData: Discrimination in data-supported decision making. FRA Focus, 2018.

EU Artificial Intelligence Act. (2024, April 19). Retrieved from https://artificialintelligenceact.eu/ai-act-explorer/

High-Level Expert Group on AI. (2019, April 8). Ethics guidelines for trustworthy AI. Retrieved from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Laux, J., Wachter, S., & Mittelstadt, B. (2024). Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. Regulation & Governance, 18(1), 3–32. https://doi.org/10.1111/rego.12512

Internet Portals:

https://eur-lex.europa.eu/eli/dir/1995/46/oj
https://eur-lex.europa.eu/eli/reg/2019/881/oj
https://eur-lex.europa.eu/eli/reg/2016/679/oj
https://eur-lex.europa.eu/eli/dir/2013/40/oj
https://eur-lex.europa.eu/eli/dir/2019/1937/oj
https://eur-lex.europa.eu/eli/dir/2016/1148/oj
https://eur-lex.europa.eu/eli/dir/2022/2555/oj
https://www.echr.coe.int/documents/d/echr/convention_ENG
https://rm.coe.int/1680081561
https://www.europol.europa.eu/crime-areas/cybercrime