Asia Pacific Academy of Science Pte. Ltd.

Metaverse 2024, 5(2), 2796.
https://doi.org/10.54517/m.v5i2.2796

Review

The role of generative AI in cyber security

Kevin Curran*, **Ethan Curran, Joseph Killen, Cormac Duffy**

School of Computing, Engineering and Intelligent Systems Derry, Ulster University, Londonderry BT48 7FL, Northern Ireland
*** Corresponding author:** Kevin Curran, kj.curran@ulster.ac.uk

CITATION

Curran K, Curran E, Killen J, Duffy C. The role of generative AI in cyber security. Metaverse. 2024; 5(2): 2796. https://doi.org/10.54517/m.v5i2.2796

ARTICLE INFO

Received: 28 June 2024
Accepted: 2 August 2024
Available online: 13 November 2024

Abstract: In the ever-evolving landscape of cyber threats, the integration of Artificial Intelligence (AI) has become popular into safeguarding digital assets and sensitive information for organisations throughout the world. This evolution of technology has given rise to a proliferation of cyber threats, necessitating robust cybersecurity measures. Traditional approaches to cybersecurity often struggle to keep pace with these rapidly evolving threats. To address this challenge, Generative Artificial Intelligence (Generative AI) has emerged as a transformative sentinel. Generative AI leverages advanced machine learning techniques to autonomously generate data, text, and solutions, and it holds the potential to revolutionize cybersecurity by enhancing threat detection, incident response, and security decision-making processes. We explore here the pivotal role that Generative AI plays in the realm of cybersecurity, delving into its core concepts, applications, and its potential to shape the future of digital security.

Keywords: GenAI; Generative AI; Artificial Intelligence; cybersecurity

1. Introduction

The field of cybersecurity is at an important stage as it deals with persistent and sophisticated threats from malicious criminals operating online. In today's world, as our dependency on technology increases, so do the potential for attackers to infiltrate organisations for ransom or their own personal gain. Organisations are discovering AI as a powerful tool in enhancing security measures to safeguard sensitive data from cyber threats in this constantly changing world. In a study within the last year, EMEA organisations had the most cyber incidents in the past year, with 20% of participants reporting 11 or more attacks. The top two countries on the list were Germany and the United Kingdom (both at 25%). Germany reported the most malware incidences in 2021; the Federal Office for Information Security (BSI) discovered 553,000 malware variants in a single day in February 2021 [1] AI has emerged as a crucial piece of software in the fight against cyber-attacks thanks to its capacity to handle enormous volumes of data, detect anomalies, and adjust in real-time due to machine learning. This article launches a thorough investigation into the role of AI in cybersecurity, providing a deep dive into numerous aspects. It covers a discussion of the critical role AI plays in combating cyberthreats, the difficulties and restrictions that come with using it, and a look at potential future breakthroughs and factors that might drastically change the field of AI in cybersecurity.

In a time where malicious actors are leveraging technology in increasingly sophisticated ways, the integration of AI into cybersecurity is a necessity. The interaction of both areas holds the possibility of preventing future assaults from happening in addition to defending against present ones. The ever-expanding digital

landscape has birthed a host of cybersecurity challenges. Data breaches, ransomware attacks, and sophisticated nation-state-sponsored cyber espionage operations are pervasive, threatening individuals, organizations, and nations alike. Traditional security measures, while indispensable, often find themselves outmatched in the face of these evolving threats [2]. In particular, the reactive nature of traditional cybersecurity measures poses a significant hurdle. These approaches tend to focus on known threats, leaving organizations vulnerable to novel and rapidly evolving attack methods. As a result, the need for innovative, proactive solutions that can adapt to the ever-changing cyber threat landscape has become evident (**Figure 1**).

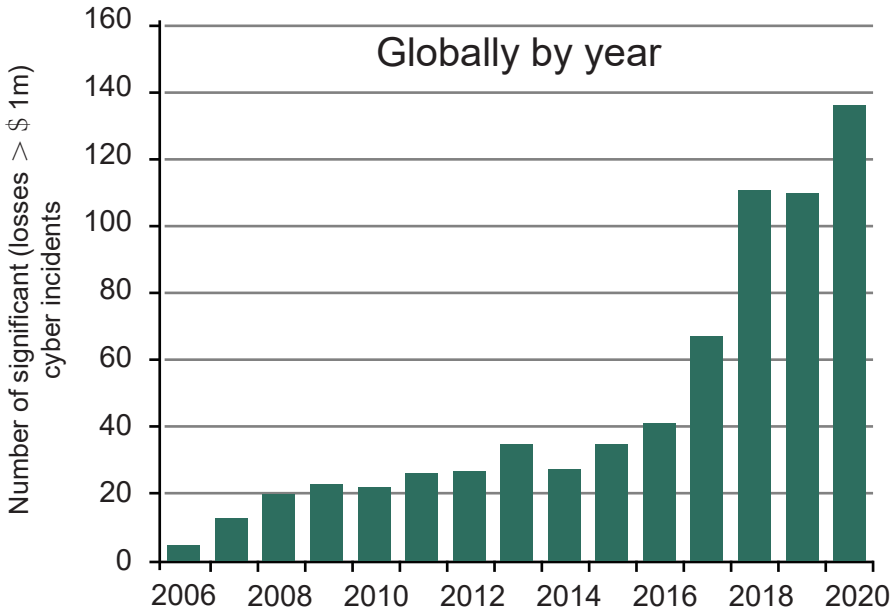

Figure 1. Cyber-attacks globally by year [3].

Open AI when they released their product called ChatGPT in November 2022 which got over 1 million users within 5 days of release, by comparison it took Instagram 2.5 months and Netflix over 3.5 years to reach 1 million users (see **Figure 2**).

Generative AI, a subset of artificial intelligence, leverages the principles of machine learning, deep learning, and neural networks to produce data, content, or solutions that were not explicitly programmed. It possesses the capacity to revolutionize the way we address cybersecurity challenges by enhancing threat detection, incident response, and security decision-making processes. We will delve into the core concepts of Generative AI, scrutinise the prevailing cybersecurity challenges it seeks to address, and explore specific applications that demonstrate its efficacy in securing our digital ecosystems. We cover an extensive investigation into AI's role and involvement in cybersecurity. It will conduct a thorough insight of several important aspects, including the use of AI in cybersecurity, the benefits of incorporating it to prevent cyberattacks, the drawbacks and challenges of doing so, and the potential developments of AI in this crucial area. The paper aims to provide a complete and accurate representation of AI's impact on cybersecurity while considering future considerations that may shape the landscape further.

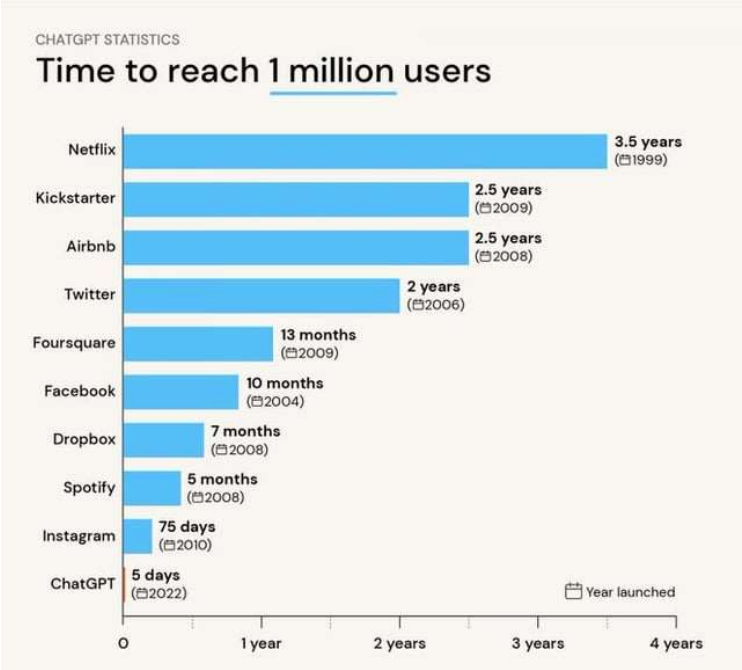

Figure 2. ChatGPT time to reach 1 million Users in comparison to other applications [4].

2. Research methods

With regards the research method, we systematically explored several databases to ensure a broad and exhaustive collection of relevant literature on Artificial Intelligence (AI), Generative AI and cybersecurity with a particular focus on generative AI being used within the area of generative AI.

The primary databases searched included Google Scholar, IEEE Explore, ACM digital library, Springerlink and JSTOR, all of which are known for their extensive repositories of academic and peer-reviewed articles.

Our search strategy employed specific keywords such as “AI & cybersecurity”, “generative AI & cybersecurity”, and “generative artificial intelligence & cybersecurity”.

To refine the search and manage the vast amount of data, filters were applied to exclude non-peer-reviewed articles and to limit the results to papers published within the last two years. This temporal filter was crucial to ensure the relevance and contemporaneity of the data especially as genAI is relatively new in the research papers arena. 80% of the articles in the end are from 2023. This of course is a natural consequence of generative AI being a recent technique – at least for the public.

Furthermore, additional filtering based on relevance scoring and citation count was utilized to prioritize highly impactful and foundational studies in the field of generative AI & cybersecurity.

This systematic approach enabled the identification of significant trends and developments, contributing to a comprehensive analysis of the current landscape of generative AI technologies being used within cybersecurity.

It is estimated that we reviewed 50+ papers.

3. Artificial Intelligence's role in combating cyber threats

Malware is a malicious software if allowed to run can cause a serious threat to systems or data when access is gained. In 2022, organisations throughout the world detected 493.33 million ransomware attempts [5]. Attackers use a variety of methods, including phishing emails, to get this malicious software into the organisation's systems. AI's capacity to evaluate malware databases and find patterns that may be utilised to stop upcoming attacks is an efficient way to deal with this danger. Malware databases will be examined using machine learning, increasing the likelihood these applications may be detected in the future. These systems can be trained easily to identify malware threats before being applied to a system (see **Figure 3**).

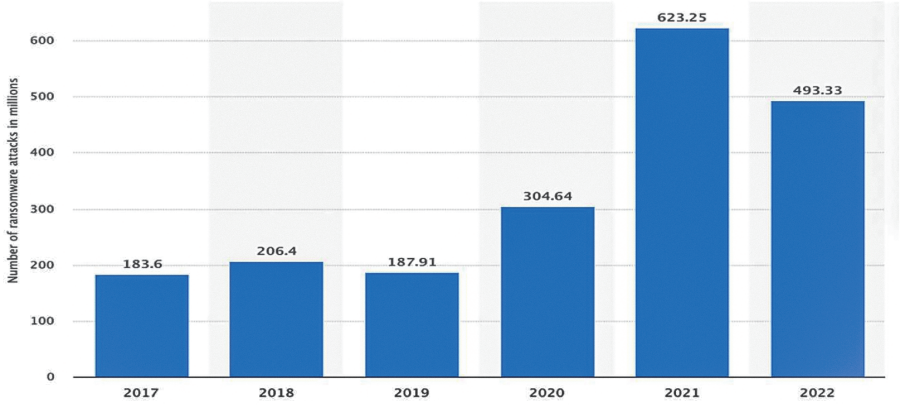

Figure 3. Advancement of ransomware attempts worldwide from 2017 to 2022 [5].

3.1. Threat intelligence

Artificial Intelligence is used as a key component in modern cybersecurity by dramatically improving threat intelligence for an organisation. It serves as a powerful tool in safeguarding digital assets from cyber threats when deployed. AI can quickly find abnormalities in network traffic, user behaviour, and system logs by utilising machine learning methods and real-time data analysis. Here threat intelligence begins with the collection of data from various sources. Open-source intelligence, dark web monitoring, internal network logs, security tools, government agencies, cybersecurity firms, and industry-specific information exchange and analysis hubs are some examples of these sources [6]. This capability enables security teams to respond promptly to potential threats, reducing the risk of data breaches and system compromises from the gained knowledge. The ability of AI's analytics to detect new attack patterns and weaknesses enables organisations to proactively bolster their defences. Additionally, AI-driven systems can act independently in response to threats, limiting possible harm by blocking malicious IP addresses or isolating vulnerable network segments [7]. Building more robust and proactive cybersecurity solutions in an ever-evolving threat requires the integration of AI in threat detection and prevention.

3.2. Constant advancement of security

Due to the advancement of the computing world, hackers are finding more sophisticated ways to target vulnerabilities in networks and information systems. Adversaries frequently change up their strategies. For instance, a malware attack,

denial-of-service assault, brute force attack, and phishing attack could all be launched simultaneously against an information system. Because of this, it is challenging for the effected user to decide which problem to tackle first, and as a result, attackers may infiltrate the information system. Artificial intelligence has the cognitive ability to learn the latest attack strategies that are used by attackers [8]. Due to it being constantly updated, AI will adapt to new exploitation techniques allowing it to combat new threats that surface. Intelligent systems can prioritise which risk to address first in the event of numerous cyberattacks to ensure the least amount of harm. Intelligent systems are used to address, mitigate, and deal with any indirect security breaches brought on by users.

3.3 Authentication

It is essential for authentication to be incorporated to a network to protect data integrity and confidentiality. Authentication is also used to support access control protocols, which allow users to access data based on the level of access associated with their credentials [9]. However, attackers can manage to find loopholes around the authentication process gaining them access to a organisations data. Once they have access to these accounts, attackers exploit the privileged information either maliciously or for their own gain. In the authentication process, artificial intelligence is used to introduce a new level of security that reinforces the already-existing process making less likely for attackers to infiltrate [10]. By extending traditional boundaries and incorporating data context, biometrics, and trends in user behaviour, AI can enable better, more secure authentication. Companies nowadays that are focused on cyber defence are particularly fond of biometric authentication, and AI plays a significant role in this. Keystroke dynamics (typing style), behavioural biometrics (analysing user behavioural patterns to create cyber fingerprints), facial recognition, and voice recognition are a few examples [11].

3.4. Vulnerability detection

An organisation should do cyber security analysis on all its assets and resources to determine the vulnerabilities and dangers they could potentially face to adequately safeguard its network and information systems. It is essential to build upon this as it can be crucial in identifying and cancelling threats and vulnerabilities. Artificial intelligence in this case is used to evaluate and analyse potential risks, current security precautions, and the best course of action [12]. It provides swift, accurate results in detecting system deficiencies. AI-driven algorithms can rapidly scan intricate software codes and configurations, pinpointing vulnerabilities that may otherwise remain concealed. Due to its effectiveness, the most crucial security tasks can be defined by determining the network and information system weak spots. By doing so, AI equips organisations with the knowledge required to strengthen their defences, thereby reducing the opportunity for malicious actors [13].

3.5. Password generation and cracking

In cyber security, AI is an effective method for password generation. It can generate strong and unique passwords that are tough for both automated systems and

human beings to crack. These passwords frequently contain more characters than manually generated ones and frequently mix upper- and lowercase letters, digits, and symbols [14]. Additionally, it can customise password generation based on account type and organisational regulations, ensuring that passwords adhere to strict security standards while yet being user-friendly. By creating new passwords when necessary and implementing password rotation rules, it also helps with password management while enhancing password security in general [15]. AI can also be used to simulate and analyse password cracking attempts, a crucial aspect of cybersecurity. Organisations can discover weak passwords vulnerable to be compromised by simulating attacks using AI, pushing users to change their passwords, or enforcing stronger restrictions. It helps evaluate an organization's resilience against password cracking attacks, allowing security professionals to strengthen defences accordingly. The development of stronger authentication techniques, like multi-factor or biometric authentication, with less reliance on passwords alone and increased security overall, can also be facilitated. Essentially, AI has two roles in password management: it helps with password generation for stronger authentication and with attack simulation to find and fix flaws [16].

4. Benefits of AI

There are many benefits of incorporating artificial intelligence (AI) to prevent cyberattacks, with User and Entity Behaviour Analytics (UEBA) being a main example of this. By closely examining user and entity behaviours, UEBA uses AI algorithms to quickly spot any threats and anomalies that by pose to an organisation's system whether they originate internally or externally. This is especially useful for spotting internal risks since it enables companies to recognise and deal with insider threats, which can be just as harmful as external cyberattacks. This advanced level of monitoring provides organizations with a proactive defence mechanism, allowing them to swiftly respond to any suspicious activities. AI-driven UEBA systems may identify deviations and highlight possible risks before they materialise by learning and comprehending the regular patterns of user and entity behaviour. This improves an organisations overall cybersecurity posture. Another significant benefit of using AI in its defence against cyberattacks is continuous learning. Traditional security measures can become out-dated in the rapidly evolving threat landscape. On the other side, AI systems continuously adapt and improve their capacity for threat identification. These systems get better at spotting new attacks and weaknesses through machine learning and data analysis. Organisations are better able to protect against sophisticated cyberattacks thanks to their ability to adapt to changing threats (as shown **Figure 4)**.

AI-driven cybersecurity solutions also provide significant cost savings. Organisations can cut back on the need for sizeable cyber teams and expensive manual processes by automating threat detection, response, and incident management. The potential for human error is reduced and operational efficiency is increased due to AI's capacity to work continuously around the clock. As a result, organisations may manage resources more wisely and reduce the financial implications of responding to cybersecurity breaches, which leads to cost savings. According to a recent study, organisations with substantial use of AI and security automation had an average cost

of a data breach of $3.60 million as opposed to $4.04 million for those with minimal use. Organisations who used no AI or security automation had breach costs of $5.36 million [18]. Overall, integrating AI into cybersecurity not only strengthens a company's defence against online threats, but also does it in a way that is affordable and long-lasting (see **Figure 4**).

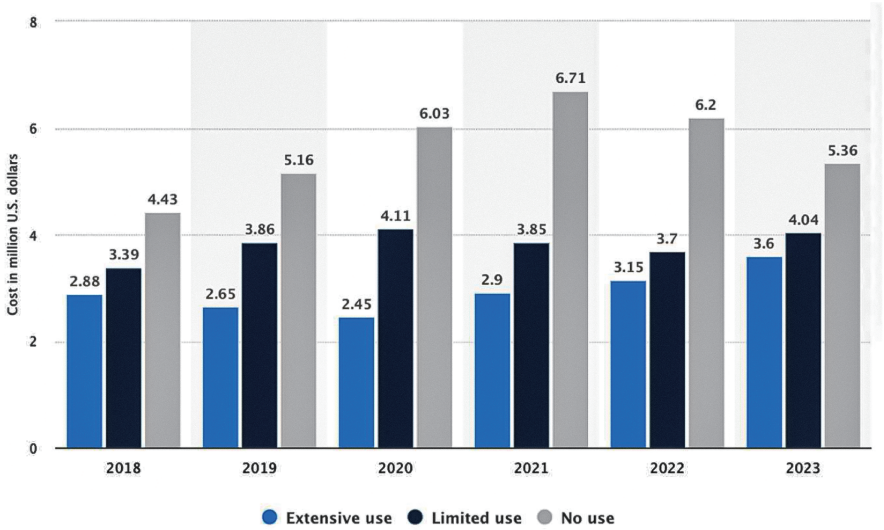

Figure 4. Average cost of a data breach by security automation deployment level [17]

5. Limitations of Artificial Intelligence

Despite its impressive development, AI systems still face technical obstacles that limit certain standards that may be used in the real world. Their failure to mimic human-level knowledge and reasoning is a major flaw. While AI is capable of excelling at certain jobs, it lacks simplistic information that humans developed. This drawback is especially obvious in dynamic, unstructured settings where appropriate awareness is essential. AI also has trouble being creative, adapting to new circumstances, and tackling difficult, abstract problems. Due to these technical limitations, AI now only serves as a tool with specialised functions rather than a complete substitute for human decision-making.

When employing AI, having insufficient data can pose a significant disadvantage. To learn and make intelligent choices, AI systems rely on large and precise datasets. If the data is limited or tainted with errors, the AI's performance and reliability can suffer. This may lead to inaccurate recommendations, poor projections, and inadequate problem-solving. AI implementation is a resource-intensive process since it can sometimes be time-consuming and expensive to gather, clean, and maintain big, high-quality datasets. As a result, the quality and quantity of data are limited, which can prevent AI from reaching its full potential and reduce its usefulness in a variety of contexts.

Of course, as artificial intelligence (AI) systems increasingly become core components of security infrastructures, the security of the AI systems themselves is paramount [19]. These systems, while enhancing capabilities in data analysis, decision-making, and automation, also present potential vulnerabilities that could be

exploited by malicious actors. The complexity of AI algorithms and the sensitivity of the data they process make them attractive targets for cyberattacks, including data breaches, unauthorized access, and manipulation of AI behaviour. Therefore, it is crucial to implement robust security measures to protect these systems [20]. This includes rigorous testing for vulnerabilities, continuous monitoring for unusual activities, and employing advanced encryption methods to safeguard data integrity. Protecting AI systems from misuse and external threats not only preserves their functionality and trustworthiness but also ensures they continue to serve as reliable assets in our broader security frameworks [21].

6. Ethical considerations

As with any new emerging technology there are ethical concerns that need to be addressed. One of the largest concerns is the potential for privacy and confidential information violations. As Generative AI models can collect and are trained on large data sets that includes personal information, organisations need to be transparent about the data they collect for their models, where they obtain it from, what it contains and what it is being used for.

FakeGPT and WormGPT are malicious tools used by bad actors and sold on the Dark Web. As the names suggest these tools are like ChatGPT, it can generate text, emails, code etc. The main difference between these tools and ChatGPT is that these tools are specifically trained on malicious content and data like malware code, phishing emails and other attack vectors that are commonly used by bad actors and whereas ChatGPT does has safeguards and guardrails that prevents this kind of use, Fraud and WormGPT do not. Bad actors often use these tools to create advanced and intricate phishing emails and messages, it will suggest where to include malicious links in this content and can even go as far as creating scam pages encouraging victims to provide personal or financial information. The mention of generative AI and generative AI tools has skyrocketed since the release of ChatGPT (see **Figure 5**).

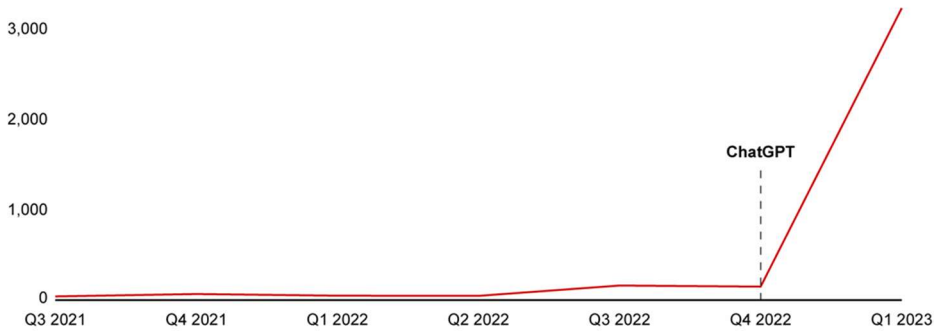

Figure 5. Number of Dark Web mentions of Generative AI [22].

Malicious Generative AI can be used to create and tweak malicious code so that it can bypass detections on organisations security systems, it can also be used to create deepfake videos, imitate voices and fake images that are eerily precise to make phishing attempts more accurate. Algorithmic bias also stands out as another significant issue. To address this problem organisations must ensure that the data used to train their models is both diverse and representational of the broader population to

avoid discrimination within their models. As generative AI continues to advance and gain widespread adoption the cybersecurity industry there is a growing concern that it will create job displacement. organisations, that are leveraging generative AI's capabilities will be able to automate many of the tasks traditionally performed by human employees.

Another concern is overreliance on AI for security, no technology is bullet proof. Over reliance on Generative AI in cybersecurity can lead to complacency, creating vulnerabilities, lax security policies and governance due to neglecting human expertise in favour of automation. It is paramount that organisations address these concerns, this can be done by developing and enforcing internal ethical guidelines for the use of Generative AI, including transparent, responsible development and deployment of AI, monitoring of AI systems and training on ethical AI use.

As regulatory frameworks like the AI Act are being drafted and refined, it is imperative for organizations to proactively address these impending regulations [23]. The AI Act aims to establish clear guidelines for AI development and deployment, focusing on safety, transparency, and accountability. Organizations must start by understanding these regulatory requirements and assessing their current AI systems and processes against them [24]. Early engagement with these regulations can offer a strategic advantage, enabling organizations to adapt their AI initiatives in alignment with legal standards, thus avoiding potential penalties and disruptions. Additionally, this proactive approach can enhance trust with stakeholders and customers by demonstrating a commitment to ethical AI practices. By integrating compliance into the fabric of their AI strategies, organizations can ensure smoother transitions when these regulations come into full effect, securing a competitive edge in a rapidly evolving technological landscape [25].

7. Future developments

Future developments of artificial intelligence in cybersecurity holds the potential to completely change our approach with digital defence with its ongoing advancement reaching new milestones daily. Organisations will be able to defend against evolving threats in real-time while also anticipating and avoiding upcoming assaults due to AI's improved threat detection capabilities, predictive analysis, and adaptive security. Cybersecurity measures will be streamlined, speeding up reaction times and boosting overall security through automated incident response and improved user authentication systems. Additionally, threat intelligence will be able to analyse security data more quickly thanks to the inclusion of natural language processing (NLP). According to IBM, NLP combines statistical, machine learning, and deep learning models with computational linguistics—rule-based modelling of human language. With the use of these technologies, computers are now able to process human language in the form of text or audio data and fully "understand" what is being said or written, including the speaker's or writer's intentions and sentiment. As the realm of Generative Artificial Intelligence (Generative AI) continues to evolve, it is poised to play an increasingly pivotal role in the field of cybersecurity. Future developments are expected to be both ground-breaking and transformative, reshaping

the way we perceive and address digital threats. Several key trends and possibilities merit exploration, which will be explored below.

7.1. Quantum computing and encryption

One of the most anticipated advancements is the intersection of Generative AI with quantum computing. Quantum computing promises unparalleled computational power, enabling it to swiftly decipher encryption methods that are currently considered unbreakable. Generative AI could be harnessed to develop post-quantum encryption solutions, ensuring that data remains secure in a quantum-computing-powered world.

Quantum-resistant cryptography, or post-quantum encryption, is becoming a pressing concern as quantum computers inch closer to practicality. Generative AI's capacity for pattern recognition and creativity can potentially contribute to the development of encryption methods that can withstand the computational capabilities of quantum computers [26]. Moreover, the synergy of Generative AI and quantum computing may also enable the creation of highly secure quantum communication systems. Quantum key distribution, for example, can benefit from Generative AI's ability to enhance the generation and distribution of encryption keys, ensuring the highest levels of security in communication [27].

7.2. Autonomous threat response

The future holds the promise of autonomous threat response systems powered by Generative AI. These systems will have the capability to identify, mitigate, and respond to cyber threats in real-time without human intervention. By continuously learning from evolving threat landscapes, they will adapt and counteract novel attack techniques swiftly. One critical aspect of this development is the integration of machine learning models that not only detect threats but also autonomously respond to them. Generative AI, with its ability to simulate and predict various threat scenarios, can contribute to more effective autonomous threat response. For example, it can generate countermeasures and patches to mitigate vulnerabilities in real-time, minimizing the impact of cyberattacks and reducing the burden on cybersecurity professionals. As autonomous threat response systems mature, they will necessitate increasingly sophisticated Generative AI algorithms that can adapt to the rapidly changing tactics of cybercriminals. The future of cybersecurity will rely on these autonomous systems to provide a proactive line of defence against cyber threats [28].

7.3. Evolution of malware and attack techniques

As Generative AI fortifies cybersecurity, cybercriminals are likely to respond by leveraging AI for their malevolent purposes. The emergence of AI-driven malware and more sophisticated attack techniques is an anticipated trend. These AI-enhanced threats will be capable of evading traditional security measures and adapting to defensive mechanisms. The future of cybersecurity is likely to be characterized by an arms race between Generative AI in cybersecurity and AI-driven cyberattacks. Cybercriminals will exploit AI's capabilities to craft highly adaptive and stealthy malware. These AI-driven threats will exhibit the ability to mimic legitimate user behaviour, making them exceptionally challenging to detect. Generative AI will need

to evolve rapidly to identify and respond to such sophisticated threats. Furthermore, the development of AI-driven attack techniques will call for advanced AI-based intrusion detection and prevention systems. These systems, underpinned by Generative AI, will be designed to anticipate, and counteract evolving attack strategies. The cooperation of AI and human cybersecurity experts will become pivotal in this dynamic cybersecurity landscape [29].

7.4. Augmented human intelligence

Generative AI has the potential to augment human intelligence in cybersecurity. By automating routine tasks and assisting with decision-making, it can free up cybersecurity professionals to focus on more complex and strategic aspects of their work. As AI-driven tools become more sophisticated, they will serve as invaluable partners to human experts, enhancing the overall effectiveness of cybersecurity efforts.

Generative AI can help bridge the skills gap in the cybersecurity workforce by automating repetitive tasks such as threat detection, incident response, and routine security maintenance. This augmentation of human capabilities can lead to faster response times and more effective security strategies. Moreover, Generative AI will empower security analysts with predictive analytics, enabling them to foresee potential threats and vulnerabilities. It will provide actionable insights based on historical and real-time data, thereby enabling more informed decision-making in the face of evolving threats. The synergy between human expertise and AI-driven tools will be critical in maintaining robust cybersecurity postures [30].

8. Conclusion

Significant progress occurs daily in the field of artificial intelligence. The use of artificial intelligence in the field of cyber security results in creative methods to combat and reduce cybercrime. Cybersecurity experts can create complex tools, new algorithms, and services using intelligent systems to tackle both old and new cyber-security issues. In contrast to traditional cyber security methods, the use of artificial intelligence in cyber security has produced cyber solutions that are reliable, versatile, and adaptable. Deep learning has strengthened cyber security measures by allowing for the early prediction of potential cyber-events. In this new stage of cyber security, assaults may now be expected and, as a result, most effectively stopped rather than just prevented. With the number of perks that comes with AI within cyber security there are some dangers that can come alongside this. Intelligent systems are being abused by cybercriminals to get access to networks and information systems. Attackers can now use sophisticated tools and algorithms made possible by artificial intelligence to exploit security flaws and circumvent defences. In the ever-expanding digital era, the role of Generative AI in cybersecurity is undeniably transformative. This technology, born from advanced machine learning techniques, empowers organizations to proactively combat cyber threats. By simulating realistic attack scenarios, automating threat detection, and autonomously generating security patches, Generative AI enhances our capacity to defend against an evolving and relentless cyber threat landscape. While the benefits are substantial, ethical concerns and the potential for AI-driven cyberattacks loom as significant challenges. Looking forward,

the fusion of Generative AI with quantum computing promises to secure our data against even the most advanced adversaries. Autonomous threat response systems driven by Generative AI will usher in a new era of proactive cybersecurity, countering evolving attack techniques. Furthermore, the augmentation of human intelligence with Generative AI will streamline cybersecurity efforts, enabling faster response times and more informed decision-making.

To conclude, AI in cyber security can be used to strengthen the defence tactics of organisations against cyber-attacks greatly. There will never be complete security as loopholes in a system will be discovered. Artificial intelligence is capable of effectively resolving any cyber challenges, even while using sophisticated cyber security measures. Therefore, to gain the most effective outcome cyber security experts should employ traditional cyber security techniques while combing with artificial intelligence. With merging these together will make the probability of attackers to succeeds less likely.

Author contributions: Conceptualization, KC; methodology, KC, EC, JK and CD; validation, KC, EC, JK and CD; investigation, EC, JK, CD; resources, KC, EC, JK and CD; data curation, EC, JK and CD; writing—original draft preparation, EC, JK and CD; writing—review and editing, KC, EC, JK, CD; supervision, KC. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

1. Fowler K, Urbanowicz K, Burns M, et al. Cybersecurity threats and incidents differ by region, Deloitte Insights. Available at: https://www2.deloitte.com/us/en/insights/topics/cyber-risk/global-cybersecurity-threat-trends.html (accessed on 3 August 2024).
2. Stouffer K, Pease M, Tang C, et al. Guide to Operational Technology (OT) Security. National Institute of Standards and Technology (U.S.); 2023. doi: 10.6028/nist.sp.800-82r3
3. Office of Budget Responsibility. The fiscal risks posed by cyberattacks. Available online: https://obr.uk/box/the-fiscal-risks-posed-by-cyberattacks/ (accessed on 3 August 2024).
4. Brandl R, Ellis C. ChatGPT Statistics 2024—All the latest statistics about OpenAI's chatbot. Available online: https://www.tooltester.com/en/blog/chatgpt-statistics/ (accessed on 3 August 2024).
5. Petrosyan AP. Number of ransomware attempts per year 2022, Statista. Available online: https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/ (accessed on 3 August 2024).
6. Sun N, Ding M, Jiang J, et al. Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. IEEE Communications Surveys & Tutorials. 2023; 25(3): 1748-1774. doi: 10.1109/comst.2023.3273282
7. Saeed S, Suayyid SA, Al-Ghamdi MS, et al. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors. 2023; 23(16): 7273. doi: 10.3390/s23167273
8. Rasel M, Salam MA, & Shovon RB. Synergizing Cyber Threat Intelligence Sharing and Risk Assessment for Enhanced Government Cybersecurity: A Holistic Approach. Journal Environmental Sciences and Technology. 2024; 3(1), 649-673.
9. Hasan MK, Weichen Z, Safie N, et al. A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. IEEE Access. 2024; 12: 61642-61666. doi: 10.1109/access.2024.3393567
10. Otta SP, Panda S, Gupta M, & Hota C. A systematic survey of multi-factor authentication for cloud infrastructure. Future Internet. 2023; 15(4): 146.

11. Frehn J. AI-powered identity authentication is here: What you need to know, Portnox. Available online: https://www.portnox.com/blog/network-security/ai-powered-identity-authentication/ (accessed on 3 August 2024).
12. Cheshkov A, Zadorozhny P, & Levichev R. Evaluation of ChatGPT model for vulnerability detection. Available online: https://arxiv.org/abs/2304.07232 (accessed on 3 August 2024).
13. Steenhoek B, Rahman MM, Jiles R, & Le W. An empirical study of deep learning models for vulnerability detection. In: 2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE). IEEE; 2023. pp. 2237-2248.
14. Curran K, Doherty J, McCann A. Turkington G. Good Practice for Strong Passwords, EDP Audit, Control and Security (EDPACS). Taylor & Francis. 2011; 44(5): 1-13. doi: 10.1080/07366981.2011.635497,
15. Curran K, Snodgrass A. A Novel Cue based Picture Word Shape Character Password Creation Scheme. International Journal of Digital Crime and Forensics. 2015; 7(3): 37-59. doi: 10.4018/ijdcf.2015070103
16. Umejiaku AP, Dhakal P, Sheng VS. Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation. Electronics. 2023; 12(10): 2159. doi: 10.3390/electronics12102159
17. DeBeck C. More organizations saving time and costs on data breaches with automation and ai, Security Intelligence. Available online: https://securityintelligence.com/posts/save-time-money-data-breach-security-ai-automation/ (accessed on 3 August 2024).
18. Gregory J. AI reduces data breach lifecycles and costs, Security Intelligence. Available online: https://securityintelligence.com/articles/ai-reduces-data-breach-lifecycles-and-costs/ (accessed on 3 August 2024).
19. Bertino E, Kantarcioglu M, Akcora CG, et al. AI for Security and Security for AI. In: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy. Association for Computing Machinery, New York, USA. 2021; 333-334.
20. Habbal A, Khalif Ali M, Ali Abuzaraid M. Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. Expert Systems with Applications. 2024; 240. doi: 10.1016/j.eswa.2023.122442.
21. Bharadiya JP. AI-driven security: how machine learning will shape the future of cybersecurity and web 3.0. American Journal of Neural Networks and Applications. 2023; 9(1): 1-7.
22. EU. EU AI Act: first regulation on artificial intelligence. Available online: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (accessed on 3 August 2024).
23. Bain. Generative AI and Cybersecurity: Strengthening Both Defenses and Threats. Available online: https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023/ (accessed on 3 August 2024).
24. Chamberlain J. 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. 2022; 14(1): 1-13. doi: 10.1017/err.2022.38
25. Rakha NA. The impacts of Artificial Intelligence (AI) on business and its regulatory challenges. International Journal of Law and Policy. 2023; 1(1).
26. Raheman F. The Future of Cybersecurity in the Age of Quantum Computers. Future Internet. 2022; 14(11): 335. doi: 10.3390/fi14110335
27. Luo H, Zhang L, Qin H, et al. Beyond universal attack detection for continuous-variable quantum key distribution via deep learning. Physical Review A. 2022; 105(4). doi: 10.1103/physreva.105.042411
28. Wang X. Ai-Enhanced Software Vulnerability and Security Patch Analysis (PhD thesis). George Mason University; 2023.
29. Hossain Faruk MJ, Shahriar H, Valero M, et al. Malware detection and prevention using Artificial Intelligence Techniques. 2021 IEEE International Conference on Big Data (Big Data). 2021. doi: 10.1109/bigdata52589.2021.9671434.
30. Wirkuttis N, and Klein H. Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security. 2017; 1(1): 103-119.