Global Trends in Science and Technology

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

AI-Cybersecurity Nexus: Rethinking Digital Defense in the Age of Intelligent Threats

Fnu Mohsin[1*]

[1]Washington University of science and technology

[1]mohsinashiq447@gmail.com

open access

Corresponding Author
Fnu Mohsin
mohsinashiq447@gmail.com

Article History:
Submitted: 05-10-2026
Accepted: 19-11-2026
Published: 22-11-2026

Key words
Artificial Intelligence, Cybersecurity, Threat Detection, Adversarial AI, Generative AI, Cyber Defense, Malware Analysis.

Global Trends in Science and Technology is licensed under a Creative Commons Attribution-Noncommercial 4.0 International (CC BY-NC 4.0).

ABSTRACT

Artificial Intelligence (AI) is revolutionizing cybersecurity with its ability to provide smart, adaptive, and automated methods of detecting threats, analyzing malware, managing vulnerabilities, and responding to incidents. The convergence of AI and cybersecurity is explored to understand its potential for defensive use and the new threat landscape it creates. AI can enhance real-time threat detection, predictive analysis, automated response and cyber-resilience. But AI can also be used by an adversary for phishing and creation of malware, social engineering, deep fakes, and attacks against AI systems. Challenges such as data quality, privacy, explain ability, false positives, and model manipulation are also mentioned in the review. Future directions towards autonomous, adaptive, trustworthy, and human-centric cyber defense are investigated.

INTRODUCTION

Digital technologies have rapidly evolved and are significantly reshaping modern society by allowing organizations, governments and individuals to increasingly rely on interconnected digital systems for communication, commerce, health, education, financial services and critical infrastructure. This dependency on the digital worlds has also created a much wider field of cybersecurity threats, however [1]. Traditional cyber security solutions that are mainly based on a set of rules, signs and manually programmed security policies are increasingly ineffective against sophisticated cyber threats that are constantly changing, advanced and automated. Artificial Intelligence (AI) is a revolutionary technology that can significantly change the dynamics of detecting, analyzing, preventing, and managing cyber threats [2].

The fusion of AI and cybersecurity is an emerging field of research in which AI-powered algorithms

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

are used to detect anomalous activity, spy attacks, anticipate attacks, automate security procedures, and inform real-time choices. AI models like machine learning, deep learning, and natural language processing can analyze vast amounts of security data and uncover intricate patterns not captured by traditional security methods [3]. As a result, AI-powered cybersecurity solutions are becoming indispensable in the face of today's cyber threats, which are massive, swift, and intricate.

Meanwhile, there is no one-sided dynamism between AI and cybersecurity. Advanced technologies that enhance the state of cyber defense can be used for more advanced attacks by bad guys. The use of AI by cybercriminals can enable phishing attack automation, create convincing social-engineering content, find vulnerabilities, and be able to bypass security measures and create adaptive malware [4]. With the advent of generative AI and large language models, these concerns have been exacerbated, as technical hurdles have been reduced for some types of cyber-enabled abuse. This makes AI a part of the complicated security landscape where it can both be a defense mechanism and a potential amplifier of threats [5].

As such, there is a need to rethink traditional digital security approaches in light of the intersection of AI and cybersecurity. Security systems need to be adaptable, predictive, context-aware, and able to react to the constantly evolving threat landscape. Furthermore, considerations like the explain ability, privacy, adversarial machine learning, data quality, ethical responsibility, human oversight, or regulatory governance need to be taken into account when deploying AI in security-critical environments [6].

This review paper aims to explore how AI and cybersecurity have gone hand in hand over time and shed light on the opportunities and risks posed by intelligent technologies. It examines how AI is being used for cyber defense, the rise of AI-powered threats and adversarial attacks on AI, issues with AI-powered defense solutions, and the future of intelligent cyber defense. This review seeks to present a holistic view of the impact of AI on cybersecurity and the need for a balanced use of intelligent digital defense.

AI'S ROLE IN DECODING CUSTOMER RELATIONSHIPS IN THE TECH INDUSTRY

The intersection of Artificial Intelligence (AI) and cybersecurity has become a major player in the advancement of digital security. Cyber threats are growing more in numbers and diversity, as well as more sophisticated, and there is a growing need for security mechanisms capable of working outside the constraints of rule-based and signature-based systems [7]. Most traditional cybersecurity solutions are based on a set of pre-designed patterns or indicators of compromise, and are extremely effective against known threats; however, they are less effective against new polymorphic or rapidly evolving attacks. AI's intelligent and adaptive features help cybersecurity systems process vast amounts of data,

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

identify emerging patterns, and speed up their reactions to threats [8].

One of the most significant technologies that link the fields of AI and cybersecurity is machine learning (ML). Security historical data can be used to train ML algorithms to identify legitimate and malicious activities. For instance, behavioral models can be used to look at network traffic, user activity, system logs, and endpoint events to detect anomalies [9]. Unlike traditional systems that have to have specific rules for all different threats or classes of threats in order to detect them, a machine learning model can learn the relations from the data and become better at detecting the threat as the data increase. Deep learning takes these features one step further by being able to process high dimensional and unstructured data, which is useful in many applications like malware classification, intrusion detection, fraud detection and behavioral analysis [10].

One of the other key elements in this convergence is the automation of cybersecurity operations. Organizations today are inundated with a vast amount of security alerts, many of which are time-consuming to investigate and require special skill sets. AI can help security analysts correlate events, prioritize alerts, pinpoint potential attack paths, and suggest the right responses. This can help security teams to ease their burden and speed up incident detection and response [11]. Another way AI can help in predictive security is by aggregating historical and real-time data to spot potential vulnerabilities and to forecast new risks before they become significant events.

But there is a dual-use issue with the combination of AI and cybersecurity. While AI technologies can bolster defense, they also have the potential to be weaponized by an adversary. AI can be used by attackers to automate their reconnaissance efforts, create convincing phishing messages, find vulnerabilities, manipulate information, or bypass detection mechanisms. In addition, AI-powered security systems could also be the subject of adversarial attacks aimed at skewing their inputs or influencing the decisions they make [12].

As such, AI and cybersecurity should not be thought of as two distinct fields of technology. This convergence is a security ecosystem that is constantly in a state of evolution, where intelligent systems, human knowledge, data and automated processes are all in conversation [13]. This means that implementing AI models successfully involves more than just accurate technical implementations, but also the trustworthiness of the data sources, the explain ability of the models, the protection of privacy, the security architecture, human control, and suitable governance structures. The knowledge of this convergence is crucial toward the creation of cybersecurity strategies that are capable of mitigating existing and future generations of intelligent cyber threats [14].

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Global Trends in Science and Technology
ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

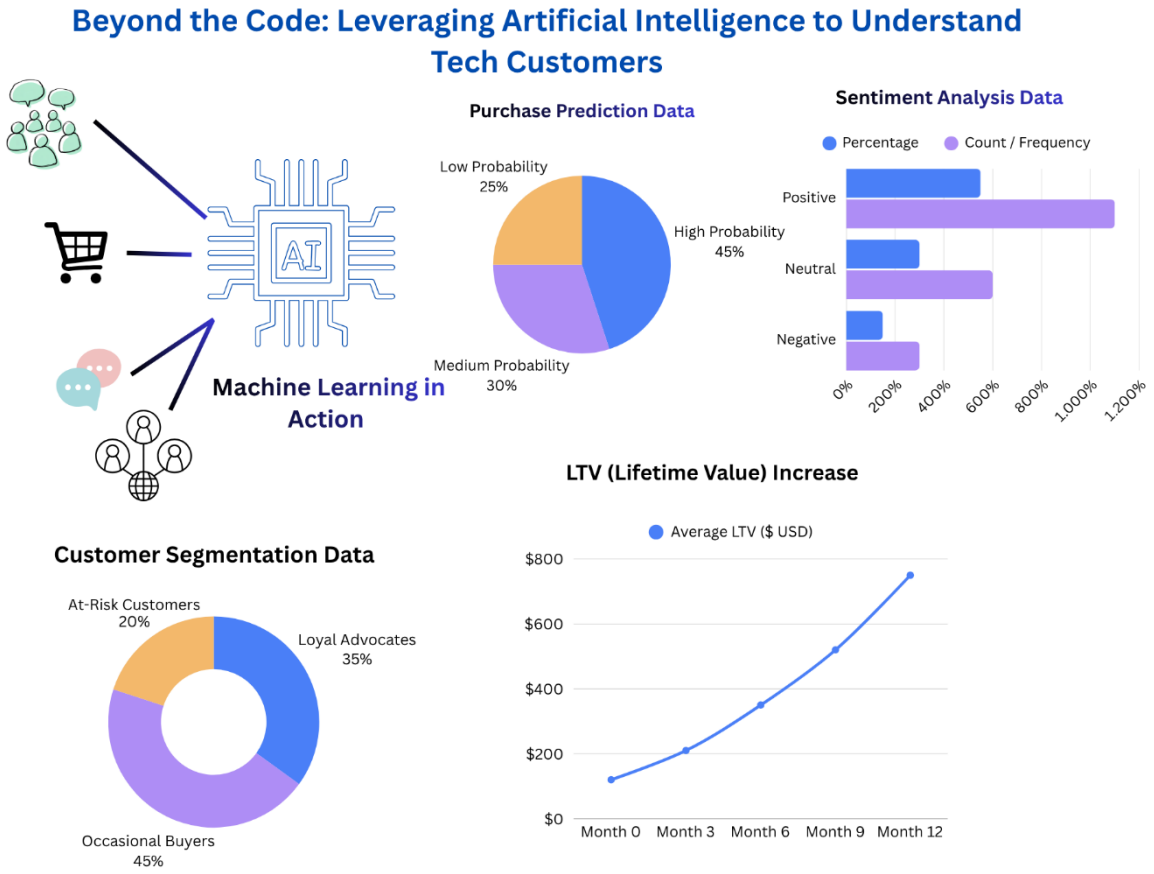


Figure 1. AI-Driven Customer Lifecycle: Decoding Relationships in the Tech Industry

ARTIFICIAL INTELLIGENCE FOR CYBER DEFENSE

The rise of AI has made it a critical piece of the modern cyber defense puzzle, as it is able to process enormous amounts of data, detect elaborate patterns, and aid in quick security decisions. Cyberattacks are becoming more sophisticated and conventional security mechanisms are not able to spot all malicious activities in real time [15]. Most of the conventional security measures rely on known attack patterns, such as signature-based antivirus, static firewall rules, and intrusion detection rules installed by hand. In contrast to traditional cyber defense methods, AI-based cyber defense offers a more adaptive approach. It allows security systems to learn from past and real-time data, and recognize potentially malicious activity [16].

Among the many applications of AI in cyber defense, one of the most popular is machine learning (ML). The supervised learning algorithms can be trained with labeled data that includes examples of legitimate and malicious activities. These models can then identify new network connections, files, e-mail or activities as safe or dangerous [17]. When labeled data for attacks is scarce, unsupervised and semi-supervised learning techniques are especially beneficial. They are able to detect strange behavior and find previously unknown patterns without having to be told up front what they are. This

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

ability is especially relevant for identifying zero-day attacks and other new dangers, as the instances of these attacks become more and more frequent [18]. As zero-day attacks and other new dangers increase in frequency, this capability is particularly relevant for detecting them.

The use of AI in cybersecurity has been further enhanced by deep learning. Neural networks can process huge and intricate data sets derived from network traffic, endpoint devices, system logs, and security events. Deep learning models can be used for malware detection, intrusion detection, identification of botnets and phishing classification and behavior analysis [19]. These systems can learn complex representations from data, which could enable them to detect subtle signals of compromise that might not be detected by traditional methods.

AI is also playing a pivotal role in the realm of security automation and incident response. Security Operations Centers (SOCs) continuously receive large numbers of alerts from different security technologies. When performing manual analysis, all alerts can cause delays and alert fatigue for cybersecurity professionals [20]. AI can search through many different data sources for information, rank alerts by threat, find connections between unrelated events, and aid in automated response actions. This allows companies to streamline response time and deploy human intelligence in more sophisticated security situations [21].

One of the other key applications is threat intelligence and predictive cybersecurity. Security reports, network activities, vulnerabilities, and past incidents can be used to feed information into AI systems that can detect trends in attacks. Predictive models can be used to help organizations determine levels of risk and prioritize vulnerabilities that need to be addressed right away [22]. Natural language processing can also be leveraged to gain relevant security information from massive amounts of unstructured text, such as threat reports and online security conversations.

While AI-powered cyber defense offers numerous benefits, it's not a magic bullet. The power of the AI model is closely tied to the volume, variety and representation of training data. If the data or information are of poor quality or biased, the predictions may be incorrect, and if input data is manipulated intentionally, it can lead to AI systems missing the mark [23]. So, AI is meant to complement and not supplant human expertise in cybersecurity. Leveraging intelligent automation and human oversight, security measures, ongoing model testing, and explainable artificial intelligence can create a more secure basis for contemporary cyber protection [24].

AI-POWERED CYBER THREATS & NEW ATTACK VECTORS

As a result of the swift advancements in Artificial Intelligence (AI), there are numerous opportunities and challenges in the field of cybersecurity, including the potential for more sophisticated, scalable and adaptive attacks from adversaries. Historically, the cybercriminals were heavily dependent on the

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

manually crafted tool and known attack methods. But as the technologies for AI grow, malicious actors can now automate several parts of the attack lifecycle: reconnaissance, social engineering, identifying vulnerabilities, creating content, and optimising attack [25]. The threat landscape is shifting away from traditional attacks to more intelligent and increasingly automated attacks.

The phishing and social engineering attacks are the most visible threats with AI-powered tools. With fewer grammatical and contextual mistakes than many traditional phishing campaigns, AI systems can craft very successful emails, messages and other communications [26]. By leveraging AI techniques, attackers can tailor their messages to individual victims or organizations based on the gathered data. This causes there to be a problem for users and traditional filtering tools to differentiate between beneficial and harmful communications [27]. The addition of generative AI has added to the worry in this regard as it can generate a huge volume of customized content, quickly.

AI can be used to create and evolve malware, as well. Intelligent systems can be used to change malicious code, gain knowledge of vulnerabilities in defensive systems, or fine-tune attack characteristics. With AI techniques and abilities, and polymorphic and metamorphic malware capabilities already in existence, the creation of adaptive malicious software can become more common [28]. These threats highlight the shortcomings of security solutions that rely mainly on static indicators and attack signatures that have been previously seen.

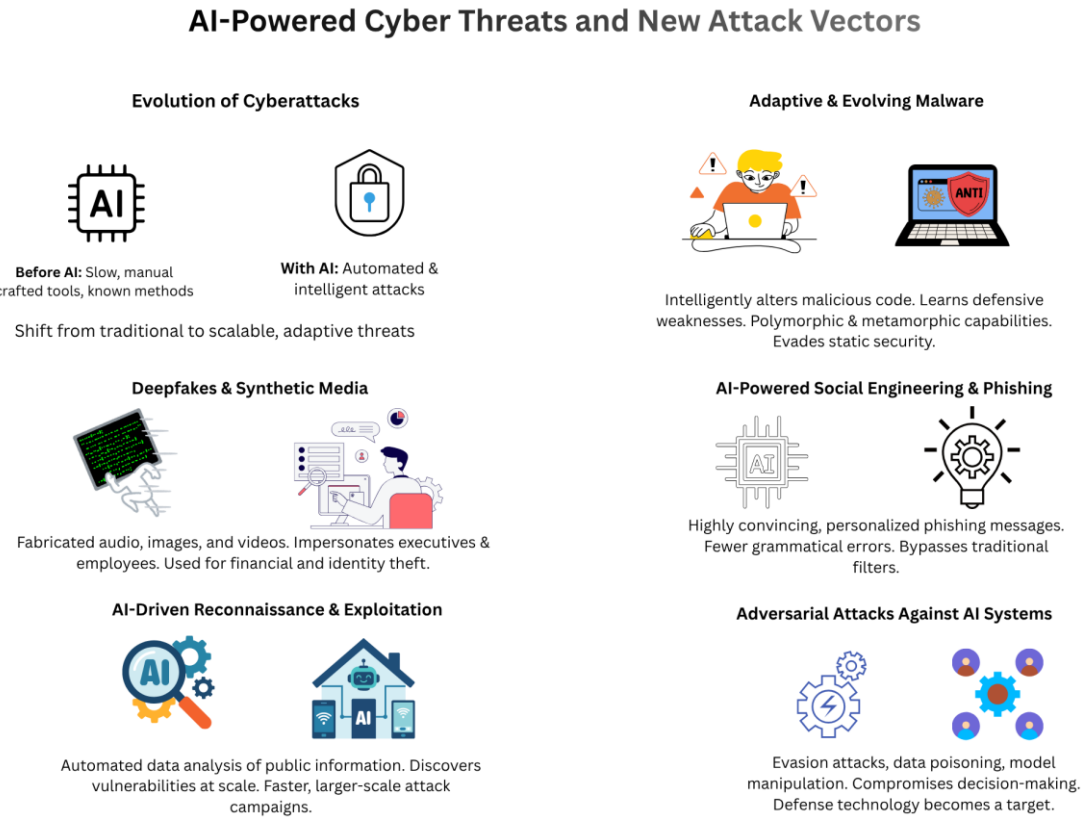


Figure 2. AI-Powered Cyber Threats and New Attack Vectors

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

AI-powered intelligence-gathering and exploitation of vulnerabilities are also an emerging concern. With the help of smart tools, cyber attackers may be able to analyze publicly available data, discover unprotected systems, map digital infrastructure and determine which systems may be susceptible [29]. Reconnaissance over large scale environments can be highly automated to avoid a lot of time. This, coupled with automated exploitation tools, can help attackers to run campaigns faster and at a larger scale. One other significant route of attack is adversarial attacks against AI systems. Rather than targeting traditional infrastructure, hackers can alter the input for the AI models and/or the data itself to impact decision making. These include: evasion attacks, data poisoning, model manipulation, and adversarial examples [30]. If effective, such attacks could result in important indicators of compromise being lost or mistaken for legitimate activity by a security system. This makes for an especially difficult situation as the defense's technology becomes a target in itself.

The use of deepfakes and Artificial Intelligence-generated synthetic media also poses major cyber security and social engineering challenges. Audio, images, and videos can be fabricated to simulate people, employees, and other information or to commit financial or identity theft. With the rising realism of synthetic media, there may be a need for more robust identity verification and authentication solutions [31].

ADVERSARIAL AI: WHEN AI IS THE WEAPON

As AI becomes increasingly embedded in cybersecurity, AI systems can be employed not just for cyber defense, but for cyber-attack and manipulation of intelligent technologies, putting a new dimension on the digital conflict. This is known as adversarial AI and involves ways that attackers try to manipulate data, inputs, models, or learning processes to influence the behavior of AI systems [32]. The protection of AI models is a crucial part of today's cybersecurity landscape as the importance of machine learning and deep learning for organizations grows in importance.

Data poisoning is another critical danger that can occur when an attacker attempts to alter the data used to train an AI model, thereby skewing its results. Machine learning models rely on training data, and if data is compromised or inaccurate, it can impact the accuracy of the model or introduce systematic weaknesses [33]. Incorporating malicious information during training could make a security model less efficient at detecting specific security threats. Secure data collection, validation, storage, and preprocessing are crucial during the AI lifecycle. Evasion is another issue in which attackers change malicious activities to evade AI security systems. While traditional attacks try to circumvent known security rules, attackers can learn to change their behavior to match the behavior of intelligent detection systems [34]. This perpetuates a vicious circle in which defense needs to adjust to attack in a continuous manner.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

Another type of attack on AI models is called model extraction and inference attacks. Model extraction: An attacker try to recreate the functionality of a target model through repeated interactions. Inference attacks, however, can try to get information about the data used to train a model that is sensitive. The risks these pose to intellectual property, privacy, and confidentiality are of great concern, especially if AI systems are handling sensitive organizational or personal data [35]. The advent of generative AI has extended the Adversarial AI space even more. Prompt injection, malicious input and other types of model abuse are ways in which generative models can be manipulated. As a result, organizations need to safeguard the infrastructure, as well as the models, datasets, interfaces, and decision-making processes used by AI systems [36].

There is a multi-layered approach to security needed to combat adversarial AI. Adversarial training, strong model architectures, data validation, continuous monitoring, anomaly detection, access control, model auditing, and explainable AI are some of these techniques that can help enhance system resilience. In addition, human input is crucial for high-stakes security decisions, as AI predictions can be wrong or might have some unexpected bias [37]. Adversarial AI illustrates that in the intelligent era, cybersecurity is a protection battle for digital infrastructure as well as the intelligence being used to protect it. The ability to build trusted, strong, transparent, and resilient AI systems will be key to continue successful digital defense against more sophisticated adversaries as that technology becomes ubiquitous [38].

GENERATIVE AI AND THE CHANGING CYBERSECURITY LANDSCAPE

In the modern digital landscape, Generative Artificial Intelligence (GenAI) has become one of the most pervasive advancements, reshaping the landscape of cybersecurity and the types of threats faced. Generative Artificial Intelligence (GenAI) has become one of the most significant developments in the modern digital environment, transforming the way cybersecurity is practiced and the nature of cyber threats [39]. Whereas traditional AI systems typically classify, predict, or detect patterns, generative AI can produce new content, such as text, images, sounds or even software codes and other digital information. Large language models (LLMs) and other generative technologies have made their way into the world, presenting new challenges and opportunities for cybersecurity professionals [40].

On the defensive side, generative AI can be used to tackle massive amounts of security data, to summarize threat intelligence reports, to aid in the investigation of incidents, to create security documentation, and to provide context to complex technical events. Security Operations Centres can benefit from LLM systems to decipher security alerts and integrate data from many sources. Generative AI can also help enhance security education by generating scenarios for simulated

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Global Trends in Science and Technology
ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

phishing exercises and realistic training situations, thereby creating more awareness and

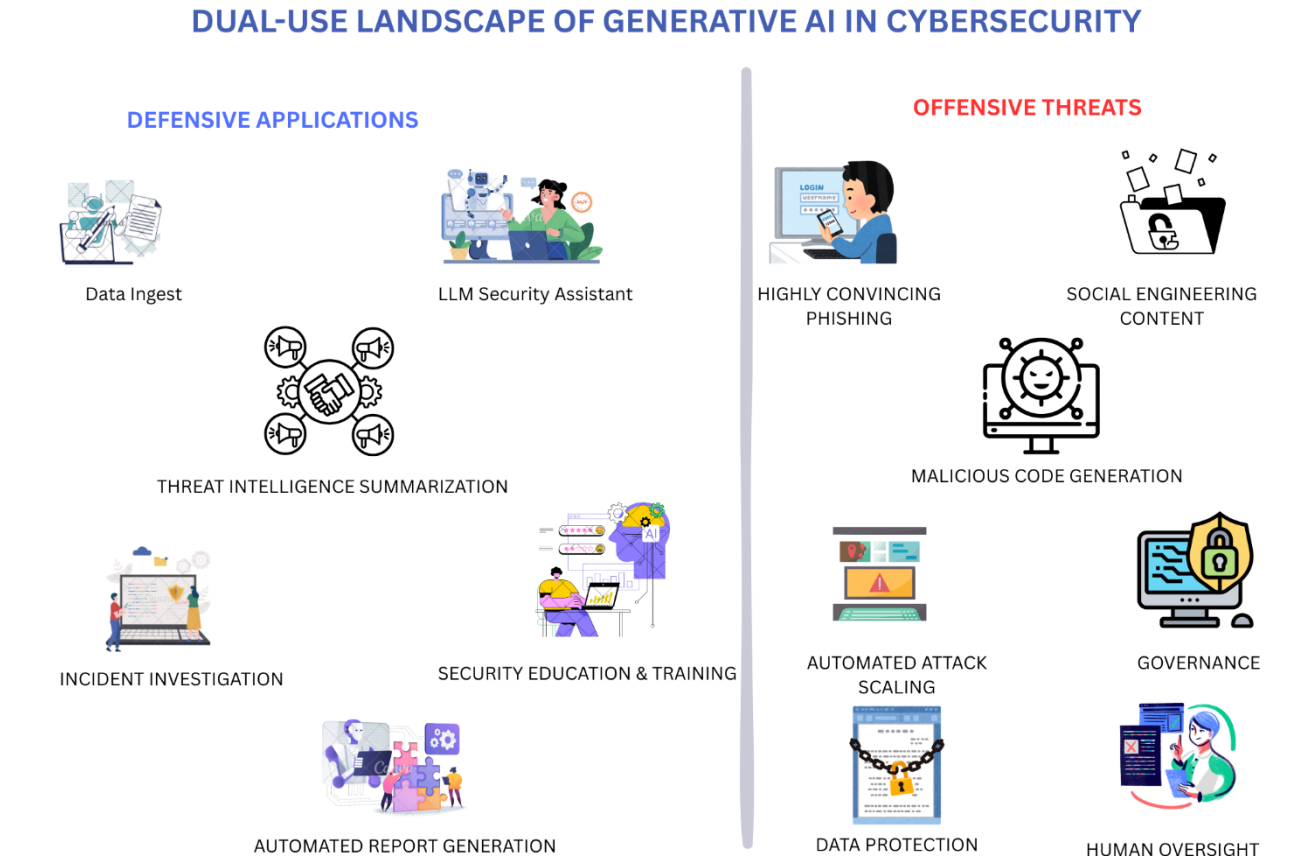


Figure 3. Navigating the Dual-Use Reality of Generative Artificial Intelligence in Modern Cybersecurity

But these features can be used by bad guys too. The ability to create very convincing phishing and social engineering content is a serious worry. Fraudulent messages can be quickly personalized for specific recipients and recipients' groups, which can enhance fraud campaign performance and reach. AI can also help attackers to write malicious code, gather information, send phishing messages, and even automate parts of an attack [42]. Therefore the difference between sophisticated human-operated attacks and automated attacks could become more and more ambiguous.

The cybersecurity aspects of generative AI are, therefore, dual-use. When deploying such technologies, organizations must put in place the proper governance, access control, data protection, model monitoring and human oversight. In conclusion, generative AI is revolutionizing cybersecurity, empowering both defenders and attackers, and responsible use, ongoing assessment, and proactive security practices that consider AI are crucial for digital resilience [43].

DATA ENCRYPTION BASICS: UNDERSTANDING AND IMPLEMENTATION

Artificial Intelligence (AI) has revolutionized threat detection and incident response by helping to analyze vast amounts of data, detect suspicious patterns, and assist in quick decision-making.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

Traditional cybersecurity environments tend to rely on predefined rules, signatures, and manual investigation for threat detection [44]. While these methods can be helpful in detecting known threats, they may not be effective in detecting more advanced attacks that evolve and adapt over time. AI-powered solutions offer a more adaptive solution, leveraging machine learning, deep learning, behavioral analytics, and automated reasoning to detect potential threats in real time [45].

Anomaly detection is one of the most crucial uses of AI. Machine learning models can determine the baseline of normal network, system and user activity, and then detect highly atypical activities. For instance, if users are logging into the system from locations other than what is expected, if there are data transfers occurring that are unusual, if network traffic is changing in ways that are not typical, or if there are unusual access patterns, these are all possible indicators of compromise [46]. This behavioral approach can be used to identify new threats that haven't been previously seen and minimize reliance on attack signatures.

Another benefit of AI is that it can enhance the analysis of security alerts from various cybersecurity technologies. Thousands of alerts may be generated for modern organizations from firewalls and intrusion detection systems, endpoint security platforms, cloud environments, and more [47]. Security personnel can find themselves inundated with such alerts, leading to “alert fatigue” when they have to manually analyze them. AI can link together related events, classify the potential impact, eliminate redundant alerts, and prioritize incidents that need to be investigated. This will help security analysts concentrate on the greatest threats [48].

AI can help organizations at various points in the incident response lifecycle. Intelligent systems may be used to determine the source of an attack, analyze compromised systems, and provide a potential path for an attack and recommendations for containment. Automated responses may contain a capability to isolate, block or limit the access of suspect devices or accounts when conditions are met. This type of automation can shorten response times and minimize the effects of cyber events [49].

AI can also play a role in predictive threat intelligence by looking at historical events, vulnerability data, network activity, and new patterns of threats. Predictive models could enable organisations to be better able to recognise systems that are likely to be targets and allocate security resources accordingly. But AI-based detection mechanisms can still make mistakes [50]. Their reliability may be compromised by poor quality training data, model bias, adversarial manipulation, and false positives.

So, for effective AI-driven incident response, you need constant monitoring, model validation, high-quality data, and a human touch. AI should be used alongside — and not in place of — human cybersecurity experts, especially for incidents with complex organizational, legal or ethical

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

implications. In sum, AI-powered threat detection and incident response are a key evolution from reactive cybersecurity to proactive, adaptive, and predictive cyber defense [51].

AI FOR MALWARE ANALYSIS AND VULNERABILITY MANAGEMENT

Artificial Intelligence (AI) has increasingly been a valuable technology for enhancing the process of malware analysis and vulnerability management. The increasing amount and sophistication of malicious software has posed serious problems for traditional security solutions [52]. Traditional methods of detecting malware rely on signatures and predetermined rules, which work well against known malware, but may not be effective against new, updated, or polymorphic variants. Adaptive techniques are those that involve examining behavior, structure, and context of potentially malicious programs in order to provide a more adaptive approach [52].

Features extracted from executable files, system activities, network activities, and application interactions can be used to classify malware using machine learning algorithms. Rather than a single set of previously identified signatures, AI models are able to learn patterns with malicious behavior and classify suspicious files based on their characteristics [53]. The static analysis techniques look at properties like file structure, imported functions and code characteristics, while the dynamic analysis are used to watch how the malware behaves when it is run in a controlled environment. It's possible to enhance identification of unknown/malformed malware when using these methods together [54].

The advent of deep learning has also improved automated malware analysis in its ability to learn complex relationships from massive amounts of data. Patterns can be discovered and learned by a neural network that are characteristic of ransomware, spyware, trojans, botnets and other types of malware. AI can also be used to help security analysts automatically cluster similar malware samples, recognize behavioral similarities, and save time on manual investigation [55]. In particular, when organizations need to filter out a large number of suspicious files and security events, this is crucial.

AI is also playing a crucial role in vulnerability management. Today's organizations have complex infrastructures; operating systems, applications, cloud systems, network devices, and Internet of Things (IoT) systems. It is challenging to identify and prioritize vulnerabilities in such an environment, since not all vulnerabilities pose the same threat [56]. Vulnerability characteristics, asset importance, historical attack information, network exposure, and other factors can be analyzed using AI-based systems to prioritize remediation efforts. Another aspect of vulnerability management where predictive analytics could be helpful is to flag systems that might be more vulnerable to being targeted or exploited. AI can process past vulnerability and attack information to uncover trends that could suggest new threats [57]. Automated code analysis can also help developers spot potentially insecure programming practices while in the software development lifecycle.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Global Trends in Science and Technology
ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

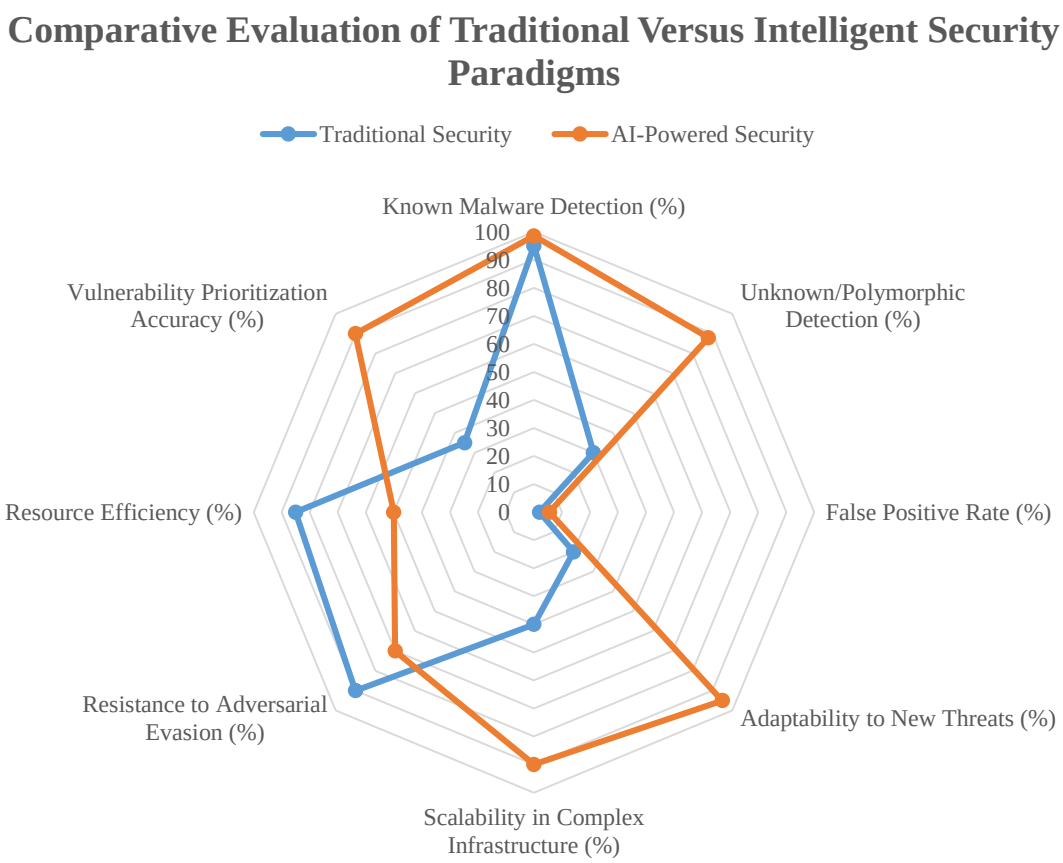


Figure 4. Comparative Evaluation of Traditional Versus Intelligent Security Paradigms

While these advantages exist, there are also some limitations in the AI-powered malware analysis and vulnerability management. AI models are as accurate as the data they are trained on, and as new malware emerges, the models' accuracy decreases [58]. Attackers can also tamper with malicious software intentionally to avoid detection by AI. Thus, ongoing model training, strong validation of models, threat intelligence integration and human knowledge and experience are still indispensable. AI promises to revolutionize malware analysis and vulnerability management from a more reactive to a more proactive, intelligent, and risk-focused approach to security [59]. Applying it effectively can help enhance its detection capabilities, expedite vulnerability prioritization, and enhance the organization's capacity to withstand new cyber threats.

ETHICAL AND LEGAL ISSUES IN AI FOR CYBERSECURITY

While Artificial Intelligence (AI) presents promising possibilities to enhance cybersecurity, there are also a few technical, operational, ethical, and organizational challenges to consider when implementing AI. AI-powered cybersecurity solutions require high-quality data, accurate algorithms, powerful computing resources, and the capacity to evolve with the ever-shifting nature of cyber threats [60]. However, using AI as a standalone solution to cybersecurity challenges should not be viewed as a one-off initiative, but rather as a continuous process that will need to be evaluated and

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

continuously improved.

Data quality and availability is among the significant challenges. For the effective training of machine learning and deep learning models, the data sets must be large and representative. Cybersecurity datasets can be incomplete, out-of-date, imbalanced, or biased, though. There are several examples where organizations are unwilling to provide security information due to privacy, confidentiality and competitive considerations [61]. AI models may not be effective in detecting advanced or new attacks if there is a lack of training data. Moreover, cyber threats are constantly evolving, which may cause models trained on past data to lessen their effectiveness over time when new attack methods are employed [62].

One of the significant constraints is the false positive and false negative results. A false positive is when something that is not a threat is marked as a threat, while a false negative is when something that is a threat is not detected. Too many alerts can cause alert fatigue, and not enough alerts can mean critical systems are compromised by attackers. A good balance of detection accuracy and operational efficiency is still not easily achieved [63].

Another issue of concern is explainability and transparency. Many of the advanced AI models in use, especially those based on deep learning, are black-box algorithms that are not easy to comprehend what decisions they make [64]. An unexplainable decision can be a problem in cybersecurity because analysts might have to determine the reasons behind the activity being considered malicious before they take significant action to defend themselves. The need for trust and accountability, then, is making explainable AI techniques more critical than ever in building trust and accountability [65].

Other challenges are computational costs, the integration of existing security environment, privacy concerns, lack of skilled professionals, and regulatory uncertainty. But, when automated systems make wrong security decisions, it can also be difficult for organizations to figure out who is responsible. The successful deployment of AI in cybersecurity necessitates a multi-layered approach, with high-quality data, powerful algorithms, ongoing monitoring, secure AI creation, human oversight, and suitable governance structures [66]. To guarantee that AI technologies deliver reliable, trustworthy, and sustainable enhancements to contemporary cyber protection, it is crucial to tackle these constraints.

FUTURE DIRECTIONS TOWARDS AUTONOMOUS AND ADAPTIVE CYBER DEFENSE

Cybersecurity is heading toward intelligent, autonomous and adaptive defense mechanisms that can adapt to the ever-changing cyber threats. The attackers are increasingly employing cutting-edge automation, AI, and sophisticated evasion strategies, which could render traditional security measures ineffective in safeguarding intricate digital ecosystems [67]. So, AI and machine learning,

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

automation, threat intelligence, and continuous monitoring are expected to be part of a more resilient and proactive cybersecurity system of the future.

The direction of developing autonomous cyber defense systems is one of them. These systems might continuously monitor networks, endpoints, applications, and user behaviour, detect suspicious activity, evaluate risks, and trigger responses to the suspicious activity with minimal human interaction. With autonomous security, the threat to response time gap may be drastically reduced in case of fast-moving cyber incidents. But, when allowing for autonomous decision making, it should be carefully managed with predefined policies, human oversight and fail-safes to prevent unintended consequences [68].

One way along these lines that appears promising is adaptive cybersecurity. Future AI-based security systems are likely to be learning systems, where they will learn about new attack patterns and security events, rather than being static systems. Organizations may evolve and adaptive models can adapt their ideas of what is normal and abnormal [69]. This functionality could help identify previously unknown, polymorphic malware and zero day attacks. But, continuous learning cannot go without robust protections against data poisoning and adversarial manipulation [70].

AI-powered threat hunting is also likely to gain more significance. Instead of relying on a security alarm, the intelligent systems can proactively look for potential indicators of compromise and suspicious activities in large digital environments. By analyzing data from network traffic, endpoint behavior, identity systems, cloud platforms, and threat intelligence sources, AI can uncover complex attack patterns that might not be detected otherwise [71].

The other important research aspect is that of collaborative and federated intelligence. Collective cyber defense can be enhanced via the sharing of threat knowledge without sharing data that is sensitive. Federated learning and privacy-preserving methods could allow AI models to learn from multiple data sources without compromising the need for centralization of sensitive data [72]. Future cybersecurity research should also focus on trustworthy and explainable AI. Security professionals need to be aware of the rationale behind the decisions taken by an AI system, particularly if automated actions are likely to impact on critical infrastructure or sensitive information [73]. Robustness, fairness, privacy, transparency, and accountability will thus be key properties of future AI-driven defense mechanisms.

CONCLUSION

Artificial Intelligence (AI) and cybersecurity are coming together and redefining the modern-day digital defense paradigm. The nature of cyber threats is becoming automated, adaptive, sophisticated, and difficult to detect and traditional security strategies, which rely on signature and rule-based

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

detection, are not enough. AI offers tremendous potential to solve these problems with intelligent threat detection, behavioral analysis, automated incident response, malware classification, vulnerability assessment, predictive threat intelligence and constant security monitoring. Cybersecurity systems can analyze large and complex datasets and facilitate quicker, more informed security decisions, thanks to machine learning, deep learning, natural language processing, and generative AI.

But the interconnection between AI and cybersecurity is intrinsically a two-way street. The technologies that enhance defensive prowess can also be used by bad guys. Adversaries are leveraging AI to speed up, scale, personalize, and make attack efforts more effective, with AI-powered phishing, automated reconnaissance, adaptive malware, deep fakes, social engineering, and more all proving to be effective methods of attack. Moreover, adversarial AI poses a direct threat to AI-powered security systems by methods like data poisoning, evasion, model manipulation, and adversarial examples. Preserving the integrity of AI systems is, therefore, a crucial part of today's cybersecurity landscape.

The review also identifies some of the drawbacks of AI-driven cybersecurity. Issues of data quality, model reliability, false positives/false negatives, explain ability, computational needs, privacy and the lack of cybersecurity professionals still face challenges. AI systems can also fail when faced with new attacks or when their inputs are tampered with. So, AI should not be viewed as a silver-bullet solution and should be deployed alongside existing cybersecurity measures, strong governance frameworks, monitoring solutions, and human expertise.

The rise of Generative AI only further emphasizes the importance of responsible and secure AI usage. It can help to enhance threat intelligence, security analysis, incident investigation, cybersecurity education, and more, but can also offer attackers new capabilities. This highlights the need for creating trustworthy AI systems that are backed up by robust access control, privacy-preserving measures, secure data handling, model validation, and human oversight.

In the future, cybersecurity is likely to move towards more autonomous, adaptive, and predictive means of defense. Other potential avenues for enhancing cyber resilience include AI-powered threat hunting, continuous learning, federated intelligence, automated incident response, and human-AI collaboration. However, this should be accompanied by transparency and accountability, controls on security, and appropriate human supervision.

In essence, AI should not be considered just another cybersecurity tool but a core component that is transforming the dynamics between attackers, defenders, data, and digital infrastructure. Intelligent automation will have to find a balance with human skills to secure the future of cybersecurity. As organizations work to create strong, transparent, adaptable, ethical, and resilient AI systems, they will

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

be better equipped to handle a changing threat landscape and shift their cybersecurity strategies from reactive to proactive and sustainable approaches to digital defense.

REFERENCES

[1]. Balasubramanian P, Liyana S, Sankaran H, Sivaramakrishnan S, Pusuluri S, Pirttikangas S, Peltonen E. Generative AI for cyber threat intelligence: applications, challenges, and analysis of real-world case studies. Artificial Intelligence Review. 2025 Aug 20;58(11):336.

[2]. Ankalaki S, Atmakuri AR, Pallavi M, Hukkeri GS, Jan T, Naik GR. Cyber-attack prediction: From traditional machine learning to generative artificial intelligence. Ieee Access. 2025 Mar 3; 13:44662-706.

[3]. Vadisetty R, Polamarasetti A. Generative AI for cyber threat simulation and defense. In2024 12th International Conference on Control, Mechatronics and Automation (ICCMA) 2024 Nov 11 (pp. 272-279). IEEE.

[4]. Alqahtani H, Kumar G. A comprehensive review of generative AI techniques and their impact on cybersecurity. Soft Computing. 2025 Jul;29(13):4945-82.

[5]. Syed SA. Adversarial AI and cybersecurity: defending against AI-powered cyber threats. Iconic Research And Engineering Journals. 2025 Mar;8(9):1030-41.

[6]. Rauf H, Shah SI, Ali T, Gul H, Soomro M. Using generative AI for simulating cyber security attacks and defense mechanisms: A new approach to AI-driven cyber threat modeling. Spectrum of Engineering Sciences. 2025 Mar 22:361-81.

[7]. Aslam MI. Generative AI revolution in cybersecurity: A comprehensive review of threat intelligence and operations. Spectrum of Engineering Sciences. 2026 May 4;4(5):87-96.

[8]. Kumari PL, Prasad R, Inampudi ST, Nagarjuna N, Chawan V. Deep Learning in Cyber Security: A Guide to Harnessing Generative AI for Enhanced Threat Detection. Generative Artificial Intelligence for Next-Generation Security Paradigms. 2026 Jan 29:25-47.

[9]. Gayathri B, Sundarakantham K, Tharani MA, Priyadharshan M. Emerging Trends in Malware Detection: The Role of Generative AI in Cyber Defense. In2026 Second International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS) 2026 Jan 8 (pp. 1-7). IEEE.

[10]. Balshetwar SV, Chiddarwar GG. Optimisation of generative AI models for cybersecurity threat detection through machine learning. International Journal of Cloud Computing. 2026;15(2):257-79.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

[11]. Kaur[1] T, Singh[1] S, Juneja A, Pal[1] K, Kaur[1] P. Artificial Intelligence for Threat Intelligence and Cyber Defense. Artificial Intelligence in Cybersecurity and Risk Management. 2026 May 1:59.

[12]. Ali SS, Mughal UA, Junaid M, Ahmad H. Securing Critical Infrastructure Through Deep Generative Artificial Intelligence: An Adaptive Framework for Real-Time Adversarial Threat Detection, Threat Analytics, and Cyber Defense. Research Consortium Archive. 2026 Jun 18;4(2):2159-80.

[13]. Aslam MU, Ali A, Sultan T, Ahmad H, Aqeel M. An Intelligent Deep Generative AI-Driven Cybersecurity Framework for Real-Time Adversarial Attack Detection, Threat Intelligence Analysis, and Adaptive Defense in FinTech Ecosystems. Research Consortium Archive. 2026 Jun 10;4(2):2606-37.

[14]. James GM. Cybersecurity Threats And Defenses In The Generative AI Era. Peer-Reviewed Journal of Computer Science (PRJCS). 2026 Apr 9;1(4):7-13.

[15]. Khan F. Advances in Artificial Intelligence for Electrical Systems: Machine Learning Methods, Applications, and Emerging Challenges. American Journal of Artificial Intelligence and Computing. 2026 Aug 12;2(2):1-9.

[16]. Saddi VR, Gopal SK, Mohammed AS, Dhanasekaran S, Naruka MS. Examine the role of generative AI in enhancing threat intelligence and cyber security measures. In2024 2nd International conference on disruptive technologies (ICDT) 2024 Mar 15 (pp. 537-542). IEEE.

[17]. Mathivilasini S, Sridevi D, Anandapriya B. Generative AI for Cybersecurity: Threat Simulation and Anomaly Detection. Jupiter Publications Consortium; 2025 Apr 1.

[18]. Tariq MU. Defending Against AI-Generated Cyber Threats: Frameworks, Models, and Real-Time Generative AI Security Defenses. InAI-Driven Cybersecurity Systems, Applications, and Resilient Infrastructure 2026 (pp. 195-220). IGI Global Scientific Publishing.

[19]. Mathivilasini S, Sridevi D, Anandapriya B. Generative AI for Cybersecurity: Threat Simulation and Anomaly Detection. Jupiter Publications Consortium; 2025 Apr 1.

[20]. Perumal R, Aithal PS. Significance of Use of Generative AI in Cyber Security. InConference Proceedings of Emerging Trends in Information Technology 2024 Dec 21 (Vol. 2, No. 1, pp. 181-191).

[21]. Uddin M, Irshad MS, Kandhro IA, Alanazi F, Ahmed F, Maaz M, Hussain S, Ullah SS. Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations. Artificial Intelligence Review. 2025 May 7;58(8):236.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

[22]. Abbasi N, Nizamullah FN, Zeb S, Fahad M, Qayyum MU. Machine learning models for predicting susceptibility to infectious diseases based on microbiome profiles. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2024 Aug 25;3(4):35-47.

[23]. Dhanushkodi K, Thejas S. Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE access. 2024 Nov 8;12:173127-36.

[24]. Chinyere LN. Artificial intelligence, machine learning, and deep learning-based cybersecurity: Techniques, challenges, and future directions. International Journal of Applied Resilience and Sustainability. 2026 Apr 28;2(2):1257-89.

[25]. Mohammed A. Artificial Intelligence-Driven Cybersecurity Crimes: Emerging Threats, AI Bots, and Advanced Defense Strategies. Euro Vantage journals of Artificial intelligence (EVJAI). 2026 Mar 13;3(1):46-65.

[26]. Singh A. Human-computer interaction: a review of usability, design, and accessibility trends. Global Research Repo. 2025 Sep 9;1(2):362-87.

[27]. Ugale SP, Sinha A. Generative AI in Cybersecurity: Threats, Vulnerabilities, and Protective Measures. In2025 International Conference on Future Technologies (ICFT) 2025 Nov 7 (pp. 1-8). IEEE.

[28]. Ibrar W, Mahmood D, Al-Shamayleh AS, Ahmed G, Alharthi SZ, Akhunzada A. Generative AI: a double-edged sword in the cyber threat landscape. Artificial Intelligence Review. 2025 Jul 1;58(9):285.

[29]. Ayyaz S, Malik SM. A comprehensive study of generative adversarial networks (GAN) and generative pre-trained transformers (GPT) in cybersecurity. In2024 Sixth International Conference on Intelligent Computing in Data Sciences (ICDS) 2024 Oct 23 (pp. 1-8). IEEE.

[30]. Rishmitha P, Mahesh B, Gupta K, Kumar K, Thippanna G. Improving the Cybersecurity Protection Using Generative AI. Journal of Security in Computer Networks and Distributed Systems. https://doi.org/10.46610/joscnds.2025:v02i01.

[31]. Mavikumbure HS, Cobilean V, Wickramasinghe CS, Drake D, Manic M. Generative AI in cyber security of cyber physical systems: Benefits and threats. In2024 16th International Conference on Human System Interaction (HSI) 2024 Jul 8 (pp. 1-8). IEEE.

[32]. Sardar TH, Pandey B, Aldasheva L. AI-Driven Detection of AI-Generated Cyber Attacks: A Framework for Defending Against Generative Adversarial Threats. In2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) 2026 Feb 18 (pp. 1-5). IEEE.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

[33]. Elatab SA, Almaktoof A. Artificial Intelligence in Cyber Security: A Comprehensive Overview. InInternational Conference on AI: Current Research, Industry Trends, and Innovations 2025 Jul 9 (pp. 108-125). Cham: Springer Nature Switzerland.

[34]. Aslam MS, Jamal M. Machine Learning in Healthcare: Revolutionizing Clinical Decision-Making with Data Analytics. Global Trends in Science and Technology. 2026 Mar 18;2(2):23-42.

[35]. Bhattacharjee D. Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring. In2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT) 2025 Dec 18 (pp. 1-6). IEEE.

[36]. Foley J. Cybersecurity Future Threats in Artificial Intelligence: A Comprehensive Analysis. Journal of Advanced Artificial Intelligence, Engineering and Technology. 2026 Apr 14.

[37]. Khan A, Jhanjhi NZ, Abdulhabeb GA, Ray SK, Wei GW. Introduction to Generative AI in Cybersecurity. InAI Techniques for Securing Medical and Business Practices 2025 (pp. 1-44). IGI Global Scientific Publishing.

[38]. Iyengar SS, Nabavirazavi S, Hariprasad Y, HB P, Mohan CK. AI-Enhanced Malware Detection: Advancing Security Through Intelligent Threat Identification. InArtificial Intelligence in Practice: Theory and Application for Cyber Security and Forensics 2025 May 30 (pp. 227-255). Cham: Springer Nature Switzerland.

[39]. Sindiramutty SR, Prabagaran KR, Jhanjhi NZ, Murugesan RK, Brohi SN, Masud M. Generative AI in network security and intrusion detection. InReshaping CyberSecurity With Generative AI Techniques 2025 (pp. 77-124). IGI Global Scientific Publishing.

[40]. Gundoor T, Sridevi. A Comprehensive Study on Deep Learning and Artificial Intelligence for Malware Analysis. Next-Generation Systems and Secure Computing. 2025 Mar 31:39-59.

[41]. Erdenetsogt T, Jamal M. Machine Learning for Big Data Analytics: A Comprehensive Review. Global Trends in Science and Technology. 2026 Apr 25;2(2):199-218.

[42]. Al-Kateb G, Khaleel I, Aljanabi M. CryptoGenSec: A hybrid generative AI algorithm for dynamic cryptographic cyber defence. Mesopotamian Journal of CyberSecurity. 2024;4(3):22-35.

[43]. Thaw MP, Sarwatt DS, Ning H, Ding J. Mitigating cyberattacks on autonomous vehicles: a comprehensive review of Generative Artificial Intelligence defense techniques. Artificial Intelligence Review. 2026 Jul 5.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

[44]. Randieri C, Tomazzoli C. Advancing Cyber Defense with Artificial Intelligence: State-of-the-Art Techniques and Future Directions. InAdvancements in Cybersecurity 2025 Jun 26 (pp. 503-526). CRC Press.

[45]. Ndayipfukamiye T, Ding J, Sarwatt DS, Philipo AG, Ning H. Adversarial defense in cybersecurity: A systematic review of GANs for threat detection and mitigation. arXiv preprint arXiv:2509.20411. 2025 Sep 24.

[46]. Neupane S, Fernandez IA, Mittal S, Rahimi S. Impacts and risk of generative AI technology on cyber defense. arXiv preprint arXiv:2306.13033. 2023 Jun 22.

[47]. Raza H, Singh A, Erdenetsogt T, Kabeer MM, Aslam MS, Farooq M. Machine Learning Driven Decision Making in the Modern Data Era. PERFECT: Journal of Smart Algorithms. 2026 Jan 6;3(1):11-22.

[48]. Kc B, Sapkota S, Adhikari A. Generative adversarial networks in anomaly detection and malware detection: A comprehensive survey. Advances in Artificial Intelligence Research. 2024 Aug 8;4(1):18-35.

[49]. Gupta M, Akiri C, Aryal K, Parker E, Praharaj L. From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. IEEE access. 2023 Aug 1;11:80218-45.

[50]. Madhumith R, Ouaissa M, Hemashree P, Mahalakshmi SB. Advancing Cybersecurity with Generative Adversarial Networks and Explainable AI: A Comprehensive Exploration. InGenerative Adversarial Networks for Cybersecurity: 2026 (pp. 155-179). Auerbach Publications.

[51]. Khan S. The Role of Artificial Intelligence in Cyber Security: Leveraging Machine Learning and Predictive Analytics for Intrusion Detection, Threat Intelligence, and Autonomous Defense Mechanisms. Threat Intelligence, and Autonomous Defense Mechanisms.

[52]. Dhoni PS, Kumar R. Synergizing generative Artificial Intelligence and cybersecurity: Roles of generative Artificial Intelligence entities, companies, agencies and government in enhancing cybersecurity. Journal of Global Research in Computer Sciences. 2023;14(3):1-6.

[53]. Kabeer MM. Utilizing Machine Learning for Continuous Process Improvement in Lean Six Sigma. Global Trends in Science and Technology. 2025 May 7;1(2):49-63.

[54]. Moamin SA, Abdulhameed MK, Al-Amri RM, Radhi AD, Naser RK, Pheng LG. Artificial intelligence in malware and network intrusion detection: a comprehensive survey of techniques, datasets, challenges, and future directions. Babylonian Journal of Artificial Intelligence. 2025 Jun 13;2025:77-98.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

[55]. Khan A, Jhanjhi N, Hamid DH, Omar HA, Amsaad F, Wassan S. Future trends and challenges in cybersecurity and generative AI. Reshaping CyberSecurity With Generative AI Techniques. 2025:491-522.

[56]. Waheed A, Arzu F, Nazir MZ, Mohamed NA, Hassan NU. Deep Generative Machine Learning Models for Real-Time Adversarial Threat Identification and Self-Adaptive Cybersecurity Framework for Financial Services. Journal of Management Science Research Review. 2026 Jun 18;5(2):2977-3010.

[57]. Ali SI. Cognitive Adversarial Security Neuro: Symbolic and Generative AI Defense Ecosystems for Self-Evolving Cyber Resilience. InAI-Driven Cybersecurity Systems, Applications, and Resilient Infrastructure 2026 (pp. 139-162). IGI Global Scientific Publishing.

[58]. Sheikh A, Rinvee TM, Sheikh MS. The new frontier of cyber-defense: Leveraging generative AI for proactive threat modeling and autonomous response. Available at SSRN 5542999. 2025 Sep 29.

[59]. Kabeer MM. Leveraging AI for process optimization: the future of quality assurance in lean six sigma. American Journal of Artificial Intelligence and Computing. 2025 May 7;1(1):87-103.

[60]. Virtosu I. Guardians or threats? The double-edged role of artificial intelligence in cyber security. InInternational Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings 2025 Dec 8 (Vol. 2, pp. 61-73).

[61]. Shahid A, Ehab A, Amina J, Sana Q, Zahida P, Basirah N, Anushya A, Imran C. A Comprehensive Survey of Artificial Intelligence Applications in Cyber Security: Taxonomy, Challenges, and Future Directions. Algorithms. 2026 Jul 1;19(7):527.

[62]. Patidar G, Pandey A, Safdari A, Kumar S, Tiwari A, Ranjan N. Leveraging Artificial Intelligence and Machine Learning Techniques for Proactive Threat Detection, Anomaly Prediction, and Adaptive Defense Mechanisms in Cybersecurity Frameworks. In2026 IEEE 6th International Conference on Computing, Power, and Communication Technologies (IC2PCT) 2026 May 15 (pp. 171-176). IEEE.

[63]. Almomani A, Aoudi S, Al-Qerem A, Aldweesh A, Alkasassbeh M. Behavioral analysis of AI-generated malware: New frontiers in threat detection. InExamining cybersecurity risks produced by generative AI 2025 (pp. 211-234). IGI Global Scientific Publishing.

[64]. Oad VD. Artificial Intelligence in Data Analytics: A Comprehensive Review. Global Journal of Universal Studies. 2024 Jun 15;1(1).

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-5761
Volume 2, Number 5, 2026
https://doi.org/10.70445/gtst.2.5.2026.108-129

[65]. Mahto SK, Singh B, Kushwaha N, Kumar R. AI-Powered Cybersecurity for Next-Generation Threats. Digital Immune System: Principles and Practices. 2026 Jan 30:289-304.

[66]. Coppolino L, D'Antonio S, Mazzeo G, Uccello F. The good, the bad, and the algorithm: The impact of generative AI on cybersecurity. Neurocomputing. 2025 Mar 28;623:129406.

[67]. Alli BA, Yusuf TA, Ederhion J, Otunlape O, Koyenikan O, Raheem TA, Olugbade A, John SA, Shonubi JA, Rahman MS, Al Mahmud MA. Self-evolving cyber defense: an analytical review of AI-driven autonomous and adversarial systems. Journal of Computer Virology and Hacking Techniques. 2026 Jul 13;22(1):59.

[68]. Mohanty RK, Sahoo SP, Kabat MR, Alhadidi B. Artificial intelligence for cybersecurity-fundamentals. Digital Defence: Harnessing the Power of Artificial Intelligence for Cybersecurity and Digital Forensics. 2025 Jul 11:1.

[69]. Oad SK. From Algorithms to Insights: A Review of AI Applications in Data Science. American Journal of Artificial Intelligence and Computing. 2026 May 14;2(1):236-51.

[70]. Hssaini A, Chlioui I, Radgui M. Towards a comprehensive landscape of AI and generative AI in cybersecurity. Discover Artificial Intelligence. 2026 Aug 6.

[71]. Gaikwad M, Pawar A. Review of adversarial activity detection in generative AI applications. InAIP Conference Proceedings 2025 Mar 10 (Vol. 3175, No. 1, p. 020090). AIP Publishing LLC.

[72]. Patel A, Sachan RC, Ragothaman H, Sheth A, Pandey P, Udayakumar SK. Leveraging generative ai for proactive cybersecurity threat detection in cloud environments. In2025 8th International Conference on Information and Computer Technologies (ICICT) 2025 Mar 14 (pp. 80-85). IEEE.

[73]. Awan M, Alam A, Khan RA, Alwageed HS, Ayouni S, Almagrabi AO. A generative AI-driven cybersecurity framework for small and medium enterprises software development: an ANN-ISM approach. Scientific Reports. 2026 Feb 7;16(1):9813.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.