Artificial Intelligence and Global Security: Strengthening International Cooperation and Diplomatic Relations.

Abstract

This study investigates how artificial intelligence (AI) can enhance global security by fostering international cooperation and diplomatic relations. It examines the dual nature of AI, where operational benefits such as improved cybersecurity, military precision, and threat detection are offset by significant ethical and geopolitical challenges. Through a mixed-methods approach, the research identifies key issues like geopolitical tensions and fragmented governance while highlighting the opportunities for collaboration through multilateral research and ethical AI governance. The findings reveal notable improvements in AI-driven cybersecurity, with detection rates increasing from 86% in 2021 to 88.25% in 2023 and mitigation rates rising from 80.75% to 83.75%. However, AI-driven attacks also increased from 11.25 incidents in 2021 to 16.25 in 2023, underscoring the risks associated with AI misuse. The study concludes that international cooperation, trust-building, and robust governance frameworks are essential to maximize AI's potential in addressing global security challenges.

Keywords: AI governance, global security, cybersecurity, international cooperation, geopolitical tensions.

1. Introduction

Artificial Intelligence (AI) has become a transformative force in global security, offering extensive potential across various domains while presenting significant challenges [1]. Its rapid development has sparked substantial interest in applications like cybersecurity, intelligence gathering, and autonomous systems, fundamentally altering how nations approach security. According to Aldoseri et al. [2], AI's ability to process large datasets with speed and precision has transformed defense strategies from predictive analytics to enhanced surveillance and the automation of complex tasks. AI technologies are increasingly shaping national responses to contemporary security threats.

In counterterrorism, AI facilitates advanced tools for data analysis by detecting threats through the examination of social media activity, financial transactions, and travel

patterns [1]. AI-driven facial recognition technologies and autonomous drones demonstrate the utility of AI in identifying and targeting individuals involved in criminal or terrorist activities. However, Dhirani et al. [3] contend that these applications raise serious ethical concerns related to privacy, autonomy, and the risk of misuse. This delicate balance between benefits and risks necessitates the establishment of robust regulatory frameworks to govern AI's use, particularly in high-risk security environments [4].

AI's integration into cybersecurity is equally essential as the number and severity of cyberattacks continue to increase globally. Chehri et al. [5] note that AI's capacity to detect anomalies in network traffic and respond in real-time has enhanced the protection of critical infrastructure, including energy grids, financial institutions, and healthcare systems. Yet, the technologies designed to strengthen cybersecurity can also be weaponized, leading to more sophisticated cyberattacks and new threats to national security [1]. These dual-use challenges highlight the urgent need for international cooperation in AI governance, particularly through the development of standardized protocols and collaborative defense measures to counter emerging cyber threats.

AI has also shown substantial potential in addressing security concerns linked to climate change. Nishant et al. [6] argue that AI-powered predictive models enable governments and international organizations to forecast climate impacts more accurately, including extreme weather events, rising sea levels, and resource shortages. This predictive capability facilitates better resource management and disaster response, helping nations mitigate climate-related threats [7][8]. Given the global nature of climate change, international cooperation is vital to harness AI's power to combat its effects fully. Nations must collaborate to ensure AI-driven technologies optimize resource use and environmental monitoring.

AI plays an increasingly critical role in nuclear non-proliferation and the monitoring of weapons of mass destruction (WMDs). Cox and Williams [9] note that AI can analyze satellite imagery and other data to monitor nuclear activities, providing valuable support for global nonproliferation efforts. Furthermore, AI's ability to track the development of chemical and biological weapons provides crucial early warning systems to prevent the proliferation of such weapons [10]. However, concerns remain about the accuracy and

reliability of AI-driven systems in this context, underscoring the need for responsible development and governance to reduce the risks of false alarms and ensure effective oversight [3].

In maritime security, AI is employed to enhance the monitoring of maritime traffic and identify illicit activities such as smuggling and piracy. Dimitrov [11], posits that AI-powered autonomous maritime vehicles and advanced data analytics offer critical surveillance and threat detection capabilities in international waters, securing sea lanes and promoting stability in key maritime regions. AI's ability to analyze vast amounts of data from sensors and satellite imagery further aids in predicting and preventing illegal activities, strengthening global security efforts in the maritime domain [3].

The Russia-Ukraine war highlights the growing influence of AI in modern warfare, with both nations employing AI technologies, such as drones and cyberattacks, to gain strategic advantages on the battlefield [12]. According to Morgan et al. [13], this conflict illustrates how AI can both enhance military capabilities and escalate conflicts, raising significant ethical concerns. AI's deployment in warfare emphasizes the need for international agreements to govern its use, particularly in conflict zones, where accountability and human oversight are paramount [5].

International cooperation is increasingly recognized as essential in managing the challenges posed by AI in global security. Several governance initiatives, such as the Global Partnership on AI (GPAI) and the OECD AI Principles, have been introduced to promote responsible AI development, with a focus on ethical considerations, privacy protection, and transparency [3]. Feijoo et al. [14] contend that AI's role in addressing global issues like climate change and cybersecurity has become central to diplomatic discussions as nations seek collaborative strategies to harness AI's potential in confronting these pressing challenges.

Beyond addressing security threats, AI offers opportunities to enhance diplomacy and international relations. According to Muñoz-Basols et al. [15], AI-powered communication tools can facilitate dialogue between nations, overcoming language barriers and fostering mutual understanding. Additionally, AI supports decision-making processes by providing data-driven insights that identify common interests and areas for cooperation [16]. Adanma and Olurotimi [17] posit that the ability of AI to promote

dialogue and mutual understanding underscores its potential to strengthen international diplomacy and foster global stability.

However, the deployment of AI in global security and diplomacy must be approached cautiously, considering that the ethical implications of AI, particularly regarding privacy, bias, and accountability, cannot be overlooked [14]. As AI systems become more autonomous, there is a growing risk of unintended consequences and loss of human oversight. To ensure the responsible development and deployment of AI, international cooperation is required to establish regulatory frameworks that prioritize transparency, human rights, and the avoidance of discriminatory practices, according to Diaz-Rodriguez et al. [18].

The future of AI in global security will depend largely on the ability of the international community to collaborate on governance, develop ethical guidelines, and address the risks associated with its use [19]. Dhirani et al. [3] argue that the intersection of AI and global security presents significant challenges and opportunities as nations strive to balance AI's capabilities with its potential risks. Through sustained international cooperation, it is possible to ensure AI serves as a tool for promoting global stability and security [20]. As a result, this study investigates the potential of artificial intelligence (AI) to enhance global security by strengthening international cooperation and diplomatic relations. The study achieves the following objectives:

1. Examines the current state of artificial intelligence (AI) technology and its applications in global security, focusing on existing research, case studies, and emerging trends in AI development.
2. Investigates the potential benefits and risks of AI deployment in global security, assessing its impact on diplomacy, international cooperation, and national security while considering ethical implications, privacy concerns, and misuse.
3. Evaluate challenges and opportunities for international cooperation in the AI era by analyzing existing international frameworks, identifying collaboration areas, and addressing barriers to cooperation.
4. Proposes policy recommendations for policymakers and international organizations to harness AI's potential for global security enhancement, emphasizing responsible AI development, governance, and international collaboration.

2. Literature Review

Artificial intelligence (AI) has emerged as a critical element in global security, significantly influencing military and defense operations through key technologies such as machine learning, autonomous systems, and predictive analytics [1] [3] [21]. These technologies provide unprecedented capabilities in surveillance, reconnaissance, and threat anticipation, transforming traditional defense strategies and machine learning systems, for instance, processing vast amounts of data to identify patterns and inform decision-making processes. In contrast, autonomous systems, such as drones, perform precision strikes with minimal human oversight [22]. According to Shah [23], predictive analytics, by utilizing historical data, has become integral to forecasting threats,thereby enabling security agencies to implement preemptive measures.

However, the incorporation of AI in military applications introduces complex ethical and legal challenges, such as autonomous weapons systems, which are designed to operate with limited human intervention and have sparked concerns regarding accountability and governance in conflict situations [2]. While these systems enhance operational efficiency, they also risk malfunctioning or exceeding their intended objectives, raising serious ethical issues; therefore, analysts emphasize that international regulation is crucial for the responsible deployment of such systems, arguing that technological advancements must be paired with ethical considerations, as posited by Dhirani et al. [3].

Another significant application of AI in global security is cybersecurity. AI-driven algorithms are now commonly employed to detect and mitigate cyber threats, with predictive models assessing patterns to prevent potential attacks [24]. This capability is particularly important in addressing cyber espionage and data breaches, both of which are growing concerns. According to Shah [23], AI enhances protection for digital infrastructures by detecting and neutralizing threats in real-time, as critics then caution that over-reliance on AI could expose vulnerabilities as malicious actors continuously adapt their tactics to exploit these technologies.

Moreover, AI has extended its reach into digital surveillance, with AI-powered systems now used to monitor public spaces, track individuals, and secure sensitive data [25]. Machine learning-based facial recognition technology plays a central role in intelligence gathering and security screenings [26]. However, such advancements have prompted debates about privacy, particularly in authoritarian regimes where AI is used for mass surveillance. Hence, studiesargue that while these systems offer security benefits, balancing these against the protection of individual privacy is essential to avoid abuses of power [3].

Thus, while AI undeniably enhances global security operations by improving efficiency and anticipation, it simultaneously raises important ethical, legal, and operational concerns [13]. These challenges necessitate ongoing dialogue to develop robust regulatory frameworks that ensure AI's responsible use in alignment with international standards and human rights [18].

Benefits and Risks of AI in Global Security

Artificial intelligence (AI) plays a pivotal role in global security, offering advantages in defense, intelligence, and disaster response. AI technologies, such as autonomous systems and predictive algorithms, enhance military operations by improving real-time intelligence and surveillance [27][28]. Autonomous drones and vehicles perform critical tasks in hostile environments, minimizing human risk and collateral damage, as contended by Chamola et al. [29]. Predictive algorithms also enable proactive measures in threat detection, improving military precision and reducing escalation risks [9][30].

In intelligence analysis, AI’s capacity to process vast datasets has transformed how potential threats are identified [1]. Machine learning models detect patterns that human analysts might overlook, providing faster, more accurate insights, which makes the growing reliance on AI raises concerns about its limitations, particularly where nuanced decision-making is needed [31]. As argued by Morgan et al. [13], over-dependence on deterministic AI logic may introduce blind spots, underscoring the need for continued human oversight in intelligence operations.

Beyond defense, AI demonstrates considerable potential in disaster response and climate change mitigation [32]. Predictive models analyze historical data to forecast natural disasters, allowing governments to implement early warning systems, as noted by Merz et al. [33]. Additionally, AI assists in assessing environmental impacts, offering critical insights for future planning, and these benefits come with risks, particularly if systems are compromised or improperly governed [34][35].

One significant concern surrounding AI in security is its impact on privacy, considering that AI-driven surveillance systems, like facial recognition technologies, gather vast amounts of personal data, raising ethical concerns about privacy infringement [3]. The lack of transparency in AI surveillance, especially in authoritarian regimes, exacerbates these issues as strong privacy protections and ethical frameworks are essential to prevent the abuse of AI in surveillance [36][37].

AI also presents risks in autonomous warfare and cyberattacks [38]. Autonomous weapons, capable of making critical decisions without human input, raise ethical

concerns about accountability in conflict zones, particularly in life-and-death scenarios [3]. Likewise, AI's role in cyberattacks is growing, with systems used to create sophisticated malware, as contended by Sarker et al.[24]. These challenges call for comprehensive international regulations to ensure responsible AI use in security contexts.

As AI's role in security grows, ethical and regulatory oversight is critical. Without robust frameworks, the rapid integration of AI creates risks related to accountability, transparency, and governance. [39][18][40].

International Cooperation in the AI Era

The growing influence of artificial intelligence (AI) has made international cooperation vital to ensure its responsible development and deployment on global frameworks such as the Global Partnership on AI (GPAI), which promotes collaboration among governments, industries, and academic institutions [14]. According to Diaz-Rodriguez et al. [18], GPAI seeks to bridge the gap between AI development and ethical considerations by facilitating dialogue and establishing best practices. Similarly, the Organisation for Economic Co-operation and Development (OECD) AI Principles advocate for transparency, accountability, and human rights, laying the foundation for responsible AI governance in advanced economies [41][42].

International agreements are also shaping AI's role in global security. Transatlantic collaborations between the European Union and the United States, for instance, emphasize the alignment of AI development with democratic values and security measures, particularly in addressing ethical concerns related to autonomous weapons and surveillance technologies [43][44][45]. In the Asia-Pacific region, countries like Japan and South Korea engage in multilateral discussions to create cohesive AI governance frameworks, balancing the need for innovation with security concerns, as posited by Habbal et al. [44].

AI has demonstrated its capacity to enhance diplomatic relations through collaborative efforts in defense technologies [46][27]. For example, joint initiatives between the United States and Israel on AI-based military systems illustrate how AI can strengthen defense capabilities while fostering bilateral ties [14][46][47]. Likewise, NATO's AI-driven cybersecurity collaborations highlight the success of multilateral partnerships in combating global cyber threats, demonstrating the potential for AI to act as a catalyst for international cooperation in addressing cross-border security challenges [48].

Beyond defense, AI is making a significant impact in sectors such as disaster response and climate change adaptation [32]. AI-driven predictive models have improved disaster forecasting, enabling nations to collaborate on early-warning systems and more effective humanitarian responses [49]. This has not only enhanced global disaster preparedness but also strengthened diplomatic ties by showing the shared benefits of AI technology. In the area of climate change, international cooperation has allowed countries to jointly model environmental impacts and develop proactive strategies, as contended by Suprayitno et al. [50].

However, achieving consensus on AI governance remains difficult due to divergent national interests and technological capabilities [39]. Some nations advocate for stringent regulation to mitigate AI's ethical risks, while others prioritize flexibility to foster innovation. According to Biden [51], these differing priorities complicate the creation of a unified global framework, where security must be balanced with technological advancement. Initiatives like the Wassenaar Arrangement, expanded to include AI-enabled technologies and the GPAI's guidelines in sectors like healthcare, represent progress in regulating AI and fostering international knowledge-sharing [17].

While challenges persist in aligning national perspectives, particularly amid geopolitical tensions, the need for international cooperation remains clear as AI continues to shape global security and governance; sustained multilateral engagement is crucial to ensure its benefits are responsibly shared across borders [14][52][53].

AI's Role in Specific Global Security Domains

Artificial intelligence (AI) has become a crucial tool in global security, transforming how threats are managed across various domains [1]. In counterterrorism, AI plays a pivotal role in data analysis, surveillance, and facial recognition, as posited by Almeida et al. [36]. Machine learning algorithms sift through large datasets to detect patterns indicating potential terrorist activities, while facial recognition identifies suspects in real-time. AI systems have successfully preempted attacks by detecting threats early, as evidenced in the ongoing Russian-Ukrainian conflict, where autonomous systems are deployed for military intelligence gathering [13][46][54]. However, ethical concerns persist regarding privacy and the accuracy of predictive analytics in conflict scenarios [3].

In the cybersecurity domain, AI is essential for detecting and neutralizing sophisticated cyberattacks and protecting critical infrastructure such as power grids and government networks [55]. National security agencies, as cited by researchers, increasingly rely on AI to combat ransomware and state-sponsored cyber intrusions. However, this dependence on AI introduces new risks as adversaries develop AI-enhanced tactics to bypass defenses, escalating the arms race in cyberspace [19]. Both attackers and defenders continuously refine their AI capabilities, adding complexity to the cybersecurity landscape [1][56].

AI's contributions also extend to climate change risk management. AI-powered models forecast natural disasters like floods and hurricanes, improving disaster response and enabling governments to manage crises more effectively [57]. International organizations are using AI to assess climate-related security risks, such as the impact of water shortages on political stability [60]. However, critics warn that AI models may introduce data biases, potentially leading to inaccurate predictions and misguided policies [58][59].

In the domain of weapons of mass destruction (WMD) monitoring, AI systems analyze global communications and satellite imagery to detect nuclear, chemical, or biological weapons development, as noted by Johnson [46]. These systems identify unusual patterns in satellite data, enhancing early detection of WMD threats such as misidentification and false alarms, which could lead to severe consequences if not managed properly [59][61].

AI also plays a significant role in maritime security, where autonomous systems monitor shipping lanes and coastal areas for illegal activities such as smuggling and illegal fishing [62]. According to analysts, AI integrates data from satellites and sonar systems to enhance maritime domain awareness [63]. However, differing international regulations pose challenges to effective collaboration in AI-driven maritime security efforts [64].

While AI holds significant potential in strengthening global security by enhancing threat detection and defense capabilities, ethical concerns, data accuracy, and international cooperation remain critical issues; therefore, the international community must address these complexities to harness the benefits of AI in security domains fully [14][66].

AI Governance and Ethical Challenges

AI governance has become increasingly important as artificial intelligence technologies expand into critical sectors like global security, healthcare, and public policy. Initiatives such as the Global Partnership on AI (GPAI) promote ethical AI development, fostering international cooperation and ensuring alignment with human rights principles, as

argued by Schmitt [65]. Similarly, regional efforts like the European Union's General Data Protection Regulation (GDPR) emphasize privacy and data protection in AI systems. According to Lescrauwaet et al. [67], striking a balance between regulation and innovation is crucial to safeguarding human rights without stifling technological advancements.

Global standards for AI governance are still in their infancy, though initiatives like the OECD AI Principles advocate for transparent, accountable, and human-centered AI systems. These principles, as noted by Shneiderman [68], urge developers and policymakers to address ethical issues in AI design. However, achieving global consensus remains elusive, with some nations favoring looser regulations to encourage innovation while others push for stricter governance to mitigate AI's societal impacts. This divergence highlights the tension between advancing AI technology and managing its ethical consequences [3][69].

One of the most significant challenges in AI governance is the use of autonomous systems in military operations, particularly in life-or-death scenarios [3]. AI's ability to make independent decisions, such as in autonomous drone strikes, raises serious concerns about accountability and human oversight, as contended by Taeihagh [43]. Critics warn that delegating critical decisions to machines could diminish the moral responsibility of human actors, creating risks that demand robust ethical frameworks to limit AI's autonomy in morally sensitive areas [70].

Another key issue is the presence of bias in AI systems and the need for transparency. AI models used in areas like predictive policing or hiring often perpetuate the biases embedded in their training data, disproportionately affecting marginalized communities, as noted by Fountain [71]. Moreover, many AI systems operate as "black boxes," making it difficult to scrutinize their decision-making processes; therefore, Scholars argue that improving transparency is essential for maintaining public trust, particularly when AI impacts fundamental rights [72][73].

Comprehensive regulatory frameworks are necessary to manage the risks associated with AI. Without such frameworks, AI systems could exacerbate harm in sensitive domains like surveillance and military applications [13]. Proposals for an international regulatory body to oversee AI governance have gained traction, reflecting the global nature of AI's challenges; however, establishing these regulations remains challenging due to differing national interests and technological capacities, According to Dwivedi et al. [74].

As AI continues to influence global policy, governance frameworks must evolve to ensure ethical considerations remain central to its development, especially in areas like bias, transparency, and military autonomy [36][75].

3. Methodology

To achieve research objective 1, a quantitative approach was used to assess AI technology and its applications in global security. Data from the AI Index Reports (2018–2023) was analyzed, focusing on AI research publications, patent filings, and private investments in security technologies. A trend analysis was conducted to evaluate the growth of AI research and innovation across regions.

As for research objective 2, which investigates the potential benefits and risks of AI deployment in global security, data from the Verizon Data Breach Investigations Report (DBIR) (2021–2023) was analyzed to investigate the benefits and risks of AI deployment in managing cyberattacks. This dataset included metrics on Phishing Incidents, Ransomware Incidents, Data Breaches, AI-driven attacks, and AI performance metrics such as Detection Rate, Mitigation Rate, Response Time, and Vulnerability Rate across four sectors—Finance, Healthcare, Government, and Education.

A trend analysis was used to calculate the annual rate of change for each metric:

$$Rate\ of\ Change\ (\%) = \left[\frac{(Value_{current}year - Value_{previous}year)}{Value_{previous}year}\right] * 100$$

A Pearson correlation analysis was conducted to assess the relationship between AI performance metrics and cyber incidents using the formula:

$$r = \frac{\Sigma[(Xi - \bar{X})(Yi - \bar{Y})]}{\sqrt{[\Sigma(Xi - \bar{X})^2 \Sigma(Yi - \bar{Y})^2]}}$$

In evaluating challenges and opportunities for international cooperation in the AI era (research objective 3), a mixed-methods approach was applied to assess international cooperation in AI defense. Data from the OECD AI Policy Observatory on bilateral collaborations, joint research projects, and policy agreements between the USA, UK, China, Germany, France, Japan, and South Korea were combined into a Total Collaboration Score:

$$Total\ Collaboration\ Score = Bilateral\ Collaborations + Joint\ Research\ Projects + Policy\ Agreements$$

A network graph was generated, with countries as nodes and edge weights reflecting the collaboration score. Key metrics such as degree centrality were calculated to identify patterns and gaps in collaboration:

Key metrics:

$$Degree = \sum Edges\ connected\ to\ a\ node$$ and

Betweenness centrality:

$$Betweenness\ Centrality = \left(\sum \frac{Shortest\ Paths\ through\ a\ node}{Total\ Shortest\ Paths}\right)$$

A meta-synthesis of different key papers on AI governance and defense identified themes such as geopolitical tensions, fragmented governance, and trust-building through ethical governance. Integrating these findings with the quantitative network analysis revealed cooperation gaps due to rivalries and opportunities for collaboration through joint research and AI governance leadership, offering a comprehensive view of structural and policy dynamics in AI defense cooperation.

4. Results and Discussion

RO1.1 AI Research Publications

The number of AI research publications globally shows steady growth, with China emerging as the leading contributor. In 2023, China accounted for 39.8% of global AI publications, followed by the EU/UK at 15.05% and the United States at 10.03%. This trend explains China's significant leadership in AI research, especially in key areas relevant to global security, such as machine learning and natural language processing (NLP).

Table 1: AI Research Publications by Region (2018–2023)

Year	China (%)	EU/UK (%)	U.S. (%)
2018	25	28	17
2019	28	27	17
2021	31.04	19.05	13.67
2022	31.04	19.05	13.67
2023	39.8	15.05	10.03

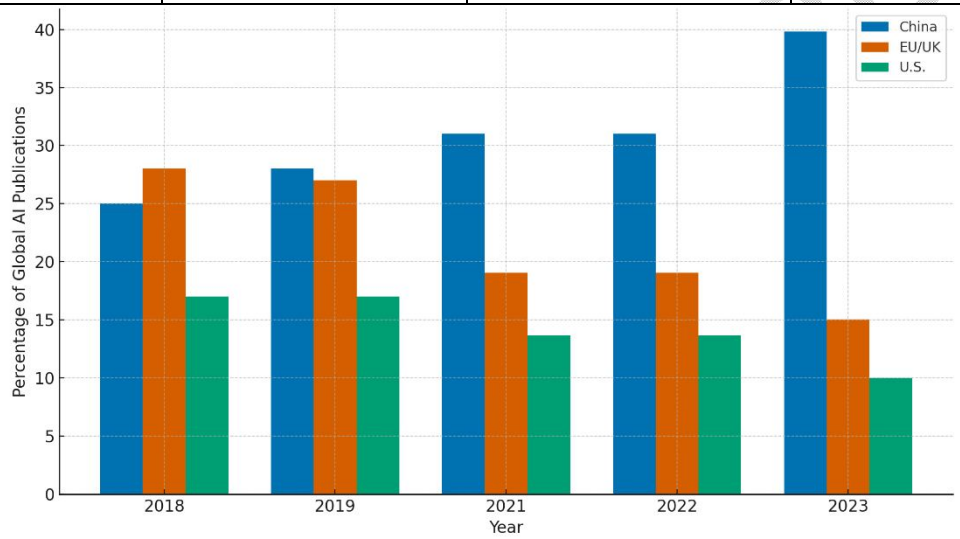

Figure 1: AI Research Publications by Region (2018–2023)

Figure 1 highlights the growth of AI publications across China, the EU/UK, and the U.S. from 2018 to 2023. It is evident that China's share of global AI research has continued to rise, while the EU/UK and U.S. have experienced relative declines in their contributions.

RO1.2 AI Patent Growth

The number of AI patents has increased significantly, particularly in EastAsia, where 62.14% of all AI patents were filed in 2022. NorthAmerica followed with 17.07%**,** while Europe contributed 4.16%**.** The rapid growth in AI patent filings highlights the significant focus on AI innovation, including in sectors related to global security, such as cybersecurity and autonomoussystems.

Table 2: AI Patent Growth by Region (2018–2022)

Year	East Asia (%)	North America (%)	Europe (%)
2018	16	30	16
2019	22	60	17
2021	62.14	17.07	4.16
2022	62.14	17.07	4.16

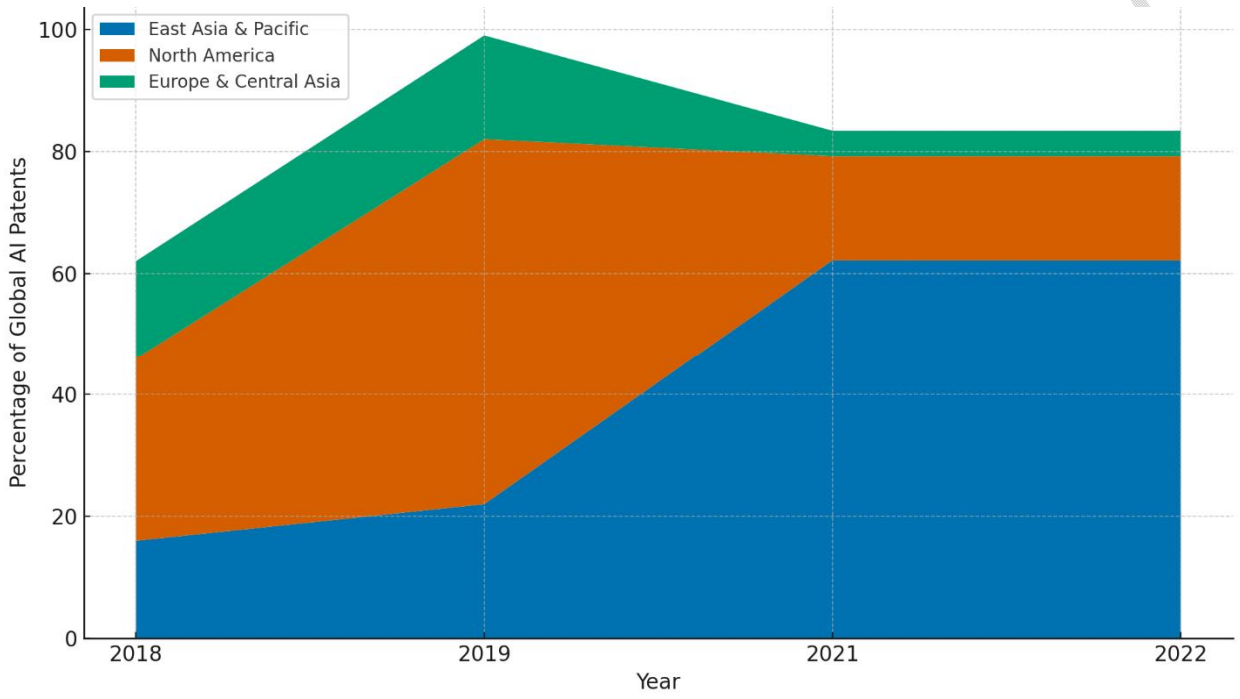

Figure 2: AI Patent Growth by Region (2018–2022)

Figure 2 illustrates the substantial increase in AI patent filings in East Asia, particularly from countries like ChinaandSouth Korea, underscoring their investment in AI innovation for global security.

RO1.3 AI Adoption in Security-Related Areas

Private investment in AI for security-related areas, such as cybersecurity**,** autonomous systems**,** andNLP**,** reached$93.5 billion in 2022. This marks a significant increase from 2020, demonstrating the growing role of AI in enhancing global security infrastructure. Technologies such as roboticsandmachine learningare increasingly used for threat detection, surveillance, and risk management.

Table 3: Private Investment in AI Security-Related Areas (2018–2022)

Year	Investment (in Billion USD)
2018	7.7

2019	70
2021	13.8
2022	93.5

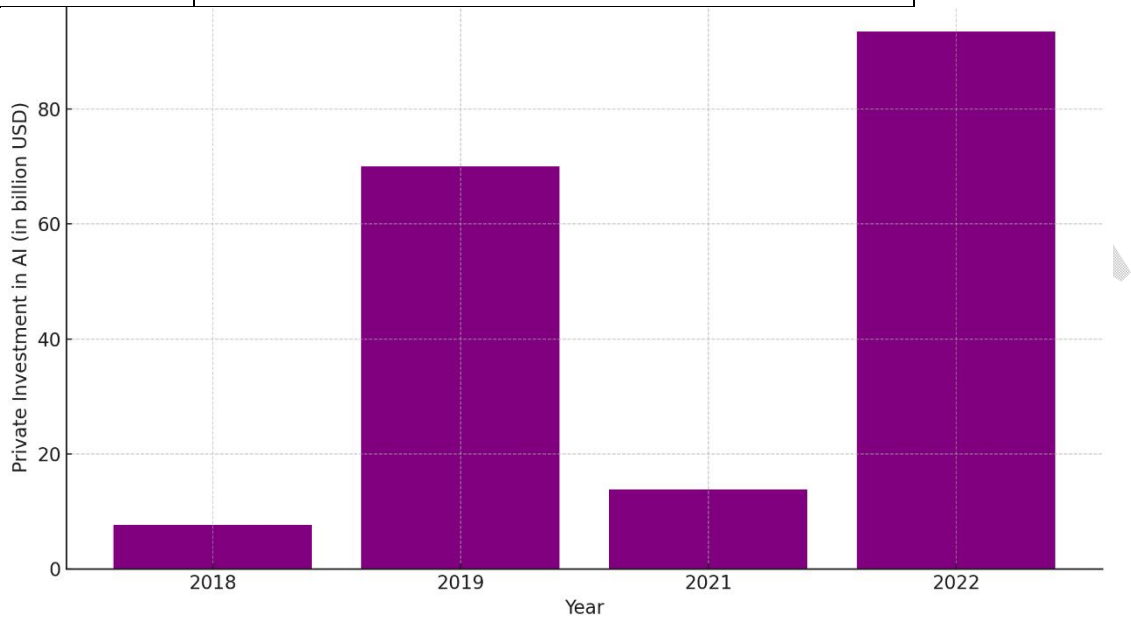

Figure 3: Private Investment in AI Security-Related Areas (2018–2022)

Figure 3 demonstrates the rapid growth in private investment in AI security applications, particularly in 2022, highlighting the increased focus on AI to address global security challenges. This analysis shows rapid growth in AI research, patents, and industry adoption, with China leading in research output and East Asia dominating patent filings. Significant investments in AI security technologies highlight its increasing role in addressing modern global security challenges.

Investigating the Potential Benefits and Risks of AI Deployment in Global Security

The objective of this analysis is **to** investigate the potential benefits and risks of AI deployment in global securityby examining its impact on the frequency and severity of cyberattacks, as well as identifying emerging risks, particularly AI-driven attacks and vulnerabilities.

RO2.1 Trends in Cyber Incidents and AI Performance (2021–2023)

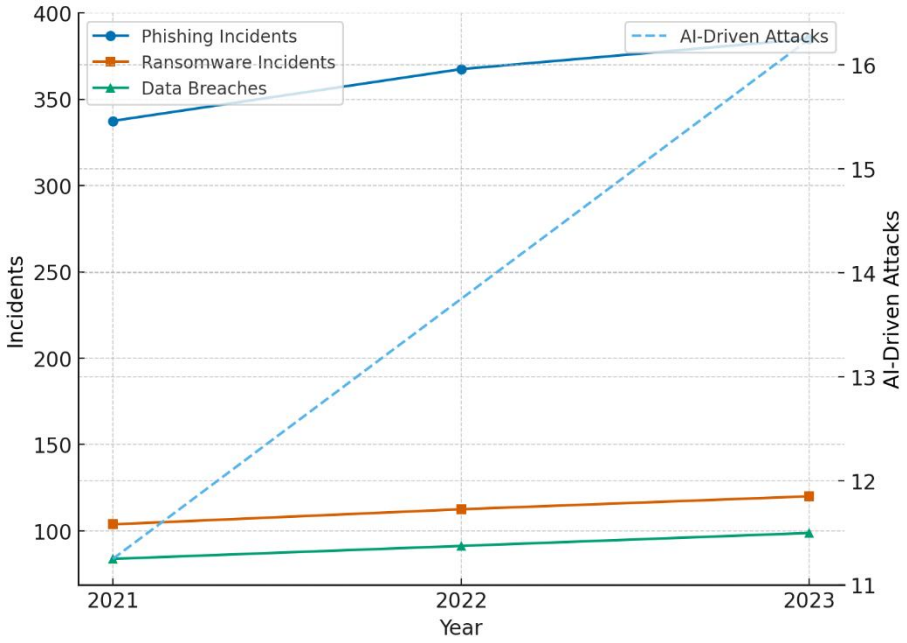

Figure 4: Trend of Phishing, Ransomware, Data Breaches, and AI-Driven Attacks (2021–2023)

Figure 4 shows an increasing trend in all three types of conventional cyberattacks (Phishing, Ransomware, Data Breaches). AI-Driven Attacks also grew, raising concerns about the misuse of AI in cyberattacks.

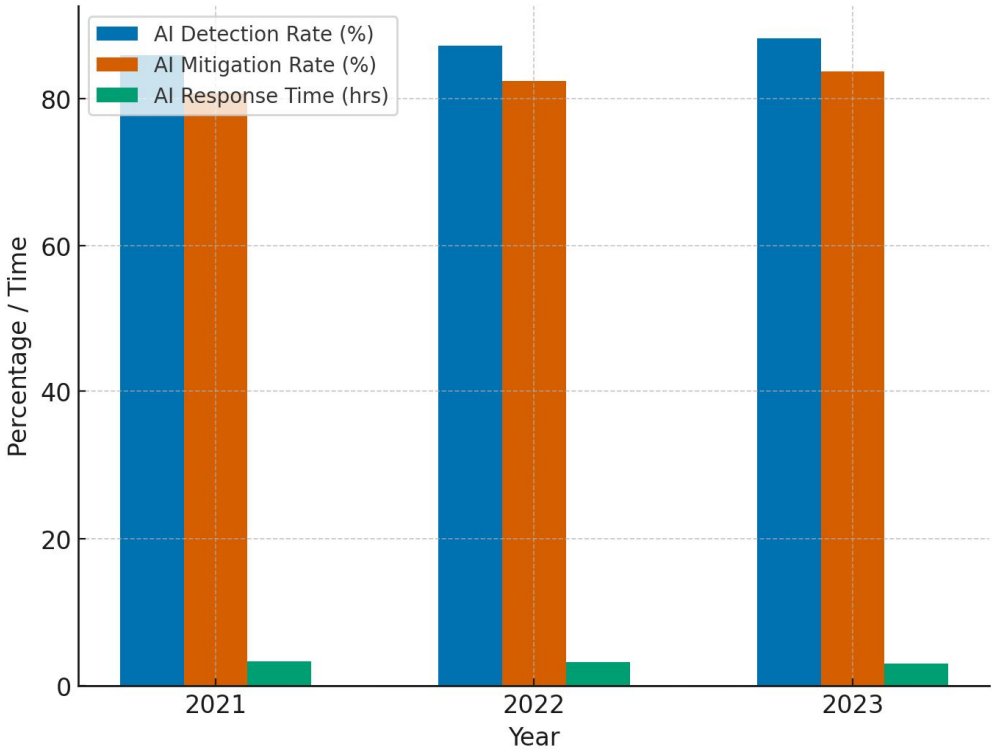

Figure 5: AI Detection Rate, Mitigation Rate, and Response Time (2021–2023):

Figure 5 shows a clear upward trend in detection and mitigation rates over the years, with detection increasing from 86% in 2021 to 88.25% in 2023, and mitigation rising from 80.75% to 83.75%. At the same time, response times have slightly decreased, from 3.37 hours in 2021 to 3.05 hours in 2023, signaling faster reactions to threats. These changes reflect an overall improvement in the ability to manage cybersecurity risks.

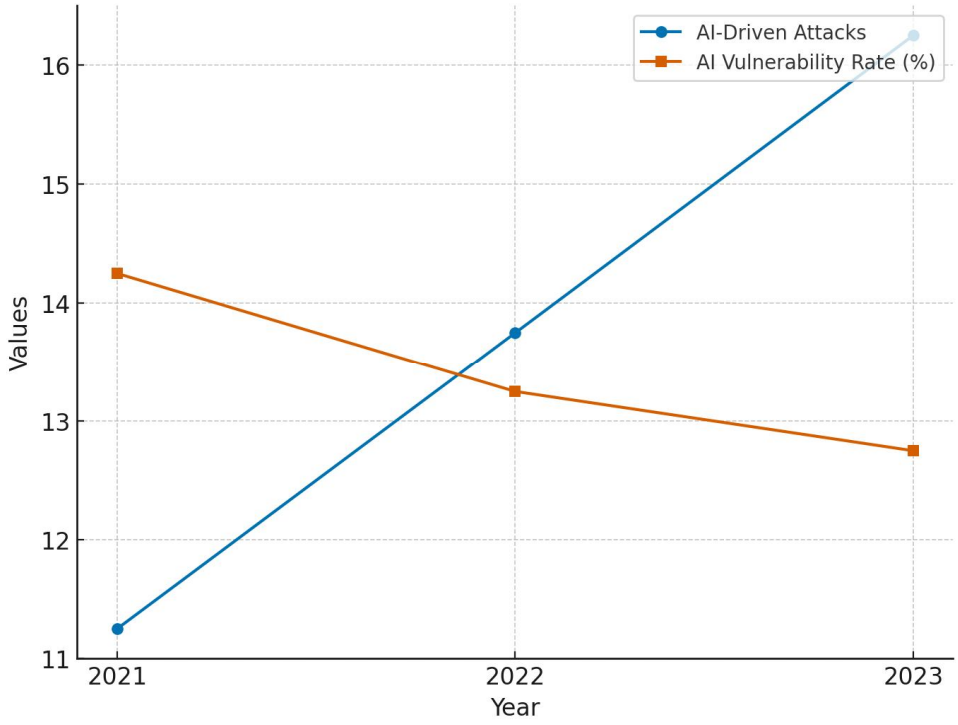

Figure 6: AI Vulnerability Rate (2021–2023):

The AI Vulnerability Rate shows a decreasing trend, from 14.25% in 2021 to 12.75% in 2023, reflecting better management of AI-related vulnerabilities. However, the concurrent rise in AI-driven attacks highlights emerging risks.

Correlation Between AI Performance and Cyber Incidents

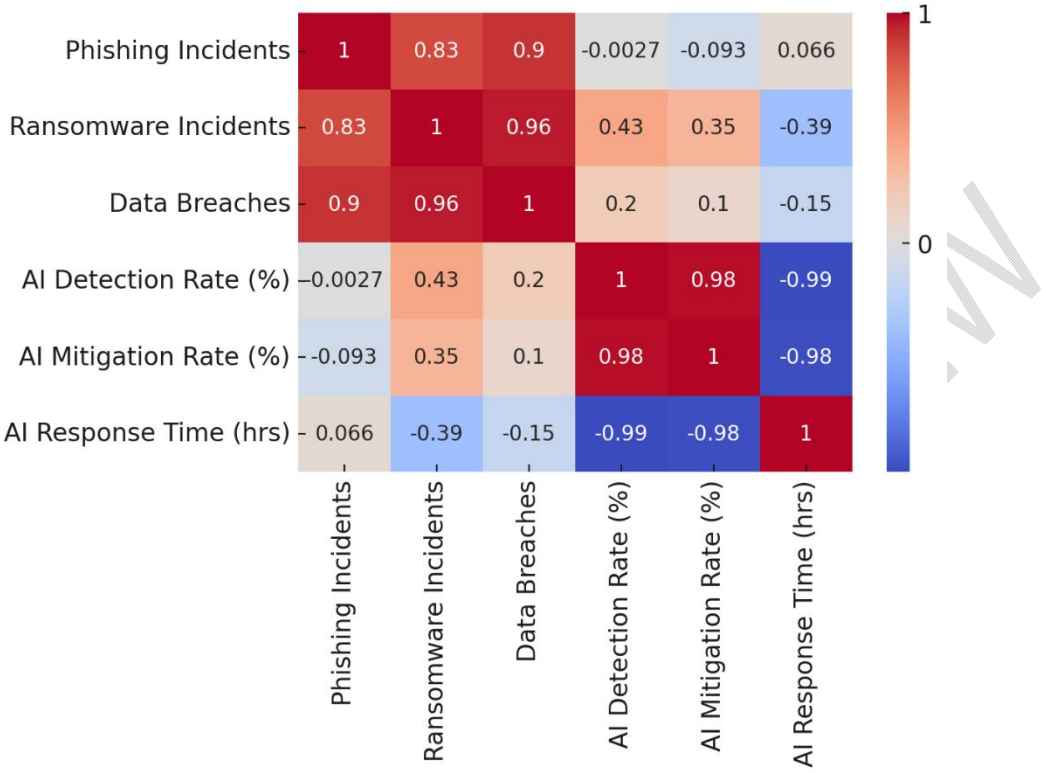

Figure 7: Correlation Matrix:

From the correlation analysis, it was observed that a strong negative correlation between AI Response Time and both AI Detection Rate (-0.99) and Mitigation Rate (-0.98), indicating that faster response times are linked to better detection and mitigation.AI Detection Rate correlates positively with Ransomware Incidents, suggesting that AI detection systems are effectively addressing this type of attack.

4. Tabular Summary of Trends:

Table 4: Trend Summary of Cyber Incidents and AI Metrics (2021–2023):

Year	Phishing Incidents	Ransomware Incidents	Data Breaches	AI-Driven Attacks	AI Detection Rate (%)	AI Mitigation Rate (%)	AI Response Time (hrs)	AI Vulnerability Rate (%)
2021	337.5	103.75	83.75	11.25	86.00	80.75	3.37	14.25
2022	367.5	112.50	91.25	13.75	87.25	82.50	3.20	13.25

2023	385.0	120.00	98.75	16.25	88.25	83.75	3.05	12.75

This analysis demonstrates that AI deployment in cybersecurity has provided clear benefits in terms of improving detection, mitigation, and response to cyber incidents. The improvement in AI performance over time correlates with better management of ransomware and data breaches.

However, the growing trend of AI-driven attacks and persistent vulnerabilities highlight the emerging risks of AI misuse. While AI strengthens defenses, it also introduces new challenges, requiring ongoing efforts to address the dual-edged nature of AI in global security.

Analysis of International Cooperation in AI Defense

The objective of this analysis is to evaluate the challenges and opportunities for international cooperation in AI defense by combining quantitative network analysis and qualitative thematic analysis, specifically addressing collaboration frameworks between countries in the AI era.

RO3.1 Quantitative Network Analysis

The networkanalysis maps the relationships between countries based on the number of bilateral collaborations, joint research projects, and policy agreements related to AI defense. A combined collaboration matrix was constructed, and the relationships were visualized to assess the strength of international cooperation.

Table 3 presents the overall strength of cooperation between the selected countries by summing up bilateral collaborations, joint research projects, and policy agreements.

Table 5: Combined Collaboration Matrix

Country	USA	UK	China	Germany	France	Japan	South Korea
USA	0	6	4	7	6	0	5
UK	9	0	0	9	4	7	4
China	3	6	0	7	6	0	3
Germany	10	5	12	0	5	9	8
France	9	6	4	8	0	4	9
Japan	6	0	4	10	5	0	8
South Korea	6	4	4	8	5	6	0

RO3.2 Network Graph of AI Defense Cooperation

Figure 8 visualizes the relationships between countries, where Nodes represent countries, Edges show the strength of collaboration (thicker edges represent stronger ties), and Nodesize reflects a country's total cooperation score.

The centralactors, such as Germany, the UK, and the USA, show strong collaborations, while gaps are visible between China and certain Western countries.

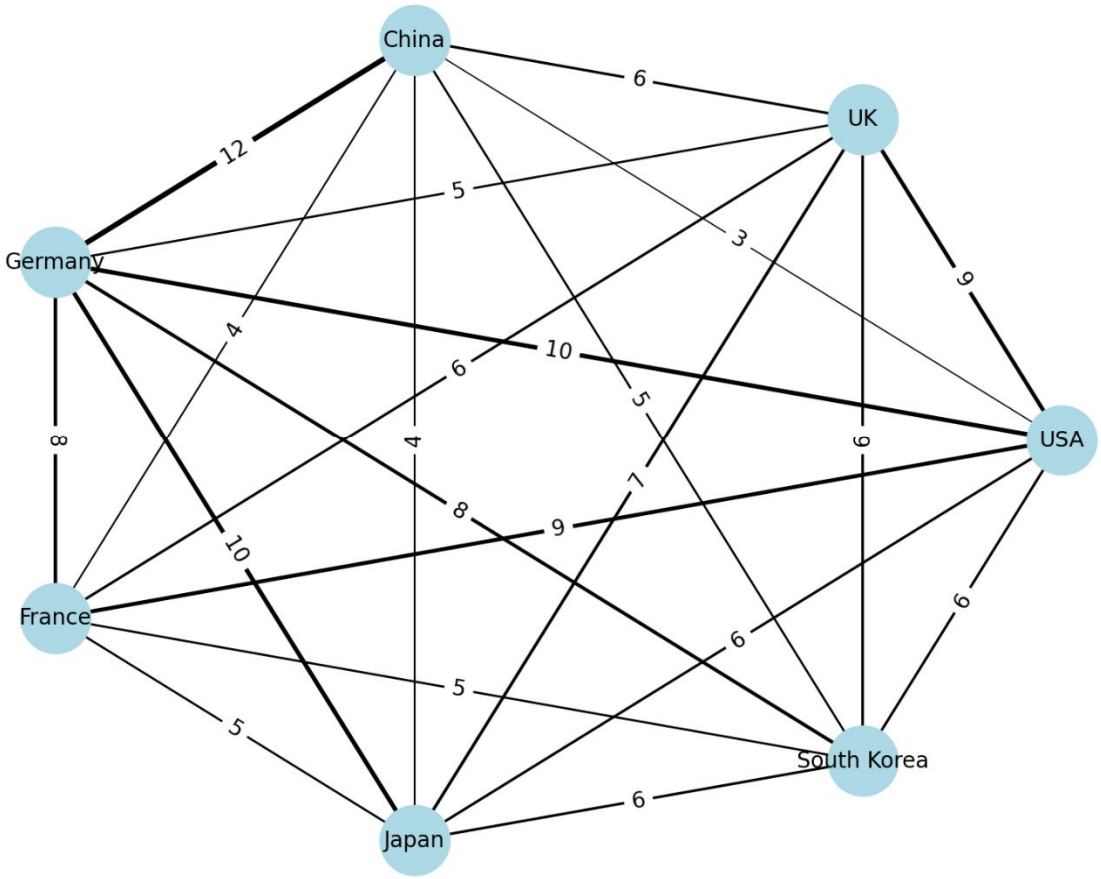

Figure 8: Network Analysis of AI Defense Collaborations

RO3.3 Qualitative Thematic Analysis

The qualitative analysis complements the network analysis by evaluating the underlying challenges and opportunities through a thematic exploration of policy documents, journal articles, and reports. A thematic analysis was conducted based on key themes derived from the literature (Table 4), highlighting the subtle factors influencing international cooperation in AI defense.

Table 6: Key Themes from Thematic Analysis

Theme	Category	Description	Relevant Papers
Geopolitical Tensions and AI Rivalry	Challenge	Geopolitical competition, particularly between China and the US, limits transparency and cooperation.	Maas (76), Zhu & Long (77), Araya &King (78)
Fragmentation of AI Governance	Challenge	A lack of unified global AI governance creates barriers to cohesive cooperation, especially in defense sectors.	Schmitt (79), Wasil et al. (80)

Multilateral Research Opportunities	Opportunity	Joint research initiatives and multilateral agreements present pathways for AI defense cooperation.	Wasil et al. (80), Zhu & Long (77)
Trust and Ethical AI Governance	Opportunity	Trust-building through transparency and ethical governance fosters collaboration across political and cultural divides.	Robinson (81), Gill (82), O'Keefe (83), Security & Order (84)
Emerging Leadership in AI Governance	Opportunity	Chinaand regional leaders like the EU are shaping AI ethics, which may serve as common ground for cooperation.	China's Leadership (85), Liebig et al. (86)

This analysis reveals significant gaps in AI defense collaboration, particularly between China and Western countries, driven by geopolitical rivalry and fragmented governance. However, opportunities for cooperation exist through multilateral agreements, joint research, and ethical governance. Emerging AI powers, like China, offer the potential for bridging divides and fostering collaboration.

RO3.4 Meta-Synthesis of Thematic Analysis

The meta-synthesis integrates the findings from the qualitative thematic analysis, summarizing the key themes, their frequency in the reviewed literature, and the strength of agreement across studies. This analysis provides a deeper understanding of the challenges and opportunities in AI defense cooperation, addressingobjective 3 of this study.

Table 7: Meta-Synthesis of Thematic Analysis

Theme	Frequency	Strength of Agreement	Notable Conflicts/Variations
Geopolitical Tensions and AI Rivalry	3/5	High – seen as a significant challenge by all sources	None
Fragmentation of AI Governance	2/5	Moderate – consistently viewed as a barrier	None
Multilateral Research Opportunities	2/5	Moderate – recognized as a pathway for cooperation	None
Trust and Ethical AI Governance	4/5	High – widely seen as a key opportunity	None
Emerging Leadership in AI Governance	2/5	Moderate – varied views on China's role in governance	Some concerns about China's influence versus potential leadership

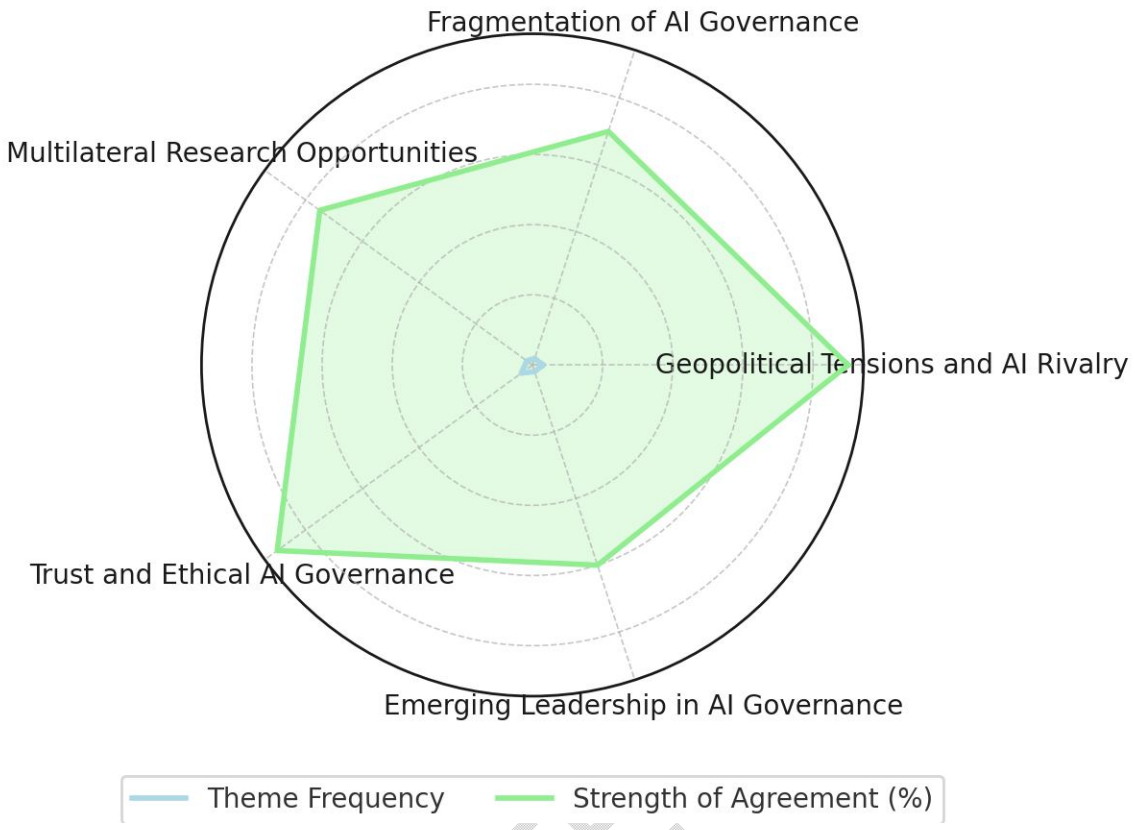

Figure 9: Meta-Synthesis of Thematic Analysis

The meta-synthesis highlights geopolitical tensions and fragmented AI governance as major challenges while trust-building and multilateral research are key opportunities for enhancing cooperation. The radar chart visually compares the frequency and strength of agreement for each theme.

Table 6 summarizes the integration of the meta-synthesis and quantitative analysis. The quantitative analysis reveals weaker ties between China and Western countries, reflecting geopolitical tensions. At the same time, stronger connections between Germany, the USA, and the UK support the meta-synthesis findings, emphasizing trust-building and multilateral research opportunities as critical pathways for enhancing cooperation.

Table 8: Integrated Meta-Synthesis and Quantitative Analysis

Theme	Category	Meta-Synthesis Frequency	Quantitative Insights
Geopolitical Tensions and AI Rivalry	Challenge	High – 3/5 papers	Weak ties between China and Western countries reflect rivalry, limiting cooperation.

Fragmentation of AI Governance	Challenge	Moderate – 2/5 papers	Uneven collaboration scores reflect fragmented governance frameworks, especially in defense sectors.
Multilateral Research Opportunities	Opportunity	Moderate – 2/5 papers	Stronger ties between Germany, USA, and UK suggest potential for multilateral cooperation.
Trust and Ethical AI Governance	Opportunity	High – 4/5 papers	Countries with established trust, like USA and Germany, show strong collaboration ties, supporting trust-driven cooperation.
Emerging Leadership in AI Governance	Opportunity	Moderate – 2/5 papers	Emerging ties between China and Germany suggest potential leadership roles in AI governance.

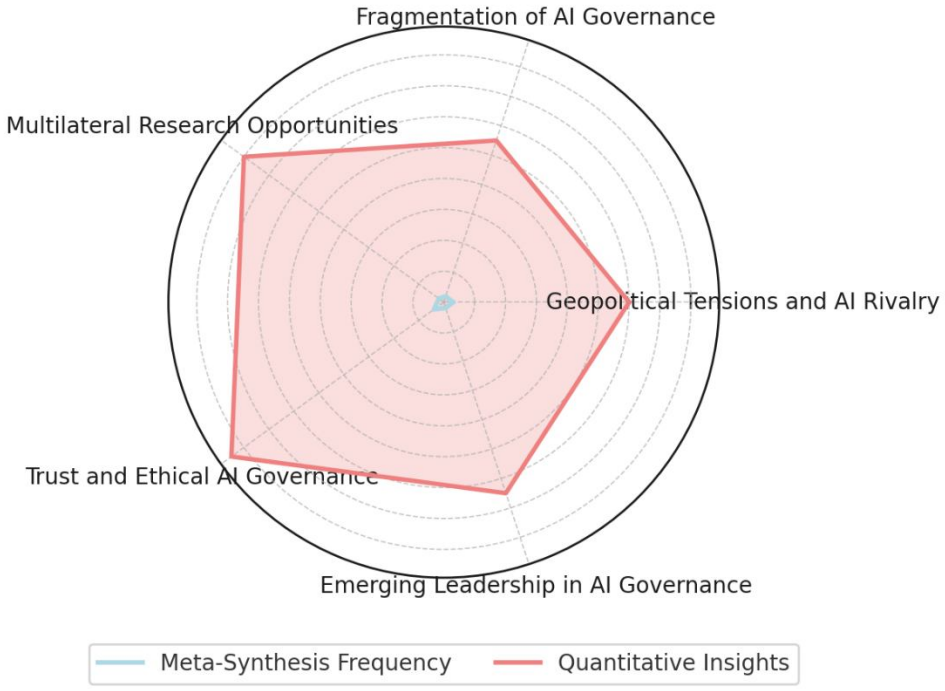

Figure 10: Integrated Meta-Synthesis and Quantitative Analysis

This integrated analysis directly supports Objective 3 by offering a comprehensive evaluation of barriers and opportunities, emphasizing the role of trust, ethics, and multilateral engagements in overcoming the challenges of geopolitical rivalry and fragmented governance in AI defense cooperation.

Discussion

This study aimed to evaluate the role of artificial intelligence (AI) in enhancing global security by examining its applications, assessing the risks and benefits of its deployment, and analyzing opportunities for international cooperation. The findings highlight the dual nature of AI, offering both operational advantages and significant ethical challenges in military operations, cybersecurity, and autonomous systems [1], [3], [21]. While AI has improved threat detection, surveillance, and efficiency, challenges remain, particularly around privacy, ethics, and the need for international regulation to govern AI responsibly [2], [3], [18].

The study's findings align with the literature, showing that AI's adoption in cybersecurity has improved detection rates from 86% in 2021 to 88.25% in 2023 and mitigation rates from 80.75% to 83.75%, reinforcing the literature's assertion that AI-driven algorithms are vital for neutralizing cyber threats [24]. At the same time, the rise in AI-driven attacks—increasing from 11.25 incidents in 2021 to 16.25 in 2023—supports the literature's concerns about AI's dual-use nature, where technological advancements also facilitate more sophisticated threats [1], [24]. Both the literature and findings underscore the need for AI innovation and robust governance frameworks to manage these risks [3], [39].

The quantitative network analysis further supports the literature's call for multilateral cooperation in AI defense. Strong collaboration ties between Germany (Total Score 10), the USA (Total Score 9), and the UK (Total Score 9) align with the literature on the success of alliances like the EU-USA in fostering AI development with democratic values [43], [44], [48]. However, the weaker ties between China (Total Score 4) and Western countries reflect the literature's emphasis on geopolitical tensions as a significant challenge to global AI cooperation [3], [18], [39]. This aligns with the difficulty of reconciling national security interests with global AI governance [18], [41].

The study's findings on the fragmentation of AI governance are consistent with the literature's observation of the global inconsistency in regulations. Initiatives like GPAI and OECD AI Principles advocate for transparency, but achieving global consensus remains challenging due to differing national priorities [14], [18], [42]. This fragmentation is evident in the study's collaboration gaps, especially among countries with geopolitical tensions.

Additionally, the study highlights the importance of multilateral research opportunities, with Western countries showing stronger collaboration ties in AI defense, supporting the literature's view that joint initiatives, such as the US-Israeli AI collaborations, are crucial for enhancing defense capabilities [14], [46]. This aligns with the literature's emphasis on AI partnerships to foster diplomatic relations [27], [47].

The study emphasizes trust-building through ethical AI governance, aligning with the literature's call for transparency, accountability, and human oversight. Countries with established trust, such as Germany (Total Score 10) and the USA (Total Score 9), are more likely to engage in cooperative AI initiatives, reinforcing the importance of shared

values and transparent governance in fostering sustainable international cooperation [41], [44].

5. Conclusion and Recommendation

This study emphasizes the transformative potential of AI in enhancing global security through improved surveillance, cybersecurity, and military operations. However, it also highlights the pressing need for robust governance frameworks to address the ethical, privacy, and geopolitical challenges AI poses. The findings demonstrate that while AI significantly improves threat detection and mitigation capabilities, its dual-use nature amplifies risks, particularly in the context of AI-driven attacks. International cooperation is essential to mitigate these risks, with trust-building, ethical governance, and multilateral research identified as key pathways for strengthening collaboration between nations.

Based on the findings of this study, the following recommendations to promote responsible AI deployment and encourage global cooperation are proposed to international policymakers, AI governance bodies, and multilateral defense organizations:

1. International policymakers, in coordination with multilateral organizations like the United Nations and OECD, should create a comprehensive international regulatory framework to govern AI use in global security, standardizing ethical standards, privacy protection, and accountability in the deployment of AI technologies, particularly in areas such as cybersecurity, military applications, and autonomous systems.

2. AI developers and international AI bodies such as the Global Partnership on AI should adopt measures to prioritize transparency, accountability, and human oversight in AI systems to improve ethical governance, especially in high-risk areas like cybersecurity and autonomous military applications, to enhance trust and cooperation between nations.

3. Policymakers and international organizations should maximize AI’s potential to address global challenges such as climate change and disaster response by fostering cross-border partnerships that focus on AI's predictive and analytical capabilities to strengthen global security and bolster diplomatic relations through shared goals.

Furthermore, the study proposes the Ethical AI-Diplomacy Model, presented in figure 11 below:

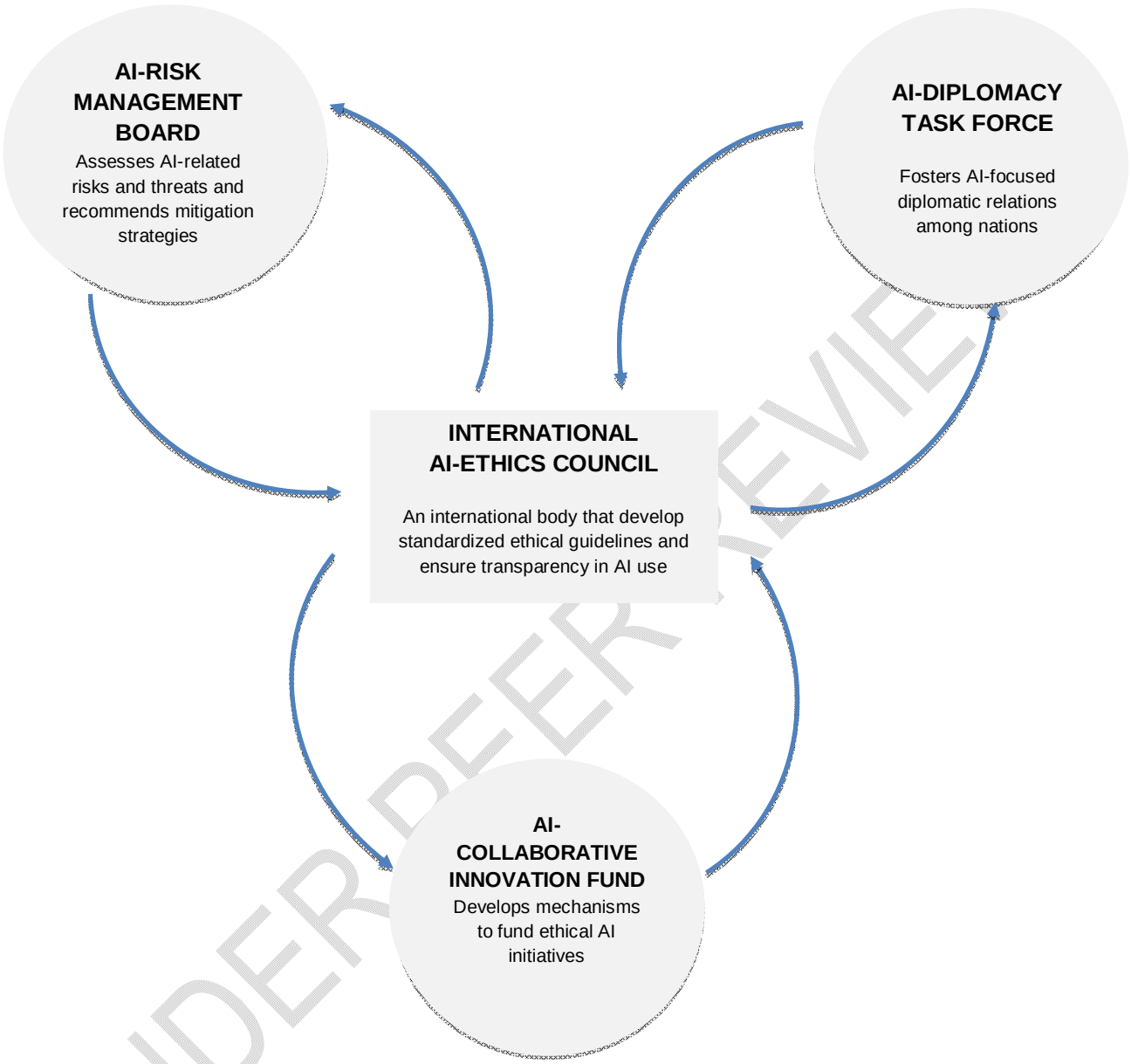

Figure 11: Ethical-AI Diplomacy (EAI-D) Model

The model emphasizes the collaborative and structured governance required for responsible AI development and global security. At the center, the **International AI-Ethics Council** plays a crucial role in establishing standardized ethical guidelines and coordinating between different entities. It interacts with three main components:

1. **AI-Diplomacy Task Force**: Focuses on fostering AI-focused diplomatic relations, encouraging international cooperation, and addressing geopolitical challenges.

2. **AI-Risk Management Board**: Assesses AI-related risks and threats, providing recommendations for mitigating potential security vulnerabilities.
3. **AI-Collaborative Innovation Fund**: Develops mechanisms to fund ethical AI initiatives, ensuring that innovation aligns with global security goals and ethical standards.

This interconnected structure promotes trust, transparency, and ethical governance, which are essential for enhancing global security and diplomatic relations in the age of AI, as outlined in the study.

References

[1] A. Bécue, I. Praça, and J. Gama, “Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities,” *Artificial Intelligence Review*, vol. 54, no. 1, Feb. 2021.

[2] A. Aldoseri, K. N. A. - Khalifa, and A. M. Hamouda, “Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges,” *Applied Sciences*, vol. 13, no. 12, pp. 7082–7082, 2023, doi: https://doi.org/10.3390/app13127082

[3] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, “Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review,” *Sensors*, vol. 23, no. 3, p. 1151, Jan. 2023, Available: https://www.mdpi.com/1424-8220/23/3/1151

[4] J. Truby, R. D. Brown, I. A. Ibrahim, and O. C. Parellada, “A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications,” *European Journal of Risk Regulation*, vol. 13, no. 2, pp. 1–29, Nov. 2021, doi: https://doi.org/10.1017/err.2021.52

[5] A. Chehri, I. Fofana, and X. Yang, “Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence,” *Sustainability*, vol. 13, no. 6, p. 3196, Mar. 2021, doi: https://doi.org/10.3390/su13063196

[6] R. Nishant, M. Kennedy, and J. Corbett, “Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda,” *International Journal of Information Management*, vol. 53, no. 53, p. 102104, Aug. 2020, doi: https://doi.org/10.1016/j.ijinfomgt.2020.102104

[7] N. Ayman, Khallaf, M. Nader, and Alqerafi, “Using Ai to Help Reduce the Effect of Global Warming,” *Power System Technology*, vol. 48, no. 1, 2024, Accessed: Sep. 10, 2024. [Online]. Available: https://powertechjournal.com/index.php/journal/article/download/464/346

[8] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, “Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441

[9] J. Cox and H. Williams, “The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability,” *The Washington Quarterly*, vol. 44, no. 1, pp. 69–85, Jan. 2021, doi: https://doi.org/10.1080/0163660x.2021.1893019

[10] M. M. Maas, “How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons,” *Contemporary Security Policy*, vol. 40, no. 3, pp. 285–311, Feb. 2019, doi: https://doi.org/10.1080/13523260.2019.1576464

[11] T. Dimitrov, “APPLYING ARTIFICIAL INTELLIGENCE FOR IMPROVING SITUATIONAL AWARENESS AND THREAT MONITORING AT SEA AS KEY FACTOR

FOR SUCCESS IN NAVAL OPERATION," *ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference*, vol. 4, no. 4, pp. 49–55, Jun. 2024, doi: https://doi.org/10.17770/etr2024vol4.8224

[12] Z. Davis, "Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise," *PRISM*, vol. 8, no. 2, pp. 114–131, 2019, Available: https://www.jstor.org/stable/26803234

[13] F. Morgan *et al.*, "Military Applications of Artificial Intelligence Ethical Concerns in an Uncertain World," 2020. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3139-1/RAND_RR3139-1.pdf

[14] C. Feijóo *et al.*, "Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy," *Telecommunications Policy*, vol. 44, no. 6, p. 101988, Jul. 2020, doi: https://doi.org/10.1016/j.telpol.2020.101988

[15] J. Muñoz-Basols, C. Neville, B. A. Lafford, and C. Godev, "Potentialities of Applied Translation for Language Learning in the Era of Artificial Intelligence," *Hispania*, vol. 106, no. 2, pp. 171–194, 2023, doi: https://doi.org/10.1353/hpn.2023.a899427

[16] F. Provost and T. Fawcett, "Data Science and its Relationship to Big Data and Data-Driven Decision Making," *Big Data*, vol. 1, no. 1, pp. 51–59, Feb. 2020, doi: https://doi.org/10.1089/big.2013.1508

[17] M. Adanma and E. Olurotimi, "Evaluating the effectiveness of global governance mechanisms in promoting environmental sustainability and international relations," *Finance & Accounting Research Journal*, vol. 6, no. 5, pp. 763–791, May 2024, doi: https://doi.org/10.51594/farj.v6i5.1151

[18] N. Díaz-Rodríguez, J. Del Ser, M. Coeckelbergh, M. López de Prado, E. Herrera-Viedma, and F. Herrera, "Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation," *Information Fusion*, vol. 99, no. 101896, p. 101896, Nov. 2023, Available: https://www.sciencedirect.com/science/article/pii/S1566253523002129

[19] J. Johnson, "Artificial Intelligence & Future warfare: Implications for International Security," *Defense & Security Analysis*, vol. 35, no. 2, pp. 147–169, Apr. 2019, doi: https://doi.org/10.1080/14751798.2019.1600800

[20] A. Calderaro and S. Blumfelde, "Artificial intelligence and EU security: the false promise of digital sovereignty," *European Security*, vol. 31, no. 3, pp. 415–434, Jul. 2022, doi: https://doi.org/10.1080/09662839.2022.2101885

[21] O. O. Olaniyi, F. A. Ezeugwa, C. G. Okatta, A. S. Arigbabu, and P. C. Joeaneke, "Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies," *Archives of current research international*, vol. 24, no. 5, pp. 124–139, Apr. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5690

[22] M. Raska and Bitzinger, “The AI Wave in Defence Innovation,” *Google Books*, 2023. https://books.google.com/books?hl=en&lr=&id=UcGxEAAAQBAJ&oi=fnd&pg=PT8&dq=AI+technologies+provide+unprecedented+capabilities+in+surveillance (accessed Sep. 10, 2024)

[23] V. Shah, “Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats,” *Revista Espanola de Documentacion Cientifica*, vol. 15, no. 4, pp. 42–66, 2021, Available: https://redc.revistas-csic.com/index.php/Jorunal/article/view/156

[24] I. H. Sarker, M. H. Furhad, and R. Nowrozy, “AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions,” *SN Computer Science*, vol. 2, no. 3, Mar. 2021, doi: https://doi.org/10.1007/s42979-021-00557-0

[25] S. Feldstein, “The Global Expansion of AI Surveillance,” 2019. Available: https://blog.fdik.org/2019-09/WP-Feldstein-AISurveillance_final1.pdf

[26] M. Xue, C. Yuan, H. Wu, Y. Zhang, and W. Liu, “Machine Learning Security: Threats, Countermeasures, and Evaluations,” *IEEE Access*, vol. 8, no. 8, pp. 74720–74742, 2020, doi: https://doi.org/10.1109/access.2020.2987435

[27] M. Bistron and Z. Piotrowski, “Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens,” *Electronics*, vol. 10, no. 7, p. 871, Apr. 2021, doi: https://doi.org/10.3390/electronics10070871

[28] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, “Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601

[29] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, “A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques,” *Ad Hoc Networks*, vol. 111, no. 111, p. 102324, Feb. 2021, doi: https://doi.org/10.1016/j.adhoc.2020.102324

[30] O. O. Olateju, S. U. Okon, U. T. I. Igwenagu, A. A. Salami, T. O. Oladoyinbo, and O. O. Olaniyi, “Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud,” *Asian Journal of Research in Computer Science*, vol. 17, no. 6, pp. 264–292, Jun. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i6472

[31] T. Araujo, N. Helberger, S. Kruikemeier, and C. H. de Vreese, “In AI We trust? Perceptions about Automated decision-making by Artificial Intelligence,” *AI & SOCIETY*, vol. 35, no. 3, Jan. 2020, doi: https://doi.org/10.1007/s00146-019-00931-w

[32] J. Cowls, A. Tsamados, M. Taddeo, and L. Floridi, “The AI gambit: Leveraging Artificial Intelligence to Combat Climate change—opportunities, challenges, and

Recommendations," *AI & SOCIETY*, vol. 38, no. 1, Oct. 2021, doi: https://doi.org/10.1007/s00146-021-01294-x

[33] B. Merz *et al.*, "Impact Forecasting to Support Emergency Management of Natural Hazards," *Reviews of Geophysics*, vol. 58, no. 4, Oct. 2020, doi: https://doi.org/10.1029/2020rg000704

[34] T. Yigitcanlar, K. C. Desouza, L. Butler, and F. Roozkhosh, "Contributions and Risks of Artificial Intelligence (AI) in Building Smarter Cities: Insights from a Systematic Review of the Literature," *Energies*, vol. 13, no. 6, p. 1473, Mar. 2020, Available: https://www.mdpi.com/1996-1073/13/6/1473

[35] O. O. Olaniyi, O. O. Olaoye, and O. J. Okunleye, "Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector," *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 18, pp. 22–35, Jul. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i181055

[36] D. Almeida, K. Shmarko, and E. Lomas, "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks," *AI and Ethics*, vol. 2, no. 3, Jul. 2021, Available: https://link.springer.com/article/10.1007/s43681-021-00077-w

[37] S. U. Okon, O. O. Olateju, O. S. Ogungbemi, S. A. Joseph, A. O. Olisa, and O. O. Olaniyi, "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*, vol. 26, no. 9, pp. 136–158, Sep. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i91269

[38] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized AI for cyber attacks," *Journal of Information Security and Applications*, vol. 57, no. 57, p. 102722, Mar. 2021, doi: https://doi.org/10.1016/j.jisa.2020.102722

[39] B. W. Wirtz, J. C. Weyerer, and B. J. Sturm, "The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration," *International Journal of Public Administration*, vol. 43, no. 9, pp. 818–829, Apr. 2020, doi: https://doi.org/10.1080/01900692.2020.1749851

[40] O. O. Olateju, S. U. Okon, O. O. Olaniyi, A. D. Samuel-Okon, and C. U. Asonze, "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*, vol. 26, no. 7, pp. 244–268, Jun. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71206

[41] A. D. Samuel-Okon, O. I. Akinola, O. O. Olaniyi, O. O. Olateju, and S. A. Ajayi, "Assessing the Effectiveness of Network Security Tools in Mitigating the Impact of Deepfakes AI on Public Trust in Media," *Archives of Current Research International*, vol. 24, no. 6, pp. 355–375, Jul. 2024, doi: https://doi.org/10.9734/acri/2024/v24i6794

[42] S. Fukuda-Parr and E. Gibbons, “Emerging Consensus on ‘Ethical AI’: Human Rights Critique of Stakeholder Guidelines,” *Global Policy*, vol. 12, no. S6, pp. 32–44, Jun. 2021, Available: https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12965

[43] A. Taeihagh, “Governance of artificial intelligence,” *Policy and Society*, vol. 40, no. 2, pp. 137–157, Apr. 2021, doi: https://doi.org/10.1080/14494035.2021.1928377

[44] A. Habbal, M. K. Ali, and M. A. Abuzaraida, “Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions,” *Expert Systems with Applications*, vol. 240, no. 122442, p. 122442, Apr. 2024, doi: https://doi.org/10.1016/j.eswa.2023.122442

[45] O. O. Olaniyi, J. C. Ugonnia, F. G. Olaniyi, A. T. Arigbabu, and C. S. Adigwe, “Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 140–156, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5444

[46] J. Johnson, “The end of military-techno Pax Americana? Washington’s strategic responses to Chinese AI-enabled military technology,” *The Pacific Review*, vol. 34, no. 3, pp. 1–28, Oct. 2019, doi: https://doi.org/10.1080/09512748.2019.1676299

[47] O. S. Ogungbemi, F. A. Ezeugwa, O. O. Olaniyi, O. I. Akinola, and O. B. Oladoyinbo, “Overcoming Remote Workforce Cyber Threats: A Comprehensive Ransomware and Bot Net Defense Strategy Utilizing VPN Networks,” *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 161–184, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81237

[48] E. Igbinenikaro and A. O. Adewusi, “NAVIGATING THE LEGAL COMPLEXITIES OF ARTIFICIAL INTELLIGENCE IN GLOBAL TRADE AGREEMENTS,” *International journal of applied research in social sciences*, vol. 6, no. 4, pp. 488–505, Apr. 2024, doi: https://doi.org/10.51594/ijarss.v6i4.987

[49] S. Gupta, S. Modgil, A. Kumar, U. Sivarajah, and Z. Irani, “Artificial intelligence and cloud-based Collaborative Platforms for Managing Disaster, extreme weather and emergency operations,” *International Journal of Production Economics*, vol. 254, no. 8, p. 108642, Dec. 2022, doi: https://doi.org/10.1016/j.ijpe.2022.108642

[50] D. Suprayitno, S. Iskandar, K. Dahurandi, T. Hendarto, and F. Rumambi, “Migration Letters Public Policy In The Era Of Climate Change: Adapting Strategies For Sustainable Futures,” 2024. Available: https://repository.ibmasmi.ac.id/assets/files/content/f_0434_20240226133456.pdf

[51] J. R. Biden, “Defense Technical Information Center,” *Dtic.mil*, 2024. https://apps.dtic.mil/sti/citations/AD1157244

[52] A. Dafoe, “AI Governance: A Research Agenda,” 2017. Available: http://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf

[53] A. D. Samuel-Okon, “Behind the Screens: A Critical Analysis of the Roles of Guilds and Associations in Standardizing Contracts, Wages, and Enforcing Professionalism amongst Players in the Entertainment Industry,” *Asian Journal of Economics Business and Accounting*, vol. 24, no. 9, pp. 166–187, Sep. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i91484

[54] A. D. Samuel-Okon, “Navigating the Shadows: Understanding and Addressing Sexual Harassment Challenges in the Entertainment Industry,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 9, pp. 98–117, Sep. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i9738

[55] S. Abdul, P. Adeghe, O. Adegoke, A. Adegoke, and H. Udedeh, “AI-enhanced healthcare management during natural disasters: conceptual insights,” *Engineering science & tecnology journal*, vol. 5, no. 5, pp. 1794–1816, May 2024, doi: https://doi.org/10.51594/estj.v5i5.1155

[56] O. O. Olaniyi, O. O. Omogoroye, F. G. Olaniyi, A. I. Alao, and T. O. Oladoyinbo, “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*, vol. 26, no. 6, p. 32, 2024, doi: https://doi.org/10.9734/JERR/2024/v26i61160

[57] S. Abdul, P. Adeghe, O. Adegoke, A. Adegoke, and H. Udedeh, “AI-enhanced healthcare management during natural disasters: conceptual insights,” *Engineering science & tecnology journal*, vol. 5, no. 5, pp. 1794–1816, May 2024, doi: https://doi.org/10.51594/estj.v5i5.1155

[58] ESCWA and W. H. O. world health organization, “WATER AND CLIMATE CHANGE The United Nations World Water Development Report 2020,” 2020. Accessed: Sep. 09, 2024. [Online]. Available: https://repository.unescap.org/bitstream/handle/20.500.12870/7402/ESCAP-2020-RP-Water-climate-change.pdf?sequence=1

[59] R. Schwartz, A. Vassilev, K. Greene, L. Perine, A. Burt, and P. Hall, “Towards a Standard for Identifying and Managing Bias in Artificial Intelligence,” *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, no. 1270, Mar. 2022, doi: https://doi.org/10.6028/nist.sp.1270

[60] S. Singh and M. K. Goyal, “Enhancing climate resilience in businesses: The role of artificial intelligence,” *Journal of Cleaner Production*, vol. 418, p. 138228, Sep. 2023, doi: https://doi.org/10.1016/j.jclepro.2023.138228

[61] A. D. Samuel-Okon, O. O. Olateju, S. U. Okon, O. O. Olaniyi, and U. T. I. Igwenagu, “Formulating Global Policies and Strategies for Combating Criminal Use and Abuse of Artificial Intelligence,” *Archives of current research international*, vol. 24, no. 5, pp. 612–629, Jun. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5735

[62] J. C. Molina-Molina, M. Salhaoui, A. Guerrero-González, and M. Arioua, “Autonomous Marine Robot Based on AI Recognition for Permanent Surveillance in Marine Protected Areas,” *Sensors*, vol. 21, no. 8, p. 2664, Jan. 2021, doi: https://doi.org/10.3390/s21082664

[63] D. Qiao, G. Liu, T. Lv, W. Li, and J. Zhang, “Marine Vision-Based Situational Awareness Using Discriminative Deep Learning: A Survey,” *Journal of Marine Science and Engineering*, vol. 9, no. 4, p. 397, Apr. 2021, doi: https://doi.org/10.3390/jmse9040397

[64] A.-S. Martin and S. Freeland, “The Advent of Artificial Intelligence in Space Activities: New Legal Challenges,” *Space Policy*, vol. 55, no. 4, p. 101408, Feb. 2021, doi: https://doi.org/10.1016/j.spacepol.2020.101408

[65] L. Schmitt, “Mapping global AI governance: a nascent regime in a fragmented landscape,” *AI and Ethics*, Aug. 2021, doi: https://doi.org/10.1007/s43681-021-00083-y

[66] O. O. Olaniyi, “Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447

[67] L. Lescrauwaet, H. Wagner, C. Y. Yoon, and S. Shukla, “Adaptive Legal Frameworks and Economic Dynamics in Emerging Tech-nologies: Navigating the Intersection for Responsible Innovation,” *Law and Economics*, vol. 16, no. 3, pp. 202–220, Oct. 2022, doi: https://doi.org/10.35335/laweco.v16i3.61

[68] B. Shneiderman, “Bridging the Gap Between Ethics and Practice,” *ACM Transactions on Interactive Intelligent Systems*, vol. 10, no. 4, pp. 1–31, Nov. 2020, Available: https://dl.acm.org/doi/abs/10.1145/3419764

[69] A. D. Samuel-Okon, “Headlines to Hard-Lines: Media Intervention in Managing Bullying and Cancel Culture in the Entertainment Industry,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 9, pp. 71–89, Aug. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i9736

[70] C. Huang, Z. Zhang, B. Mao, and X. Yao, “An Overview of Artificial Intelligence Ethics,” *IEEE Transactions on Artificial Intelligence*, vol. 4, no. 4, pp. 1–21, 2022, doi: https://doi.org/10.1109/tai.2022.3194503

[71] J. E. Fountain, “The moon, the ghetto and artificial intelligence: Reducing systemic racism in computational algorithms,” *Government Information Quarterly*, vol. 39, no. 2, p. 101645, Oct. 2021, doi: https://doi.org/10.1016/j.giq.2021.101645

[72] S. C. Robinson, “Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI),” *Technology in Society*, vol. 63, p. 101421, Oct. 2020, doi: https://doi.org/10.1016/j.techsoc.2020.101421

[73] O. I. Akinola, O. O. Olaniyi, O. S. Ogungbemi, O. B. Oladoyinbo, and A. O. Olisa, “Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks,” *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 112–134, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81234

[74] Y. K. Dwivedi *et al.*, “Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging challenges, opportunities, and Agenda for research, Practice and Policy,” *International Journal of Information Management*, vol. 57, no. 101994, Aug. 2021, doi: https://doi.org/10.1016/j.ijinfomgt.2019.08.002

[75] C. U. Asonze, O. S. Ogungbemi, F. A. Ezeugwa, A. O. Olisa, O. I. Akinola, and O. O. Olaniyi, “Evaluating the Trade-offs between Wireless Security and Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances,” *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 411–432, Aug. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81255

[76]M. M. Maas, “How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons,” *Contemporary Security Policy*, vol. 40, no. 3, pp. 285–311, Feb. 2019, doi: https://doi.org/10.1080/13523260.2019.1576464

[77]Q. Zhu and K. Long, “How will artificial intelligence impact Sino–US relations?,” *China International Strategy Review*, vol. 1, no. 1, pp. 139–151, Jun. 2019, doi: https://doi.org/10.1007/s42533-019-00008-9

[78]D. Araya and M. King, “The impact of artificial intelligence on military defence and security,” *www.econstor.eu*, 2022. https://www.econstor.eu/handle/10419/299735 (accessed Sep. 17, 2024).

[79]L. Schmitt, “Mapping global AI governance: a nascent regime in a fragmented landscape,” *AI and Ethics*, Aug. 2021, doi: https://doi.org/10.1007/s43681-021-00083-y

[80]A. R. Wasil, T. Reed, J. W. Miller, and P. Barnett, “Verification methods for international AI agreements,” *arXiv.org*, 2024. https://arxiv.org/abs/2408.16074 (accessed Sep. 17, 2024).

[81]S. C. Robinson, “Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI),” *Technology in Society*, vol. 63, p. 101421, Oct. 2020, doi: https://doi.org/10.1016/j.techsoc.2020.101421

[82]A. S. Gill, “Artificial Intelligence and International Security: The Long View,” *Ethics & International Affairs*, vol. 33, no. 02, pp. 169–179, 2019, doi: https://doi.org/10.1017/s0892679419000145

[83]C. O'keefe, “How Will National Security Considerations Affect Antitrust Decisions in AI? An Examination of Historical Precedents Introduction: The Confluence of AI, National Security, and Antitrust,” 2020. Accessed: Sep. 17, 2024. [Online]. Available: https://www.fhi.ox.ac.uk/wp-content/uploads/How-Will-National-Security-Considerations-

Affect-Antitrust-Decisions-in-AI-Cullen-OKeefe.pdf

[84]S. Security and Order, “AFTER THE FOUNDATIONAL AGREEMENTS: AN AGENDA FOR US-INDIA DEFENSE AND SECURITY COOPERATION,” 2021. Accessed: Sep. 17, 2024. [Online]. Available: https://www.brookings.edu/wp-content/uploads/2021/01/FP_20210111_us_india_white.pdf

[85]“China’s Incoming AI Ethics Leadership Push,” *Manifund.org*, 2023. https://manifund.org/projects/chinas-incoming-ai-ethics-leadership-push (accessed Sep. 17, 2024).

[86]E. Lin-Greenberg, “Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making (Spring 2020),” *repositories.lib.utexas.edu*, 2020, Accessed: Sep. 17, 2024. [Online]. Available: https://repositories.lib.utexas.edu/items/4e3969e7-996c-4298-acde-7c85011add17/