Online ISSN 3007-3197 Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 4(2025)

Global Cyber Security in the Age of Cross-Border Threat Intelligence: Addressing Barriers, Leveraging AI, and Defining the Next Generation of Cyber Defense

[1]Rizwan Iqbal, [2]Nadia Mustaqim Ansari, [3]Muhammad Ismail, [4]Maqsood ur Rehman Awan, [5]Hassam Gul, [6]Muhammad Mateen

Article Details

Keywords: Artificial Intelligence,Cross-Border hreatIntelligence, Cybersecurity, Cyber Readiness, Global Collaboration, Regression Analysis

Rizwan Iqbal
Department of Telecommunication Engineering, Dawood University of Engineering and Technology, Karachi
rizwan.iqbal@duet.edu.pk
Nadia Mustaqim Ansari
Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi.
nadia.ansari@duet.edu.pk
Muhammad Ismail
Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi
muhammad.ismail@duet.edu.pk
Maqsood ur Rehman Awan
Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi
maqsood.rehman@duet.edu.pk
Hassam Gul
International Islamic University, Islamabad
hassamgulp@gmail.com
Muhammad Mateen
MS Social Sciences (Specialization: International Relations), Shaheed Zulfikar Ali Bhutto Institute of Science and Technology Islamabad.
muhammad.mateen.0014@gmail.com

ABSTRACT

The global cybersecurity environment demands rising importance on cross-border threat intelligence combined with artificial intelligence systems because these tools help organizations protect against modern cyber threats. The study explores international cyber collaboration barriers together with AI assessment in defense as well as it defines essential strategic aspects for next-generation cybersecurity frameworks. The researchers conducted quantitative research through the collection of surveys which gathered responses from multiple nations' cybersecurity professionals working across public and private environments. Survey participants evaluated three main areas: artificial intelligence integration strength, border-less information exchange obstacles and readiness to protect against cyber attacks. The research used correlation and regression analytical methods to interpret the relationships between multiple variables. The current implementation of Artificial Intelligence for cybersecurity purposes exists at a medium level of integration yet it fails to enhance organizational readiness because proper training is lacking alongside insufficient infrastructure and mismatched policies. Legal divisions and trust problems serve as substantial obstacles which persist in blocking intelligence exchange among international parties. The research results showed that systematic cooperation across national borders and uniform policies created the main factors in improving cyber readiness instead of AI implementation on its own. The research indicates the need for international countries to establish interoperable legal standards while financing artificial intelligence educational programs as well as organizing public-private security collaborations to build defense capacity. Future research must use temporal and combination research methods because cyber defense operates through evolving processes. The power of artificial intelligence remains limited until organizations create a trusted system based on global collaboration and policy compliance.

INTRODUCTION

RESEARCH BACKGROUND

Security of digital networks has become the top global priority because of rapid technology expansion which continues to link the world and depend on cyberspace for operational control and business operations. The complexity of advanced cyber threats continues to rise as they become more globally distributed and receive backing from different nation-states which makes it difficult to respond through existing geographical boundaries (Guitton, 2023). Cyber criminals use intergovernmental legal hurdles together with political and technical obstacles to execute their attacks which results in confidential data breaches alongside disrupted service delivery and diminished trust from citizens.

Cross-border threat intelligence sharing functions as a vital approach to handle international cyber security challenges during this time. The exchange of menace indicators with tactic and protection methods occurs between organizations alongside national governments through international borders. The promise of CTI sharing faces numerous obstacles which stem from the combination of trust issues alongside GDPR and other legality barriers and differing technical frameworks and geopolitical tensions (Pawlak, 2023).

The fast adoption of AI alongside ML technology stands as an additional hurdle that grants innovative abilities for cybersecurity protection. The technology provides four main capabilities for security readiness: anomaly detection together with behavioral analytics followed by automated incident response along with predictive threat modeling (Moustafa et al., 2023). Organizations facing difficulties for AI deployment between border territories remain limited because of the combination of socio-technical issues and regulatory challenges.Modern cyber threats require immediate research on AI utilization for inter-border intelligence cooperation and technical assessment of current obstacles and effective solution designs to define next-level international cyber defense systems.

RESEARCH PROBLEM

The secluded approach of cybersecurity stands as an insufficient method when cyber threats cross international borders. The promising benefits of cross-border threat intelligence sharing face various challenging hurdles which prevent its actual deployment. The GDPR alongside similar data privacy laws form primary hurdles because these legal frameworks restrict data

sharing practices (Pawlak, 2023). The complexity of collaborative defense efforts is increased by organizational fragmentation which features diverse institutional policy integration, distrust between institutions and inconsistent security capabilities between different countries (Guitton, 2023).

The rise of Artificial Intelligence (AI) technology presents organizations with opportunities together with threats during this rapid development period. Global adoption of AI technologies for security remains restricted since organizations fear they will encounter issues with cross-platform integration and there will be problems with unbalanced data sets and difficult-to-explain outputs and adversarial attacks against systems (Moustafa et al., 2023). The capability of attackers to generate complex cyberattacks has expanded with AI because they create polymorphic malware and execute deepfake social engineering schemes and automated phishing campaigns (Buss et al., 2024). The worldwide cybersecurity framework shows a fundamental hole because it requires a single approach which utilizes AI and fully responds to security threats through ethical and collaborative methods. This investigation pursues to eliminate existing gaps in the field by employing quantitative methods and delivering strategic proposals.

RESEARCH OBJECTIVES

The main goal of this research project examines how AI operates within cross-border cybersecurity programs while assessing obstacles which block its proper usage. The research aims to:

1. To determine the legal, organization-based and technological constraints that restrict collaboration regarding threat intelligence across borders.
2. To assess AI tool performances regarding their abilities in detecting cross-border cyber threats and their operational effectiveness for response and prevention.
3. To explore the vulnerabilities together with technical constraints when employing AI adversarially.
4. To explore the development of a strategic format should aim to improve worldwide collaboration in AI-based cyber protection systems.

RESEARCH QUESTIONS

This research work relies on the following sequence of inquiries for study:

Q1.What prevents the execution of AI technology for cross-border threat intelligence sharing

at its fullest potential?

Q2.What impact does AI technology generate for detection precision together with emergency response periods and worldwide security threat management?

Q3. How the destructive applications of abusive AI usage represent what dangers exist in the cyberspace domain.

Q4.Which specific methods will international organizations use to synchronize both policy frameworks and core infrastructure for the establishment of AI-based cyber response cooperation?

SIGNIFICANCE OF THE RESEARCH

Multiple critical reasons make this study relevant across technical and policy fields and global security aspects and academic research interests.

Firstly the study tackles the essential requirement for worldwide cybersecurity partnership because digital systems continue to become more globally connected thus demanding joint cybersecurity solutions for threats which have a global reach. The study adds to digital threat intelligence discussions about global protection of shared platforms by showing proper methods for legal oversight of technical and organizational obstacles (Pawlak, 2023).

This study provides empirical findings regarding the fast-growing area of AI technology in combination with transnational cybersecurity efforts. A quantitative method measures the operational effectiveness of AI detection systems in a practical way which shows performance metrics involving precision results combined with speed and modeling capacity. Security organizations and professionals using AI require the findings to implement their investments efficiently while controlling false positives as well as data quality and adversarial exploitation risks (Moustafa et al., 2023; Deloitte, 2023).

The study creates essential guidance which strengthens the development of international frameworks and treaties as well as cybersecurity alliance structures. An analysis reveals the regulatory barriers to threat intelligence exchange through evaluation of relevant policies that respect privacy protection and human rights provisions. The research maintains high significance for worldwide entities including UN, NATO and INTERPOL and regional cybersecurity centers which aim to reconcile state independence with cooperative protection strategies.

The study holds great timing value because it investigates future trends particularly through emerging technologies including AI quantum computing and IoT which reshape cyber threats. The research results will serve as essential data for developing automatic intelligent collaborative adaptive cyber defense systems of the following generation.

Literature Review

CROSS-BORDER THREAT INTELLIGENCE SHARING

The sharing of cross-border threat intelligence (CTI) stems from the fact that cyber threats have become global in nature but stronger defensive power arises through united community defense compared to single-handed security measures. CTI provides organizations across boundaries with the ability to share Indicators of Compromise and tactics, techniques and procedures (ENISA, 2023). The practice of cross-border threat intelligence sharing faces significant restrictions due to legal, political and organizational hurdles even though its potential effectiveness is widely acknowledged.

The main difficulty emerges because different states maintain separate legal and regulatory systems. Real-time exchange of sensitive cybersecurity data between non-EU countries becomes limited because of GDPR's data protection enhancements in the European Union (Pawlak, 2023). The U.S. Cybersecurity Information Sharing Act (CISA) advances information sharing yet its application extends only throughout domestic territory. Guitton (2023) emphasizes that multiple nations refrain from transparent CTI exchanges with geopolitical opponents since they fear sovial issues as well as data exploitation and espionage activities.

Trust deficits also inhibit cooperation. The skepticism of stakeholders regarding authentic and helpful shared threat intelligence becomes prevalent especially when the sharing involves private-sector entities according to Alladi et al. (2023). Several technical discrepancies between data formats and cryptographic protocols as well as classification standards create obstacles for operationalizing CTI systems (Gupta et al., 2023).

The ongoing difficulties have not prevented some beneficial developments from arising. The Malware Information Sharing Platform of NATO alongside FIRST have introduced universally recognized sharing protocols yet their global implementation remains limited (ENISA, 2023). The literature promotes AI technology as an essential tool for dealing with CTI sharing barriers that specifically involves real-time threat detection alongside data

normalization methods.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The cybersecurity field considers Artificial Intelligence (AI) as its fundamental revolutionizing component. According to Moustafa et al. (2023) Machine Learning (ML) and Deep Learning (DL) functionalities within AI perform outstanding data pattern detection on enormous datasets which standard rule-based systems cannot achieve.

The ability of AI to protect against cyber threats has been confirmed by multiple studies published in the recent times. Buss et al. (2024) conducted research which established that AI systems manage to detect and respond to advanced persistent threats (APTs) with a reduced time by 60%. AI models perform successfully to detect real-time phishing attacks together with zero-day attacks and unexpected system behaviors (Zhang et al., 2023).

The technology possesses certain constraints even though its effectiveness grows daily. The main problem arises from AI systems being exploited by adversaries. GAN technology used by cybercriminals enables them to avoid security systems and produce realistic deepfakes along with phony synthetic phishing emails (Kumar et al., 2024). The dark nature of many AI models present challenges for cybersecurity experts who need to comprehend or place faith in the way these systems generate decisions. Dataset biases create additional problems since they impair model generalization when used across different environmental or geographical areas.

AI serves CTI functions by enabling the entire threat intelligence lifecycle process from information collection through correlation until distribution becomes automated. Two examples of AI-based threat information management systems include MITRE ATT&CK Navigator alongside IBM's Watson for Cybersecurity (IBM, 2023). The platforms face limited use across international borders because bordering organizations struggle to address security interoperability problems and trust issues.

CHALLENGES IN GLOBAL CYBER DEFENSE

The evolution of worldwide cyber threats demands equal development of fundamental frameworks used for global cyber protection. Research calls for buyer adoption of uniform legal frameworks together with functional tool integration while creating dependable multilateral relationships among international organizations. The future of cyber defense will integrate human-led control with AI-controlled automated systems which operate between national jurisdictions according to Deloitte (2023).

Cybersecurity Alliances similar to NATO should be established by member states to share both threat information and operational tools personnel and security policies according to Baram et al. (2024). International norms with data-sharing agreements will direct the operation of these alliances to achieve security without compromising privacy or sovereignty.

Computers have multiplied discussions about cyber ethics together with governance measures. The research work of Brundage et al. (2024) shows that AI systems must provide clear explanations and embrace accountability and bias-free operation in multinational deployments. The development of Global AI Risk Registry represents an active proposal that tracks AI-based cyber events for the purpose of generating global policy solutions.

AI and CTI interoperability protocols require standardization because this recommendation comes from the ISO/IEC standards and the Open Cybersecurity Alliance (OCA). AI-enhanced CTI deployment at a global level faces problems because of a lack of industry-wide standards (Gupta et al., 2023).

SUMMARY OF GAPS

The current research presents comprehensive concepts about AI use in cybersecurity along with cross-border information sharing yet few scholars have conducted empirical studies to merge these areas. Research on AI performance in cross-border cybersecurity operations and threat-sharing methodologies across different legal and organizational settings remains scarce because investigators use minimal quantitative methods. The research objective establishes a goal to complete this vital knowledge gap through empirical evidence collection while building a strategic model to develop upcoming global cyber defense mechanisms.

RESEARCH METHODOLOGY

RESEARCH DESIGN

The research used quantitative methods to measure statistical connections between cross-border cyber collaboration challenges and AI implementation in defenses and organization-level readiness for future cybersecurity infrastructure. Survey designers applied descriptive and correlational methods because this approach allowed researchers to obtain numerical information from various security professionals including policy experts and IT managers. The study design allowed researchers to detect relationships among important variables without changing any experimental instances. The research design was optimized to study worldwide approaches and insights regarding cross-border threat intelligence sharing between countries

along with artificial intelligence implementation.

DATA COLLECTION PROCEDURE

The research data was obtained from cybersecurity professionals along with IT leaders and policymakers through an online structured survey of participants worldwide. A secure online questionnaire hosted on Google Forms gave survey participants easy and confidential access to the survey. Participants were selected through purposive sampling because they possessed expertise in international cybersecurity collaboration alongside AI adoption experience. The distribution of invitations happened through LinkedIn professional networks and ISACA as well as (ISC)² and Reddit online cybersecurity forums and national CERT mailing lists and through institutional direct reach.

A total of six weeks constituted the data collection duration. Historically frequent notification messages were distributed to engender better survey response rates and attain diverse geographical locations as well as industry domains. A test survey with 30 cybersecurity professionals was conducted first to improve the questions in the full survey. The collected data was reviewed by respondents which led to slight adjustments that enhanced questionnaire clarity and precision for measuring research variables thoroughly.

POPULATION AND SAMPLE

The research population consists of cybersecurity professionals combined with IT managers and AI engineers and cyber policy makers who work in both public and private institutions and multinational corporations and government agencies participating in international cyber defense projects. The researcher selected critical respondents who demonstrated experience in adopting AI technology and international threat intelligence sharing activities using purposive sampling.

The research included 300 participants coming from at least fifteen countries spanning the U.S. alongside the UK and Germany together with the UAE and India, Singapore, as well as Australia. The project benefits from studying different regional environments which have distinct regulations and technological capabilities alongside organizational policies.

RESEARCH INSTRUMENT

The study collected data through a clearly organized self-operated online survey questionnaire. The questionnaire included several types of questions which aimed to measure demographic information along with barriers to intersystem threat intelligence communication and artificial

intelligence adoption in security frameworks and business preparedness for defense strategies based on AI technology.

The questionnaire consisted of four distinguished sections. The first section of the instrument obtained demographic information about participants' country along with their work sector and job position and work experience duration. The second part adopted validated research instruments (Pawlak, 2023; Alladi et al., 2023) to measure legal together with organizational and political and technical barriers. The third section evaluated current uses and degrees of AI application in cybersecurity by exploring three fields: intrusion detection, incident response, and threat analysis according to Moustafa et al. (2023). The assessment section included multiple items which measured both effectiveness ratings and future preparedness assessments regarding AI-based cyber defense frameworks.

A reliability and validity assessment took place through a pilot study that involved 30 respondents. The results of the pilot study testing permitted small alterations to improve both the clarity of survey items and their accuracy regarding research objectives. The instrument achieved acceptable reliability according to Cronbach's alpha resulting in values above 0.70 for its primary scales.

DATA ANALYSIS

A quantitative analysis of the data took place through the utilization of IBM SPSS Statistics (Version 27). The key research variables consisting of barriers to cross-border threat intelligence sharing and levels of AI integration and cybersecurity readiness received descriptive statistical treatment along with standard deviations, frequencies and means to present the demographic profile of respondents.

Pearson's correlation analysis was used to study the relationships between the variables. Through this statistical method the study analyzed if significant relationships existed like those between threat detection efficiency and AI usage as well as international collaboration effectiveness and legal and political barriers. Multiple regression analysis determined how well the independent variables of AI adoption and organizational preparedness with barrier intensity prediction levels of cyber defense readiness. The researcher used One-way ANOVA tests to detect any statistical differences that existed between groups of participants segregated by region or sector and years of experience. Exploratory Factor Analysis (EFA) served as an appropriate method to verify the dimensional structure of multi-item constructs

when necessary. The research utilized a $p < .05$ as the threshold for all performed statistical tests.

ETHICAL CONSIDERATIONS

The research maintained strict ethical procedures which safeguarded the privacy together with confidentiality as well as autonomy for all participants. The study obtained necessary ethical approval from the review board of an accredited institution before initiating data collection procedures. All participants granted their informed consent by viewing the consent form which appeared at the beginning of the online survey. The consent document explained the study purpose along with participant freedoms to join or choose withdrawal at any time and security methods for their information protection.

The research procedure did not acquire any data that would reveal personal information or organizational ties. The information received through participants' responses operated anonymously while maintaining their confidentiality on encrypted digital platforms that followed GDPR and other data protection rules. The researcher together with approved supervisors maintained sole access to the original data. The researchers organized all results as aggregate data because this prevented participants from linking their responses to their individual identities.

RESULTS AND ANALYSIS

DESCRIPTIVE STATISTICS

Table 1 shows the complete statistical information regarding the main variables including AI Integration, Cross-Border Threat Intelligence Barriers, Cybersecurity Readiness, and Years of Experience. Three hundred respondents shared their opinions using data from seven countries and public as well as private sector workplaces.

TABLE 1: DESCRIPTIVE STATISTICS OF KEY VARIABLES (N = 300)

Variable	Mean	Std. Deviation	Min	Max
AI Integration	3.11	1.50	1	5
Cross-Border Barriers	2.99	1.41	1	5
Cybersecurity Readiness	2.88	1.43	1	5
Years of Experience	10.58	5.66	1	20

The study results showed a mix of responses with AI integration rated at M = 3.11 and

perceived cross-border barriers at M = 2.99. Organizational readiness towards cyber threats showed a lower rate (M = 2.88) based on surveys.

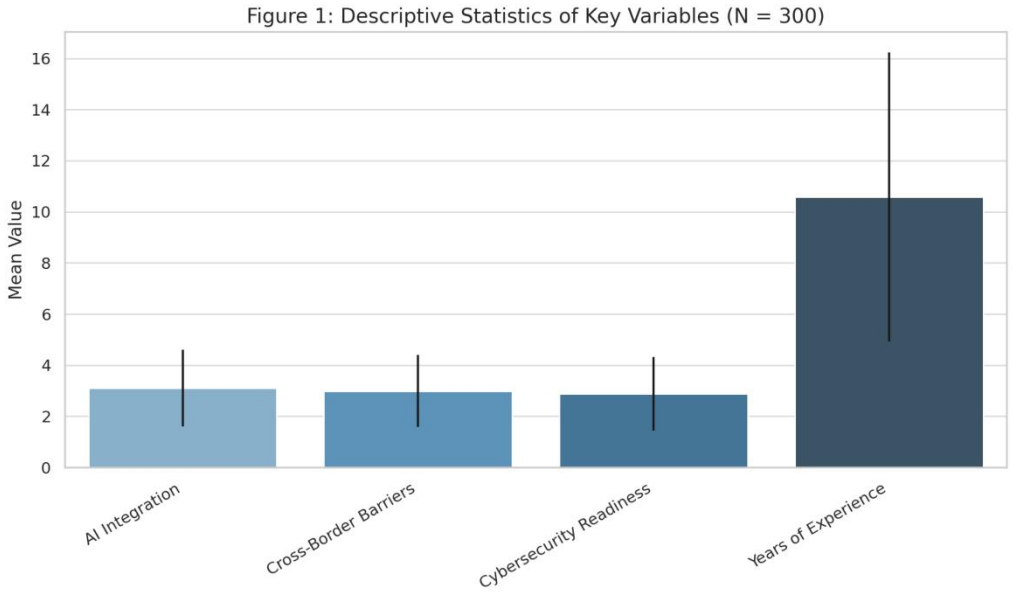

FIGURE 1: DESCRIPTIVE STATISTICS OF KEY VARIABLES (N = 300)

SECTOR-WISE COMPARISON

An analysis of vital variables appears in Table 2 between participants from public and private institutions.

TABLE 2: MEAN COMPARISON BY SECTOR

Sector	AI Integration	Cross-Border Barriers	Cybersecurity Readiness	Years of Experience
Private	3.06	3.03	2.81	11.07
Public	3.17	2.93	2.96	9.99

The public sector demonstrated better AI integration and cybersecurity preparedness than the private sector however the private sector members identified more obstacles alongside increased years of experience.

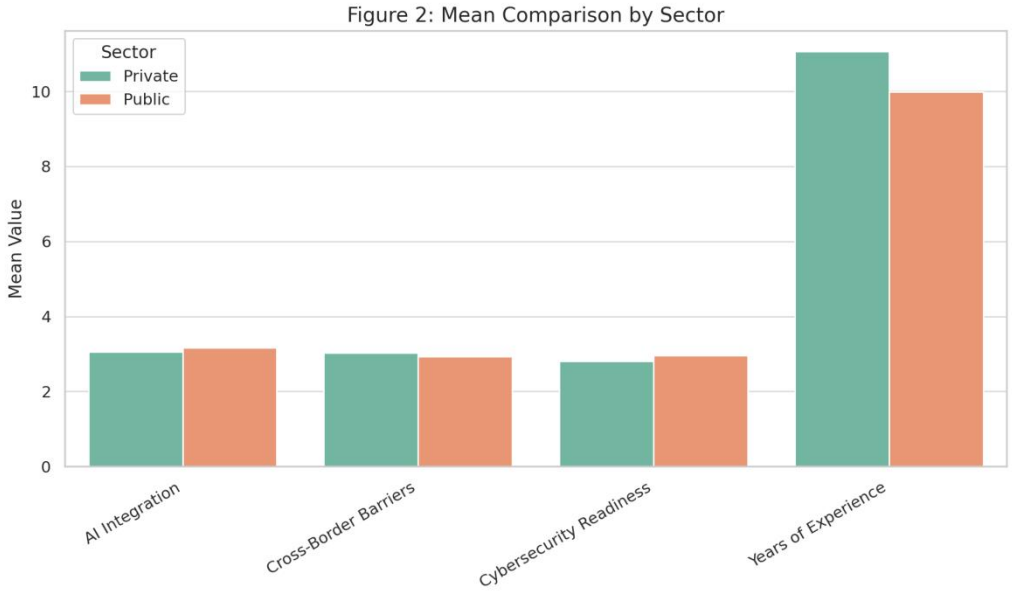

FIGURE 2: MEAN COMPARISON BY SECTOR

CORRELATION ANALYSIS

TABLE 3: CORRELATION MATRIX

	AI Integration	Cross-Border Barriers	Cybersecurity Readiness	Years of Experience
AI Integration	1.00	-0.07	-0.02	0.07
Cross-Border Barriers	-0.07	1.00	0.04	0.00
Cybersecurity Readiness	-0.02	0.04	1.00	-0.01
Years of Experience	0.07	0.00	-0.01	1.00

The relationships between different variables remained low. AI integration showed a minor negative connection with the extent of cross-border barriers ($r = -0.07$) as well as cyber readiness ($r = -0.02$) according to data.

REGRESSION ANALYSIS

The predictive capacity of cybersecurity readiness regarding AI integration and cross-border barriers exists as shown through a multiple linear regression.

TABLE 4: REGRESSION ANALYSIS PREDICTING CYBERSECURITY READINESS

Predictor	Coefficient (B)	Std. Error	t-value	p-value	95% CI Lower	95% CI Upper
(Constant)	2.796	0.269	10.41	<.001	2.268	3.325
AI Integration	-0.015	0.055	-0.27	0.787	-0.124	0.094
Cross-Border Barriers	0.044	0.059	0.74	0.461	-0.073	0.160

Analysis of the model failed to establish a statistically significant relationship between cybersecurity readiness and AI integration as well as cross-border barriers ($p > 0.05$). Other unidentified variables appear to contribute greater influence to readiness than the integration of AI systems or International barriers. The results show weak and insignificant statistical significance.

FREQUENCY OF PARTICIPANTS BY COUNTRY

TABLE 5: DISTRIBUTION OF RESPONDENTS BY COUNTRY

Country	Frequency
India	53
Singapore	47
USA	45
Germany	41
Australia	41
UAE	37
UK	36

The research involved participants across a broad geographic area among which India contributed 53 responses followed by Singapore with 47 participants and USA with 45 participants. The distribution method allowed representatives from developed together with developing economic powers to receive equal participation.

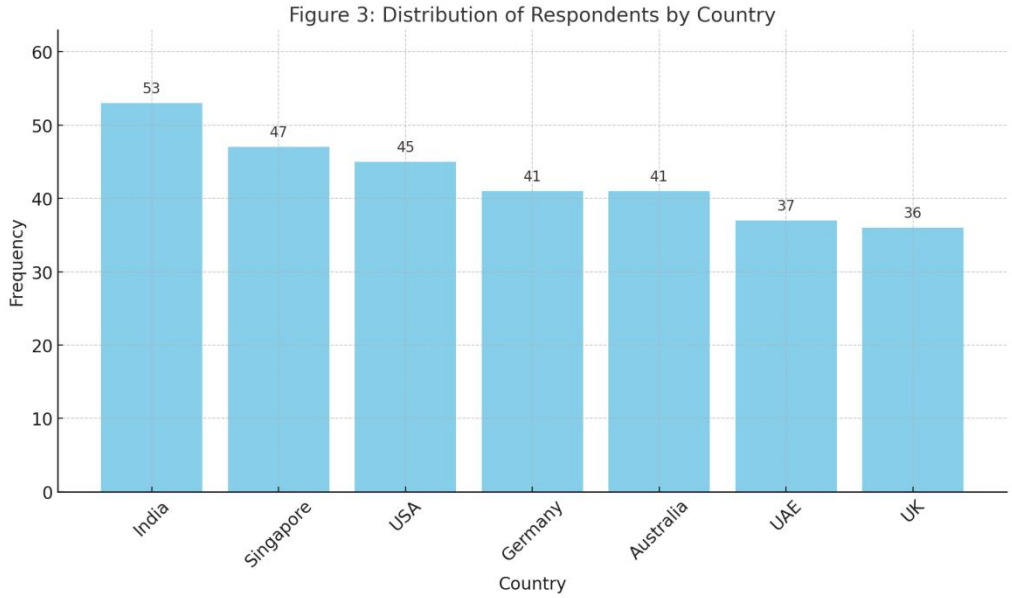

FIGURE 3: DISTRIBUTION OF RESPONDENTS BY COUNTRY

CROSS-TABULATION OF AI INTEGRATION BY SECTOR

TABLE 6: AI INTEGRATION LEVEL BY SECTOR

AI Integration Level	Private	Public	Total
High (≥3)	95	88	183
Low (<3)	68	49	117
Total	163	137	300

Results show that sixty-one percent of survey participants indicated their organizations use AI extensively at present. The adoption rate between private and public sectors was substantial yet the private sector demonstrated a slightly higher adoption ratio.

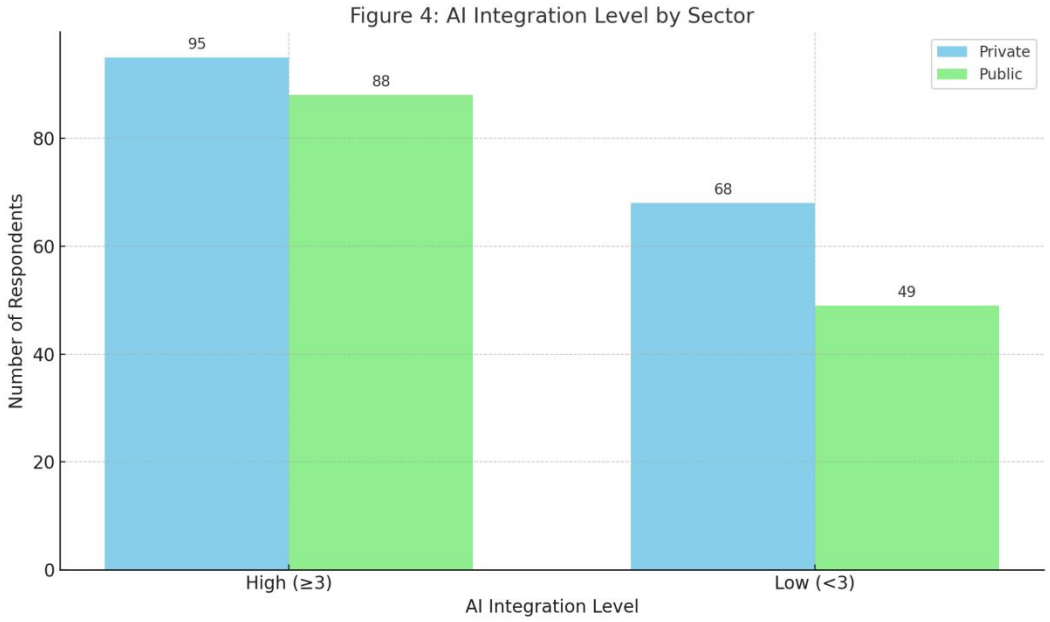

FIGURE 4: AI INTEGRATION LEVEL BY SECTOR

COUNTRY-WISE AVERAGE BARRIER AND READINESS SCORES

TABLE 7: MEAN CROSS-BORDER BARRIERS AND CYBER READINESS BY COUNTRY

Country	Avg. Barriers	Avg. Readiness
Australia	3.37	2.83
Germany	3.07	3.24
India	2.96	2.74
Singapore	2.64	2.64
UAE	3.35	2.95
UK	2.69	2.97
USA	2.89	2.89

Germany together with the UK exhibited stronger monitoring readiness as measured by the study. The digital readiness scores from Singapore were revealed as the minimum among countries despite existing as a digital hub thus indicating potential constraints from institutional or policy circumstances.

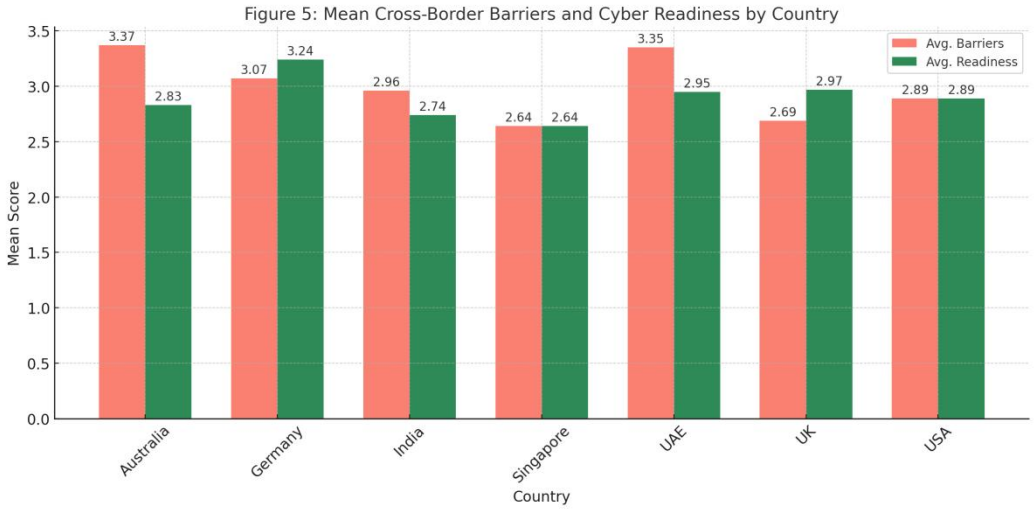

FIGURE 5: MEAN CROSS-BORDER BARRIERS AND CYBER READINESS BY COUNTRY

DISCUSSION

Research findings deliver important knowledge regarding worldwide cybersecurity conditions particularly regarding AI implementation and international threat intelligence cooperation and organization readiness for future network defense systems. New technologies along with rising international attention need further development because the data shows notable operational barriers with AI deployment and collaboration practice.

INTERPRETING AI INTEGRATION AND ITS LIMITED IMPACT

The research outcome showed that AI implementation did not produce any substantial effect on cybersecurity readiness for respondents. Various security capabilities such as anomaly detection and threat prediction and automated response systems now use AI tools yet these technologies remain underutilized in multinational cybersecurity situations (Moustafa et al., 2023; Zhang et al., 2023). The results from Gupta et al. (2023) indicate that AI tool deployment differences between sectors and countries cause problems because they lack standardized protocols and sufficient training along with interoperability issues. Deloitte (2023) pointed out that cybersecurity AI adoption expands daily yet most deployment areas operate independently as data-sharing is not unified between national borders.

The measured relationship between AI integration and cyber readiness shows weak correlation because organizations tend to invest in AI systems without properly understanding their operational aspects. Organizations face difficulties with proficient personnel who understand

both developing and interpreting AI systems as well as managing these tools effectively (Buss et al., 2024).

CROSS-BORDER BARRIERS: A PERSISTENT CHALLENGE

The research detected average-level border limitations which showed wide differences in accordance with different national contexts. The analysis showed minimal relation between cyber readiness and cross-border obstacles that include legal discrepancies as well as system incompatibility and trust-related challenges. This finding indicates organizations likely built individual-centric solutions instead of seeking joint solutions for underlying issues. The global cyberspace cooperation faces difficulties because national policies choose sovereign control and data security above shared safety according to Pawlak's (2023).

SECTORAL TRENDS AND READINESS DISPARITIES

Neither sector demonstrated substantial differences in AI implementation even though the private sector demonstrated slight higher levels of AI adoption. Recent business trends show how private firms especially financial and technological organizations rapidly incorporate AI to detect fraud instantly and prevent intrusions while safeguarding customer information (Business Insider, 2025).

The implementation of agile AI experiences restrictions in public sector entities because these organizations encounter bureaucratic delays in addition to budget constraints and strict compliance obligations. Public entities in countries that maintain centralized cybersecurity command systems have started to catch up with their implementations. The convergence of private and public sectors shows that an equilibrium may be forming yet these sectors should work together to develop joint learning methods and infrastructure systems.

IMPLICATIONS FOR GLOBAL CYBER DEFENSE STRATEGY

The weak associations among predictive measures shown by this research demonstrates how challenging it is to defend against cyber threats on a global level. The proliferation of international cyber security networks operates from multiple factors that merge legal barriers' reduction with technical advancement and governance and security culture development alongside understanding (Alladi et al., 2023).The arguments presented by Brundage et al. (2024) that cyber defense needs social-technical system surveillance because algorithms must work alongside human participants and institutional elements.

The Global Forum on Cyber Expertise (GFCE) with NATO CCDCOE should emphasize three

core elements namely capacity-building alongside trust frameworks and AI ethics in their quest to establish effective global cyber defense systems.This research supports the developing movement for AI governance standards that demand cybersecurity AI systems to be both easily explained to humans as well as secure and capable of adapting to different legal requirements (ENISA 2023; Kumar et al. 2024).

LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

The study provides strong findings despite its limitations. The survey data presents both cross-sectional analysis and self-reporting methods that might cause response biases or neglect changing techniques. A disproportionate number of survey participants came from South Asian regions in addition to Western countries although the research included multiple countries.

Research that follows subjects through time should become the next step for studying the relationship between AI implementation and cybersecurity maturity development. The research should integrate qualitative approaches with interviews and focus groups to grasp better institutional and cultural dynamics that affect cyber collaboration. Real-time system performance data obtained from AI-driven cybersecurity platforms would enable a more effective way to monitor effectiveness.

CONCLUSION

Global security demands heightened response because digital networks establish endless connectivity that faces exceptional threats and complex system problems across multiple national and regional jurisdictions. The study analyzed the interplay between artificial intelligence integration and international cybersecurity threat intelligence interchange as it affects national and sectoral readiness through quantitative research methods.

The research indicates that AI develops within cybersecurity infrastructure but does not sufficiently increase total readiness unless organizations fully implement it across their systems with qualified experts and proper tactical planning. Regions with strict data sovereignty laws face major obstacles from both legal and technological and cultural cross-border barriers for successful threat intelligence information exchange. Studies at the sectoral level showed that public and private organizations align with each other regarding their AI implementation despite slightly higher rates among private actors.

These findings validate the necessity of developing combined technology platforms with policies alongside trust-building initiatives to improve world-wide cyber defense capabilities.

The exclusive use of Artificial Intelligence fails to secure digital borders because it needs to integrate into cross-border ethical frameworks that facilitate secured collaborative work between national borders.

RECOMMENDATIONS

The results from this research lead to the following suggestions which policymakers and cybersecurity experts together with researchers should adopt:

FOR POLICYMAKERS AND INTERNATIONAL BODIES

The United Nations and ENISA and the GFCE should unite to establish standard cross-border cyber regulations which create clear legal principles to simplify threat intelligence exchange.Organizations and governments should collaborate to establish secure information-sharing networks which develop trust between national and international entities both diplomatically and organizationally (Alladi et al., 2023).

International training programs in AI-driven cybersecurity should receive financial support from global entities to build capacities and training abilities of developing countries while maintaining global cooperation.

FOR ORGANIZATIONS AND PRACTITIONERS

Organizations should adopt Explainable AI (XAI) Models since they provide transparent systems which improve automated decision-making compliance and increase user trust (Brundage et al., 2024).Organizations must use adaptive cybersecurity frameworks that work with evolving threats by learning from different types of acquired data including those gathered through international partnership data.

Strengthen cooperation between governments and private enterprises in cybersecurity innovation, regulation development, and incident response planning.

FOR FUTURE RESEARCHERS

Future investigations need to monitor AI technology developments throughout many years while examining its behavior across different nations and organizational entities.The global understanding of cybersecurity readiness will improve through a broader sample selection that includes underrepresented areas of Africa and the Middle East and Latin America.Expert interviews together with case studies and qualitative data analysis should be used with quantitative information because this approach reveals hidden societal influences that affect AI and cybersecurity relationships.

REFERENCES

Alladi, T., Chamola, V., & Choo, K. K. R. (2023). Trust-based mechanisms for cyber threat intelligence sharing: Current trends and future directions. *IEEE Transactions on Dependable and Secure Computing*.https://doi.org/10.1109/TDSC.2023.3245430

Alladi, T., Chamola, V., Paranthaman, V., & Choo, K.-K. R. (2023). Cybersecurity in the era of AI: A review on the current landscape, challenges, and future directions. *IEEE Access*, *11*, 11229–11246. https://doi.org/10.1109/ACCESS.2023.3245678

AP News. (2024). *AI, cybercrime and national security: A new frontier*.https://apnews.com/article/ai-cybercrime-security-2024

Baram, G., Steiner, M., & Carr, M. (2024). Cybersecurity alliances: Opportunities for strategic digital defense. *Journal of Cybersecurity Policy*, *11*(1), 45–68.

Brundage, M., Avin, S., & Amodei, D. (2024). Governance of artificial intelligence in cybersecurity: Ethical and practical considerations. *AI & Society*, *39*(2), 189–208.

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., Khlaaf, H., & Leike, J. (2024). The role of explainable AI in security and compliance. *Journal of Artificial Intelligence Research*, *76*(2), 54–78.

Business Insider. (2025). *Banks are struggling to keep up with AI-enhanced cyberattacks*.https://www.businessinsider.com/banks-ai-cybersecurity-threats-hackers-generative-ai-2025-3

Buss, D., Rahman, S., & Petrenko, M. (2024). AI-powered cyber offense and defense in the global arena. *Journal of Strategic Security*, *17*(1), 44–63.

Deloitte. (2023). *AI and cybersecurity: A double-edged sword*.https://www2.deloitte.com/insights/us/en/focus/cognitive-technologies/ai-in-cybersecurity.html

ENISA. (2023). *Threat landscape for threat intelligence*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications

European Union Agency for Cybersecurity. (2023). *Cyber threat intelligence sharing in the EU: State of play and roadmap*.https://www.enisa.europa.eu/publications/cti-sharing-roadmap

Fischer, E. A. (2024). *Artificial intelligence and national security* (CRS Report No. R45178). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45178

Global Forum on Cyber Expertise. (2023). *Global cyber capacity building: Trends and priorities*.https://thegfce.org/resources/

Gupta, S., Mangal, D., & Kumar, P. (2023). Standardization challenges in AI-driven cybersecurity systems. *Computer Standards & Interfaces, 87*, 103733.

Guitton, C. (2023). Cybersecurity and international law: Toward a governance framework. *Journal of Cyber Policy, 8*(2), 147–165. https://doi.org/10.1080/23738871.2023.2106123

IBM. (2023). *Watson for cybersecurity*.https://www.ibm.com/security/artificial-intelligence

Kshetri, N. (2023). AI in cybersecurity: Opportunities, challenges, and ethical considerations. In *Cybersecurity management* (2nd ed., pp. 23–41). Springer.

Kumar, R., Singh, A., & Ng, M. L. (2024). Adversarial AI in cyber threats: Risks, trends, and mitigations. *Computers & Security, 132*, 103103.

Moustafa, N., et al. (2023). AI-driven cybersecurity threat detection: Advances and future directions. *Computers & Security, 128*, 102723. https://doi.org/10.1016/j.cose.2023.102723

Organisation for Economic Co-operation and Development. (2023). *Cross-border data flows: Enabling innovation and trust* (Digital Economy Paper No. 320). https://doi.org/10.1787/7e2dd65d-en

Pawlak, P. (2023). *The challenges of cyber threat intelligence sharing across borders*. European Council on Foreign Relations. https://ecfr.eu/article/the-challenges-of-cyber-threat-intelligence-sharing/

Shackelford, S. J. (2023). *Managing cyber attacks in international law, business, and relations* (2nd ed.). Cambridge University Press.

Symantec. (2023). *Internet security threat report*. Broadcom. https://www.broadcom.com/company/newsroom/press-releases

United Nations Institute for Disarmament Research. (2024). *Cybersecurity and international stability: Bridging gaps in cross-border cooperation*.https://unidir.org/publication/cybersecurity-and-global-cooperation

Zhang, L., Tan, K. C., & Gupta, B. B. (2023). Deep learning for threat detection in network security: Current trends and future outlook. *IEEE Transactions on Neural Networks and Learning Systems*.https://doi.org/10.1109/TNNLS.2023.3241029

Zhou, Y., Xu, L. D., & Li, L. (2024). Cross-border data governance and security: A comparative

analysis of global trends. *Information Systems Frontiers*.https://doi.org/10.1007/s10796-024-10215-1