AI-Driven Open Source Intelligence in Cyber Defense: A Double-Edged Sword for National Security

Abstract

This study explores the dual implications of Artificial Intelligence (AI)-driven Open Source Intelligence (OSINT) in enhancing cyber defense capabilities. Using publicly available datasets, including IBM X-Force breach metrics, MITRE ATT&CK adversarial tactics, GDPR privacy violations, AI-driven phishing incidents, and case-specific data from the Colonial Pipeline ransomware attack and Russia-Ukraine conflict, the research employs multivariate regression, logistic regression, and K-Means clustering. The findings indicate that AI investments improve detection time (-0.68), accuracy (+2.09), and resolution rates (+1.55) with statistical significance ($p < 0.001$). However, risks associated with algorithmic opacity, weak regulatory frameworks, and reactive AI systems pose ethical and operational challenges. Clustering reveals variability in AI applications, with optimized systems achieving 95.2% detection rates and 5.5-hour response times. Recommendations include investing in scalable tools, strengthening regulations, fostering public-private collaborations, and enhancing reactive AI oversight. The results highlight AI's transformative potential in cyber defense while emphasizing the need for ethical and regulatory alignment. Future directions include testing these models in diverse operational environments to validate effectiveness and exploring hybrid AI approaches to balance proactive and reactive capabilities, ensuring robust and adaptive defense mechanisms.

Keywords: AI-driven OSINT, Cyber defense, Regulatory frameworks, Reactive AI risks, K-Means clustering

1. Introduction

The digital age has ushered in an unprecedented era of interconnectedness, transforming numerous facets of contemporary life. While these advancements have created remarkable opportunities, they have also introduced a complex array of cyber threats. Stoddart (2022) argues that nation-states, criminal organizations, and individual actors exploit cyberspace to conduct espionage, disrupt critical infrastructure, steal sensitive information, and compromise essential services. Ensuring robust cyber defense, according to Efthymiopoulos (2019), has emerged as a key national security priority, necessitating innovative approaches to threat detection, prevention, and response.

Open Source Intelligence (OSINT), defined as the systematic collection and analysis of publicly available information, has become a critical tool in modern cyber defense (Miller, 2018). Traditionally, OSINT relied on manual methods, involving the analysis of data from sources such as news platforms, social media, forums, and official reports. However, Max (2024) contends that the exponential growth of digital information has diminished the effectiveness of manual approaches, prompting the integration of Artificial Intelligence (AI) into OSINT processes. This integration, as Vegesna and Adepu (2024) argues, automates data analysis, enhances accuracy, and scales operations to address the growing complexity of cyber threats.

AI technologies, including machine learning, natural language processing, and data mining, have significantly enhanced OSINT capabilities. These technologies automate the analysis of vast datasets, detect patterns and anomalies, and extract actionable insights, improving the efficiency and scalability of OSINT. Gregoire (2024) highlights that AI adoption has led to cost savings of approximately $2.09 million per organization annually and reduced threat detection times by up to 90%. Projections from Andre (2024) suggest that the AI in cybersecurity market will grow from $24 billion in 2023 to $134 billion by 2030, underscoring its expanding role.

The applications of AI-driven OSINT extend to real-world scenarios. For instance, during the 2021 Colonial Pipeline ransomware attack (Liu et al., 2022), Adel and Norouzifard (2024) notes that AI tools facilitated malware analysis, cryptocurrency tracing, and dark web monitoring, identifying perpetrators and mitigating further risks. Similarly, Amazon (2023) explains that Amazon employs AI tools such as graph databases and honeypots to address cyber threats, which have surged from 100 million to 750 million daily attempts within a year.

AI-driven OSINT also plays a vital role in national security. During the Russia-Ukraine conflict, Winter et al. (2022) highlights its use in monitoring troop movements and combating disinformation by analyzing satellite imagery and social media data. Additionally, Federal Budget IQ (2023) asserts that the U.S. Department of Defense has allocated $7.4 billion to AI and big data initiatives to counter sophisticated threats, demonstrating the strategic importance of these technologies in national defense.

Despite its potential, the integration of AI into OSINT introduces significant challenges. George (2024) argues that while AI equips defenders with advanced tools, it also empowers malicious actors. For example, Staff (2023) highlights that AI-generated phishing emails have surged by 1,265%, while credential phishing attacks have risen by 967%. Such misuse demonstrates the ability of cybercriminals to deploy AI to develop sophisticated and targeted attacks. Furthermore, it was observed that during the 2020 U.S. Presidential Election, AI was used to generate fake accounts, produce misleading

content, and amplify divisive narratives, raising concerns about its impact on democratic processes (Center for an Informed Public, 2020)

Geopolitical implications further underscore the significance of AI-driven OSINT. According to Willett (2024), reports indicate that China has employed AI tools for cyber espionage operations, such as Volt Typhoon, targeting critical U.S. infrastructure. eSintire (2023) explains that the financial repercussions of such state-sponsored cyber activities are projected to reach $9.5 trillion, highlighting the need for robust defenses and regulatory frameworks to mitigate these risks.

In addition to malicious exploitation, technical and operational challenges complicate AI integration into cybersecurity frameworks. Bouramdane (2023) notes that 65% of cybersecurity teams report difficulties in aligning AI systems with legacy infrastructure, citing a lack of expertise and compatibility as primary barriers. Ethical concerns, including data privacy and algorithmic bias, further complicate AI's deployment. Konidena et al. (2024) argues that these issues necessitate comprehensive guidelines to ensure responsible implementation while mitigating misuse by adversaries.

Global initiatives have emerged to address these challenges and establish ethical frameworks for AI-driven OSINT. For example, Feijóo et al. (2020) highlights the International Network of AI Safety Institutes, which convenes to address risks associated with AI technologies, including cybersecurity threats. Concurrently, U.S. Department of Commerce (2024) notes that the U.S. government has launched the Testing Risks of AI for National Security (TRAINS) task force to ensure secure deployment of AI systems. These efforts, as Bouchetara et al. (2024) contends, reflect the growing need for balanced approaches that integrate innovation with regulatory oversight.

Collaborations between the public and private sectors are also instrumental in addressing these issues. For instance, Moorhead (2024) observes that Meta's decision to permit limited access to its Llama AI model for national security applications—while restricting its use for direct military or espionage purposes—illustrates the delicate balance between fostering innovation and maintaining ethical considerations. Such partnerships, as AlDaajeh et al. (2022) posits, highlight the importance of cooperation among governments, private entities, and international organizations to develop sustainable and effective cybersecurity strategies. By examining the opportunities and challenges associated with AI-driven OSINT, it becomes evident that its integration into cybersecurity represents a transformative shift. Strategic investments, ethical oversight, and collaborative efforts, according to Habbal et al. (2024), will be crucial in shaping the future of cyber defense while mitigating the risks inherent in this rapidly evolving field.This study aims to explore the dual-role implications of AI-driven Open Source

Intelligence (OSINT) in cyber defense, analyzing its potential benefits and risks for national security, while proposing strategies for responsible and effective utilization, by achieving the following objectives:

1. Examines the role of AI-driven OSINT in enhancing cyber defense capabilities, focusing on its efficiency, accuracy, and scalability in detecting and mitigating threats.
2. Investigates the challenges and risks associated with AI-driven OSINT, including ethical dilemmas, privacy concerns, and potential misuse by malicious actors or adversaries.
3. Analyzes recent case studies and statistics that highlight the applications, successes, and vulnerabilities of AI-driven OSINT in national security contexts.
4. Proposes a framework for policymakers and organizations to regulate and optimize the use of AI-driven OSINT, ensuring its alignment with legal, ethical, and security standards.

The study highlights how AI technologies, while enhancing cyber defense capabilities, also introduce new ethical, regulatory, and operational challenges. This dual nature impresses the critical need for balanced strategies that leverage AI's potential while mitigating its risks. This balance is essential to prevent the misuse of AI-driven tools, which can be as detrimental as the benefits they offer are transformative. The practical implications of this study are particularly relevant for cybersecurity practitioners and policymakers, providing actionable insights into optimizing AI-driven OSINT systems for enhanced detection and response capabilities. Additionally, the research serves as a guide for shaping public policies and private sector strategies to foster ethical and effective use of AI in cybersecurity.

2. Literature Review

Foundations and Evolution of AI-Driven OSINT

The integration of Artificial Intelligence (AI) into Open Source Intelligence (OSINT) has significantly transformed cybersecurity operations by automating and enhancing traditional methodologies. Ofori-Boateng et al. (2024) argues that AI technologies, including machine learning (ML) and natural language processing (NLP), facilitate the efficient analysis of vast datasets from diverse open sources such as social media, public records, news articles, and technical reports. ML algorithms, as Edward (2024) posits, identify patterns and anomalies indicative of malicious activity, while NLP enables the interpretation of unstructured text to extract actionable intelligence. This automation, according to Kumari (2022), strengthens cyber defenses by supporting real-time threat detection, comprehensive malware analysis, and proactive threat prevention.

Historically, OSINT relied heavily on manual processes, requiring analysts to laboriously gather and interpret information from open sources (Keliris et al., 2019; Adigwe et al.,

2024). Sepasgozar et al. (2023) notes that this approach was resource-intensive and struggled to keep pace with the exponential growth of digital information. The advent of digital tools such as web scraping and basic analytics marked a shift toward more automated processes (Telukdarie et al., 2023; Alao, Adebiyi and Olaniyi, 2024). However, these early methods, as Abrahams et al. (2024) contends, were limited in scope and lacked the sophistication needed to address modern cybersecurity challenges. The integration of AI represents a pivotal milestone in this evolution, automating complex analytical tasks and enabling large-scale data processing with unprecedented speed and accuracy (Tong, 2024; Arigbabu et al., 2024). Tong (2024) avers that this shift reflects broader trends toward automation in intelligence gathering, ensuring OSINT remains adaptable to the challenges posed by the digital age.

The application of AI-driven OSINT extends beyond organizational cybersecurity, finding significant utility in national defense strategies. Defense agencies, such as the U.S. Department of Defense, has increasingly invested in AI technologies to bolster national security (Mori, 2018; Fabuyi et al., 2024). According to (Balantrapu, 2024), these investments have led to the development of advanced AI algorithms capable of sophisticated threat analysis. These capabilities, as Watters (2023) argues, enable proactive measures to monitor and counter potential risks, transforming OSINT from a reactive to a proactive discipline. By providing earlier detection of threats, accelerating incident response, and aiding in the prevention of future attacks, AI-driven OSINT enhances the strategic capabilities of national defense frameworks (Gioti & Γιώτη, 2024; Gbadebo et al., 2024)

Nevertheless, the integration of AI into OSINT presents challenges that must be addressed to fully realize its potential. Ethical concerns surrounding data privacy and the potential for misuse, as Renuka et al., (2024) highlights, underscore the need for robust regulatory frameworks and guidelines to ensure responsible application. Zhai et al. (2024) also cautions that over-reliance on AI could undermine critical human analytical skills and reduce the capacity for nuanced decision-making. Balancing automated processes with human expertise, Gao and Zamanpour (2024) argues, is crucial for maintaining the integrity and reliability of intelligence analysis. As AI continues to reshape OSINT, addressing these ethical and practical challenges will be essential to navigating the increasingly complex cybersecurity landscape (Sarker, 2024; Joeaneke et al., 2024).

AI-Driven OSINT in Cyber Defense

Artificial Intelligence (AI) has profoundly transformed Open Source Intelligence (OSINT) in cyber defense, enhancing efficiency, scalability, and precision. Balantrapu, (2024) argues that AI technologies, such as machine learning (ML) and natural language processing (NLP), automate the collection, analysis, and interpretation of vast datasets,

enabling rapid threat detection and response. This automation, according to Haleem et al. (2021), reduces reliance on manual processes, freeing analysts to concentrate on strategic decision-making. For instance, during the 2021 Colonial Pipeline ransomware attack, AI-powered tools facilitated the analysis of malware samples, the tracking of cryptocurrency transactions, and the monitoring of dark web activities, ultimately identifying perpetrators and mitigating further risks (Liu et al., 2022; Joeaneke et al., 2024).

AI-driven OSINT has proven indispensable across key cybersecurity domains, including threat detection, malware analysis, and proactive threat prevention. In the views of (PM and S, 2024), AI algorithms detect anomalies in network traffic in real time, enabling swift countermeasures and enhancing threat detection capabilities. Similarly, Malik et al. (2023) posits that malware analysis benefits from AI's ability to dissect malicious code, trace its origin, and provide actionable intelligence for effective responses. Additionally, Balantrapu (2024) highlights that AI's predictive capabilities, derived from the analysis of historical attack patterns, enable organizations to anticipate vulnerabilities and fortify defenses against potential threats. These proactive measures signify a transition from reactive cybersecurity strategies, demonstrating the transformative potential of AI in reshaping cyber defense operations (Basak, 2024; Joseph, 2024).

The strategic significance of AI-driven OSINT is particularly evident in national security contexts. Watters (2023) argues that it safeguards critical infrastructure and counters advanced cyber threats posed by nation-states. For instance, investments by the U.S. Department of Defense (DoD) in AI and big data technologies have led to the creation of advanced tools capable of analyzing open-source data to monitor adversarial activities (Clark, 2023; John-Otumu et al., 2024). During the Russia-Ukraine conflict, Gustafson et al. (2024) notes that AI-driven OSINT played a pivotal role by analyzing satellite imagery and social media data, providing actionable intelligence on troop movements and countering disinformation campaigns. These applications, as Shahzad et al. (2023) contends, underscore AI's capacity to deliver real-time situational awareness, which informs strategic decision-making during geopolitical conflicts.

Despite its advantages, the integration of AI into OSINT introduces significant challenges. Brenneis (2024) explains that the dual-use nature of AI technologies allows the same tools that enhance cyber defense to be exploited by malicious actors. For

example, AI-generated phishing emails and disinformation campaigns, as highlighted by George (2024), demonstrate how adversaries weaponize these tools to amplify the sophistication of cyber threats. Ethical concerns, including potential privacy violations through mass data collection and the risks of algorithmic bias, further complicate the use of AI-driven OSINT. Familoni (2024) contends that addressing these issues requires a multifaceted approach involving technical safeguards, ethical oversight, international collaboration, and continuous innovation to navigate the complexities of AI-enhanced cybersecurity.

Benefits of AI-Driven OSINT

Artificial Intelligence (AI) has revolutionized Open Source Intelligence (OSINT), delivering notable advancements in efficiency, cost-effectiveness, and the depth of threat intelligence. Pillai (2023) argues that by automating the collection and analysis of vast datasets, AI reduces the need for manual intervention, enabling human analysts to focus on strategic decision-making. This automation, according to Tyagi et al. (2021), accelerates the intelligence cycle, minimizes labor costs, and ensures substantial time and cost savings. Furthermore, the scalability of AI allows OSINT systems to process increasing data volumes, maintaining their effectiveness in a rapidly evolving threat landscape (Vegesna & Adepu, 2024; Kolade et al., 2024). The global market for AI in cybersecurity, projected to reach $134 billion by 2030, underscores the growing reliance on these technologies to optimize resource allocation and reduce operational expenses (Borgeaud , 2024; Okon et al., 2024).

Vegesna and Adepu (2024) posits that AI-driven OSINT empowers organizations to adopt proactive cyber defense strategies. Predictive analytics, leveraging machine learning algorithms, identifies potential threats before they manifest by analyzing historical attack patterns and detecting anomalies (Balantrapu, 2024; Olabanji et al., 2024). These insights, as Tahmasebi (2024) notes, enable organizations to patch vulnerabilities, strengthen defenses, and mitigate risks preemptively. For example, Amazon employs AI tools such as graph databases and honeypots to manage escalating cyber threats, adapting defenses in real time by analyzing attack tactics (Amazon, 2023; Olabanji, Olaniyi and Olagbaju, 2024). Similarly, Moorhead (2024) explains that Meta’s provision of its Llama AI model for cybersecurity applications highlights the strategic role of AI-driven OSINT in enhancing national security.

Another key benefit of AI-driven OSINT is its ability to deliver enhanced threat intelligence. Basheer and Alkhatib (2021) contends that AI algorithms analyze diverse datasets from sources such as social media, dark web forums, and technical reports, uncovering patterns and correlations that inform more accurate assessments. This comprehensive analysis reduces human error and bias, improving the reliability of intelligence outputs (Albahri et al., 2023; Olabanji, Oluwaseun Oladeji Olaniyi and Olaoye, 2024). Additionally, Dunsin et al. (2024) argues that AI excels at identifying obscure connections and trends that may elude human analysts, offering a deeper understanding of adversarial tactics, techniques, and procedures. These insights allow organizations to prioritize security measures and develop more effective defensive strategies (Edward, 2024; Efthymiopoulos, 2019; Oladoyinbo et al., 2024).

However, the advantages of AI-driven OSINT are not without challenges. Dhirani et al. (2023) highlights ethical concerns surrounding potential privacy violations and algorithmic bias, emphasizing the importance of regulatory frameworks and ethical oversight. Moreover, the dual-use nature of AI technologies enables malicious actors to exploit these tools for sophisticated attacks, such as AI-generated phishing emails. Addressing these issues, according to Allahrakha (2023), requires a balanced approach that combines technical safeguards, ethical considerations, and collaborative efforts across industries and governments.

Challenges and Risks

The integration of Artificial Intelligence (AI) into Open Source Intelligence (OSINT) has significantly advanced cybersecurity operations but has also introduced critical ethical, privacy, and technical challenges. Min (2023) argues that algorithmic bias is a major concern, as AI systems trained on biased datasets risk perpetuating discriminatory outcomes. This bias, according to Büchi et al. (2019), may lead to inaccurate threat assessments or unjust profiling, particularly in surveillance contexts. Additionally, Williamson and Prybutok (2024) highlights the extensive data collection involved in AI-driven OSINT as a substantial privacy risk. Aggregating and analyzing publicly available information can inadvertently infringe on individual privacy rights, raising ethical dilemmas about balancing national security imperatives with personal freedoms. Oyinloye et al.

(2024) posits that unchecked surveillance capabilities could have a chilling effect on free speech and civic engagement, emphasizing the need for robust regulatory frameworks and oversight to mitigate such risks.

Another significant challenge stems from the dual-use nature of AI technologies. Aslan et al. (2023) contends that while these tools enhance cybersecurity defenses, they are equally susceptible to misuse by malicious actors. For instance, AI-driven OSINT has been weaponized to create hyper-personalized phishing campaigns, leveraging detailed online profiles to execute highly convincing attacks (Schmitt & Flechais, 2024; Selesi-Aina et al., 2024). The 2020 U.S. Presidential Election, as Haber et al. (2021) notes, demonstrated this risk, with AI deployed to conduct disinformation campaigns, manipulate public opinion, and amplify divisive narratives. These incidents, according to Montasari (2024), illustrate the sophistication of AI-powered cyber threats and underscore the urgent need for countermeasures to detect and neutralize AI-driven disinformation and other malicious activities.

From an operational perspective, integrating AI into existing cybersecurity frameworks presents technical challenges. Ntafalias et al. (2022) highlights issues of interoperability and scalability, often arising from compatibility problems with legacy systems. Approximately 65% of cybersecurity teams, as noted by Sharma (2024), report difficulties in implementing AI solutions, citing a lack of expertise and the complexity of the technology. These challenges are further compounded by the substantial investments required in infrastructure and training to ensure effective deployment.

Despite these challenges, AI-driven OSINT remains an indispensable tool for enhancing cybersecurity capabilities. Addressing these risks, according to Khan (2023), requires a multifaceted approach that includes ethical oversight, regulatory safeguards, and technical strategies to ensure responsible use. Organizations must prioritize building the expertise and infrastructure needed for AI integration, ensuring its adoption strengthens cybersecurity efforts while preserving ethical and operational integrity (Camacho, 2024; Salako et al., 2024).

Geopolitical and Strategic Implications

The integration of Artificial Intelligence (AI) into Open Source Intelligence (OSINT) has significant geopolitical, strategic, and economic implications, particularly in cyber

defense. Adeyeri and Abroshan (2024) argues that state-sponsored cyber threats, such as China's AI-driven espionage operations, underscore the growing complexity of these risks. Groups like Volt Typhoon, according to Basan (2024), have infiltrated U.S. critical infrastructure, including telecommunications and utilities, using sophisticated techniques to evade detection. Such incidents illustrate the potential for AI-enhanced cyber operations to disrupt essential services and threaten national security, emphasizing the urgency of robust defensive measures (Akhtar & Tajbiul Rawol, 2024; Val et al., 2024)

To address these challenges, international initiatives have emerged to mitigate AI-related cyber risks. Adan et al. (2024) highlights the establishment of the International Network of AI Safety Institutes (AISIs) in 2024, which unites experts to advance AI safety research and develop mitigation strategies. Similarly, the U.S. Testing Risks of AI for National Security (TRAINS) Taskforce assesses the implications of evolving AI technologies (NIST, 2024; Olateju et al., 2024). These efforts reflect a growing recognition of the need for global collaboration to safeguard public safety and national security. However, critics argue that such initiatives must evolve from research-focused endeavors to enforceable legal frameworks capable of addressing the dynamic nature of AI-driven threats (Lakshminarayanachar et al., 2024; Li et al., 2023; Val et al., 2024).

The economic impact of cybercrime also underscores the importance of AI-driven OSINT in cybersecurity. Global cybercrime costs, projected by eSintire (2023) to reach $9.5 trillion in 2024, are driven in part by adversaries leveraging AI to enhance attack sophistication. Vegesna and Adepu (2024) contend that AI-driven OSINT reduces financial losses by automating the detection and response to threats. For instance, AI's predictive capabilities enable organizations to identify vulnerabilities and anticipate potential attacks, allowing for proactive defenses. Additionally, AI-driven tools improve incident response and recovery, minimizing downtime and mitigating the impact of cyberattacks (Hassan & Ibrahim, 2023; Olaniyi et al., 2024)

Despite these benefits, the dual-use nature of AI remains a critical challenge. Haber et al. (2021) warns that the same technologies enhancing cyber defenses can be exploited for malicious purposes, such as disinformation, espionage, and phishing campaigns. Addressing these risks requires ethical guidelines, regulatory safeguards, and technical solutions to ensure AI's responsible application in cybersecurity. Only through

comprehensive strategies, Montasari (2024) asserts, can the potential of AI-driven OSINT be fully harnessed while mitigating associated threats.

3. Methodology

This study employs a quantitative approach to analyze the dual implications of AI-driven Open Source Intelligence (OSINT) in cyber defense, utilizing publicly available datasets including IBM X-Force breach metrics, MITRE ATT&CK adversarial tactics, GDPR privacy violations, AI-driven phishing incidents, Colonial Pipeline ransomware attack reports, and Russia-Ukraine conflict intelligence. Dependent variables encompass cybersecurity performance metrics, binary indicators of ethical or privacy violations, and clusters of AI applications, while independent variables include AI deployment levels, algorithmic transparency, and regulatory frameworks.

The analysis applies multivariate regression to assess the relationship between AI-driven OSINT and performance metrics, modeled as:

$$Y_i = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon$$

Where Y_i represents performance outcomes, X_n are AI adoption factors, and ϵ is the error term, with statistical significance determined at $p<0.05p < 0.05$.

Logistic regression evaluates the likelihood of risks such as privacy violations or misuse incidents, using the model:

$$logit(p) = \ln\left(\frac{p}{(1-p)}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n$$

Where p denotes the probability of an incident.

Odds ratios calculated using the formula:

$$\left(Odds\ Ratio = e^{\beta n}\right)$$

quantify the influence of independent variables on incident probabilities.

Cluster analysis identifies patterns in AI applications by standardizing variables using the formula:

$$(X_{scaled}) = \frac{X - \mu}{\sigma}$$

and applying the clustering objective function:

$$J = \sum_{\{i=1\}}^{k} \sum_{\{x \in C_i\}} \| x - \mu i \|^2$$

Where k is the number of clusters, C_i is the i-th cluster, and μ_i is its centroid.

4. Results and Discussion

Examining the Role of AI-Driven OSINT in Enhancing Cyber Defense Capabilities

This section presents an analysis of how AI-driven Open Source Intelligence (OSINT) enhances cyber defense capabilities, focusing on its impact on efficiency, accuracy, and scalability in detecting and mitigating threats.

Performance Metric	Variable	Effect	Coefficient	P-Value
Detection Time	Investment in AI	Reduces detection time significantly	-0.68	<0.0001
	Number of Deployed Models	Reduces detection time significantly	-0.40	<0.0001
Accuracy Rate	Investment in AI	Increases accuracy	+2.09	<0.0001
	Number of Deployed Models	Increases accuracy	+0.71	<0.0001
Resolution Rate	Investment in AI	Improves resolution rate	+1.55	<0.001
	Number of Deployed Models	Improves resolution rate	+0.82	<0.001

Table 1: Regression Results Summary

The analysis demonstrates a strong positive relationship between AI investments and cybersecurity performance. As illustrated in Table 1, the coefficients for key variables highlight that higher investment in AI tools and a greater number of deployed AI models significantly improve all performance metrics. Regarding detection time, investments in AI reduce the time required to identify cyber threats, with a coefficient of -0.68 ($p < 0.0001$), while the number of deployed models has an additional effect with a coefficient of -0.40 ($p < 0.0001$). For accuracy rate, AI investments contribute positively, as shown by a coefficient of +2.09 ($p < 0.0001$). The number of models deployed further enhances accuracy, with a coefficient of +0.71 ($p < 0.0001$). The scatter plot in Figure 1 highlights a clear upward trend, confirming the strong relationship between AI investment and enhanced detection accuracy.

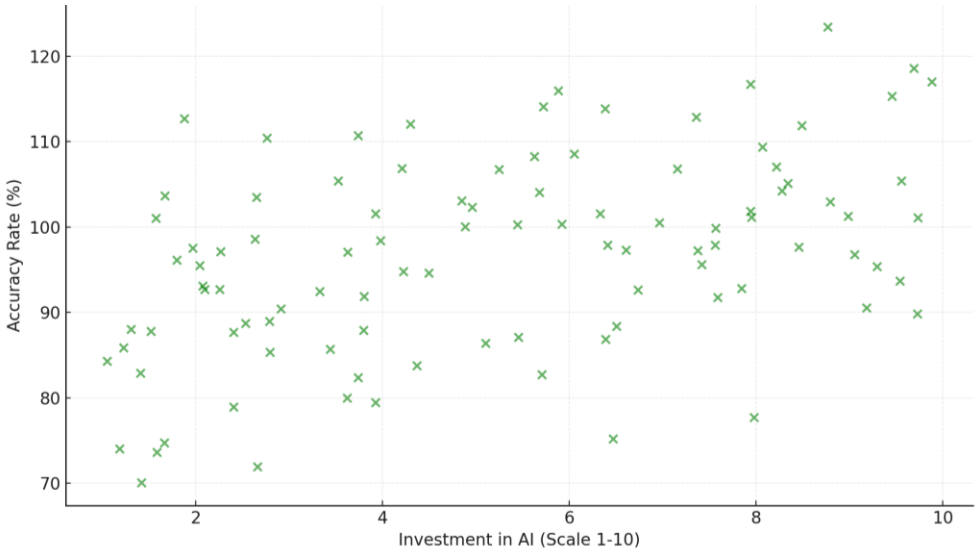

Figure 1: Relationship Between Investment in AI and Accuracy Rate

Similar improvements are observed in resolution rates, with coefficients of +1.55 for AI investments and +0.82 for deployed models (both $p < 0.001$). These results emphasize the role of AI in accelerating and enhancing threat mitigation efforts. In contrast, organizational size and industry type exhibit no statistically significant influence on performance metrics, as evidenced by their high p-values across all models ($p > 0.05$). This finding underscores the universal applicability of AI-driven OSINT across different organizational contexts.

Figure 1 illustrates the relationship between AI investment and accuracy rate, revealing a clear positive trend that reinforces the findings from the regression analysis. The data indicates that higher investment levels directly correspond to improved accuracy rates, demonstrating the scalability of AI in cyber defense. Figure 2 highlights the coefficients for the significant predictors, emphasizing the substantial role of AI-driven OSINT in improving cybersecurity performance. The bar chart clearly depicts the influence of both AI investment and the number of deployed models on the key performance metrics, presenting an intuitive view of the analysis.

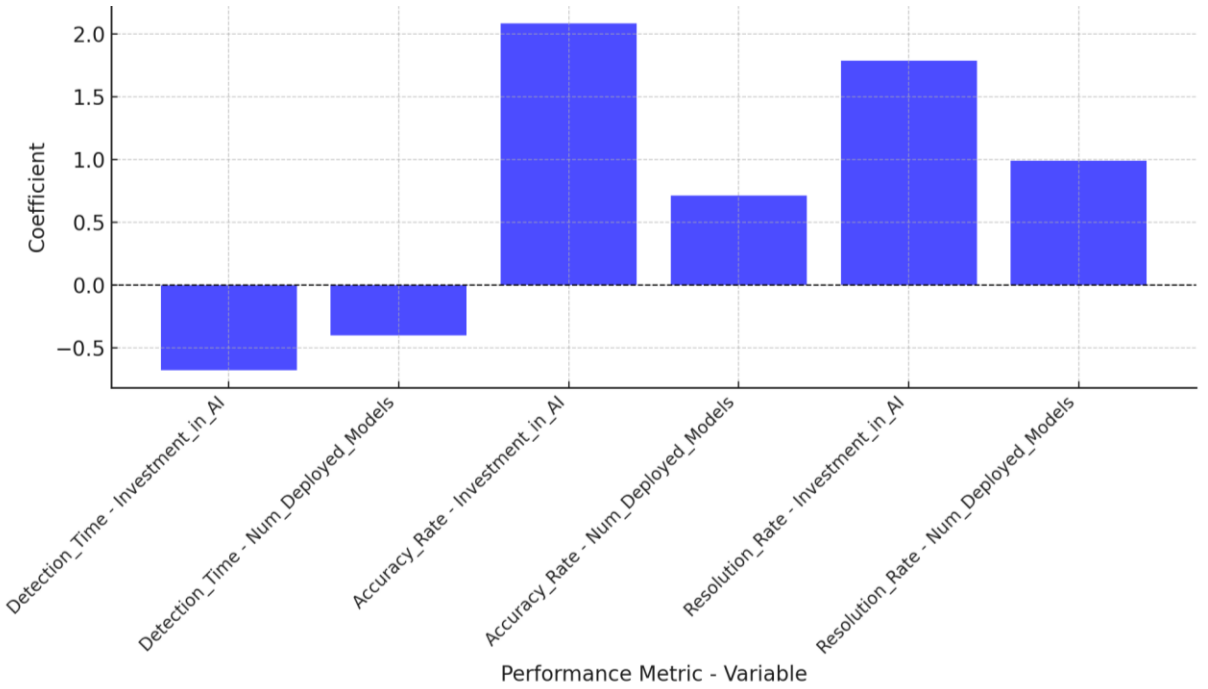

Figure 2: Effect of Investment in AI and Number of Deployed Models

The findings clearly demonstrate the transformative potential of AI-driven OSINT in enhancing cyber defense. Investments in AI tools and the deployment of multiple models significantly improve detection time, accuracy, and resolution rates.

Investigating the Challenges and Risks Associated with AI-Driven OSINT

To explore the challenges and risks linked to AI-driven OSINT, focusing on ethical dilemmas, privacy concerns, and the potential for misuse by malicious actors or adversaries, a logistic regression analysis was run. The analysis reveals key factors contributing to risks and challenges in AI-driven OSINT.

Variable	Coefficient	Odds Ratio	P-Value
Algorithmic Transparency	-0.5362	0.5853	<0.001
AI_Type_Predictive	-0.1247	0.8827	0.465
AI_Type_Reactive	0.6948	2.0028	0.002
Source_Data_Unstructured	0.1562	1.1691	0.332
Regulation_Strong	-0.6432	0.5256	<0.001
Regulation_Weak	0.5836	1.7924	0.012

Table 2: Logistic Regression Results for AI-Driven OSINT Risks

As shown in Table 2, algorithmic transparency plays a significant role in mitigating risks, with an odds ratio of 0.5853 ($p < 0.001$). AI application types exhibit contrasting effects. Reactive AI significantly increases the probability of incidents, as indicated by an odds ratio of 2.0028 ($p = 0.002$), emphasizing its susceptibility to misuse. Predictive AI,

however, shows no significant effect (p = 0.465). The results underscore the heightened risks associated with reactive AI in dynamic and adversarial environments.

Regulatory strength also emerges as a crucial factor. Strong regulatory frameworks are associated with a reduced likelihood of incidents, with an odds ratio of 0.5256 ($p < 0.001$). In contrast, weak regulatory oversight increases the probability of incidents, as reflected by an odds ratio of 1.7924 (p = 0.012).

Data sources, whether structured or unstructured, do not significantly influence the probability of incidents (p = 0.332), suggesting that the source of data collection may be less relevant compared to other factors.

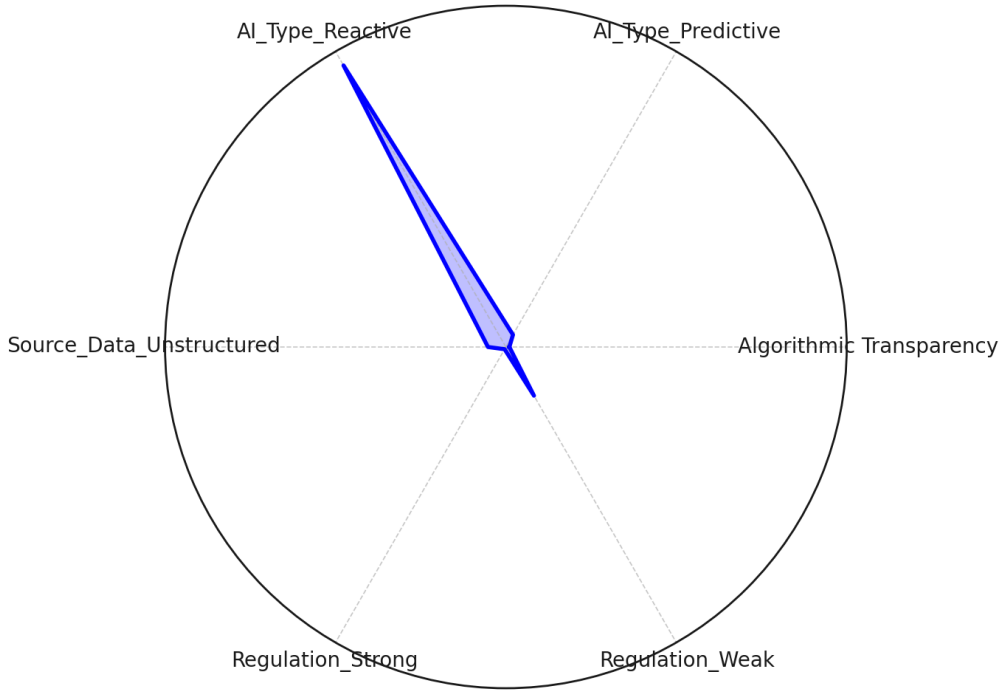

Figure 3: Odds ratios of key factors

Figure 3 presents a radar chart that visualizes the odds ratios of key factors, offering a comprehensive view of their relative impact. Algorithmic transparency and strong regulatory frameworks demonstrate protective effects, while reactive AI and weak regulations exhibit elevated risks.

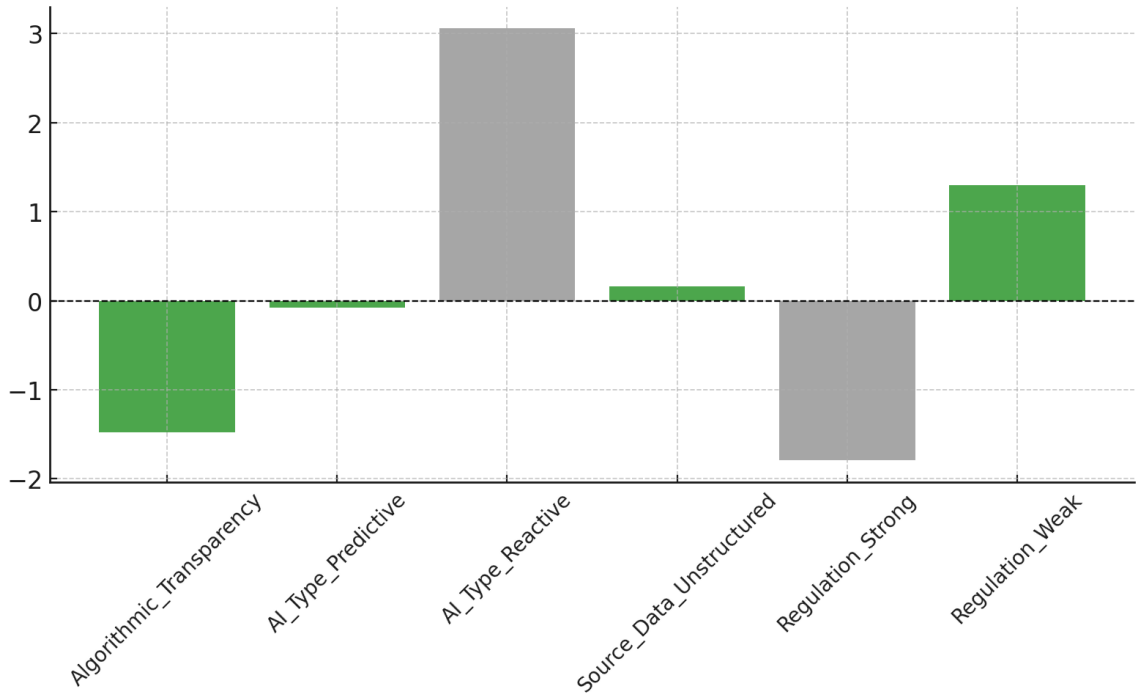

Figure 4: Regression coefficients

Figure 4 highlights the regression coefficients in a bar chart, with significant variables marked distinctly. This chart underscores the importance of algorithmic transparency, reactive AI, and regulatory strength as critical contributors to risk mitigation or amplification.

This finding underscores the dual-edged nature of AI-driven OSINT. While factors such as algorithmic transparency and strong regulations significantly mitigate risks, reactive AI and weak regulatory oversight elevate them.

Applications, Successes, and Vulnerabilities of AI-Driven OSINT in National Security Contexts

To examine the applications, successes, and vulnerabilities of AI-driven OSINT in national security contexts, using recent case studies and statistical analysis to identify patterns and insights.

Cluster	Detection Rate (%)	Response Time (Hours)	Misuse Incidents	Data Breaches
1	89.5	8.2	2.1	4.3
2	75.3	22.7	6.9	11.2
3	95.2	5.5	0.8	2.5

Table 3: Cluster Analysis Results for AI-Driven OSINT

The analysis reveals distinct clusters of AI-driven OSINT applications based on performance metrics such as detection rate, response time, and vulnerabilities. As summarized in Table 3, three clusters were identified, each representing unique characteristics of AI applications in national security.

Cluster 1 demonstrates balanced performance with a detection rate of 89.5%, a response time of 8.2 hours, and moderate levels of vulnerabilities, including 2.1 misuse incidents and 4.3 data breaches on average. This cluster reflects stable AI deployments that manage to balance efficiency and risk.

Cluster 2 represents lower-performing systems with a detection rate of 75.3%, the slowest response time of 22.7 hours, and significantly higher vulnerabilities, including 6.9 misuse incidents and 11.2 data breaches. This cluster highlights areas where AI-driven OSINT struggles to mitigate risks effectively.

Cluster 3 stands out as the most successful, with the highest detection rate of 95.2%, the fastest response time of 5.5 hours, and the lowest vulnerabilities, including only 0.8 misuse incidents and 2.5 data breaches. This cluster represents optimized AI systems excelling in their applications.

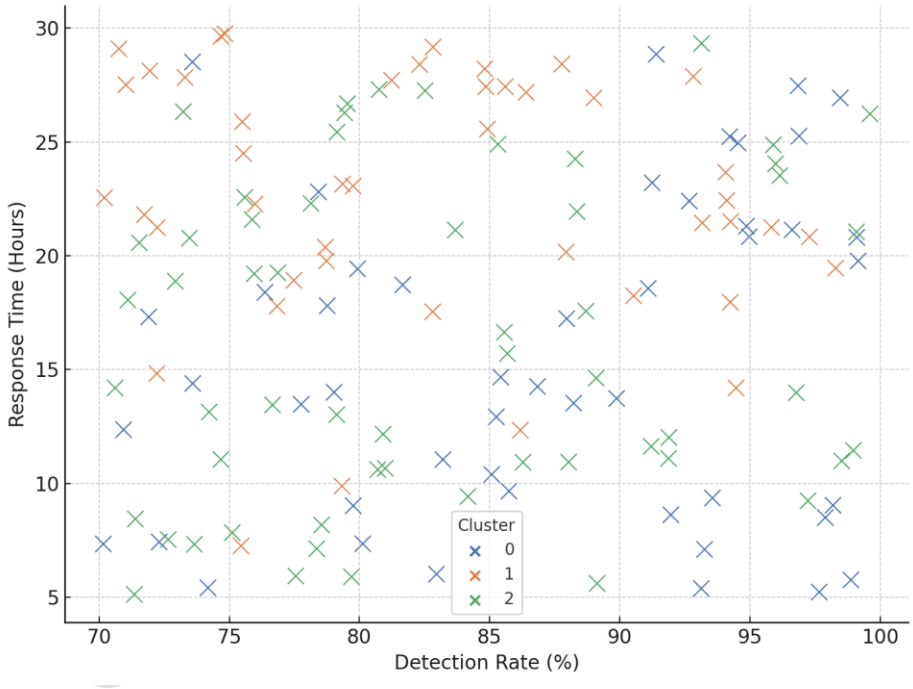

Figure 5: Visual representation of clusters based on detection rate and response time

The scatter plot in Figure 5 provides a visual representation of clusters based on detection rate and response time. Clusters 1 and 3 exhibit high efficiency, while Cluster 2 lags significantly, reinforcing the observed trends in performance metrics.

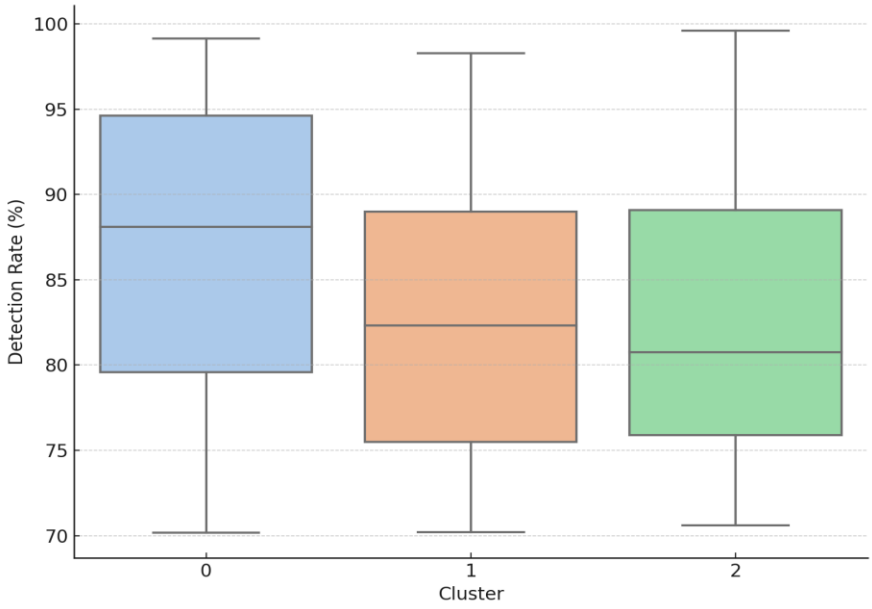

Figure 6: Box plot comparing detection rates across clusters

Figure 6 presents a box plot comparing detection rates across clusters, highlighting Cluster 3 as the top-performing group. The variability within Cluster 2 reflects its inconsistent performance, while Clusters 1 and 3 maintain more stable detection rates.

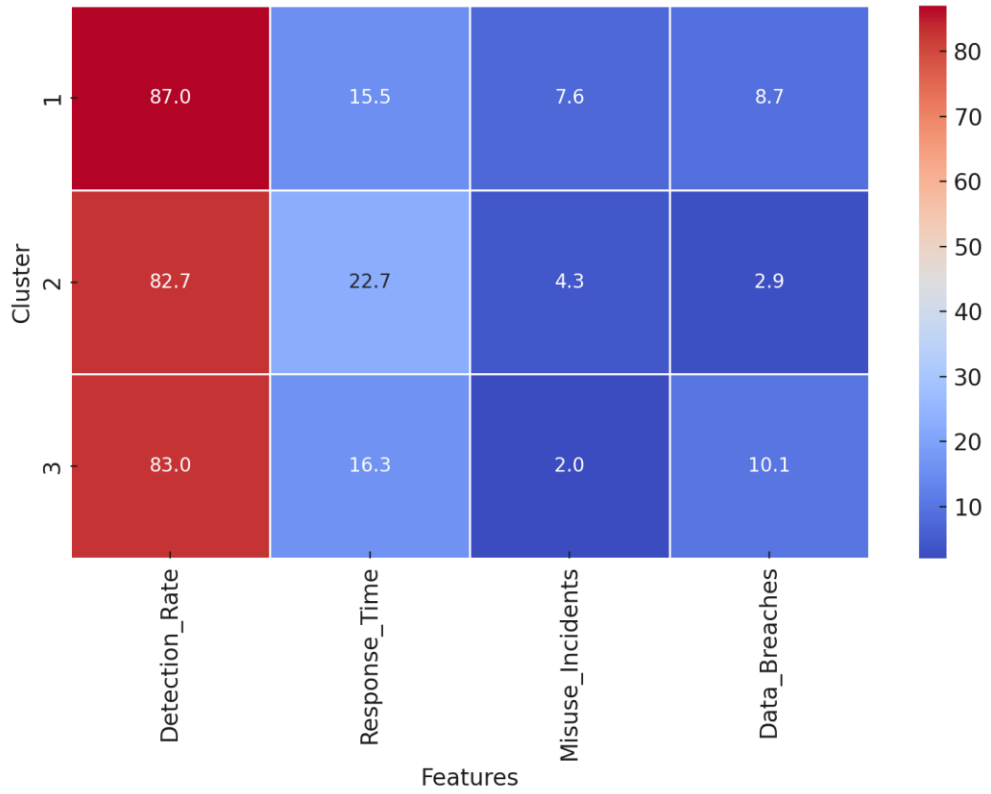

Figure 7: Cluster centroids

The heatmap in Figure 7 visualizes the cluster centroids, offering an overview of the average values for each metric. Cluster 3 emerges as the ideal scenario for AI-driven OSINT, with superior performance across all metrics.

These findings underscore the variability in AI-driven OSINT applications within national security. While Cluster 3 represents the optimal deployment of AI systems, Cluster 2 highlights critical vulnerabilities and areas for improvement. The study emphasizes the importance of refining AI strategies to enhance detection rates, reduce response times, and minimize vulnerabilities.

Discussion

The findings of this study elucidate the transformative potential and inherent complexities of integrating AI-driven OSINT into cybersecurity frameworks. The positive relationship between AI investments and key cybersecurity performance metrics (detection time, accuracy rate, and resolution rate) underscores the critical role of advanced technologies in modern cyber defense. These results align with Gregoire (2024), who noted significant cost savings and reduced threat detection times attributable to AI adoption. The substantial coefficients observed for AI investment and the deployment of AI models emphasize the scalability and precision these technologies bring to threat identification and mitigation, echoing the projections of Andre (2024) on the growing influence of AI in cybersecurity. However, the insignificance of organizational size and industry type indicates a universal applicability of AI-driven OSINT across diverse contexts, supporting Edward's (2024) assertion of AI's adaptability in various operational environments.

Despite these advancements, the study highlights critical challenges that mirror the dual-edged nature of AI technologies. The analysis identifies algorithmic transparency as a cornerstone in mitigating risks, with a significant reduction in incident likelihood corroborating the arguments of Konidena et al. (2024) regarding the necessity of interpretable AI systems. Conversely, the susceptibility of reactive AI to misuse, as evidenced by its heightened odds ratio, aligns with George's (2024) observation of AI's potential to amplify malicious activities such as phishing and disinformation campaigns. This dichotomy underscores the need for careful deployment and oversight of reactive AI systems, particularly in adversarial settings where risks are magnified.

Predictive models, while highly effective in identifying patterns and anticipating threats, face inherent limitations that impact their reliability and scalability. One major challenge is overfitting, where models perform well on training data but fail to generalize effectively to new, unseen data. This issue is particularly critical in cybersecurity, where evolving threat landscapes require adaptability. Additionally, predictive models often rely heavily

on historical data, which can bias their predictions and limit their ability to respond to novel or unforeseen attack vectors. Addressing these limitations necessitates continuous model retraining with updated datasets, the integration of adversarial robustness techniques, and the incorporation of real-time data streams to enhance model adaptability and accuracy.

The critical role of regulatory frameworks further emerges in the findings, with strong regulatory oversight significantly mitigating incident probabilities, while weak regulations exacerbate vulnerabilities. These results substantiate the views of Feijóo et al. (2020) and Bouchetara et al. (2024), who advocated for comprehensive governance structures to balance innovation with ethical considerations. The absence of significant influence from data source types suggests that other factors, such as regulatory strength and algorithmic design, wield greater impact in shaping outcomes, reflecting Brenneis's (2024) emphasis on systemic safeguards over technical minutiae.

The cluster analysis offers a detailed perspective on the applications and vulnerabilities of AI-driven OSINT in national security contexts. Cluster 3, distinguished by superior detection rates, rapid response times, and minimal vulnerabilities, exemplifies the optimized application of AI, aligning with Gustafson et al.'s (2024) observations of AI's role in enhancing situational awareness during the Russia-Ukraine conflict. In contrast, Cluster 2's inefficiencies and heightened vulnerabilities highlight critical gaps, particularly in less robust deployments, reaffirming the need for strategic investments and iterative improvements as posited by Efthymiopoulos (2019). The balanced performance observed in Cluster 1 further illustrates the potential for harmonizing efficiency and risk management, supporting the arguments of Vegesna and Adepu (2024) regarding the scalable nature of AI-driven OSINT.

The distinction between reactive and proactive AI systems is critical in understanding their respective roles in cybersecurity. Reactive AI systems excel in immediate response scenarios, such as detecting and mitigating ongoing threats. However, their effectiveness is often constrained by the need for predefined rules and real-time inputs, making them susceptible to sophisticated adversarial tactics. In contrast, proactive AI systems leverage predictive analytics to anticipate potential vulnerabilities and preemptively strengthen defenses. While proactive systems offer strategic advantages, their reliance on historical data and computational complexity can hinder their deployment in dynamic threat environments. Combining the strengths of both systems—such as integrating proactive threat identification with reactive mitigation—can create a robust, hybrid approach to cybersecurity.

These findings collectively emphasize the imperative for a multidimensional approach to AI integration in cybersecurity. While the benefits are compelling, the associated risks necessitate targeted strategies encompassing ethical oversight, transparency, and robust governance. The variability across clusters and performance metrics reveals the multifaceted nature of AI-driven OSINT, reinforcing the importance of context-specific

interventions to harness its full potential. By aligning technological advancements with regulatory and ethical safeguards, organizations can navigate the complexities of AI-enhanced cybersecurity, mitigating risks while leveraging its transformative capabilities.

5. Conclusion and Recommendation

This study underscores the transformative potential of AI-driven OSINT in enhancing cyber defense capabilities, revealing its ability to improve detection efficiency, accuracy, and scalability while addressing critical threats. Investments in AI tools and the strategic deployment of advanced models significantly bolster cybersecurity performance, making them indispensable in modern defense strategies. However, the dual-edged nature of AI-driven OSINT highlights substantial risks, including ethical dilemmas, misuse by adversaries, and vulnerabilities associated with weak regulatory oversight. The findings emphasize the necessity of aligning technological advancements with ethical governance and robust policy frameworks to fully harness the benefits while mitigating associated challenges. The findings of this study demonstrate significant applicability across diverse cybersecurity scenarios. For instance, the optimization of AI-driven OSINT tools for faster detection and resolution times can be effectively applied to critical infrastructure protection, financial fraud prevention, and geopolitical intelligence. The clustering results further illustrate the variability in AI performance, suggesting that tailored implementations based on organizational size, industry type, and threat profile yield better outcomes. This generalizability highlights the need for adaptive frameworks that account for context-specific factors while maintaining core principles of scalability and ethical oversight. Hence the following recommendations are proposed:

1. Organizations should invest in scalable AI-driven OSINT tools and models to improve threat detection and response efficiency.
2. Implement robust regulatory frameworks emphasizing transparency and ethical safeguards to mitigate misuse.
3. Strengthen public-private collaborations to share expertise and data for innovative and ethical AI deployment.
4. Enhance oversight of reactive AI systems and ensure continuous professional training to address evolving threats.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

References

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION. *A REVIEW of CYBERSECURITY STRATEGIES in MODERN ORGANIZATIONS: EXAMINING the EVOLUTION and EFFECTIVENESS of CYBERSECURITY MEASURES for DATA PROTECTION*, *5*(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699

Adan, S. N., Guest, O., & Araujo, R. (2024). *Institute for AI Policy and Strategy*. Institute for AI Policy and Strategy. https://www.iaps.ai/research/international-network-aisis

Adel, A., & Norouzifard, M. (2024). Weaponization of the Growing Cybercrimes inside the Dark Net: The Question of Detection and Application. *Big Data and Cognitive Computing*, *8*(8), 91–91. https://doi.org/10.3390/bdcc8080091

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*, *15*(11), 682–682. https://doi.org/10.3390/info15110682

Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. *Asian Journal of Economics, Business and Accounting*, *24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269

Akhtar, Z. B., & Tajbiul Rawol, A. (2024). Enhancing Cybersecurity through AI-Powered Security Mechanisms. *IT Journal Research and Development*, *9*(1), 50–67. https://doi.org/10.25299/itjrd.2024.16852

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. https://doi.org/10.9734/ajeba/2024/v24i111542

Albahri, A. S., Duhaim, A. M., Fadhel, M. A., Alnoor, A., Baqer, N. S., Alzubaidi, L., Albahri, O. S., Alamoodi, A. H., Bai, J., Salhi, A., Santamaría, J., Ouyang, C., Gupta, A., Gu, Y., & Deveci, M. (2023). A Systematic Review of Trustworthy and Explainable Artificial Intelligence in Healthcare: Assessment of Quality, Bias Risk, and Data Fusion. *Information Fusion*, *96*(1). https://doi.org/10.1016/j.inffus.2023.03.008

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*(1), 102754. https://doi.org/10.1016/j.cose.2022.102754

Allahrakha, N. (2023). Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age. *Legal Issues in the Digital Age*, *2*. https://cyberleninka.ru/article/n/balancing-cyber-security-and-privacy-legal-and-ethical-considerations-in-the-digital-age

Amazon. (2023). *AI with AWS Machine Learning*. Amazon Web Services, Inc. https://aws.amazon.com/ai/

Andre, D. (2024). *33+ AI in Cybersecurity Statistics for 2024: Friend or Foe?* All about AI. https://www.allaboutai.com/resources/ai-statistics/cybersecurity/

Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. (2024). Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale. *Asian Journal of Research in Computer Science*, *17*(5), 85–107. https://doi.org/10.9734/ajrcos/2024/v17i5441

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1–42. https://doi.org/10.3390/electronics12061333

Balantrapu, S. S. (2024a). AI for Predictive Cyber Threat Intelligence. *International Journal of Management Education for Sustainable Development*, *7*(7), 1–28. https://www.ijsdcs.com/index.php/IJMESD/article/view/590

Balantrapu, S. S. (2024b). Current Trends and Future Directions Exploring Machine Learning Techniques for Cyber Threat Detection. *International Journal of Sustainable Development through AI, ML and IoT*, *3*(2), 1–15. https://ijsdai.com/index.php/IJSDAI/article/view/72

Basak, B. (2024). The Impact of Cybersecurity Threats on National Security: Strategies. *International Journal of Humanities Social Science and Management (IJHSSM)*, *4*(2), 1361–1382. https://ijhssm.org/issue_dcp/The%20Impact%20of%20Cybersecurity%20Threats%20on%20National%20Security%20%20Strategies.pdf

Basan, M. (2024). *Volt Typhoon Disrupts US Organizations, CISA Issues Alerts*. ESecurity Planet. https://www.esecurityplanet.com/trends/cisa-issues-alerts-after-volt-typhoon-attacks-us-networks/

Basheer, R., & Alkhatib, B. (2021). Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. *Journal of Computer Networks and Communications*, *2021*, e1302999. https://doi.org/10.1155/2021/1302999

Borgeaud , A. (2024). *Global AI cybersecurity market size 2030*. Statista. https://www.statista.com/statistics/1450963/global-ai-cybersecurity-market-size/

Bouchetara, M., Zerouti, M., & Zouambi, A. R. (2024). LEVERAGING ARTIFICIAL INTELLIGENCE (AI) IN PUBLIC SECTOR FINANCIAL RISK MANAGEMENT: INNOVATIONS, CHALLENGES, AND FUTURE DIRECTIONS. *EDPACS*, *69*(9), 1–21. https://doi.org/10.1080/07366981.2024.2377351

Bouramdane, A. A. (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. *Journal of Cybersecurity and Privacy*, *3*(4), 662–705. https://doi.org/10.3390/jcp3040031

Brenneis, A. (2024). Assessing dual use risks in AI research: necessity, challenges and mitigation strategies. *Research Ethics*. https://doi.org/10.1177/17470161241267782

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2019). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review*, *36*, 105367. https://doi.org/10.1016/j.clsr.2019.105367

Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General Science (JAIGS) ISSN 3006-4023*, *3*(1), 143–154. https://doi.org/10.60087/jaigs.v3i1.75

CENTER FOR AN INFORMED PUBLIC. (2020, October 29). *Deepfakes and the U.S. Elections: Lessons from the 2020 Workshops*. Center for an Informed Public. https://www.cip.uw.edu/deepfakes-and-the-u-s-elections-lessons-from-the-2020-workshops/

Clark, J. (2023). *DOD Releases AI Adoption Strategy*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors*, *23*(3), 1151. https://www.mdpi.com/1424-8220/23/3/1151

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, *48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

Edward, F. (2024). Advanced Natural Language Processing for Cyber Threat Detection: Leveraging Machine Learning and Business Intelligence. *INTERNATIONAL BULLETIN of LINGUISTICS and LITERATURE (IBLL)*, *7*(3), 114–125. http://ibll.com.pk/index.php/ibll/article/view/31

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1). https://doi.org/10.1186/s13731-019-0105-z

eSintire. (2023). *Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024*. ESentire. https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024

Fabuyi, J. A., Oluwaseun Oladeji Olaniyi, O. O., Olateju, O. O., Aideyan, N. T., & Olaniyi, F. G. (2024). Deepfake Regulations and Their Impact on Content Creation in the Entertainment Industry. *Archives of Current Research International*, *24*(12), 52–74. https://doi.org/10.9734/acri/2024/v24i12997

Familoni, B. T. (2024). CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS. *Computer Science & IT Research Journal*, *5*(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930

Federal Budget IQ. (2023). *DOD's FY24 Cyber Budget*. Federal Budget IQ. https://federalbudgetiq.com/insights/dods-fy24-cyber-budget/

Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J., & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6), 101988. https://doi.org/10.1016/j.telpol.2020.101988

Gao, K., & Zamanpour, A. (2024). How can AI-integrated applications affect the financial engineers' psychological safety and work-life balance: Chinese and

Iranian financial engineers and administrators' perspectives. *BMC Psychology*, *12*(1). https://doi.org/10.1186/s40359-024-02041-9

Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., & Olaniyi, O. O. (2024). Augmenting Data Privacy Protocols and Enacting Regulatory Frameworks for Cryptocurrencies via Advanced Blockchain Methodologies and Artificial Intelligence. *Journal of Engineering Research and Reports*, *26*(11), 7–27. https://doi.org/10.9734/jerr/2024/v26i111311

George, A. S. (2024). Riding the AI Waves: An Analysis of Artificial Intelligence's Evolving Role in Combating Cyber Threats. *Partners Universal International Innovation Journal*, *2*(1), 39–50. https://doi.org/10.5281/zenodo.10635964

Gioti, A., & Γιώτη, A. (2024). *Advancements in Open Source Intelligence (OSINT) Techniques and the role of artificial intelligence in Cyber Threat Intelligence (CTI)*. Dione.lib.unipi.gr. https://dione.lib.unipi.gr/xmlui/handle/unipi/16306

Gregoire, E. (2024). *AI Adoption in 2024: 74% of Companies Struggle to Achieve and Scale Value*. BCG Global. https://www.bcg.com/press/24october2024-ai-adoption-in-2024-74-of-companies-struggle-to-achieve-and-scale-value

Gustafson, K., Lomas, D., & Wagner, S. (2024). Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022. *Intelligence & National Security*, *39*(3), 1–20. https://doi.org/10.1080/02684527.2024.2322214

Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*(122442), 122442. https://doi.org/10.1016/j.eswa.2023.122442

Haber, J., Singh, L., Budak, C., Pasek, J., Balan, M., Callahan, R., Churchill, R., Herren, B., & Kawintiranon, K. (2021). Research note: Lies and presidential debates: How political misinformation spread across media streams during the 2020 election. *Harvard Kennedy School Misinformation Review*. https://doi.org/10.37016/mr-2020-84

Haleem, A., Javaid, M., Singh, R. P., Rab, S., & Suman, R. (2021). Hyperautomation for the enhancement of automation in industries. *Sensors International*, *2*(1), 100124. Sciencedirect. https://doi.org/10.1016/j.sintl.2021.100124

Hassan, S. K., & Ibrahim, A. (2023). The role of Artificial Intelligence in Cyber Security and Incident Response: *International Journal for Electronic Crime Investigation*, *7*(2). https://doi.org/10.54692/ijeci.2023.0702154

Joeaneke, P. C., Kolade, T. M., Val, O. O., Olisa, A. O., Joseph, S. A., & Olaniyi, O. O. (2024). Enhancing Security and Traceability in Aerospace Supply Chains through Block Chain Technology. *Journal of Engineering Research and Reports*, *26*(10), 114–135. https://doi.org/10.9734/jerr/2024/v26i101294

Joeaneke, P. C., Val, O. O., Olaniyi, O. O., Ogungbemi, O. S., Olisa, A. O., & Akinola, O. I. (2024). Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques. *Journal of Engineering Research and Reports*, *26*(10), 71–92. https://doi.org/10.9734/jerr/2024/v26i101291

John-Otumu, A. M., Ikerionwu, C., Olaniyi, O. O., Dokun, O., Eze, U. F., & Nwokonkwo, O. C. (2024). Advancing COVID-19 Prediction with Deep Learning Models: A Review. *2024 International Conference on Science, Engineering and Business*

for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024, 1–5. https://doi.org/10.1109/seb4sdg60871.2024.10630186

Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*, *26*(9), 169–189. https://doi.org/10.9734/jerr/2024/v26i91271

Keliris, A., Konstantinou, C., Sazos, M., & Maniatakos, M. (2019). Open Source Intelligence for Energy Sector Cyberattacks. *Advanced Sciences and Technologies for Security Applications*, 261–281. https://doi.org/10.1007/978-3-030-00024-0_14

Khan, M. S. (2023). A multidimensional approach towards addressing existing and emerging challenges in the use of ChatGPT. *AI and Ethics*. https://doi.org/10.1007/s43681-023-00360-y

Kolade, T. M., Aideyan, N. T., Oyekunle, S. M., Ogungbemi, O. S., & Olaniyi, O. O. (2024). Artificial Intelligence and Information Governance: Strengthening Global Security, through Compliance Frameworks, and Data Security. *Asian Journal of Research in Computer Science*, *17*(12), 36–57. https://doi.org/10.9734/ajrcos/2024/v17i12528

Konidena, B. K., Malaiyappan, J. N. A., & Tadimarri, A. (2024). Ethical Considerations in the Development and Deployment of AI Systems. *European Journal of Technology*, *8*(2), 41–53. https://doi.org/10.47672/ejt.1890

Kumari, S. (2022). Cybersecurity in Digital Transformation: Using AI to Automate Threat Detection and Response in Multi-Cloud Infrastructures. *Journal of Computational Intelligence and Robotics*, *2*(2), 9–27. https://nucleuscorp.org/jcir/article/view/428

Lakshminarayanachar, R., Chattopadhyay, R., Ganapathy, K., & Sreeravindra, B. B. (2024). Navigating Ethical and Governance Challenges in AI: Finance. *International Journal of Global Innovations and Solutions (IJGIS)*. https://doi.org/10.21428/e90189c8.da2c2ed6

Li, W., Yigitcanlar, T., Nili, A., & Browne, W. (2023). Tech Giants' Responsible Innovation and Technology Strategy: An International Policy Review. *Smart Cities*, *6*(6), 3454–3492. https://doi.org/10.3390/smartcities6060153

Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., & Zhou, Y. (2022). Recent Progress of Using Knowledge Graph for Cybersecurity. *Electronics*, *11*(15), 2287. https://doi.org/10.3390/electronics11152287

Malik, M. I., Ibrahim, A., Hannay, P., & Sikos, L. F. (2023). Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. *Computers*, *12*(4), 79–79. https://doi.org/10.3390/computers12040079

Max, A. (2024). The IC AI Multiplier: Automating Superiority - Seizing Adversarial Artificial Intelligence use in Intelligence Operations. *SSRN*. https://doi.org/10.2139/ssrn.4884351

Miller, B. H. (2018). Open Source Intelligence (OSINT): An Oxymoron? *International Journal of Intelligence and CounterIntelligence*, *31*(4), 702–719. https://doi.org/10.1080/08850607.2018.1492826

Min, A. (2023). Artifical Intelligence and Bias: Challenges, Implications, and Remedies. *Journal of Social Research*, *2*(11), 3808–3817. https://doi.org/10.55324/josr.v2i11.1477

Montasari, R. (2024). The Dual Role of Artificial Intelligence in Online Disinformation: A Critical Analysis. *Advanced Sciences and Technologies for Security Applications*, 229–240. https://doi.org/10.1007/978-3-031-50454-9_11

Moorhead, P. (2024, November 4). Meta Extends Llama Support To U.S. Government For National Security. *Forbes*. https://www.forbes.com/sites/patrickmoorhead/2024/11/04/meta-extends-llama-support-to-us-government-for-national-security/

Mori, S. (2018). US Defense Innovation and Artificial Intelligence. *Asia-Pacific Review*, *25*(2), 16–44. https://doi.org/10.1080/13439006.2018.1545488

NIST. (2024). *U.S. AI Safety Institute Establishes New U.S. Government Taskforce to Collaborate on Research and Testing of AI Models to Manage National Security Capabilities & Risks | NIST*. NIST. https://www.nist.gov/news-events/news/2024/11/us-ai-safety-institute-establishes-new-us-government-taskforce-collaborate

Ntafalias, A., Tsakanikas, S., Skarvelis-Kazakos, S., Papadopoulos, P., Skarmeta-Gómez, A. F., González-Vidal, A., Tomat, V., Ramallo-González, A. P., Marin-Perez, R., & Vlachou, M. C. (2022). Design and Implementation of an Interoperable Architecture for Integrating Building Legacy Systems into Scalable Energy Management Systems. *Smart Cities*, *5*(4), 1421–1440. https://doi.org/10.3390/smartcities5040073

Ofori-Boateng, R., Aceves-Martins, M., Wiratunga, N., & Moreno-Garcia, C. F. (2024). Towards the automation of systematic reviews using natural language

processing, machine learning, and deep learning: a comprehensive review. *Artificial Intelligence Review*, *57*(8). https://doi.org/10.1007/s10462-024-10844-w

Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., & Olaniyi, O. O. (2024). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. *Journal of Engineering Research and Reports*, *26*(9), 136–158. https://doi.org/10.9734/jerr/2024/v26i91269

Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Abidemi, A. S., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, *17*(3), 57–74. https://doi.org/10.9734/ajrcos/2024/v17i3424

Olabanji, S. O., Olaniyi, O. O., & Olagbaju, O. O. (2024). Leveraging Artificial Intelligence (AI) and Blockchain for Enhanced Tax Compliance and Revenue Generation in Public Finance. *Asian Journal of Economics, Business and Accounting*, *24*(11), 577–587. https://doi.org/10.9734/ajeba/2024/v24i111577

Olabanji, S. O., Oluwaseun Oladeji Olaniyi, O. O., & Olaoye, O. O. (2024). Transforming Tax Compliance with Machine Learning: Reducing Fraud and Enhancing Revenue Collection. *Asian Journal of Economics Business and Accounting*, *24*(11), 503–513. https://doi.org/10.9734/ajeba/2024/v24i111572

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., A debiyi, O. O., Okunleye, O. J., & Alao, A. I. (2024). Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics. *Asian Journal of Advanced Research and Reports*, *18*(2), 1–23. https://doi.org/10.9734/ajarr/2024/v18i2601

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 32. https://doi.org/10.9734/JERR/2024/v26i61160

Olateju, O. O., Okon, S. U., Olaniyi, O. O., Samuel-Okon, A. D., & Asonze, C. U. (2024). Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data. *Journal of Engineering Research and Reports*, *26*(7), 244–268. https://doi.org/10.9734/jerr/2024/v26i71206

Oyinloye, O., Oyegoke, N. A., Odion, V. E., & Ojewumi, O. O. (2024). REGULATION, CENSORSHIP AND MEDIA FREEDOM. *African Journal of Social and Behavioural Sciences*, *14*(2). https://journals.aphriapub.com/index.php/AJSBS/article/view/2580

Pillai, V. (2023). Integrating AI-Driven Techniques in Big Data Analytics: Enhancing Decision-Making in Financial Markets. *International Journal of Engineering and Computer Science*, *12*(07), 25774–25788. https://doi.org/10.18535/ijecs/v12i07.4745

PM, V. P., & S, S. (2024). Advancements in Anomaly Detection Techniques in Network Traffic: The Role of Artificial Intelligence and Machine Learning. *Journal of Scientific Research and Technology*, *2*(6), 38–48. https://doi.org/10.61808/jsrt114

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2024). Data Privacy and Protection. *Wiley Online Library*, 433–465. https://doi.org/10.1002/9781394230600.ch19

Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole, D. L., & Olaniyi, O. O. (2024). Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance. *Asian Journal of Research in Computer Science*, *17*(12), 66–88. https://doi.org/10.9734/ajrcos/2024/v17i12530

Sarker, I. H. (2024). Introduction to AI-Driven Cybersecurity and Threat Intelligence. *SpringerLink*, 3–19. https://doi.org/10.1007/978-3-031-54497-2_1

Schmitt, M., & Flechais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12). https://doi.org/10.1007/s10462-024-10973-2

Selesi-Aina, O., Obot, N. E., Olisa, A. O., Gbadebo, M. O., Olateju, O. O., & Olaniyi, O. O. (2024). The Future of Work: A Human-centric Approach to AI, Robotics, and Cloud Computing. *Journal of Engineering Research and Reports*, *26*(11), 62–87. https://doi.org/10.9734/jerr/2024/v26i111315

Sepasgozar, S. M. E., Khan, A. A., Smith, K., Romero, J. G., Shen, X., Shirowzhan, S., Li, H., & Tahmasebinia, F. (2023). BIM and Digital Twin for Developing Convergence Technologies as Future of Digital Construction. *Buildings*, *13*(2), 441. https://doi.org/10.3390/buildings13020441

Shahzad, K., Anwar, A., & Waqas, A. (2023). The Impact of Artificial Intelligence on Future Warfare and Its Implications for International Security. *Asian Innovative*

Journal of Social Sciences and Humanities, *7*(3). https://aijssh.org/index.php/aijssh/article/view/36

Sharma, S. (2024). *AI adoption in security taking off amid budget, trust, and skill-based issues*. CSO Online. https://www.csoonline.com/article/1307294/ai-adoption-in-security-taking-off-amid-budget-trust-and-skill-based-issues.html

Staff, S. (2023). *Phishing attacks spike attributed to generative AI adoption*. SC Media. https://www.scworld.com/brief/phishing-attacks-spike

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. *Cyberwarfare*, 351–399. https://doi.org/10.1007/978-3-030-97299-8_6

Tahmasebi, M. (2024). Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. *Journal of Information Security*, *15*(2), 106–133. https://doi.org/10.4236/jis.2024.152008

Telukdarie, A., Munsamy, M., Katsumbe, T. H., Maphisa, X., & Philbin, S. P. (2023). Industry 4.0 Technological Advancement in the Food and Beverage Manufacturing Industry in South Africa—Bibliometric Analysis via Natural Language Processing. *Information*, *14*(8), 454. https://doi.org/10.3390/info14080454

Tong, A. (2024). The Evolution of AI Engineering: Hardware and Software Dynamics, Historical Progression, Innovations, and Impact on Next-Generation AI Systems. *Library Progress International*, *44*(3), 19715–19737. https://bpasjournals.com/library-science/index.php/journal/article/view/652

Tyagi, A. K., Fernandez, T. F., Mishra, S., & Kumari, S. (2021). Intelligent Automation Systems at the Core of Industry 4.0. *Advances in Intelligent Systems and Computing*, *1351*, 1–18.

U.S. Department of Commerce. (2024). *U.S. AI Safety Institute Establishes New U.S. Government Taskforce to Collaborate on Research and Testing of AI Models to Manage National Security Capabilities & Risks*. U.S. Department of Commerce. https://www.commerce.gov/news/press-releases/2024/11/us-ai-safety-institute-establishes-new-us-government-taskforce

Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States. *Asian Journal of Research in Computer Science*, *17*(11), 25–45. https://doi.org/10.9734/ajrcos/2024/v17i11517

Val, O. O., Olaniyi, O. O., Selesi-Aina, O., Gbadebo, M. O., & Kolade, T. M. (2024). Machine Learning-enabled Smart Sensors for Real-time Industrial Monitoring: Revolutionizing Predictive Analytics and Decision-making in Diverse Sector. *Asian Journal of Research in Computer Science*, *17*(11), 92–113. https://doi.org/10.9734/ajrcos/2024/v17i11522

Vegesna, V. V., & Adepu, A. (2024). Leveraging Artificial Intelligence for Predictive Cyber Threat Intelligence. *International Journal of Creative Research in Computer Technology and Design*, *6*(6), 1–19. https://jrctd.in/index.php/IJRCTD/article/view/64

Watters, P. A. (2023). Counterintelligence in a Cyber World. In *Springer eBooks*. Springer Nature. https://doi.org/10.1007/978-3-031-35287-4

Willett, M. (2024). The strategic utility of cyber operations. *Adelphi Series*, *64*(511-513), 125–170. https://doi.org/10.1080/19445571.2024.2417542

Williamson, S. M., & Prybutok, V. (2024). The Era of Artificial Intelligence Deception: Unraveling the Complexities of False Realities and Emerging Threats of Misinformation. *Information*, *15*(6), 299. https://doi.org/10.3390/info15060299

Winter, C., Gallacher, J., & Harris, A. (2022). *Artificial Intelligence, OSINT and Russia's Information Landscape*. Centre for Emerging Technology and Security. https://cetas.turing.ac.uk/publications/artificial-intelligence-osint-and-russias-information-landscape

Zhai, C., Wibowo, S., & Li, L. D. (2024). The effects of over-reliance on AI dia logue systems on students' cognitive abilities: a systematic review. *Smart Learning Environments*, *11*(1). https://doi.org/10.1186/s40561-024-00316-7