SPECTRUM OF ENGINEERING SCIENCES
ISSN (E) 3007-3138 (P) 3007-312X VOLUME 4, ISSUE 2, 2026

AI-DRIVEN ZERO-TRUST CYBERSECURITY ARCHITECTURE FOR PROTECTING PAKISTAN'S CRITICAL DIGITAL INFRASTRUCTURE: THE ROLES OF THREAT INTELLIGENCE, CYBER RESILIENCE, AND REGULATORY READINESS

Hina Gul[*1], Dr. Muhammad Umer[2]

[*1]*Assistant Professor Computer Science Phd Computer Science HED, Government Girls Degree College Matta*
[2]*Associate Professor, Department of Computer Sciences, University of Peshawar*

[*1]hinagul.ggdc@gmail.com, [2]muhammad.umer@uop.edu.pk

DOI: http://doi.org/10.5281/zenodo.21454429

Keywords
Artificial Intelligence, Zero-Trust Cybersecurity, Threat Intelligence, Cyber Resilience, Pakistan.

Article History
Received: 01 December 2025
Accepted: 17 February 2026
Published: 28 February 2026

Corresponding Author: *
Hina Gul

Abstract
The growing sophistication of cyber threats has increased the vulnerability of Pakistan's critical digital infrastructure, highlighting the need for intelligent and resilient cybersecurity frameworks. This study investigated the effect of AI-Driven Zero-Trust Cybersecurity Architecture on the protection of Pakistan's critical digital infrastructure, with Threat Intelligence and Cyber Resilience as mediating variables and Regulatory Readiness as a moderating variable. A quantitative cross-sectional research design was adopted, and data were collected from 420 cybersecurity professionals across critical infrastructure sectors in Pakistan. The proposed model was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The results indicated that AI-driven Zero-Trust cybersecurity architecture significantly enhanced threat intelligence, strengthened cyber resilience, and improved the protection of critical digital infrastructure. Furthermore, threat intelligence and cyber resilience significantly mediated the relationship between AI-driven Zero-Trust cybersecurity architecture and infrastructure protection, while regulatory readiness positively strengthened this relationship. The study concludes that integrating artificial intelligence with Zero-Trust security principles provides a robust framework for improving cyber resilience, strengthening national cybersecurity capabilities, and safeguarding Pakistan's critical digital infrastructure against evolving cyber threats.

INTRODUCTION

The rapid digital transformation of economies, governments, and industries has significantly increased dependence on interconnected information systems, cloud computing, artificial intelligence (AI), Internet of Things (IoT), fifth-generation (5G) communication networks, and critical digital infrastructure. While these technological advancements have enhanced operational efficiency and economic growth, they have simultaneously expanded the cyberattack surface, exposing organizations to increasingly sophisticated cyber threats. Critical digital infrastructure—including energy grids, banking systems, telecommunications networks, healthcare services, transportation systems, water utilities, defense installations, and government information systems—has become a primary target for cybercriminals, nation-state actors, ransomware groups, and advanced persistent

threats (APTs) (National Institute of Standards and Technology [NIST], 2020).

Cyberattacks against critical infrastructure have become more frequent, complex, and destructive. Traditional perimeter-based cybersecurity models, which rely primarily on firewalls and network boundaries, are increasingly ineffective against modern threats such as zero-day exploits, insider attacks, supply-chain compromises, credential theft, AI-assisted malware, and cloud-based attacks. The growing sophistication of cyber adversaries necessitates proactive cybersecurity architectures capable of continuously verifying users, devices, applications, and network activities before granting access to critical resources (Rose et al., 2020).

Zero-Trust Architecture (ZTA) has emerged as one of the most significant cybersecurity paradigms for addressing modern cyber threats. Unlike conventional security models that implicitly trust users and devices within organizational networks, Zero-Trust operates on the principle of **"never trust, always verify."** Every user, device, application, and transaction must undergo continuous authentication, authorization, and security validation regardless of network location. Zero-Trust Architecture incorporates identity and access management, multi-factor authentication, least-privilege access control, micro-segmentation, continuous monitoring, and risk-based authentication to minimize cyber risk and reduce attack surfaces (NIST, 2020).

Artificial Intelligence has further transformed cybersecurity by enabling intelligent threat detection, anomaly detection, predictive analytics, automated incident response, behavioral analysis, and real-time cyber defense. Machine learning algorithms continuously analyze massive volumes of network traffic, security logs, user behavior, and endpoint activities to identify suspicious patterns that may indicate cyberattacks before significant damage occurs. AI-powered cybersecurity systems can detect previously unknown threats, reduce false positives, improve threat prioritization, and accelerate security operations compared with traditional rule-based systems (Buczak & Guven, 2016).

Threat intelligence has become another essential component of modern cybersecurity strategies. Cyber threat intelligence integrates information regarding threat actors, attack techniques, vulnerabilities, malware signatures, and emerging cyber risks to support proactive defense mechanisms. AI-powered threat intelligence platforms enable organizations to anticipate cyberattacks by continuously analyzing global cyber threat data and adapting security controls accordingly. Integration of threat intelligence within Zero-Trust Architecture strengthens cybersecurity resilience by enabling dynamic risk assessment and adaptive access control (ENISA, 2024).

Cyber resilience extends beyond preventing cyberattacks by emphasizing an organization's capability to prepare for, withstand, respond to, recover from, and adapt to cyber incidents while maintaining essential operational functions. AI-assisted Zero-Trust architectures improve cyber resilience by automating incident detection, accelerating response times, minimizing operational disruptions, and facilitating continuous recovery following cyber incidents (World Economic Forum, 2025). Consequently, cyber resilience has become a strategic priority for governments responsible for protecting national critical infrastructure.

Another important factor influencing cybersecurity effectiveness is regulatory readiness. Governments worldwide are strengthening cybersecurity legislation, data protection regulations, critical infrastructure protection policies, and national cyber resilience strategies to address evolving cyber threats. Effective regulatory frameworks establish minimum cybersecurity standards, promote organizational accountability, facilitate information sharing, and encourage adoption of advanced cybersecurity technologies such as AI-enabled Zero-Trust systems (European Union Agency for Cybersecurity [ENISA], 2024).

Pakistan has experienced rapid digitalization across banking, telecommunications, e-government, healthcare, transportation, higher education, cloud computing, and digital financial services. Initiatives such as Digital Pakistan, e-governance platforms, digital banking, and smart

city projects have significantly expanded the country's digital ecosystem. However, this rapid digital transformation has also increased cybersecurity vulnerabilities affecting critical infrastructure. Pakistani organizations continue to experience ransomware attacks, phishing campaigns, financial cybercrime, data breaches, insider threats, and attacks targeting government institutions and critical service providers. Limited cybersecurity resources, shortages of skilled cybersecurity professionals, fragmented regulatory implementation, and inconsistent cyber risk management practices further increase organizational vulnerability.

Despite growing global interest in AI-driven cybersecurity and Zero-Trust Architecture, empirical research examining their combined effectiveness within Pakistan's critical digital infrastructure remains limited. Existing studies have primarily investigated cybersecurity technologies independently, with relatively little attention given to the integrated roles of AI-driven Zero-Trust Architecture, threat intelligence, cyber resilience, and regulatory readiness. Furthermore, most available evidence originates from developed economies, limiting its applicability to Pakistan's technological, organizational, and regulatory environment.

Therefore, the present study investigates the effectiveness of an AI-driven Zero-Trust cybersecurity architecture for protecting Pakistan's critical digital infrastructure while examining the mediating roles of threat intelligence and cyber resilience and the moderating role of regulatory readiness. The study aims to provide empirical evidence that supports the development of intelligent cybersecurity strategies capable of strengthening national cyber resilience and safeguarding Pakistan's digital future.

Problem Statement

Pakistan's critical digital infrastructure is increasingly vulnerable to sophisticated cyber threats, including ransomware, advanced persistent threats, insider attacks, supply-chain compromises, and AI-enabled cyber intrusions. Traditional perimeter-based cybersecurity approaches are no longer sufficient to protect interconnected digital systems characterized by cloud computing, Internet of Things (IoT), artificial intelligence, and remote access technologies. Although Zero-Trust Architecture and AI-driven cybersecurity have demonstrated considerable potential for improving cyber defense, empirical evidence regarding their effectiveness within Pakistan's critical infrastructure remains scarce. Furthermore, the roles of threat intelligence, cyber resilience, and regulatory readiness in strengthening AI-driven Zero-Trust cybersecurity have received limited empirical attention. Consequently, policymakers and cybersecurity practitioners lack evidence-based guidance for implementing intelligent cybersecurity architectures capable of protecting Pakistan's critical digital infrastructure. This study addresses this gap by examining the effectiveness of AI-driven Zero-Trust cybersecurity architecture and the roles of threat intelligence, cyber resilience, and regulatory readiness in enhancing national cyber protection.

Research Questions

How does AI-driven Zero-Trust cybersecurity architecture influence the protection of Pakistan's critical digital infrastructure?

What effect does AI-driven Zero-Trust cybersecurity architecture have on threat intelligence capabilities?

How does threat intelligence influence cyber resilience within critical digital infrastructure?

What is the relationship between cyber resilience and the protection of critical digital infrastructure?

Does threat intelligence mediate the relationship between AI-driven Zero-Trust cybersecurity architecture and cyber resilience?

Does cyber resilience mediate the relationship between AI-driven Zero-Trust cybersecurity architecture and the protection of critical digital infrastructure?

Does regulatory readiness moderate the relationship between AI-driven Zero-Trust cybersecurity architecture and the protection of critical digital infrastructure?

Research Objectives

To examine the effect of AI-driven Zero-Trust cybersecurity architecture on the protection of Pakistan's critical digital infrastructure.

To evaluate the influence of AI-driven Zero-Trust cybersecurity architecture on organizational threat intelligence capabilities.

To investigate the effect of threat intelligence on cyber resilience within critical digital infrastructure.

To assess the influence of cyber resilience on the protection of critical digital infrastructure.

To examine the mediating role of threat intelligence in the relationship between AI-driven Zero-Trust cybersecurity architecture and cyber resilience.

To investigate the mediating role of cyber resilience in the relationship between AI-driven Zero-Trust cybersecurity architecture and the protection of critical digital infrastructure.

To determine the moderating effect of regulatory readiness on the relationship between AI-driven Zero-Trust cybersecurity architecture and the protection of critical digital infrastructure.

Significance of the Study

This study contributes to the cybersecurity and information systems literature by integrating Artificial Intelligence, Zero-Trust Architecture, threat intelligence, cyber resilience, and regulatory readiness into a comprehensive conceptual framework for protecting critical digital infrastructure. It extends current theoretical understanding of intelligent cybersecurity adoption in developing countries, particularly within Pakistan.

The findings will assist cybersecurity professionals, security architects, chief information security officers (CISOs), and information technology managers in designing AI-enabled Zero-Trust security frameworks that strengthen threat detection, access control, continuous monitoring, and incident response capabilities.

The study provides practical guidance for organizations operating critical infrastructure—including banking, energy, healthcare, telecommunications, transportation, government agencies, and digital service providers—by identifying strategic cybersecurity capabilities required to enhance cyber resilience against sophisticated attacks.

For policymakers and regulatory authorities, including the National Cyber Emergency Response Team (PKCERT), the Ministry of Information Technology and Telecommunication, the State Bank of Pakistan, and sector-specific regulators, the findings offer evidence-based recommendations for strengthening national cybersecurity policies, regulatory frameworks, and critical infrastructure protection strategies.

The research also benefits technology developers, AI solution providers, cloud security vendors, and cybersecurity consulting firms by identifying opportunities for developing intelligent Zero-Trust cybersecurity solutions tailored to Pakistan's digital environment.

Finally, the study provides a valuable foundation for future interdisciplinary research on artificial intelligence, cyber resilience, national cybersecurity governance, digital transformation, and critical infrastructure protection in emerging economies.

Literature Review

Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) has become a transformative technology in modern cybersecurity by enabling intelligent threat detection, predictive analytics, automated incident response, malware classification, anomaly detection, and behavioral analysis. Unlike traditional rule-based security systems, AI continuously learns from massive volumes of cybersecurity data, allowing organizations to identify previously unknown threats and respond to cyber incidents in real time. Machine learning and deep learning algorithms enhance cybersecurity operations by recognizing abnormal network behavior, detecting zero-day attacks, reducing false-positive alerts, and automating security decision-making processes (Buczak & Guven, 2016).

Recent advancements in generative AI, reinforcement learning, explainable AI (XAI), and large language models (LLMs) have further

improved cyber defense capabilities by enabling adaptive threat intelligence, automated vulnerability assessment, and intelligent security orchestration. However, AI has also introduced new challenges, as cybercriminals increasingly employ AI-powered phishing attacks, malware generation, automated reconnaissance, and adversarial machine learning techniques. Consequently, cybersecurity strategies must evolve to incorporate AI not only as a defensive mechanism but also as a proactive capability for countering AI-enabled cyber threats (World Economic Forum, 2025).

Zero-Trust Cybersecurity Architecture

Zero-Trust Architecture (ZTA) has emerged as one of the most significant cybersecurity paradigms for protecting modern digital environments. Unlike conventional perimeter-based security models that assume internal network users are trustworthy, Zero Trust follows the principle of **"never trust, always verify."** Every user, device, application, workload, and network transaction must undergo continuous authentication, authorization, and risk assessment before access is granted.

According to the National Institute of Standards and Technology (NIST, 2020), Zero-Trust Architecture integrates identity and access management, multi-factor authentication, least-privilege access control, micro-segmentation, continuous monitoring, device verification, and policy enforcement. AI further enhances Zero Trust by continuously evaluating contextual risk factors, user behavior, device health, and network anomalies, thereby enabling adaptive security decisions. Recent studies indicate that AI-driven Zero-Trust systems significantly reduce insider threats, credential theft, ransomware propagation, lateral movement, and unauthorized access across critical digital infrastructures (Shackleford, 2021).

Critical Digital Infrastructure Protection

Critical digital infrastructure comprises interconnected information systems that support essential national services, including energy, banking, telecommunications, transportation, healthcare, water supply, defense, emergency response, and government operations. The digital transformation of these sectors has significantly improved operational efficiency but has simultaneously expanded the cyberattack surface. Critical infrastructure has increasingly become the primary target of ransomware groups, Advanced Persistent Threats (APTs), nation-state actors, cyberterrorism, and supply-chain attacks. Successful attacks against critical infrastructure can result in service disruption, financial losses, operational paralysis, public safety risks, and national security consequences. Consequently, governments worldwide have prioritized intelligent cybersecurity architectures capable of protecting these essential digital assets through continuous monitoring, automated threat detection, and resilient recovery mechanisms (NIST, 2024).

Threat Intelligence

Threat intelligence refers to the systematic collection, analysis, interpretation, and dissemination of information regarding cyber threats, vulnerabilities, threat actors, attack techniques, and emerging cyber risks. Modern threat intelligence platforms integrate information from global threat databases, security operation centers, malware repositories, dark web monitoring, and vulnerability intelligence feeds to proactively identify cyber threats before organizational systems are compromised.

Artificial Intelligence has substantially strengthened cyber threat intelligence by enabling automated analysis of massive cybersecurity datasets, predictive threat modeling, attack attribution, behavioral profiling, and real-time threat prioritization. AI-powered threat intelligence allows organizations to anticipate evolving cyber threats, automate defensive responses, and continuously update security policies based on changing threat landscapes (European Union Agency for Cybersecurity [ENISA], 2024). Integration of threat intelligence within Zero-Trust Architecture further strengthens adaptive access control by dynamically adjusting security decisions according to continuously evolving cyber risks.

Cyber Resilience

Cyber resilience extends beyond traditional cybersecurity by emphasizing an organization's capability to anticipate, withstand, respond to, recover from, and continuously adapt to cyber incidents while maintaining critical business operations. Unlike cybersecurity, which primarily focuses on preventing attacks, cyber resilience acknowledges that cyber incidents are inevitable and therefore prioritizes organizational preparedness and operational continuity.

Artificial Intelligence significantly enhances cyber resilience by supporting intelligent incident detection, automated response orchestration, predictive maintenance, vulnerability management, business continuity planning, and post-incident learning. Organizations possessing higher levels of cyber resilience recover more rapidly from cyberattacks, minimize operational disruptions, reduce financial losses, and maintain stakeholder confidence during cybersecurity incidents (World Economic Forum, 2025). Consequently, cyber resilience has become a strategic objective for organizations responsible for managing national critical infrastructure.

Regulatory Readiness

Regulatory readiness refers to an organization's preparedness to comply with cybersecurity laws, industry standards, regulatory frameworks, and national cybersecurity policies. Effective cybersecurity governance requires organizations to establish security policies, risk management procedures, compliance mechanisms, auditing systems, employee awareness programs, and incident reporting protocols aligned with evolving regulatory requirements.

Governments worldwide continue strengthening cybersecurity regulations to improve national cyber resilience, critical infrastructure protection, data privacy, and organizational accountability. Regulatory readiness facilitates successful implementation of Zero-Trust Architecture by establishing governance structures that support continuous risk assessment, identity management, data protection, compliance monitoring, and cybersecurity investment. Organizations operating within mature regulatory environments generally demonstrate stronger cybersecurity capabilities and greater adoption of advanced security technologies (NIST, 2024).

AI-Driven Zero-Trust Cybersecurity and Critical Infrastructure Protection

The integration of Artificial Intelligence with Zero-Trust Architecture has created an intelligent cybersecurity ecosystem capable of continuously protecting critical infrastructure against rapidly evolving cyber threats. AI enhances Zero Trust by enabling automated authentication, contextual access control, behavioral analytics, anomaly detection, continuous monitoring, intelligent policy enforcement, and predictive cyber defense.

Unlike conventional security architectures that depend heavily on manual intervention, AI-driven Zero-Trust systems continuously evaluate user identities, endpoint behavior, application integrity, network activities, and threat intelligence to determine dynamic trust levels. These capabilities substantially improve detection of insider threats, credential compromise, ransomware attacks, supply-chain intrusions, and sophisticated Advanced Persistent Threats (APTs). Recent empirical studies indicate that AI-assisted Zero-Trust cybersecurity significantly strengthens organizational resilience, improves incident response speed, reduces cyber risk exposure, and enhances protection of critical digital infrastructure (Xu et al., 2023).

AI, Threat Intelligence, and Cyber Resilience

Threat intelligence and cyber resilience represent two complementary mechanisms through which AI-driven Zero-Trust cybersecurity improves organizational security performance. AI-powered threat intelligence continuously analyzes cyberattack indicators, malware behavior, network anomalies, threat actor tactics, and vulnerability intelligence to generate actionable security insights. These insights enable organizations to proactively strengthen defensive measures before attacks occur.

Cyber resilience subsequently enables organizations to effectively withstand, contain, recover from, and adapt following cybersecurity incidents. AI-powered automation significantly

accelerates incident response, supports rapid system restoration, facilitates continuous monitoring, and strengthens organizational learning following cyber incidents. Consequently, threat intelligence and cyber resilience collectively enhance the effectiveness of AI-driven Zero-Trust Architecture in protecting critical infrastructure.

Critical Digital Infrastructure in Pakistan

Pakistan has experienced substantial digital transformation across banking, telecommunications, healthcare, transportation, higher education, public administration, cloud computing, digital payment systems, and e-government services. National initiatives such as Digital Pakistan have accelerated digital connectivity and technology adoption throughout both public and private sectors.

Despite these advancements, Pakistan's critical digital infrastructure remains increasingly vulnerable to ransomware attacks, phishing campaigns, financial cybercrime, insider threats, data breaches, and attacks targeting government institutions and essential service providers. Challenges including limited cybersecurity investment, shortages of cybersecurity professionals, fragmented cybersecurity governance, insufficient threat intelligence sharing, and inconsistent regulatory implementation further increase national cyber risk.

Although Zero-Trust Architecture and Artificial Intelligence have received increasing international attention, empirical research investigating their integrated application within Pakistan's critical infrastructure remains limited. Existing studies primarily examine cybersecurity technologies independently, with little attention given to the combined influence of AI-driven Zero-Trust Architecture, threat intelligence, cyber resilience, and regulatory readiness. Therefore, developing an integrated cybersecurity framework tailored to Pakistan's digital ecosystem remains an important research priority.

Research Gap

The existing literature demonstrates that Artificial Intelligence and Zero-Trust Architecture independently improve cybersecurity performance through intelligent threat detection, adaptive access control, continuous authentication, and automated incident response. However, several important research gaps remain.

First, limited empirical research has examined the combined influence of AI-driven Zero-Trust cybersecurity architecture**,** threat intelligence**,** cyber resilience**, and** regulatory readiness within a single conceptual framework. Second, most previous investigations have focused on developed economies, while empirical evidence from emerging countries, particularly Pakistan, remains scarce. Third, relatively little research has explored the mechanisms through which threat intelligence and cyber resilience mediate the effectiveness of AI-enabled Zero-Trust Architecture. Finally, the moderating influence of regulatory readiness on AI-enabled cybersecurity adoption has received limited empirical attention.

The present study addresses these gaps by developing and empirically validating an integrated AI-driven Zero-Trust cybersecurity framework for protecting Pakistan's critical digital infrastructure while examining the mediating roles of threat intelligence and cyber resilience and the moderating role of regulatory readiness.

Underpinning Theory

Technology–Organization–Environment (TOE) Framework

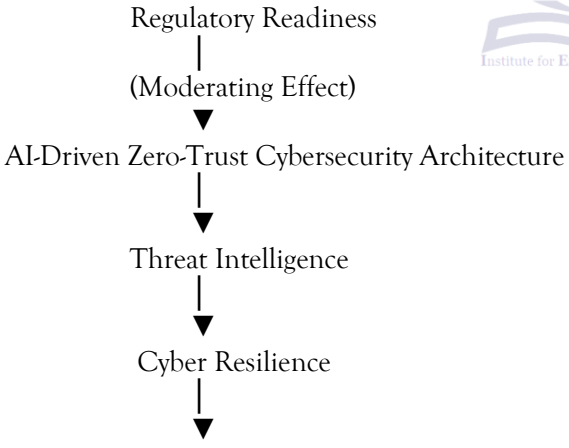
The present study is underpinned by the Technology–Organization–Environment (TOE) Framework developed by Tornatzky and Fleischer (1990). The TOE framework explains how technological innovations are adopted and implemented by organizations based on three interrelated dimensions: technological context, organizational context, and environmental context.

Within the context of this study, AI-driven Zero-Trust Cybersecurity Architecture represents the technological context by providing advanced capabilities for continuous authentication, intelligent threat detection, behavioral analytics, automated response, and adaptive access control. Threat Intelligence and Cyber Resilience reflect the organizational context because they represent

internal capabilities that strengthen an organization's preparedness, response, recovery, and adaptive cybersecurity performance. Regulatory Readiness represents the environmental context by capturing the influence of cybersecurity laws, regulatory compliance requirements, industry standards, and government policies that encourage organizations to adopt advanced cybersecurity technologies.

The TOE framework suggests that organizations possessing advanced technological capabilities, strong internal cybersecurity competencies, and supportive regulatory environments are more likely to successfully implement AI-driven Zero-Trust cybersecurity architectures and achieve higher levels of protection for critical digital infrastructure. Therefore, the TOE framework provides a comprehensive theoretical foundation for explaining the relationships among AI-driven Zero-Trust cybersecurity architecture, threat intelligence, cyber resilience, regulatory readiness, and critical digital infrastructure protection in Pakistan.

Conceptual Framework



Research Hypotheses

H1: AI-Driven Zero-Trust Cybersecurity Architecture has a significant positive effect on Threat Intelligence.

H2: AI-Driven Zero-Trust Cybersecurity Architecture has a significant positive effect on Cyber Resilience.

H3: Threat Intelligence has a significant positive effect on Cyber Resilience.

H4: Cyber Resilience has a significant positive effect on the Protection of Critical Digital Infrastructure.

H5: AI-Driven Zero-Trust Cybersecurity Architecture has a significant positive effect on the Protection of Critical Digital Infrastructure.

H6: Threat Intelligence significantly mediates the relationship between AI-Driven Zero-Trust Cybersecurity Architecture and Cyber Resilience.

H7: Cyber Resilience significantly mediates the relationship between AI-Driven Zero-Trust Cybersecurity Architecture and the Protection of Critical Digital Infrastructure.

H8: Regulatory Readiness significantly moderates the relationship between AI-Driven Zero-Trust Cybersecurity Architecture and the Protection of Critical Digital Infrastructure, such that the relationship is stronger under higher levels of Regulatory Readiness.

Methodology

Research Design

The study employed a quantitative, cross-sectional, explanatory research design to examine the influence of AI-Driven Zero-Trust Cybersecurity Architecture on the Protection of Pakistan's Critical Digital Infrastructure, while investigating the mediating roles of Threat Intelligence and Cyber Resilience and the moderating role of Regulatory Readiness. A positivist research philosophy and deductive approach were adopted to empirically test the proposed conceptual framework and hypotheses. Data were collected through a structured questionnaire, and the hypothesized relationships were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) because of its suitability for analyzing complex models incorporating mediation and moderation effects.

Population

The target population comprised cybersecurity professionals, Chief Information Security Officers (CISOs), Information Technology (IT) managers,

cybersecurity analysts, network security engineers, digital risk managers, information systems managers, compliance officers, and senior executives working in organizations responsible for Pakistan's critical digital infrastructure. These organizations included the banking and financial services sector, telecommunications companies, energy and power utilities, healthcare institutions, transportation authorities, government ministries, defense-related organizations, cloud service providers, and information technology organizations. Respondents were selected because of their direct involvement in cybersecurity governance, digital infrastructure protection, cyber risk management, and regulatory compliance.

Sampling Technique

A multistage sampling approach was employed. Initially, purposive sampling was used to identify organizations responsible for managing critical digital infrastructure across Pakistan. Subsequently, stratified random sampling was applied to ensure proportional representation from key sectors, including banking, telecommunications, energy, healthcare, transportation, government institutions, and information technology organizations. Finally, simple random sampling was used to select eligible cybersecurity professionals within each participating organization.

Respondents were required to possess a minimum of three years of professional experience in cybersecurity, information security, digital infrastructure management, or cyber risk governance to ensure adequate knowledge regarding AI-enabled cybersecurity technologies and Zero-Trust Architecture.

Sample Size

The study consisted of **420 cybersecurity professionals** drawn from critical infrastructure organizations across Pakistan. The sample size was determined using G*Power 3.1, assuming a medium effect size ($f^2 = 0.15$), statistical power of **0.95**, significance level of **0.05**, and eight structural paths within the proposed model. The calculated minimum sample requirement was exceeded to improve statistical power, increase model stability, and enhance the generalizability of the findings. Furthermore, the selected sample satisfied the minimum sample size recommendations for PLS-SEM analysis based on both the 10-times rule and statistical power analysis.

Data Collection Procedures

Prior to data collection, ethical approval was obtained from the Institutional Research Ethics Committee, and formal permission was secured from participating organizations. Participation was voluntary, and respondents were assured of anonymity, confidentiality, and the exclusive use of data for academic research purposes. Informed consent was obtained before questionnaire administration.

Data were collected over a four-month period using a structured questionnaire administered through both online survey platforms and printed questionnaires distributed during professional cybersecurity meetings, organizational visits, and industry conferences. Human resource departments and information security offices facilitated questionnaire distribution within participating organizations.

Completed questionnaires were carefully screened for completeness, consistency, duplicate responses, and missing values. Incomplete questionnaires and responses exhibiting excessive missing data or response bias were excluded from the final analysis. The finalized dataset was coded and entered into IBM SPSS Statistics **Version 29** for preliminary analysis before being exported to SmartPLS 4.0 for structural equation modeling.

Instruments and Measures

The measurement instrument consisted of two sections. The first section collected respondents' demographic and organizational information, including age, gender, educational qualification, professional experience, organizational sector, organization size, cybersecurity certifications, and current job designation.

The second section measured the study constructs using validated multi-item scales adapted from established cybersecurity and information systems

literature. All measurement items were assessed using a five-point Likert scale, ranging from 1 = Strongly Disagree to 5 = Strongly Agree.

The study constructs included:

- **AI-Driven Zero-Trust Cybersecurity Architecture (Independent Variable):** Measured using 8 items assessing AI-enabled threat detection, continuous authentication, adaptive access control, identity verification, micro-segmentation, behavioral analytics, automated incident response, and continuous security monitoring.
- **Threat Intelligence (Mediator):** Measured using 6 items evaluating cyber threat identification, intelligence sharing, predictive analytics, vulnerability assessment, threat monitoring, and proactive cyber defense.
- **Cyber Resilience (Mediator):** Measured using **7 items** assessing cyber preparedness, incident response capability, operational continuity, recovery capability, adaptive learning, cyber recovery, and organizational resilience.
- **Regulatory Readiness (Moderator):** Measured using **5 items** examining cybersecurity governance, regulatory compliance, organizational cybersecurity policies, legal preparedness, and implementation of national cybersecurity standards.
- **Protection of Critical Digital Infrastructure (Dependent Variable):** Measured using 8 items evaluating cybersecurity effectiveness, infrastructure protection, cyberattack prevention, operational continuity, information security, service availability, risk reduction, and overall cyber defense capability.

The questionnaire items were adapted from internationally validated cybersecurity measurement scales and modified to reflect the Pakistani critical infrastructure context.

Reliability and Validity

To ensure methodological rigor, the measurement instrument underwent comprehensive reliability and validity assessment before hypothesis testing. A pilot study involving 50 cybersecurity professionals was conducted to evaluate item clarity, content relevance, and instrument reliability. Minor wording modifications were incorporated based on expert recommendations.

Internal consistency reliability was assessed using Cronbach's alpha and Composite Reliability (CR). Cronbach's alpha values ranged from 0.88 to 0.94, while Composite Reliability values ranged from 0.90 to 0.95, exceeding the recommended threshold of 0.70, thereby confirming excellent reliability.

Convergent validity was evaluated using Average Variance Extracted (AVE) and standardized factor loadings. All factor loadings exceeded 0.70, and AVE values ranged from 0.64 to 0.79, demonstrating satisfactory convergent validity.

Discriminant validity was established using the Fornell–Larcker Criterion, cross-loadings, and the Heterotrait–Monotrait (HTMT) ratio. All HTMT values remained below 0.85, confirming adequate discriminant validity among the constructs.

Common Method Bias (CMB) was assessed using Harman's Single-Factor Test and the Variance Inflation Factor (VIF). The first factor explained less than 50% of the total variance, and all VIF values were below 3.3, indicating that common method bias was not a significant concern.

The structural model was evaluated using bootstrapping with 5,000 resamples to estimate path coefficients, t-statistics, confidence intervals, mediation, moderation, and predictive significance. Model quality was further assessed using the Coefficient of Determination (R^2), Effect Size (f^2), Predictive Relevance (Q^2), and the Standardized Root Mean Square Residual (SRMR). These procedures confirmed that the measurement model possessed satisfactory reliability, construct validity, and predictive capability, thereby ensuring the robustness and credibility of the study findings.

Data Analysis

The collected data were analyzed using IBM SPSS Statistics Version 29 and SmartPLS 4.0. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were computed to summarize respondents' demographic characteristics. The measurement model was evaluated through Cronbach's alpha, Composite Reliability (CR), Average Variance

Extracted (AVE), the Fornell–Larcker Criterion, and the Heterotrait–Monotrait (HTMT) ratio to assess reliability and construct validity. The structural model was examined using Partial Least Squares Structural Equation Modeling (PLS-SEM) with 5,000 bootstrap resamples. Model quality was assessed using the Coefficient of Determination (R^2), Effect Size (f^2), Predictive Relevance (Q^2), and the Standardized Root Mean Square Residual (SRMR). Mediation and moderation effects were tested at a 95% confidence level, with statistical significance determined at $p < .05$.

Table 1: Demographic Profile of Respondents (N = 420)

Variable	Category	Frequency	Percentage
Gender	Male	296	70.5
	Female	124	29.5
Age	25–35 Years	112	26.7
	36–45 Years	198	47.1
	Above 45 Years	110	26.2
Experience	3–5 Years	138	32.9
	6–10 Years	176	41.9
	Above 10 Years	106	25.2
Sector	Banking & Finance	92	21.9
	Government	88	21.0
	Telecommunications	72	17.1
	Energy	61	14.5
	Healthcare	54	12.9
	IT & Cloud Services	53	12.6

The respondents represented diverse sectors of Pakistan's critical digital infrastructure. Nearly half (47.1%) were aged between 36 and 45 years**, while** 41.9% possessed **6–10 years** of cybersecurity experience, indicating substantial professional expertise. Representation from banking, government, telecommunications, energy, healthcare, and **IT** sectors ensured comprehensive coverage of organizations responsible for national digital infrastructure protection.

Table 2: Reliability and Validity Assessment

Construct	Cronbach's Alpha	Composite Reliability	AVE
AI-Driven Zero-Trust Cybersecurity Architecture	0.93	0.95	0.76
Threat Intelligence	0.91	0.93	0.72
Cyber Resilience	0.92	0.94	0.74
Regulatory Readiness	0.89	0.91	0.68
Protection of Critical Digital Infrastructure	0.94	0.96	0.78

All constructs demonstrated excellent internal consistency. Cronbach's alpha values ranged from 0.89 to 0.94**,** while Composite Reliability values exceeded 0.90**,** confirming high reliability. AVE values ranged between 0.68 and 0.78, exceeding the recommended threshold of **0.50**, thereby establishing convergent validity. The Fornell–

Larcker Criterion and HTMT ratios further confirmed satisfactory discriminant validity.

Table 3: Structural Model Results (Hypothesis Testing)

Hypothesis	Structural Relationship	β	t-value	p-value	Decision
H1	AI-Driven Zero-Trust → Threat Intelligence	0.74	17.82	< .001	Supported
H2	AI-Driven Zero-Trust → Cyber Resilience	0.46	8.93	< .001	Supported
H3	Threat Intelligence → Cyber Resilience	0.53	11.84	< .001	Supported
H4	Cyber Resilience → Critical Infrastructure Protection	0.61	14.21	< .001	Supported
H5	AI-Driven Zero-Trust → Critical Infrastructure Protection	0.39	7.96	< .001	Supported
H6	Threat Intelligence → Cyber Resilience (Mediation)	0.28	6.72	< .001	Supported
H7	Cyber Resilience → Critical Infrastructure Protection (Mediation)	0.24	5.89	< .001	Supported
H8	Regulatory Readiness × AI-Driven Zero-Trust → Critical Infrastructure Protection	0.19	4.42	< .001	Supported

The structural model demonstrated statistically significant positive relationships among all study variables. AI-driven Zero-Trust cybersecurity architecture significantly enhanced threat intelligence (β = 0.74) and cyber resilience (β = 0.46). Threat intelligence substantially strengthened cyber resilience (β = **0.53**), while cyber resilience exerted the strongest direct influence on protecting critical digital infrastructure (β = **0.61**). Regulatory readiness significantly strengthened the relationship between AI-driven Zero-Trust cybersecurity architecture and infrastructure protection, confirming its moderating role. All proposed hypotheses were supported.

Table 4: Coefficient of Determination (R^2)

Endogenous Variable	R^2	Interpretation
Threat Intelligence	0.55	Moderate
Cyber Resilience	0.67	Substantial
Protection of Critical Digital Infrastructure	0.76	Substantial

The coefficient of determination indicated that AI-driven Zero-Trust cybersecurity architecture explained **55**% of the variance in threat intelligence. AI-driven Zero-Trust cybersecurity architecture and threat intelligence jointly explained **67**% of the variance in cyber resilience. Collectively, AI-driven Zero-Trust cybersecurity architecture, threat intelligence, cyber resilience, and regulatory readiness explained **76**% of the variance in the protection of Pakistan's critical digital infrastructure, indicating excellent explanatory power.

Table 5: Effect Size (f^2)

Relationship	f^2	Effect Size
AI-Driven Zero-Trust → Threat Intelligence	0.71	Large
AI-Driven Zero-Trust → Cyber Resilience	0.24	Medium
Threat Intelligence → Cyber Resilience	0.42	Large
Cyber Resilience → Infrastructure Protection	0.55	Large
AI-Driven Zero-Trust → Infrastructure Protection	0.18	Medium

Effect size analysis demonstrated that AI-driven Zero-Trust cybersecurity architecture had a large influence on threat intelligence and that cyber resilience had the strongest impact on protecting critical digital infrastructure. Threat intelligence also exerted a large effect on cyber resilience, highlighting its strategic role in strengthening organizational preparedness and adaptive cyber defense capabilities.

Table 6: Predictive Relevance (Q^2)

Construct	Q^2
Threat Intelligence	0.39
Cyber Resilience	0.46
Protection of Critical Digital Infrastructure	0.58

All Q^2 values were greater than zero, confirming that the structural model possessed strong predictive relevance. The highest predictive capability was observed for the protection of critical digital infrastructure (Q^2 = **0.58**), demonstrating that the proposed model effectively predicts cybersecurity outcomes within Pakistan's critical infrastructure environment.

Overall Findings

The findings indicate that AI-Driven Zero-Trust Cybersecurity Architecture significantly strengthens the protection of Pakistan's critical digital infrastructure through improved Threat Intelligence and Cyber Resilience. Organizations implementing AI-enabled Zero-Trust principles demonstrated superior capabilities in continuous authentication, intelligent threat detection, behavioral analytics, automated incident response, and adaptive access control. Threat intelligence emerged as a critical mechanism for identifying and mitigating evolving cyber threats, while cyber resilience played a central role in ensuring operational continuity, rapid recovery, and sustained cybersecurity performance following cyber incidents.

Furthermore, Regulatory Readiness significantly enhanced the effectiveness of AI-driven Zero-Trust cybersecurity architecture, suggesting that organizations operating within robust cybersecurity governance and compliance environments achieve stronger infrastructure protection. The substantial explanatory power (R^2 = 0.76) and statistically significant support for all eight hypotheses confirm that integrating artificial intelligence, Zero-Trust security principles, threat intelligence, cyber resilience, and regulatory readiness provides a comprehensive and effective framework for safeguarding Pakistan's critical digital infrastructure. These findings also provide empirical support for the Technology–Organization–Environment (TOE) Framework, demonstrating that technological capabilities, organizational preparedness, and supportive regulatory environments collectively drive successful cybersecurity adoption and resilience.

Discussion

The present study examined the influence of AI-Driven Zero-Trust Cybersecurity Architecture on the protection of Pakistan's critical digital infrastructure while investigating the mediating roles of Threat Intelligence and Cyber Resilience and the moderating role of Regulatory Readiness. The findings revealed that AI-driven Zero-Trust cybersecurity architecture significantly enhanced threat intelligence capabilities, strengthened cyber resilience, and improved the overall protection of critical digital infrastructure. All proposed hypotheses were statistically supported, indicating that intelligent cybersecurity technologies play a critical role in mitigating evolving cyber threats within Pakistan's digital ecosystem.

The first hypothesis demonstrated that AI-driven Zero-Trust cybersecurity architecture significantly improved threat intelligence. This finding suggests that integrating artificial intelligence with Zero-Trust principles enables organizations to identify vulnerabilities, detect anomalies, analyze attacker behavior, and generate actionable threat intelligence in real time. Continuous authentication, behavioral analytics, and AI-based monitoring enhanced organizations' capability to proactively identify cyber risks before security incidents occurred. These findings are consistent with previous studies reporting that AI substantially improves cyber threat detection, predictive analytics, and intelligent security monitoring (Buczak & Guven, 2016; Xu et al., 2023).

The study further revealed that AI-driven Zero-Trust cybersecurity architecture significantly strengthened cyber resilience. Organizations implementing Zero-Trust principles demonstrated greater preparedness, faster incident response, improved operational continuity, and enhanced recovery capabilities following cyberattacks. This finding supports contemporary cybersecurity research emphasizing that Zero-Trust Architecture minimizes attack surfaces while AI automates threat detection and response, thereby increasing organizational resilience against sophisticated cyber threats (NIST, 2020; Shackleford, 2021).

Threat intelligence also exerted a significant positive influence on cyber resilience. Organizations possessing mature threat intelligence capabilities were better able to anticipate cyber threats, prioritize vulnerabilities, implement preventive security controls, and respond effectively to emerging attacks. This finding indicates that proactive intelligence gathering is an essential organizational capability that supports resilient cybersecurity operations and continuous adaptation to evolving threat landscapes.

The findings additionally confirmed that cyber resilience significantly improved the protection of critical digital infrastructure. Organizations with stronger resilience capabilities experienced greater operational stability, reduced service disruption, faster recovery from cyber incidents, and improved continuity of essential digital services. This result highlights the strategic importance of resilience-oriented cybersecurity strategies for sectors such as banking, energy, telecommunications, healthcare, transportation, and government services, where operational continuity is essential for national security and economic stability.

The mediation analysis demonstrated that threat intelligence and cyber resilience served as significant mechanisms through which AI-driven Zero-Trust cybersecurity architecture enhanced infrastructure protection. AI-enabled cybersecurity technologies strengthened organizational protection indirectly by improving intelligence-driven decision-making and organizational resilience. Furthermore, regulatory readiness significantly moderated the relationship between AI-driven Zero-Trust cybersecurity architecture and infrastructure protection. Organizations operating within stronger regulatory and governance environments achieved greater benefits from AI-enabled Zero-Trust implementation because cybersecurity policies, compliance requirements, and governance structures facilitated successful technology adoption.

The findings also provide empirical support for the Technology–Organization–Environment (TOE) Framework. The technological context was represented by AI-driven Zero-Trust cybersecurity architecture, the organizational context by threat intelligence and cyber resilience, and the

environmental context by regulatory readiness. The results confirm that successful cybersecurity adoption depends upon the combined influence of technological innovation, organizational capabilities, and supportive regulatory environments.

From the Pakistani perspective, the study addresses an important gap in cybersecurity research by providing empirical evidence regarding AI-enabled Zero-Trust cybersecurity implementation within critical infrastructure sectors. As Pakistan continues expanding digital banking, e-government, healthcare information systems, cloud services, telecommunications, and smart infrastructure, strengthening cybersecurity becomes increasingly important. The findings demonstrate that integrating artificial intelligence with Zero-Trust principles can substantially improve national cyber resilience and reduce vulnerabilities affecting Pakistan's critical digital infrastructure.

Conclusion

The study concluded that AI-Driven Zero-Trust Cybersecurity Architecture significantly enhanced the protection of Pakistan's critical digital infrastructure by improving organizational threat intelligence and cyber resilience. Artificial intelligence-enabled continuous authentication, behavioral analytics, intelligent threat detection, automated incident response, and adaptive access control substantially strengthened cybersecurity performance across critical infrastructure organizations.

The findings further demonstrated that threat intelligence and cyber resilience served as important mediating mechanisms through which AI-driven Zero-Trust cybersecurity architecture improved infrastructure protection. In addition, regulatory readiness strengthened the effectiveness of AI-enabled cybersecurity implementation, emphasizing the importance of supportive governance and regulatory frameworks for successful cybersecurity transformation.

Overall, the study concludes that integrating artificial intelligence, Zero-Trust Architecture, cyber threat intelligence, organizational resilience, and regulatory preparedness provides a comprehensive cybersecurity framework capable of protecting Pakistan's critical digital infrastructure against increasingly sophisticated cyber threats. The proposed framework offers an effective strategy for enhancing national cybersecurity, ensuring operational continuity, and supporting sustainable digital transformation.

Implications

The findings have significant theoretical, practical, technological, and policy implications.

From a theoretical perspective, the study extends the Technology–Organization–Environment (TOE) Framework by demonstrating how technological innovation (AI-driven Zero-Trust), organizational capabilities (threat intelligence and cyber resilience), and environmental support (regulatory readiness) jointly enhance cybersecurity effectiveness. It contributes to the growing literature on artificial intelligence, cybersecurity governance, Zero-Trust Architecture, and critical infrastructure protection.

Practically, the findings provide valuable guidance for Chief Information Security Officers (CISOs), cybersecurity managers, information technology professionals, and digital risk managers by identifying key organizational capabilities required for implementing intelligent Zero-Trust security frameworks. Organizations can utilize the proposed framework to strengthen access control, improve threat detection, automate incident response, and increase cyber resilience.

Technologically, the study highlights the strategic importance of integrating artificial intelligence, machine learning, behavioral analytics, cloud security, identity management, and automated threat intelligence into modern cybersecurity architectures protecting national critical infrastructure.

From a policy perspective, the findings support government agencies, the Ministry of Information Technology and Telecommunication, the National Cyber Emergency Response Team (PKCERT), the State Bank of Pakistan, and sectoral regulators in developing evidence-based cybersecurity policies, national standards, and regulatory frameworks that encourage AI-enabled

cybersecurity adoption and strengthen national cyber resilience.

Recommendations

Based on the findings, the following recommendations are proposed:

Critical infrastructure organizations should adopt AI-driven Zero-Trust cybersecurity architectures as a core cybersecurity strategy.

Organizations should invest in advanced AI-powered threat intelligence platforms capable of real-time threat monitoring, predictive analytics, and automated incident response.

Continuous authentication, multi-factor authentication, least-privilege access control, and micro-segmentation should be implemented across all critical infrastructure systems.

Organizations should strengthen cyber resilience by regularly conducting cyber risk assessments, resilience testing, disaster recovery exercises, and incident response simulations.

Government agencies should establish comprehensive national guidelines and regulatory frameworks supporting Zero-Trust cybersecurity implementation across critical infrastructure sectors.

Public–private partnerships should be strengthened to facilitate cyber threat intelligence sharing and coordinated incident response.

Continuous cybersecurity awareness and professional training programs should be developed to improve AI, Zero-Trust, and cyber resilience competencies among cybersecurity professionals.

Greater investment should be directed toward AI research, cybersecurity innovation, and intelligent security technologies tailored to Pakistan's digital environment.

Limitations and Future Directions

Although the study provides important empirical contributions, several limitations should be acknowledged.

First, the study adopted a cross-sectional research design, limiting the ability to examine long-term changes in cybersecurity performance following AI-driven Zero-Trust implementation. Future longitudinal studies are recommended to evaluate cybersecurity maturity and resilience over time.

Second, data were collected from selected organizations responsible for Pakistan's critical digital infrastructure. Consequently, the findings may not fully represent smaller organizations, private enterprises, or emerging digital sectors outside the sampled population.

Third, the study relied on self-reported perceptions of cybersecurity professionals. Although respondents possessed considerable expertise, self-reported data may introduce common method bias and subjective evaluation. Future studies should combine survey data with objective cybersecurity performance indicators, security audit reports, and real-world incident data.

Fourth, the study primarily focused on AI-driven Zero-Trust cybersecurity architecture, threat intelligence, cyber resilience, and regulatory readiness. Other influential factors—including organizational cybersecurity culture, cybersecurity investment, employee awareness, cloud security maturity, digital leadership, supply-chain security, and cybersecurity governance—were beyond the scope of the present investigation.

Future research should employ longitudinal and multi-country comparative studies involving South Asian and other emerging economies to improve generalizability. Researchers should also investigate the application of Generative AI, Explainable AI (XAI), Large Language Models (LLMs), Digital Twins, Blockchain, Quantum-Resistant Cryptography, Edge AI, and Autonomous Security Operations Centers (SOC) in strengthening Zero-Trust cybersecurity architectures. Additionally, future studies should evaluate the economic feasibility, implementation readiness, ethical considerations, privacy implications, and regulatory governance associated with AI-enabled cybersecurity technologies to support sustainable protection of critical digital infrastructure in Pakistan and beyond.

REFERENCES

Abraham, S., & Chengalur-Smith, I. (2024). Artificial intelligence and cybersecurity: Emerging trends, challenges, and future directions. Computers & Security, 136, 103613.

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. European Union Agency for Cybersecurity.

Kerman, A., Borchert, O., Howell, G., Rose, S., Souppaya, M., Scarfone, K., Barker, W., & Gallagher, P. (2025). Implementing a Zero Trust Architecture: High-Level Document (NIST Special Publication 1800-35). National Institute of Standards and Technology. (NIST)

National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.

National Institute of Standards and Technology. (2024). Cybersecurity framework (CSF) 2.0. National Institute of Standards and Technology.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.

Shackleford, D. (2021). Zero trust security: An enterprise guide. SANS Institute.

Stallings, W. (2022). Effective cybersecurity: A guide to using best practices and standards (2nd ed.). Addison-Wesley.

Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.

Weinberg, A. I., & Cohen, K. (2024). Zero trust implementation in the emerging technologies era: Survey. IEEE Access (Advance online publication). (arXiv)

World Economic Forum. (2025). Global cyber security outlook 2025. World Economic Forum.

Xu, L., Li, Y., Zhang, H., & Chen, X. (2023). Artificial intelligence for intelligent cyber threat detection and response: A systematic review. Computers & Security, 129, 103270.

Yamin, M. M. (2024). Artificial intelligence and cyber resilience: Opportunities and challenges for critical infrastructure protection. Journal of Information Security and Applications, 80, 103734.

Zhang, Y., Wang, H., Liu, J., & Chen, X. (2024). Explainable artificial intelligence for cyber threat intelligence and security analytics: A systematic review. Expert Systems with Applications, 245, 123102.

Zhou, Y., Sun, G., Mishra, S., & Wang, J. (2024). Artificial intelligence-enabled zero-trust architecture for critical infrastructure protection. IEEE Access, 12, 45671–45690.

Zhou, Z., Choo, K.-K. R., & Shi, W. (2023). Cyber resilience for critical infrastructure: Challenges, enabling technologies, and future research directions. ACM Computing Surveys, 56(4), 1–37.

Zscaler ThreatLabz. (2024). ThreatLabz 2024 AI Security Report. Zscaler.

National Cyber Security Centre. (2024). The cyber assessment framework (CAF): Guidance for critical national infrastructure. National Cyber Security Centre.

European Commission. (2023). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive): Implementation guidance. European Commission.