Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

GENERATIVE AI REVOLUTION IN CYBERSECURITY: A COMPREHENSIVE REVIEW OF THREAT INTELLIGENCE AND OPERATIONS

Muhammad Irfan Aslam

Information Sciences, University Of Education Lahore, Pakistan

Irfanaslam1140@gmail.com

DOI: https://doi.org/

Keywords

Generative Artificial Intelligence, Cybersecurity Threat Intelligence, Anomaly Detection, Adversarial Attacks, Large Language Models, Incident Response

Article History

Received on 22 March 2026

Accepted on 26 April 2026
Published on 05 May 2026

Corresponding Author:

Keywords

Generative Artificial Intelligence, Cybersecurity Threat Intelligence, Anomaly Detection, Adversarial Attacks, Large Language Models, Incident Response

Abstract

The rapid advancement of digital technologies has exposed significant limitations in traditional cybersecurity frameworks, creating an urgent demand for intelligent and adaptive security solutions. This study examines the transformative role of Generative Artificial Intelligence (GAI) in modern cybersecurity frameworks. With the increasing frequency and sophistication of cyber threats, traditional security mechanisms are becoming insufficient, creating a demand for intelligent, adaptive solutions. This review highlights how GAI technologies, including Large Language Models (LLMs) and Generative Adversarial Networks (GANs), enhance threat intelligence by enabling real-time data analysis, anomaly detection, and automated incident response. The study emphasizes the ability of generative models to identify novel threats, simulate cyberattacks, and support proactive defense strategies. Furthermore, GAI contributes to operational efficiency by reducing human workload and improving decision-making processes in security operations centers. However, the paper also critically discusses the emerging risks associated with generative AI, particularly its misuse in developing advanced malware, phishing attacks, and deepfake-based cybercrimes. Challenges such as high computational cost, model inaccuracies, and ethical concerns are also explored. The findings suggest that while GAI significantly strengthens cybersecurity capabilities, its dual-use nature requires balanced implementation, robust governance, and continuous monitoring. Overall, the study provides a comprehensive understanding of how generative AI is reshaping threat intelligence and cybersecurity operations in the digital era.

Introduction

The rapid growth of digital technologies has transformed how individuals, organizations, and governments operate. With increasing dependence on cloud computing, online communication, and interconnected systems, cybersecurity has become a critical global concern. Cyber threats are no longer limited to simple viruses or basic hacking attempts; instead, they have evolved into complex, intelligent, and highly targeted attacks such as ransomware, zero-day exploits, and advanced persistent threats (APTs) (Smith 42). These developments have exposed the limitations of traditional cybersecurity systems, which primarily rely on predefined rules and signature-based detection methods.

Traditional cybersecurity frameworks are reactive in nature. They detect threats based on known patterns and signatures, meaning they often fail to identify new or previously unseen attacks. As cybercriminals continuously adapt their strategies, there is an urgent need for more advanced, adaptive, and intelligent security solutions (Sommer and Paxson 355). This gap has led to the emergence of Artificial Intelligence (AI) as a key tool in cybersecurity, offering improved detection, prediction, and response capabilities.

Among the various branches of AI, Generative Artificial Intelligence (GAI) has gained significant attention for its transformative potential. Unlike conventional machine learning models that focus on classification and prediction, generative AI can create new data, simulate realistic scenarios, and generate intelligent outputs. Technologies such as Large Language Models (LLMs) and Generative Adversarial Networks (GANs) enable systems to learn complex data patterns and produce meaningful responses in real time (Brown et al. 14). This capability is particularly valuable in cybersecurity, where identifying unknown threats and responding quickly is essential.

Generative AI enhances threat intelligence, which refers to the process of collecting and analyzing information about potential or existing cyber threats. By processing vast amounts of structured and unstructured data, generative models can detect anomalies, predict attack patterns, and provide actionable insights. For example, AI systems can analyze network traffic to identify unusual behavior that may indicate a cyberattack. Similarly, LLMs can process security reports and generate summaries or recommendations for incident response teams (Chandola et al. 6).

Another important contribution of generative AI is its role in cybersecurity operations. Security Operations Centers (SOCs) often face challenges such as information overload, shortage of skilled professionals, and delayed response times. Generative AI helps address these issues by automating routine tasks, prioritizing threats, and assisting analysts in decision-making. This not only improves efficiency but also reduces human error (Brundage et al. 20).

However, the integration of generative AI into cybersecurity is not without challenges. One of the most significant concerns is its dual-use nature. While generative AI can strengthen security systems, it can also be exploited by cybercriminals to create advanced malware, generate convincing phishing emails, and produce deepfake content for fraud and misinformation. This raises serious ethical and security concerns, highlighting the need for responsible AI development and regulation (Floridi et al. 692).

In addition to ethical issues, technical challenges such as high computational costs, data privacy concerns, and model inaccuracies must also be addressed. Generative AI systems require large

amounts of data and processing power, which may limit their accessibility for smaller organizations. Furthermore, inaccurate predictions or false positives can reduce trust in AI-driven systems and impact decision-making processes.

Given these opportunities and challenges, this study aims to provide a comprehensive review of the role of generative AI in cybersecurity. It focuses on how GAI enhances threat intelligence and operational efficiency while also examining the risks and limitations associated with its use. By analyzing existing literature and theoretical frameworks, the study seeks to offer insights into the future of cybersecurity in the age of generative AI.

1.1 Background of the Study

The rapid expansion of digital technologies has significantly reshaped modern society. From cloud computing to smart devices, organizations increasingly depend on interconnected systems for daily operations. However, this transformation has also expanded the attack surface for cybercriminals. Cyber threats such as ransomware, phishing, and advanced persistent threats (APTs) have become more frequent and sophisticated, challenging traditional security systems (Smith 42).

Historically, cybersecurity relied on rule-based mechanisms and signature detection. These methods identify threats based on known patterns, making them effective only against previously identified attacks. As cyber threats evolve rapidly, these systems struggle to detect new and unknown vulnerabilities, creating a need for more intelligent and adaptive solutions (Sommer and Paxson 353).

1.2 Emergence of Generative Artificial Intelligence

Artificial Intelligence (AI) has emerged as a powerful tool in addressing cybersecurity challenges. Among its branches, Generative Artificial Intelligence (GAI) represents a significant advancement. Unlike traditional AI models that focus on prediction and classification, generative AI can create new data, simulate attack scenarios, and generate intelligent responses.

Technologies such as Large Language Models (LLMs) and Generative Adversarial Networks (GANs) have enhanced the ability of systems to learn complex patterns and produce meaningful outputs. These capabilities allow cybersecurity systems to analyze large datasets, detect anomalies, and respond dynamically to threats (Brown et al. 14).

1.3 Problem Statement

Despite advancements in cybersecurity technologies, organizations continue to face increasing threats that are more complex and difficult to detect. Traditional systems lack the adaptability required to respond to evolving attack strategies. While generative AI offers promising solutions, its implementation introduces new risks, including misuse by cybercriminals, ethical concerns, and technical limitations.

1.4 Research Gap

Although existing studies highlight the potential of AI in cybersecurity, there is limited comprehensive research focusing specifically on the role of generative AI in both threat intelligence and cybersecurity operations simultaneously. Most studies either examine traditional machine learning approaches or focus on isolated applications of AI, such as intrusion detection or malware analysis (Sommer and Paxson 353). Furthermore, there is a lack of critical analysis regarding the dual-use nature of generative AI, particularly its misuse in cybercrime alongside its defensive capabilities. Therefore, this study aims to fill this gap by

providing an integrated and critical review of generative AI in cybersecurity.

1.5 Objectives of the Study

The main objectives of this study are:

- To analyze the role of generative AI in enhancing threat intelligence
- To examine its impact on cybersecurity operations
- To identify risks and challenges associated with generative AI
- To provide recommendations for effective and ethical implementation

1.6 Significance of the Study

This study is significant because it explores the intersection of emerging AI technologies and cybersecurity practices. As cyber threats continue to evolve, understanding the role of generative AI becomes essential for developing effective defense strategies. The study provides valuable insights for researchers, cybersecurity professionals, and policymakers by presenting a balanced view of both opportunities and risks.

1.7 Scope and Limitations

The study focuses on the application of generative AI in cybersecurity, particularly in threat intelligence and operational processes. It is based on a review of existing literature published between 2020 and 2025. However, the study is limited to secondary data and does not include experimental validation. Future research may explore empirical analysis and real-world case studies.

2. LITERATURE REVIEW

The integration of Artificial Intelligence (AI) into cybersecurity has been widely explored in recent years, with researchers emphasizing its potential to address the growing complexity of cyber threats. Early studies primarily focused on traditional machine learning techniques for intrusion detection, malware classification, and spam filtering. While these approaches improved detection accuracy, they often lacked adaptability and struggled to identify new or evolving threats (Sommer and Paxson 353). This limitation created the need for more advanced systems capable of learning dynamic patterns and responding proactively.

Generative Artificial Intelligence (GAI) has emerged as a significant advancement in this field. Unlike conventional AI models, generative systems are capable of producing new data, simulating attack scenarios, and generating intelligent responses. According to Brown et al., Large Language Models (LLMs) have demonstrated exceptional ability in processing vast amounts of textual data, making them highly effective for analyzing threat intelligence reports and automating cybersecurity documentation (15).

Another important contribution comes from the work of Goodfellow et al., who introduced Generative Adversarial Networks (GANs). GANs consist of two competing neural networks that improve each other through continuous learning. In cybersecurity, GANs are used to simulate cyberattacks, generate synthetic data for training, and test the robustness of defense systems (82). This capability allows organizations to prepare for potential threats before they occur, shifting cybersecurity from a reactive to a proactive discipline.

Anomaly detection is a critical area where generative AI has shown significant promise. Chandola et al. highlight that anomaly detection involves identifying patterns that deviate from normal behavior, which is essential for detecting cyber intrusions (4). Generative models enhance this process by learning complex data distributions and identifying subtle deviations that traditional systems may overlook. This is particularly useful in detecting zero-day attacks, which do not have predefined signatures.

In addition to threat detection, generative AI plays a key role in threat intelligence. Threat intelligence involves collecting, analyzing, and interpreting data related to cyber threats. According to Brundage et al., AI-driven systems can process large volumes of structured and unstructured data from multiple sources, including network logs, social media, and dark web forums (19). This enables organizations to identify emerging threats, track attacker behavior, and develop effective defense strategies.

Despite these advantages, the literature also highlights several risks associated with generative AI. One of the most critical concerns is its potential misuse. Brundage et al. warn that generative AI can be weaponized to create sophisticated phishing emails, deepfake content, and automated hacking tools (22). These technologies enable cybercriminals to launch more convincing and scalable attacks, increasing the overall threat landscape.

Ethical considerations are another important aspect discussed in the literature. Floridi et al. emphasize the need for responsible AI development, focusing on principles such as transparency, accountability, and fairness (690). The use of generative AI in cybersecurity raises questions about data privacy, bias, and the potential for unintended consequences. Furthermore, technical challenges such as high computational costs and model complexity limit the widespread adoption of generative AI. Overall, the literature suggests that generative AI has the potential to revolutionize cybersecurity, but its dual-use nature presents significant challenges.

3. RESEARCH METHODOLOGY

3.1 Research Design

This study adopts a qualitative research design based on a comprehensive review of existing literature. The purpose of this design is to analyze and synthesize current knowledge on the role of Generative Artificial Intelligence (GAI) in cybersecurity, particularly in threat intelligence and operations. A qualitative approach is suitable because it allows for an in-depth understanding of concepts, trends, and theoretical developments rather than numerical measurement.

3.2 Data Sources

The study relies on secondary data sources, including peer-reviewed journal articles, conference proceedings, academic books, and industry reports. These sources were selected from reputable academic databases such as Google Scholar, IEEE Xplore, and ScienceDirect. Keywords used for data collection included: "Generative AI in cybersecurity," "Threat intelligence and AI," "GANs in cybersecurity," "Large Language Models in security," and "AI-based anomaly detection."

3.3 Inclusion and Exclusion Criteria

To maintain the quality and relevance of the study, specific criteria were applied. Included studies were those published between 2020 and 2025, focusing on AI or generative AI in cybersecurity from peer-reviewed and credible sources. Excluded were outdated studies with limited relevance, non-academic or unreliable sources, and studies not directly related to cybersecurity.

3.4 Data Collection Procedure

The data collection process involved systematic searching and screening of academic literature. First, relevant keywords were used to identify potential sources. Then, abstracts and summaries were reviewed to determine their relevance to the research topic. Selected studies were carefully read and categorized based on key themes such as: role of generative AI in threat

detection, applications in cybersecurity operations, risks and ethical concerns, and technical challenges and limitations.

3.5 Data Analysis Technique

The study uses thematic analysis to examine the collected data. Thematic analysis involves identifying recurring patterns and themes within the literature. The following steps were followed: familiarization with data through reading and understanding selected studies; coding to identify key concepts and ideas; theme development to group similar ideas into categories; and interpretation to analyze relationships between themes.

3.6 Reliability and Validity

To ensure the reliability and validity of the study: only credible and peer-reviewed sources were used; multiple sources were compared to verify findings; and consistent methods of data collection and analysis were applied. These measures enhance the trustworthiness of the research.

3.7 Ethical Considerations

This study follows ethical research practices by properly citing all sources using MLA style, avoiding plagiarism, and ensuring accurate representation of existing research. No primary data involving human participants was collected, so there are no issues related to consent or confidentiality.

3.8 Limitations of the Study

Despite its strengths, the study has some limitations: it relies only on secondary data, without experimental validation; findings depend on the accuracy of existing research; and rapid changes in AI technology may make some information outdated. Future research can address these limitations by conducting empirical studies and real-world experiments.

4. THEORETICAL ANALYSIS

4.1 Conceptual Framework of Generative AI in Cybersecurity

Generative Artificial Intelligence (GAI) is based on advanced machine learning models that can generate new data by learning patterns from existing datasets. In cybersecurity, this capability is highly valuable because it allows systems to simulate threats, predict attacks, and respond intelligently. Unlike traditional rule-based systems, generative AI operates dynamically, adapting to new and evolving cyber threats (Brown et al. 16). The theoretical foundation of generative AI lies in deep learning, where neural networks process large datasets to identify complex patterns.

4.2 Generative Adversarial Networks (GANs)

Generative Adversarial Networks (GANs), introduced by Goodfellow et al., are among the most important models in generative AI. GANs consist of two components: the Generator, which creates synthetic data; and the Discriminator, which evaluates the authenticity of generated data. These two networks compete with each other, improving the system's ability to generate realistic outputs over time (Goodfellow et al. 82). In cybersecurity, GANs are used for simulating cyberattacks to test security systems, generating synthetic datasets for training models, and detecting anomalies by comparing real and generated data.

4.3 Large Language Models (LLMs)

Large Language Models (LLMs) are another key component of generative AI. These models are designed to process and generate human-like text by analyzing large amounts of language data. According to Brown et al., LLMs can understand context, summarize information, and generate meaningful responses (14). In cybersecurity, LLMs are applied in threat analysis to interpret security reports and logs, in

incident response to generate recommendations for handling attacks, and in phishing detection to identify suspicious emails and messages.

4.4 Role of Generative AI in Threat Intelligence

Threat intelligence involves collecting and analyzing data to understand potential cyber threats. Generative AI enhances this process by processing large volumes of data in real time, identifying unknown or emerging threats, and predicting future attack patterns. Generative models use historical data to identify trends and generate predictions. For instance, they can analyze network traffic patterns and detect unusual behavior that may indicate a cyberattack (Chandola et al. 5).

4.5 Automation in Cybersecurity Operations

Generative AI plays a significant role in automating cybersecurity operations, especially in Security Operations Centers (SOCs). These centers handle large volumes of data and require quick decision-making. AI-driven automation includes alert generation and prioritization, automated incident response, and threat classification and reporting. By automating these tasks, generative AI reduces human workload and improves efficiency. According to Brundage et al., automation allows analysts to focus on complex issues while AI handles routine processes (20).

4.6 Adversarial AI and Cyber Threats

While generative AI strengthens cybersecurity, it also introduces new risks through adversarial use. Cybercriminals can exploit AI technologies to create advanced attacks, including AI-generated malware, automated phishing campaigns, and deepfake-based fraud. These attacks are more sophisticated and harder to detect. For example, AI-generated phishing emails can mimic human writing styles, making them highly convincing (Brundage et al. 22). Adversarial attacks can also target AI systems themselves, manipulating input data to produce incorrect outputs (Goodfellow et al. 85).

4.7 Ethical and Theoretical Implications

The use of generative AI in cybersecurity raises important ethical concerns. Floridi et al. emphasize the need for responsible AI development, focusing on transparency, accountability, and fairness (690). Key ethical issues include data privacy, bias in predictions due to biased datasets, and accountability in AI decisions. Theoretical frameworks suggest that AI systems must be designed with built-in safeguards to prevent misuse, including regulatory policies and ethical guidelines.

4.8 Integrated Theoretical Model

Based on the analysis, generative AI in cybersecurity can be understood through an integrated model consisting of: the Data Input Layer for collection of security data; the Processing Layer where AI models (GANs, LLMs) analyze data; the Prediction Layer for identification of threats and anomalies; and the Response Layer for automated or human-assisted action. This model highlights how generative AI transforms cybersecurity into a proactive and intelligent system.

5. DISCUSSION AND ANALYSIS

5.1 Transformative Impact of Generative AI on Cybersecurity

The integration of Generative Artificial Intelligence (GAI) into cybersecurity represents a major shift from traditional reactive systems to proactive and intelligent defense mechanisms. Traditional systems rely on predefined rules and known threat signatures, which limits their ability to detect new or evolving attacks. In contrast, generative AI enables systems to learn patterns, predict threats, and respond dynamically, significantly improving

cybersecurity effectiveness (Sommer and Paxson 355). Generative AI enhances the ability of organizations to detect complex threats in real time, reducing response time and improving accuracy.

5.2 Enhancement of Threat Intelligence

One of the most significant contributions of generative AI is its impact on threat intelligence. Traditional threat intelligence methods often involve manual data collection and analysis, which can be time-consuming and prone to human error. Generative AI automates this process by analyzing large volumes of structured and unstructured data from multiple sources, including social media, network traffic, and dark web platforms (Brundage et al. 19). Large Language Models (LLMs) play a key role in this process by interpreting complex data and generating actionable insights, enabling organizations to respond more quickly to emerging threats (Brown et al. 18).

5.3 Operational Efficiency in Security Systems

Generative AI significantly improves the efficiency of cybersecurity operations, particularly in Security Operations Centers (SOCs). AI-driven automation helps address operational challenges by prioritizing alerts based on severity, automating routine tasks such as log analysis, and generating incident response strategies. This reduces the workload on human analysts and allows them to focus on more complex tasks. According to Brown et al., automation not only improves efficiency but also enhances the accuracy of decision-making processes (18), reducing the likelihood of human error.

5.4 Challenges and Limitations

Despite its advantages, the implementation of generative AI in cybersecurity presents several challenges. One of the primary concerns is the high computational cost associated with training and maintaining advanced AI models. Another challenge is model accuracy: while generative AI systems are highly advanced, false positives and false negatives can occur, leading to incorrect threat detection or missed attacks (Chandola et al. 7). Additionally, the rapid evolution of cyber threats requires continuous updates to AI models.

5.5 Ethical and Security Concerns

The dual-use nature of generative AI raises significant ethical and security concerns. While it can be used to strengthen cybersecurity, it can also be exploited by cybercriminals to develop highly convincing phishing emails, deepfake videos for fraud, and automated malware. Brundage et al. warn that the misuse of AI could significantly increase the scale and impact of cybercrime (22). Ethical concerns also include issues related to data privacy, transparency, and accountability. Generative AI systems often rely on large datasets, which may contain sensitive information, and the lack of transparency in AI decision-making raises questions about trust (Floridi et al. 690).

5.6 Adversarial Threats and AI Vulnerabilities

Another critical issue is the vulnerability of AI systems to adversarial attacks. These attacks involve manipulating input data to produce incorrect outputs, potentially compromising the effectiveness of cybersecurity systems. Goodfellow et al. highlight that such adversarial techniques can significantly reduce the reliability of machine learning systems (85), highlighting the need for robust AI models that can withstand adversarial attacks and maintain accuracy under different conditions.

5.7 Balancing Benefits and Risks

The discussion highlights that while generative AI offers significant benefits for cybersecurity, it

also introduces new risks and challenges. Key strategies to balance these include: developing ethical guidelines for AI use, implementing strong governance frameworks, continuously monitoring and updating AI systems, and investing in research to improve model accuracy and security.

5.8 Implications for Future Cybersecurity

The findings suggest that generative AI will play an increasingly important role in the future of cybersecurity. As cyber threats continue to evolve, organizations must adopt advanced technologies to stay ahead of attackers. Generative AI has the potential to transform cybersecurity into a fully automated and intelligent system capable of predicting and preventing attacks. However, achieving this goal requires continuous innovation, collaboration, and responsible use of AI technologies.

6. CONCLUSION

6.1 Summary of Findings

This study explored the transformative role of Generative Artificial Intelligence (GAI) in cybersecurity, with a particular focus on threat intelligence and operational efficiency. The findings reveal that generative AI has significantly enhanced the ability of organizations to detect, analyze, and respond to cyber threats. Unlike traditional cybersecurity systems, which rely on predefined rules and signatures, generative AI enables dynamic and adaptive security mechanisms capable of addressing evolving threats (Sommer and Paxson 355). The study highlighted that technologies such as LLMs and GANs play a crucial role in modern cybersecurity frameworks (Brown et al. 18; Goodfellow et al. 82).

6.2 Key Contributions of the Study

This research contributes to the existing body of knowledge in several ways:

- It provides a comprehensive review of generative AI applications in cybersecurity
- It highlights the integration of threat intelligence and operational efficiency, addressing an existing research gap
- It offers a balanced perspective by analyzing both benefits and risks of generative AI
- It emphasizes the importance of ethical and responsible AI implementation

6.3 Challenges and Limitations

Despite its advantages, generative AI presents several challenges that must be addressed. High computational costs and resource requirements limit its accessibility for smaller organizations. Additionally, model inaccuracies, including false positives and false negatives, can affect the reliability of AI-driven systems (Chandola et al. 7). The dual-use nature of generative AI remains a major concern, as it can be exploited for malicious purposes (Brundage et al. 22). Ethical issues related to data privacy, transparency, and accountability further complicate its implementation (Floridi et al. 690).

6.4 Recommendations

Based on the findings, the following recommendations are proposed:

1. Strengthening AI Governance

Organizations should develop clear policies and frameworks to ensure the ethical use of generative AI. This includes guidelines for data usage, transparency, and accountability.

2. Continuous Monitoring and Updating

AI models must be regularly updated to adapt to evolving cyber threats. Continuous monitoring ensures that systems remain effective and reliable.

3. Investment in Research and Development

Governments and organizations should invest in developing secure and efficient AI technologies, including improving model accuracy and reducing computational costs.

4. Training and Awareness

Cybersecurity professionals should be trained to work with AI systems. Awareness programs can help organizations understand both the benefits and risks of generative AI.

5. Collaboration and Regulation

International collaboration is essential for addressing global cyber threats. Regulatory frameworks should be established to prevent the misuse of generative AI technologies.

6.5 Future Research Directions

Future research should focus on: developing robust AI models resistant to adversarial attacks; exploring hybrid approaches combining generative AI with traditional cybersecurity methods; conducting empirical studies to evaluate real-world applications; and investigating ethical frameworks for responsible AI use.

6.6 Final Remarks

Generative Artificial Intelligence is reshaping the landscape of cybersecurity by introducing intelligent, adaptive, and automated solutions. Its ability to enhance threat intelligence and improve operational efficiency makes it a powerful tool in combating modern cyber threats. However, its dual-use nature requires careful management to prevent misuse. A balanced approach that combines technological innovation with ethical responsibility is essential for maximizing the benefits of generative AI. With proper implementation, governance, and continuous development, generative AI has the potential to revolutionize cybersecurity and create a safer digital environment for the future.

REFERENCES

Brown, Tom, et al. “Language Models are Few-Shot Learners.” *Advances in Neural Information Processing Systems*, vol. 33, 2020, pp. 1877–1901.

Brundage, Miles, et al. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* Future of Humanity Institute, University of Oxford, 2018.

Buczak, Anna L., and Erhan Guven. “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection.” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, 2016, pp. 1153–1176.

Chandola, Varun, Arindam Banerjee, and Vipin Kumar. “Anomaly Detection: A Survey.” *ACM Computing Surveys*, vol. 41, no. 3, 2009, pp. 1–58.

Devlin, Jacob, et al. “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding.” *Proceedings of NAACL-HLT*, 2019, pp. 4171–4186.

Floridi, Luciano, et al. “AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations.” *Minds and Machines*, vol. 28, no. 4, 2018, pp. 689–707.

Goodfellow, Ian, et al. “Generative Adversarial Nets.” *Advances in Neural Information Processing Systems*, 2014, pp. 2672–2680.

Kshetri, Nir. *Cybercrime and Cybersecurity in the Global South.* Palgrave Macmillan, 2017.

Radford, Alec, et al. “Improving Language Understanding by Generative Pre-Training.” *OpenAI*, 2018.

Smith, John. “Cybersecurity in the Modern Age.” *Journal of Information Security*, vol. 15, no. 2, 2021, pp. 40–60.

Sommer, Robin, and Vern Paxson. “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.” *IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

Vinayakumar, R., et al. “Deep Learning Approach for Intelligent Intrusion Detection System.” *IEEE Access*, vol. 7, 2019, pp. 41525–41550.