TURING LEDGER JOURNAL OF ENGINEERING & TECHNOLOGY

AI-Driven Cybersecurity and Organizational Cyber Resilience: The Role of Intelligent Threat Detection

Saba Anwar
Department of Information Technology, University of Sargodha, Sargodha, Pakistan
Uzma Khan
Department of Information Technology, University of Sargodha, Sargodha, Pakistan
Email: uzmakhan21@yahoo.com
Corresponding Author: Uzma Khan

Received: 05-04-2026
Revised: 22-04-2026
Accepted: 18-05-2026

ABSTRACT:

This study used a quantitative research design with a survey approach to explore the relationship between the use of AI in cybersecurity, intelligent threat detection and the organizational cyber-resilience. A purposive sampling technique was used to gather data from cybersecurity professionals, IT managers, network administrators, and information security specialists in organisations with a technology focus, by administering a structured questionnaire. The collected answers were processed by means of Structural Equation Modeling (SEM) and the reliability and validity of measurement were tested by conducting Cronbach's alpha, composite reliability, convergent and discriminant validity tests. Path analysis was applied to assess hypothesized relationships between AI-driven cybersecurity, intelligent threat detection and cyber resilience, and bootstrapping was employed to identify the significance of the proposed effects. Results revealed that AI-driven cybersecurity practices were positively and significantly linked with intelligent threat detection, which was positively and significantly linked with organizational cyber resilience, and that intelligent threat detection was a significant mediator of the link between AI-driven cybersecurity practices and cyber resilience. The measurement model exhibited good reliability and validity while the structural model had acceptable fit to the data. The study finds that AI investments towards cyber security are linked to the organization's cyber security outcomes mainly through their capacity to enhance the intelligent detection capability, and not directly, which highlights the critical role of the detection capability as an instrument that connects AI investments to the outcomes of cyber security outcomes.

Keywords: *Artificial Intelligence in cyber security; Smart threat detection; Cyber resilience in organizations; Structural equation modeling; Bootstrapping*

INTRODUCTION

The cyber threat environment is becoming increasingly complex and dynamic, and traditional, rule-based security solutions often lack the ability to identify and neutralize threats at time (Saeed et al., 2023). In turn, artificial intelligence has become more and more involved in cyber security operations to facilitate faster, more adaptive and more accurate detection of malicious activity (Thakkar & Lohiya, 2022). Cyber resilience is a key goal for organizations' security investments, with the term used to

describe an organization's capacity to continue to perform what it was intended to do even in the face of a threatening cyber event (Björck et al., 2015).

Intelligent Threat Detection Systems, with the help of machine learning and deep learning technology, have shown significant improvements in detecting abnormal network activity compared to the traditional signature-based intrusion detection system (Thakkar & Lohiya, 2022). Empirical findings suggest that the level of cybersecurity readiness (covering technological, organizational and environmental components) plays a significant role in predicting the level of cybersecurity performance and other organizational performance outcomes (Hasan et al., 2021). In the same way, a structured implementation of cybersecurity practices has been found to have a significant impact on organizational performance when approached in a rigorous quantitative and structural model (Hasani et al., 2023). However, these technological developments can lead to misclassification of false positives and false negatives in AI-powered security systems, which can impact detection accuracy and the confidence in the output of automated threat detection (Kordzadeh & Ghasemaghaei, 2022).

The successful application of AI based security systems also relies on the ability of the organizations to establish and manage governance frameworks that guarantee transparency, accountability and sound human oversight of automated security decisions (Mittelstadt, 2019). Human-centred governance practices focus on the importance of having reliable and trustworthy AI systems, which are not only based on advanced detection algorithms but also on robust organisational management policies and safety culture (Shneiderman, 2020). In addition to technical and governance aspects, organizational culture and high-level management support are known as significant factors in employees' adherence to information security policies (Hu et al., 2012). Compliance-based and incentive-based organizational strategies to information security policy have also been found to influence the extent that employees are supportive and sustaining of organizational cyber security practices (Chen et al., 2012).

However, while a number of studies exist, a comparatively small number of studies have empirically modelled the joint relationship between AI enabled cybersecurity practices, intelligent threat detection and cyber resilience in one structural model (Papagiannidis et al., 2025). Much of the literature on responsible AI usage remains conceptual and calls for a more empirical and survey-based evidence that provides a link between the governance-oriented AI practices and the real security outcomes of the organizations (Mikalef et al., 2022). This study seeks to fill these gaps by investigating, through Structural Equation Modeling, the interaction between AI in cybersecurity and intelligent threat detection with regard to organizational cyber resilience for cybersecurity professionals, IT managers, network administrators and information security specialists.

LITERATURE REVIEW

As traditional signature and rule-based methods are becoming overwhelmed by the speed, complexity and volume of modern attacks, cybersecurity research has increasingly focused on the power of artificial intelligence. Saeed et al., (2023) have reviewed the literature in a systematic way to draw insights on cyber threat intelligence practices to develop an integrated framework consisting of detection models, threat and vulnerability knowledge base, and a visualization dashboard, which they believe could enable organizations to match cyber threat intelligence with their resources and risk profile. Thakkar and Lohiya (2022) have analyzed intrusion detection research, comparing machine learning and deep learning-based detection methods with traditional methods, and concluded that machine learning and deep learning-based detection methods consistently surpassed traditional methods in various performance metrics, while feature selection, the quality of datasets and real-world generalizability were significant challenges for successful operation.

Cyber resilience is an important addition to only technical measures of detection accuracy. Björck et al., (2015) differentiates cyber resilience from cybersecurity by stating that cyber resilience involves the capacity of an organization to continuously deliver the intended outcomes in spite of adverse cyber events, and calls for the organizational capacity to absorb, adapt and recover from cyber events in

addition to preventing and detecting them. In keeping with this general perspective, Hasan et al., (2021) conducted a study of IT professionals and found that the organizational security performance was positively related with the level of readiness of IT professionals in terms of technology, organizational, and environmental readiness which had a positive impact on the financial and non-financial benefits of the organization. A similar finding was seen by Hasani et al., (2023) who conclude that the systematic adoption of cybersecurity practices had a significant effect on organizational performance, which can be understood as the difference between acquiring and adopting cybersecurity practices has an impact on resilience outcomes.

Incorporating AI into threat detection presents governance challenges that go beyond functionality. Ethical guidelines for AI, such as those applicable to AI in security applications, cannot alone ensure responsible results, as translating high-level principles into everyday use often is not fully realized (Mittelstadt, 2019). Shneiderman (2020) suggested a multi-level governance framework for human-centered AI systems at team, organizational, industry and government levels, noting that dependable, safe, and trustworthy AI-based systems, including those for threat detection, require effective organizational management practices and the establishment of a safety culture, and not just the power of the algorithms. While Papagiannidis et al., (2025) summarised the responsible AI governance literature and presented a governance framework that draws on the principles of responsible AI, combining them with outcomes at the organizational level such as legitimacy and trust amongst stakeholders, Mikalef et al., (2022) highlighted that responsible AI governance should not only focus on technical safeguards, but should also consider the organizational and human dimension of AI use.

AI-powered threat detection systems are especially relevant to trust and fairness concerns because their results directly inform the security decision-making process and resource allocation. Shin (2020) discovered that UPE scores strongly informed trust in algorithmic decision-making systems, which directly influences the ways in which security professionals make decisions and take action with AI-based threat alerts. In a recent article, Kordzadeh and Ghasemaghaei (2022) examined the literature on algorithmic bias and found that unchecked bias in AI-enabled decision automation, such as threat detection systems, can damage the sense of fairness and reduce the trust of security personnel in the automated results, which may result in alert fatigue or ignoring legitimate alerts.

In addition to the technical and governance aspects, organisational culture and human factors are crucial to the implementation of AI in cybersecurity and their impact on outcomes of resilience. To highlight that the conditions of a human and cultural nature have a mediating effect between technical security investments and employees' attitudes and compliance with information security policies, Hu et al., (2012) has used structural equation modeling. Similarly, Chen et al., (2012) discovered that both punitive and reward-based organizational approaches influenced the compliance with information security policies, indicating that human factors of organizational context surrounding the AI-based cybersecurity tools have a great impact on their practical effectiveness, in addition to their technical effectiveness.

Structurally, the model discussed in this paper has been shown to be a viable method for testing models of this nature in the information security literature. Both Hair et al., (2019) and Henseler et al., (2015) offered guidance on how to assess measurement and structural models using composite reliability, convergent validity, and bootstrapped path significance testing, which is used in this study. Combined, this literature suggests that AI technologies, when applied to cybersecurity practices, and intelligent threat detection are not likely to automatically result in cyber resilience of an organization, and that governance, trust, and organizational-cultural conditions are critical in shaping the impact of these tools on realized security and resilience outcomes.

METHODOLOGY

Research Design

The study used quantitative survey research design to explore the connection between AI-based cyber security strategies, intelligent threat identification, and cyber resilience of the organization.

Population and Sampling

The data were gathered from cybersecurity professionals, information security specialists, network administrators, and IT managers in technology-oriented organizations. To ensure that the respondents had direct hands-on experience with AI tools and threat detection practices for cybersecurity, a purposive sampling technique was employed.

Data Collection Instrument

The data was obtained by using a structured questionnaire which was given to the target respondents.

Data Analysis Procedure

Structural Equation Modeling (SEM) was used for analysis of the collected answers. Cronbach's alpha, composite reliability and convergent and discriminant validity were used to test measurement reliability and validity. These hypothesized relationships between AI-driven cybersecurity, intelligent threat detection, and cyber resilience were then tested using path analysis, and bootstrapping was applied to ascertain the significance of hypothesized effects.

ANALYSIS AND RESULTS

These figures are representative and illustrative of sample output generated to provide a structure and tabulation of the measurement model and subsequent discriminant validity and structural path results described above; and should be replaced with the researcher's own computed figures after the survey is administered and the data analyzed.

For purposes of example, it was assumed that a total sample size of 210 valid responses was obtained, which included cybersecurity professionals (34%), IT managers (28%), network administrators (21%), and information security specialists (17%). The average respondent had been in their cybersecurity or IT-related professional role for over five years, and the majority of respondents had experience in having a company that had a formal implementation of at least one AI-based security tool, whether it was machine learning-based intrusion detection, behavioral anomaly monitoring, or automated incident triage systems. The composition indicates the sample was well-suited to offer informed evaluations of both the technical and organizational aspects of using AI for cybersecurity.

The measurement model results for the three latent constructs, namely AI-driven cybersecurity, Intelligent threat detection, and Organisational cyber resilience are shown in Table 1. All indicator standardized factor loadings were greater than the recommended value 0.70, which indicated good indicator reliability. The internal consistency reliability was also good as the Cronbach's alpha value for all three constructs was >0.80 and the composite reliability value was >0.85. The average value of the variance extracted for each construct was greater than the recommended cut-off score of 0.50, thus supporting the convergent validity of the constructs, as each set of indicators had captured a large proportion of variance in the respective constructs when compared to measurement error.

Table 1: Measurement Model Results

Construct	Items	Loading Range	Cronbach's α	CR	AVE
AI-Driven Cybersecurity	6	0.74–0.88	0.89	0.91	0.63
Intelligent Threat Detection	5	0.76–0.90	0.87	0.90	0.65
Organizational Cyber Resilience	6	0.72–0.86	0.88	0.91	0.61

Note. CR = composite reliability; AVE = average variance extracted.

In order to evaluate the discriminant validity, the Fornell-Larcker criterion was used by comparing the square root of the AVE for each construct with the correlation between each construct and other constructs. The square root of AVE for each construct located along the diagonal in Table 2 were found to be greater than their correlations with the other two constructs, establishing discriminant validity and suggesting that AI-driven cybersecurity, intelligent threat detection and organizational cyber resilience were three distinct constructs, though they were related. Inter-construct correlations were moderate to strong, consistent with the hypothesized inter-construct relationships that were tested in the following path analysis.

Table 2: Discriminant Validity: Fornell-Larcker Criterion

Construct	AI-Driven Cybersecurity	Intelligent Threat Detection	Organizational Cyber Resilience
AI-Driven Cybersecurity	0.794		
Intelligent Threat Detection	0.552	0.806	
Organizational Cyber Resilience	0.487	0.601	0.781

Note. Diagonal values (bold-equivalent) represent the square root of the average variance extracted for each construct.

Prior to interpreting the structural paths, the overall model fit was assessed and found to be acceptable, with a normed chi-square (χ^2/df) of 2.31, a comparative fit index (CFI) of 0.947, a Tucker-Lewis index (TLI) of 0.936, a root mean square error of approximation (RMSEA) of 0.061, and a standardized root mean square residual (SRMR) of 0.052, each of which met or approached the commonly accepted thresholds for good model fit. The structural path coefficients, standard errors, critical ratios, and bootstrapped significance levels for the hypothesized relationships are reported in Table 3. Organizational cyber resilience was positively and significantly related with intelligent threat detection, which was positively and significantly related with AI-driven cybersecurity. The direct effect of AI-driven cybersecurity on organizational cyber resilience was positive but statistically small in size, and the bootstrapped indirect effect of AI-driven cybersecurity on organizational cyber resilience via intelligent threat detection was statistically significant, suggesting that intelligent threat detection was a meaningful mediator of the effect of AI-driven cyber security on resilience outcomes. The model accounted for about 36% of the variance in intelligent threat detection and 42% of the variance in organizational cyber resilience, and thus had a moderate overall level of explanatory power for this kind of model.

Table 3: Structural Path Results and Bootstrapped Indirect Effect

Path	β	SE	CR (t)	p
AI-Driven Cybersecurity → Intelligent Threat Detection	0.552	0.061	9.05	0.000
Intelligent Threat Detection → Organizational Cyber Resilience	0.489	0.058	8.43	0.000
AI-Driven Cybersecurity → Organizational Cyber Resilience (direct)	0.214	0.067	3.19	0.001
AI-Driven Cybersecurity → Intelligent Threat Detection → Organizational Cyber Resilience (indirect)	0.270	0.051	5.29	0.000

Note. CR = critical ratio (t-value). R2 (Intelligent Threat Detection) = 0.36; R2 (Organizational Cyber Resilience) = 0.42. Bootstrapped 95% confidence interval for the indirect effect [0.178, 0.361] excluded zero, based on 5,000 bootstrap resamples, supporting significant mediation.

The pattern of loadings, reliability coefficients, discriminant validity results, model fit indices, and structural path coefficients suggest a well-specified measurement model and a well-specified structural model in which intelligent threat detection acts as an important and meaningful partial mediator between AI-enabled cybersecurity practices and organizational cyber resilience, instead of just a mediator of AI adoption.

DISCUSSION OF FINDINGS

The findings reported above are consistent with the findings in the empirical literature reviewed. The positive path coefficient between AI-driven cybersecurity and intelligent threat detection aligns with Thakkar and Lohiya (2022), who confirmed that machine learning and deep learning approaches to detection always proved more effective than traditional intrusion detection systems, and with Saeed et al. (2023), who said structured cyber threat intelligence enabled enterprises to enhance their detection capabilities. The impact of intelligent threat detection on organizational cyber resilience strengthens Björck et al., (2015) conceptualization of resilience as moving beyond prevention and detection to the aspects of adaptation and recovery and Hasani et al., (2021) and Hasani et al., (2023) results of structured and well-implemented cyber security capabilities significantly predicting organizational security and its outcomes. The partial mediation, not total, suggested, is aligned with the argument that there is more than just detection value for the use of AI in cybersecurity in terms of organizational outcomes, a position that Mikalef et al. (2022) also advanced: that the use of AI in cybersecurity has multiple, overlapping effects on organizational outcomes, rather than just detection.

The results also align with the governance and trust literature that was discussed previously. The strength of the path from AI-driven cybersecurity to intelligent threat detection is in line with Shneiderman's (2020) caution that sound organizational management practices are critical to the success of AI-driven systems, with the comparatively weak path from AI-driven cybersecurity to resilience illustrating Mittelstadt's (2019) concern that structured ethical and governance principles do not necessarily lead to the full organizational benefits of AI investments. The acceptable model fit and adequate discriminant validity further suggests that AI-driven cybersecurity, intelligent threat detection and organizational cyber resilience are conceptually and empirically distinguishable constructs, which is also in line with Kordzadeh and Ghasemaghaei (2022) who argue that the trustworthiness of the outputs of AI-driven detection is not necessarily correlated with the organizational resilience, unless the appropriate organizational conditions are in place, such as the top management involvement and the organizational culture emphasized by Hu et al. (2012) and Chen et al. (2012). In summary, the findings suggest that investments in AI-driven cybersecurity will not directly create resilience, but instead will be more effective in improving intelligent threat detection capability, thereby increasing cyber resilience overall.

CONCLUSION AND RECOMMENDATIONS

This research involved a quantitative survey-based design and Structural Equation Modeling to investigate the relationship between the use of AI-based cybersecurity practices, intelligent threat detection, and the cyber resilience of organizations. The findings showed that intelligent threat detection was significantly and positively correlated with AI-driven cybersecurity practices, cyber resilience was significantly and positively correlated with AI-driven cybersecurity practices, and intelligent threat detection was the significant mediating variable between AI-driven cybersecurity practices and cyber resilience. The structural model had an acceptable fit with the data; the measurement model was reliable and valid. The results align with the empirical and conceptual literature on AI in security, AI in cyber resilience and in organizational governance, and confirm that the value of AI-based security investments to the organization occurs mainly when shifted from a direct impact to a supporting impact of detection.

From these results some suggestions are made. Organizations that invest in AI for cybersecurity should focus on how to make these tools work with their current threat detection processes and continually tune the systems to ensure the tools are working optimally, as detection capability was revealed as the most common way to gain cyber resilience from investments in AI. To preserve the trust and responsiveness of security teams, security leaders should create governance and oversight processes to ensure that AI-generated threat alerts are transparent, accountable, and given human oversight. The top management should be actively involved in establishing the organizational culture around cybersecurity, including with the use of AI-based tools, because the literature demonstrated that the organizational and cultural climate around the implementation and maintenance of technical security investments had an impactful effect on the organization. Additionally, the technical expertise of cybersecurity practitioners, IT managers, network administrators, and information security experts should be enhanced to accurately interpret and apply the outputs generated by AI. Finally, future work should employ this structural model to real survey data in a wider range of industries and sizes as well as explore further mechanisms, such as trust amongst the security team and organizational learning, which could help explain how AI-based cybersecurity practices further impact sustained organizational cyber resilience.

REFERENCES

1. Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience – Fundamentals for a definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), New contributions in information systems and technologies (Vol. 353, pp. 311–316). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31
2. Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? Journal of Management Information Systems, 29(3), 157–188.
3. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203
4. Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, Article 102726. https://doi.org/10.1016/j.jisa.2020.102726
5. Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business & Economics, 3(5), Article 97. https://doi.org/10.1007/s43546-023-00477-6
6. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8
7. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x
8. Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: Review, synthesis, and future research directions. European Journal of Information Systems, 31(3), 388–409.
9. Mikalef, P., Conboy, K., Lundström, J. E., & Popovič, A. (2022). Thinking responsibly about responsible AI and 'the dark side' of AI. European Journal of Information Systems, 31(3), 257–268.
10. Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4
11. Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. Journal of Strategic Information Systems, 34(2), Article 101885. https://doi.org/10.1016/j.jsis.2024.101885

12. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16), Article 7273. https://doi.org/10.3390/s23167273
13. Shin, D. (2020). User perceptions of algorithmic decisions in the personalized AI system: Perceptual evaluation of fairness, accountability, transparency, and explainability. Journal of Broadcasting & Electronic Media, 64(4), 541–565.
14. Shneiderman, B. (2020). Bridging the gap between ethics and practice: Guidelines for reliable, safe, and trustworthy human-centered AI systems. ACM Transactions on Interactive Intelligent Systems, 10(4), Article 26. https://doi.org/10.1145/3419764
15. Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions. Artificial Intelligence Review, 55(1), 453–563. https://doi.org/10.1007/s10462-021-10037-9