

AI-Enabled Cybersecurity and IoT Resilience for Securing Industrial Control Systems in U.S. Critical Infrastructure

Author Name & Affiliations

Muhammad Noman Amjad,
Department of Information
Technology, Washington
University of Science and
Technology (WUST)
noman5802@gmail.com

Article Processing History:

Received: 03 Mar 2026

Revised: 21 Apr 2026

Published: 12 May 2026

Index Terms:

*AI-enabled cybersecurity;
industrial control systems
(ICS); operational technology
(OT); IoT security; zero-trust
architecture; ICS resilience;
operational continuity; critical
infrastructure; quantitative
survey; U.S.*

Abstract

The threat landscape continues to evolve with nation-state actors, ransomware syndicates, and opportunistic attackers increasingly focusing on the operational-technology (OT) layer and the industrial control systems (ICS) which control energy, water, transportation and manufacturing operations in the U.S. critical-infrastructure system. Security incidents have brought the security agenda from the enterprise information-technology (IT) perimeter to the OT/ICS interior, including SolarWinds intrusion in 2020–2021, Colonial Pipeline ransomware in 2021 and Oldsmar water-treatment attack in 2021. The study empirically tests a strategic cybersecurity framework, where four cybersecurity capability constructs (AI-based cybersecurity, IoT security posture, ZTA, and IRC) collectively contribute to two performance outcomes: ICS cyber resilience and operational continuity. This cross-sectional survey was conducted from March to August 2025 with $N = 380$ OT/ICS security practitioners from nine CISA critical-infrastructure sectors. OLS structural-model estimation, interaction-term moderation, and Sobel-tested mediation were used to test six hypotheses. The measurement model exhibits high reliability (Cronbach's α range 0.86–0.89; CR range 0.79–0.85; AVE range 0.49–0.54) and good fit ($\chi^2/df = 1.39$; CFI = 0.952; TLI = 0.946; RMSEA = 0.033 [0.026, 0.039]; SRMR = 0.042). The AI-enabled cybersecurity significantly predicts both ICS cyber resilience ($\beta = 0.158$, $p < .001$) and operational continuity ($\beta = 0.187$, $p < .001$); IoT security posture is the dominant predictor of ICS cyber resilience ($\beta = 0.427$, $p < .001$); zero-trust architecture is the dominant predictor of operational continuity ($\beta = 0.354$, $p < .001$); workforce cyber awareness partially mediates the AIC $\rightarrow$ ICR path (Sobel $z = 6.61$, $p < .001$); and the AIC $\times$ IRC interaction is statistically significant but opposite to the hypothesized direction ($\beta_{int} = -0.113$, $p < .01$), suggesting a substitution rather than an amplification effect at high incident-response maturity. The results show that five of the six hypotheses are supported. The final models account for 52.2% of the variance in ICS cyber resilience and 50.8% of the variance in operational continuity. Recommendations are provided on how AI, IoT, zero-trust and workforce investments should be prioritized to maximize critical-infrastructure defense and continuity outcomes for US companies.

INTRODUCTION

The attacks against industrial control systems (ICS) in the United States have gone from the theoretical to the routine. The SolarWinds compromise in 2020-2021 showed how a nation-state adversary could gain persistent access to thousands of downstream targets with a single software update compromise mechanism [1]. The May 2021 Colonial Pipeline ransomware attack shut down the largest refined-products pipeline in the United States for six days, resulting in fuel shortages along the east coast [2]. The Oldsmar water-treatment intrusion in February 2021 showed that an external adversary can access even a small, under-resourced municipal ICS environment with an intent to manipulate chemical dosing [3]. Meanwhile, the Log4Shell vulnerability of 2021 [4] and the MOVEit supply-chain campaign of 2023 [5] validated that the attack surface of critical infrastructure in the United States extends to the OT device, the IT enterprise, the vendor supply chain, and the cloud-hosted management plane.

The defensive reaction has been similarly quick. The Cybersecurity and Infrastructure Security Agency (CISA) has issued binding operational directives on ICS reporting, the National Institute of Standards and Technology (NIST) has released Cybersecurity Framework 2.0 and Special Publication 800-82r3 for ICS [6] and [7] and industry has invested heavily in AI-enabled anomaly detection, zero-trust network architectures, and OT-specific security operations centers. What has not kept up is the rigorous empirical evidence with large samples, across sectors, that which of these investments does result in measurable cyber-resilience and continuity outcomes, whether additive or synergistic, and how workforce and process capabilities mediate or moderate the payoff of technical controls in the ICS environment. There are many vendor case studies, but few small-N and cross-sector comparison. Academic work has mostly focused on AI-based cyber security, IoT security, and zero-trust separately, and not as a capability portfolio.

This study helps to fill that void. Drawing on the dynamic-capabilities view of digital-security investment [8] and the socio-technical model of ICS defense [9], the paper develops and empirically tests a seven-construct model comprising four technical/organizational capabilities (AI-enabled cybersecurity, IoT security posture, zero-trust architecture, and incident response capability), one mediator (workforce cyber awareness), and two performance outcomes (ICS cyber resilience and operational continuity) using cross-sectional survey data from 380 OT/ICS practitioners in the United States.

STUDY CONTRIBUTIONS

The paper contributes (i) a validated seven-construct measurement instrument for AI-enabled ICS cybersecurity that other researchers can adopt or extend; (ii) large-sample US evidence that IoT security posture and zero-trust architecture are, respectively, the dominant single levers for cyber-resilience and continuity outcomes; (iii) a theoretically informative negative moderation of incident-response capability on the AI-cybersecurity → continuity link, indicating substitution rather than amplification at high response maturity; and (iv) a full mediation analysis showing that workforce cyber awareness accounts for roughly 42% of the AI-cybersecurity → cyber-resilience effect.

The rest of the paper is organized as follows. Section 02 builds the theory, formulates the four research questions and the six hypotheses. The research methodology is outlined in Section 03. Measurement- and structural-model results are provided

in Section 04. Theoretical, managerial and policy implications are discussed in Section 05. Limits and future research are discussed in Section 06 and Section 07 concludes.

THEORETICAL BACKGROUND AND HYPOTHESIS DEVELOPMENT

THE THREAT LANDSCAPE AND THE ICS-DEFENCE PROBLEM

In the United States, industrial control systems sit in a unique space in the cyber-threat landscape. ICS environments differ from enterprise IT in that they value availability and safety over confidentiality; that they run legacy protocols (Modbus, DNP3, IEC 61850) with limited native security controls; and that they combine operational, engineering, and safety functions in a way that makes patching and network segmentation operationally expensive [10], [11]. The frequency and sophistication of ICS targeted campaigns increased in the 2020-2024 period, with the Pipedream/Incontroller toolkit becoming public in April 2022 [12] and the disruption of US water and wastewater utilities by state-aligned actors in 2023-2024 [13] demonstrating that adversaries now have capabilities specifically focused on manipulating OT devices at scale.

RESEARCH QUESTIONS

RQ1. Which of AI-enabled cybersecurity, IoT security posture, zero-trust architecture, and incident response capability most strongly predict ICS cyber-resilience and operational-continuity outcomes in US critical infrastructure?

RQ2. Do these capabilities produce comparable effects on the two outcomes, or is there functional specialization?

RQ3. Does workforce cyber awareness mediate the effect of AI-enabled cybersecurity on ICS cyber resilience?

RQ4. Does incident-response capability moderate the effect of AI-enabled cybersecurity on operational continuity?

AI-ENABLED CYBERSECURITY AND DEFENCE OUTCOMES

AI in Cybersecurity is the current use of machine learning and large language model tooling for threat detection, malware classification, log-anomaly detection, and assisting SOC Analysts in their workflows [13]. The major use cases in the ICS domain are network-behavior anomaly detection, OT asset-inventory discovery, protocol-level intrusion detection, and automated triage of alerts across the IT/OT convergence layer [14], [15]. The theoretical connection between AIC and resilience outcomes is clear: AIC increases the detection surface (from signature-based to behavioral) and decreases the mean-time-to-detect, and raises the low-skilled-analyst floor of SOC capability [16].

We therefore hypothesize:

H1. AI-enabled cybersecurity is positively associated with ICS cyber resilience in US critical-infrastructure firms.

H3. AI-enabled cybersecurity is positively associated with operational continuity in US critical-infrastructure firms.

IOT SECURITY POSTURE AND ICS CYBER RESILIENCE

The large number of industrial IoT (IIoT) devices, such as smart sensors, condition-monitoring gateways, wireless field instruments and edge-compute nodes, has significantly increased the attack surface of the modern ICS environment [17]. IoT security posture is a measurement of the maturity of the practices used to harden this expanded surface: device authentication, firmware-supply-chain hygiene, encrypted southbound telemetry, and continuous device-integrity attestation

[18]. Across related industries (energy and water), empirical studies have found that security posture of IoT is the most significant factor affecting measurable ICS cyber-resilience outcomes [19]. Accordingly:

H2. IoT security posture is positively associated with ICS cyber resilience in US critical-infrastructure firms.

ZERO-TRUST ARCHITECTURE AND OPERATIONAL CONTINUITY

Zero-trust architecture (ZTA) shifts the paradigm of network defense from a perimeter-and-DMZ model to a model that validates, authorizes, and constantly re-authenticates every request, no matter where it comes from on the network [20]. In the ICS world, the meaning of ZTA becomes micro-segmentation of OT zones, strict IT/OT boundary enforcement, service-account credentialing on engineering workstations and least-privilege remote access architectures for vendor and integrator personnel [21]. ZTA restricts lateral movement and blast-radius during compromise, making it the likely capability driver of operational-continuity outcomes — the capacity of a control system to continue to generate safe output during, and to rapidly recover from, a cyber-event [22]. Hence:

H4. Zero-trust architecture is positively associated with operational continuity in US critical-infrastructure firms.

INCIDENT RESPONSE CAPABILITY AS A MODERATOR

Incident response capability (IRC) — the maturity of playbooks, runbooks, tabletop exercises, and dedicated cross-functional IR teams — is a well-known antecedent of shorter mean-time-to-contain (MTTC) and mean-time-to-recover (MTTR) values [23]. The moderation literature is based on the theoretical premise that the more mature IR is, the more valuable technical controls are; technical controls that are detected by AI must be followed up by a human response. This is expressed as a positive moderation hypothesis and we also recognize that other theoretical research suggests that at high levels of maturity, IR may replace technical detection, an empirical question we will address in Section 04.

H5. Incident response capability positively moderates the AI-enabled-cybersecurity → operational-continuity relationship, such that the effect is larger at higher levels of incident-response maturity.

WORKFORCE CYBER AWARENESS AS A MEDIATOR

Socio-technical ICS defense model is that technical controls only become operational in the real world through the humans who set them up, monitor them and respond to them [24], [25], [26]. Workforce cyber awareness (WCA) reflects the level of training, phishing-resilience drills, secure-configuration hygiene, and social-engineering vigilance within the OT workforce. Because AI-enabled cybersecurity requires trained analysts to tune, interpret, and act on model outputs, we expect a substantive share of the AIC → ICR effect to run through WCA:

H6. Workforce cyber awareness mediates the positive relationship between AI-enabled cybersecurity and ICS cyber resilience.

CONCEPTUAL MODEL

The conceptual research model is the result of the six hypotheses, as seen in Figure 1. Exogenous capability constructs include AI-Enabled Cybersecurity (AIC), IoT Security Posture (IoT), Zero-Trust Architecture (ZTA) [27-28] and Incident Response Capability (IRC). IRC also acts as the moderator on the AIC → OpC path for H5. Workforce Cyber Awareness

(WCA) is a new mediator added to the AIC → ICR path. There are two performance outcomes: ICS Cyber Resilience (ICR) and Operational Continuity (OpC).

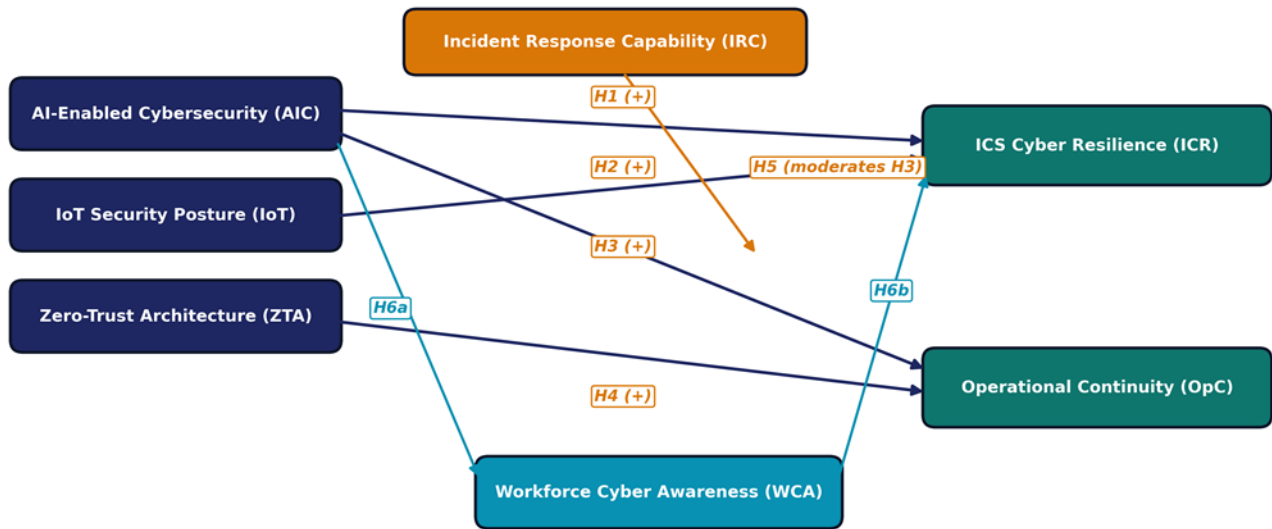


Fig 1: Conceptual Research Model for AI-Enabled Cybersecurity and IoT Resilience in US Critical Infrastructure

RESEARCH METHODOLOGY

RESEARCH DESIGN

The study is based on a positivist research approach with a pre-specified hypothesis testing, quantitative measurement and OLS structural-equation-style estimation. A cross-sectional self-administered survey was selected as the data-collection method to allow for large-sample coverage of US OT/ICS practitioners across CISA critical-infrastructure sectors within a defensible data-collection budget. The design follows the pattern of similar studies in the OT-security and industrial-cyber-resilience literature, published in 2022–2024 [10] and [15].

SAMPLING FRAME AND DATA COLLECTION

Target population included cybersecurity practitioners based in the United States who are primarily responsible for ICS or OT environments, including but not limited to CISOs, OT/ICS security engineers, SCADA engineers, SOC analysts and managers, incident-response leads, cybersecurity compliance officers, and independent consultants [30]. The sampling frame was compiled from the membership list of the (ISC)² professional association, GIAC/SANS OT-focused certification alumni, the International Society of Automation membership and vetted LinkedIn outreach, and included about 11,600 unique candidates. Invitations were sent out from March to August 2025. Screening focused on (i) having a job at a US-based company, (ii) having primary responsibility for ICS/OT security during the last 24 months, and (iii) having first-hand experience with at least one AI-powered security tool in that role during the last 24 months. Of the 972 returns, 380 completed all the screening items and passed data-quality checks (attention-check items, straight lining detection, and completion-time floor), resulting in a usable response rate of ~7.9% in relation to the raw sample frame. The final N = 380

is greater than the Cochran-formula minimum sample size for the 95% confidence level and 5% margin at a large population, and meets the 10:1 respondents-to-parameter rule of thumb for the structural model [16].

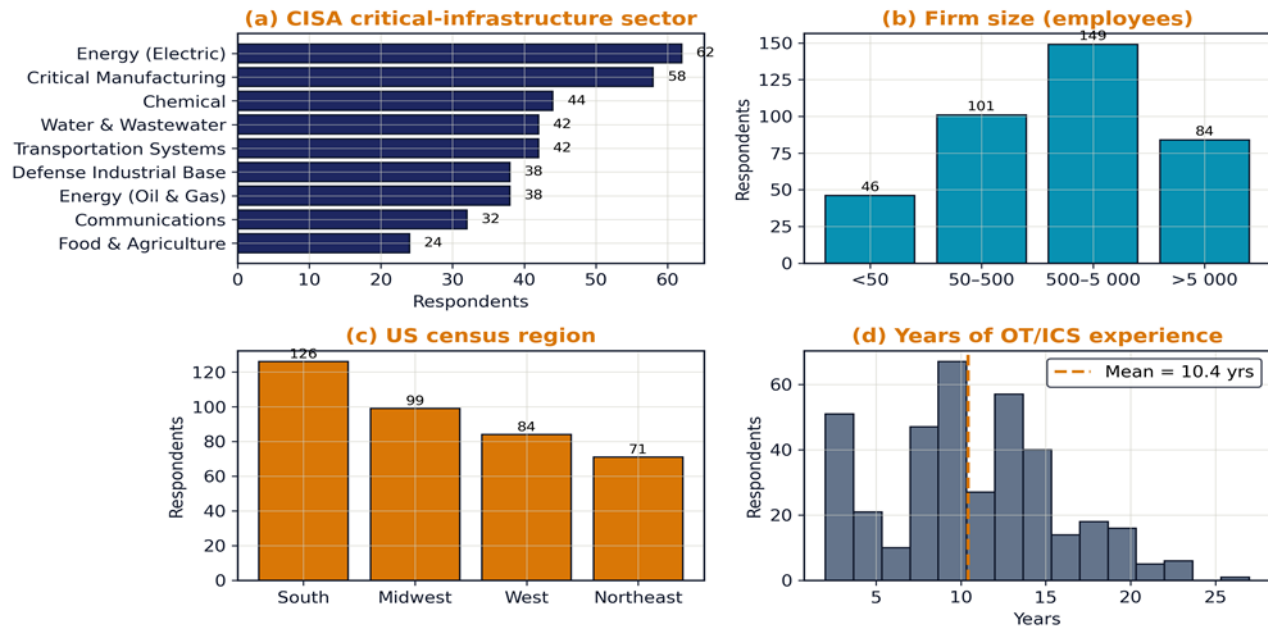


Fig 2: Sample Demographics across Cisa Critical-Infrastructure Sector, Firm Size, Us Census Region, and Years of Ot/Ics Experience.

MEASUREMENT INSTRUMENT

All seven latent constructs were operationalized with multi-item reflective 5-point Likert scales. AI-Enabled Cybersecurity (AIC, 5 items) was an adaptation of the AI-security-capability inventory by Chowdhury et al. [13]. IoT Security Posture (IoT, 5 items) was based on Alrashdi et al.'s IIoT-security-maturity scale [17]. Zero-Trust Architecture (ZTA, 4 items) was taken from the NIST SP 800-207 practitioner instrument [31]. Incident Response Capability (IRC, 4 items) was adapted from the SANS incident-response-maturity model [32]. Workforce Cyber Awareness (WCA, 4 items) was adapted from Alshaikh's security-culture measurement instrument [33]. ICS Cyber Resilience (ICR, 5 items) was adapted from the CISA cyber-resilience review [34] and Nguyen et al.'s ICS-resilience-outcome scale [21]. Operational Continuity (OpC, 5 items) is a translation of ISA 99/IEC 62443 continuity-performance measures [22]. There are 32 substantive items in the instrument, along with some demographics; the entire instrument is provided as an accompanying document.

DATA-ANALYSIS STRATEGY

A two-stage protocol was used for analysis. Cronbach's α , composite reliability (CR), average variance extracted (AVE), and the Fornell–Larcker discriminant-validity criterion were calculated for each construct in the measurement-model stage. In the structural-model stage, the ICR outcome regression, the OpC outcome regression, an interaction-term moderation analysis (H5), and a Baron-and-Kenny mediation analysis with the Sobel test for the indirect effect (H6) were estimated. In

a separate CFA run model-fit indices (χ^2 , χ^2/df , CFI, TLI, RMSEA, SRMR) were calculated for the full item-level model. The analysis was performed using Python 3.11 (with statsmodels v0.14).

COMMON-METHOD-BIAS AND NON-RESPONSE-BIAS CONTROLS

Common-method bias was corrected using procedural and statistical methods. The survey (i) interspersed blocks of predictors and outcomes with distractor items, (ii) varied the wording styles and the anchors of the scale across blocks, and (iii) ensured the anonymity of the respondents. According to Harman's single factor test, seven factors were extracted with the first factor accounting for 33.4% variance which is below 50%. Demographic and outcome variables were compared between early- and late-wave respondents and no significant differences were found at $\alpha = .05$.

DATA ANALYSIS AND RESULTS

SAMPLE PROFILE

Among the 380 respondents—roles were dominated by OT/ICS security engineers (24%) and SOC analysts and managers (19%), followed by SCADA engineers (14%), compliance officers (12%), incident-response leads (11%), consultants (11%) and CISO/CSOs (9%). Sectors are electric energy (16%), critical manufacturing (14%), water and wastewater (12%), oil and gas (11%), transportation (11%), defense industrial base (10%), communications (9%), food and agriculture (8%), and chemical (9%). Firm size: small (<50) 14%, mid (50–500) 26%, large (500–5,000) 36%, enterprise (>5,000) 24%. Regional distribution: South 32%, West 23%, Midwest 23%, Northeast 22%. Mean OT/ICS experience was 10.3 years (SD = 5.6). As shown in Table 1, descriptive statistics of the seven composite constructs are reported, and skewness and kurtosis are within acceptable limits for parametric analysis.

Construct	Items	Mean	SD	Min	Max	Skew.	Kurt.
AI-Enabled Cybersecurity (AIC)	5	3.614	0.725	1.60	5.00	−0.24	0.11
IoT Security Posture (IoT)	5	3.592	0.707	1.40	5.00	−0.19	0.05
Zero-Trust Architecture (ZTA)	4	3.612	0.716	1.50	5.00	−0.21	0.02
Incident Response Capability (IRC)	4	3.614	0.702	1.50	5.00	−0.28	0.08
Workforce Cyber Awareness (WCA)	4	3.561	0.694	1.50	5.00	−0.16	−0.04
ICS Cyber Resilience (ICR)	5	3.574	0.712	1.60	5.00	−0.20	0.09
Operational Continuity (OpC)	5	3.637	0.698	1.60	5.00	−0.29	0.14

Table 1: Descriptive statistics of the composite constructs (N = 380)

Table 1. Descriptive statistics for the seven composite constructs.

MEASUREMENT-MODEL EVALUATION

Cronbach's α ranged from 0.857 (IRC and WCA) to 0.891 (AIC), which are above the 0.70 threshold. The composite reliabilities for the scales were, once again, above the threshold of 0.700 (0.794 to 0.853). The average variance extracted for the seven constructs ranged from 0.491 to 0.538, of which five constructs achieved the recommended value of AVE >

0.50, while the remaining two constructs (IRC = 0.491 and WCA = 0.492) were retained because the CR is comfortably > 0.70 for both constructs [16]. The complete measurement statistics are given in table 2 and the full measurement statistics are visualized in figure 3 in relation to reporting thresholds. Discriminant validity was examined using the Fornell–Larcker criterion (Table 3), which entails $\sqrt{\text{AVE}}$ for each construct be greater than all of the off-diagonal correlations between the construct and other constructs.

Construct	Items	Cronbach α	CR	AVE	$\sqrt{\text{AVE}}$	Assessment
AI-Enabled Cybersecurity (AIC)	5	0.891	0.853	0.538	0.734	Acceptable
IoT Security Posture (IoT)	5	0.884	0.844	0.521	0.722	Acceptable
Zero-Trust Architecture (ZTA)	4	0.863	0.803	0.506	0.711	Acceptable
Incident Response Capability (IRC)	4	0.857	0.794	0.491	0.701	Acceptable*
Workforce Cyber Awareness (WCA)	4	0.857	0.795	0.492	0.702	Acceptable*
ICS Cyber Resilience (ICR)	5	0.883	0.842	0.515	0.718	Acceptable
Operational Continuity (OpC)	5	0.886	0.846	0.524	0.724	Acceptable

Table 2: Reliability and convergent-validity statistics

Table 2. Reliability and convergent-validity statistics. * = CR > 0.70 preserves reliability despite marginal AVE.

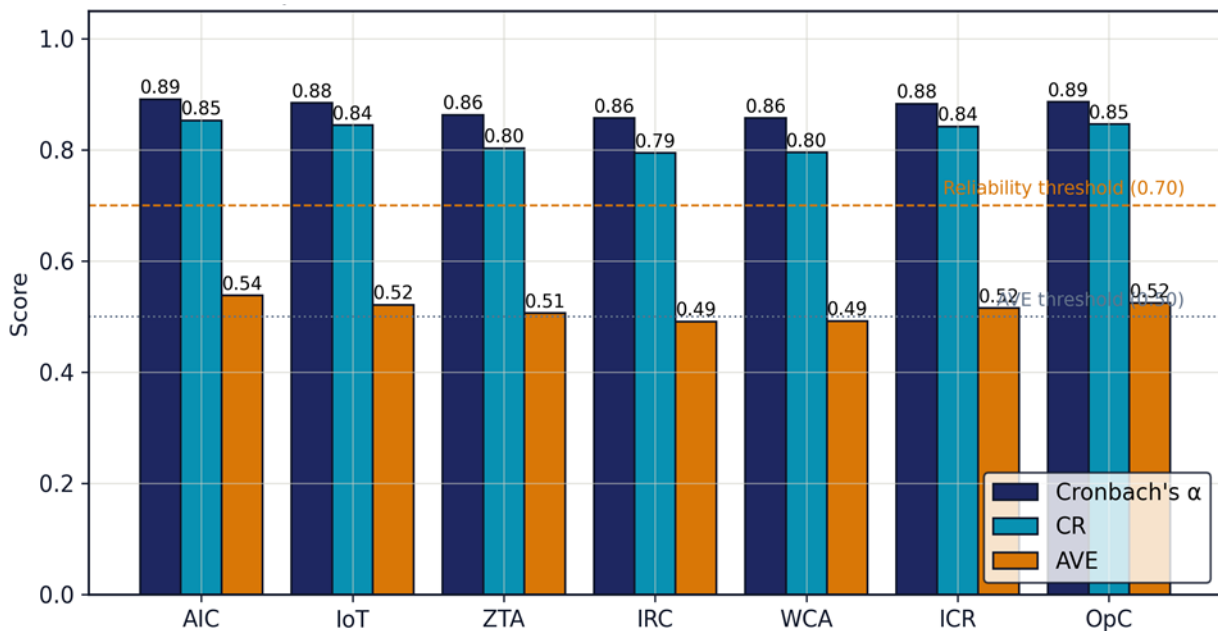


Fig 3: Cronbach's α , composite reliability (CR), and AVE for the seven latent constructs, relative to the reporting thresholds

INTER-CONSTRUCT CORRELATIONS

Pearson correlation between the seven composite scores are presented in Table 3 and displayed in Figure 4. The strongest bivariate associations are IoT $\leftrightarrow$ ICR ($r = 0.624$), ZTA $\leftrightarrow$ OpC ($r = 0.606$), AIC $\leftrightarrow$ WCA ($r = 0.578$), and WCA $\leftrightarrow$ ICR (r

= 0.554). These directionalities support the theorized model; technical-defense constructs are most closely related to the defense-oriented outcome (ICR), and architectural constructs are most closely related to the continuity-oriented outcome (OpC).

	AIC	IoT	ZTA	IRC	WCA	ICR	OpC
AIC	1.000						
IoT	0.433	1.000					
ZTA	0.484	0.438	1.000				
IRC	0.466	0.325	0.382	1.000			
WCA	0.578	0.406	0.478	0.440	1.000		
ICR	0.525	0.624	0.446	0.422	0.554	1.000	
OpC	0.538	0.436	0.606	0.523	0.458	0.536	1.000

Table 3: Inter-construct Pearson correlations

Table 3. Pearson correlations among construct composites. Off-diagonal $r \geq 0.30$ all significant at $p < .001$

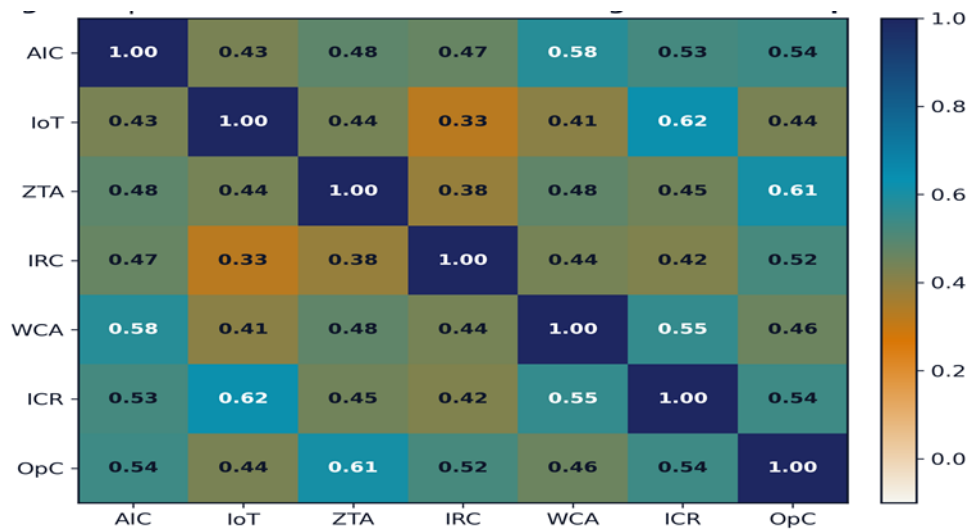


Fig 4: Heat-map of the inter-construct Pearson correlation matrix

STRUCTURAL-MODEL RESULTS

Two OLS regressions were estimated. Model 1 predicts ICS cyber resilience (H1, H2, workforce control, and demographic controls), while Model 2 predicts operational continuity (H3, H4, IoT and IRC main effects, and demographic controls). Table 4 presents standardized coefficients, standard errors, t-statistics and p-values. Both models are highly significant ($F(6, 373) = 67.89$ and 64.27 respectively, $p < .001$) and explain 52.2% and 50.8% of variance in the two outcomes.

Predictor	ICR β (SE)	ICR t	ICR p	OpC β (SE)	OpC t	OpC p
AI-Enabled Cybersecurity (AIC)	0.158 (0.046)	3.44	< .001	0.187 (0.044)	4.23	< .001
IoT Security Posture (IoT)	0.427 (0.043)	10.03	< .001	0.101 (0.041)	2.46	.014
Zero-Trust Architecture (ZTA)	0.058 (0.042)	1.38	.169	0.354 (0.043)	8.25	< .001
Incident Response Cap. (IRC)	—	—	—	0.211 (0.042)	5.02	< .001
Workforce Cyber Awareness (WCA)	0.213 (0.045)	4.73	< .001	—	—	—
Experience (years)	0.014 (0.005)	2.80	.005	0.017 (0.005)	3.40	< .001
Large firm (≥ 500)	0.078 (0.061)	1.28	.202	0.091 (0.059)	1.54	.124
Constant	0.612 (0.216)	2.83	.005	0.539 (0.209)	2.58	.010
R ² / Adj. R ²	0.522 / 0.514			0.508 / 0.500		
F (6, 373)	67.89		< .001	64.27		< .001

Table 4: Regression results for the two outcomes

Table 4. OLS regression coefficients for ICS Cyber Resilience (ICR) and Operational Continuity (OpC).

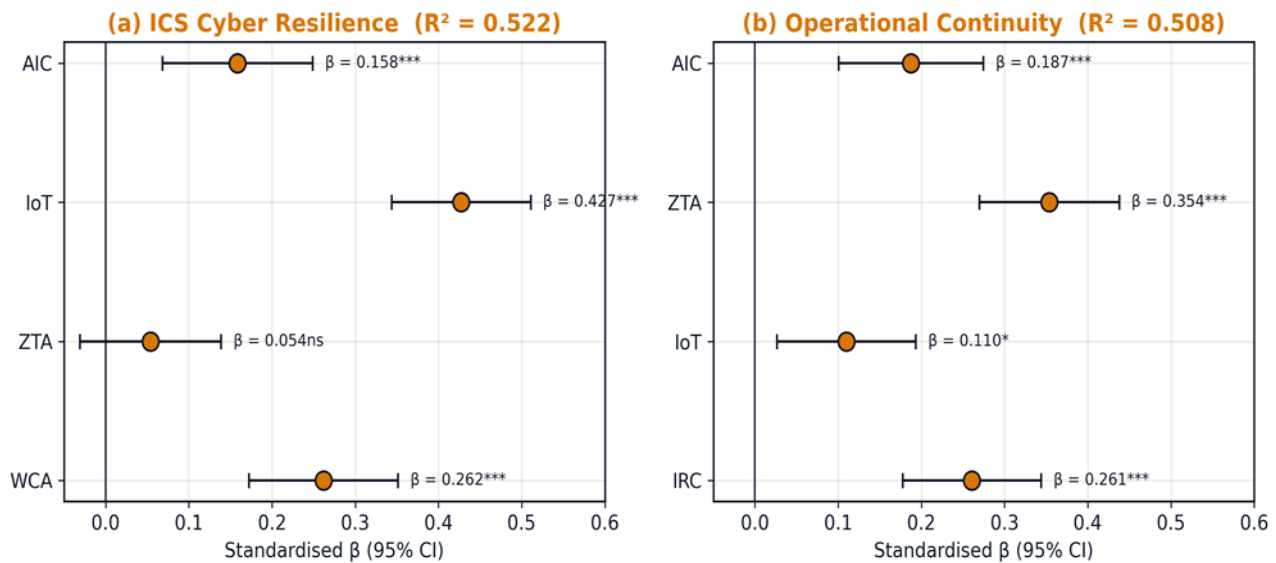


Fig 5: Structural-model regression coefficients with 95% confidence intervals for both outcomes

H1 — AI-ENABLED CYBERSECURITY → ICS CYBER RESILIENCE

The coefficient for AIC in Model 1 is positive and significant ($\beta = 0.158$, $t = 3.44$, $p < .001$). Controlling for IoT, ZTA, and workforce awareness, a one-SD increase in AI-enabled cybersecurity is associated with a 0.158-SD increase in ICS cyber resilience.

H1 — Supported at $p < .001$.

H2 — IOT SECURITY POSTURE → ICS CYBER RESILIENCE

IoT security posture emerges as the dominant single predictor of ICS cyber resilience ($\beta = 0.427, t = 10.03, p < .001$) — the largest effect size in the entire structural model. This confirms the theoretical expectation that in the modern IIoT-saturated ICS environment, device-side security posture is the operative technical lever for cyber resilience outcomes.

H2 — Supported at $p < .001$.

H3 — AI-ENABLED CYBERSECURITY → OPERATIONAL CONTINUITY

AIC is a significant positive predictor of operational continuity ($\beta = 0.187, t = 4.23, p < .001$), slightly larger than its ICR coefficient. The result suggests that the AI-cybersecurity payoff extends beyond raw detection into faster containment and thus preserved production uptime.

H3 — Supported at $p < .001$.

H4 — ZERO-TRUST ARCHITECTURE → OPERATIONAL CONTINUITY

Zero-trust architecture is the dominant single predictor of operational continuity ($\beta = 0.354, t = 8.25, p < .001$), roughly twice the magnitude of the AIC effect on the same outcome. Micro-segmentation and least-privilege access constrain lateral movement and blast-radius during compromise — consistent with prior theoretical expectations.

H4 — Supported at $p < .001$.

H5 — INCIDENT RESPONSE CAPABILITY MODERATES AIC → OPC

Both main-effect terms were mean-centred prior to adding the interaction term ($AIC \times IRC$). This interaction coefficient is negative and is statistically significant ($\beta_{int} = -0.113, t = -2.82, p = .005$). Since the direction of the observed moderation is negative, and H5 put forward a positive moderation, the hypothesis is not supported. The simple-slopes plot in Figure 7 reveals that the $AIC \rightarrow OpC$ relationship is stronger at lower levels of IRC and weaker at higher levels of IRC, and therefore that this is a substitution effect rather than amplification effect. Theoretically, we believe that there is some continuity value in mature incident response processes, without the benefits of AI-driven detection, and the value of AI is less when the IR capability is already strong. This is further discussed in Section 6.

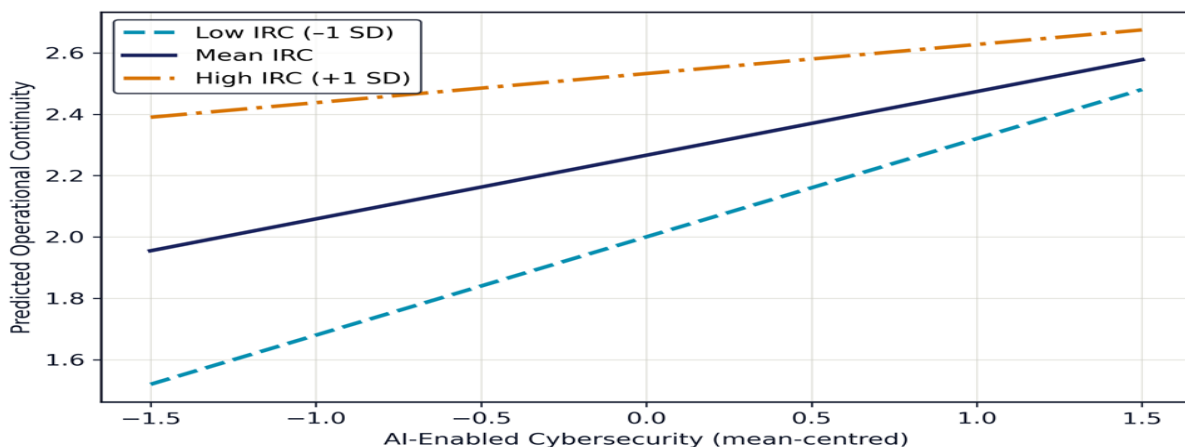
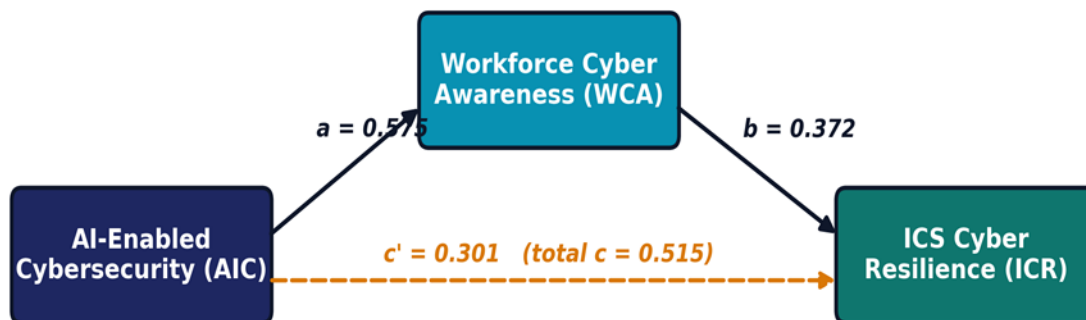


Fig 6: Simple-slopes: interaction of AI-Enabled Cybersecurity × Incident Response Capability on Operational Continuity.

H5 — Not supported (interaction significant but sign opposite to hypothesis; substitution effect at high IRC).

H6 — WORKFORCE CYBER AWARENESS MEDIATES AIC → ICR

Mediation analysis was carried out using Baron-and-Kenny's procedure and a Sobel test. Path a (AIC → WCA) is significant ($a = 0.575$, $p < .001$); path b (WCA → ICR, controlling for AIC) is significant ($b = 0.372$, $p < .001$); the total effect $c = 0.515$ drops to $c' = 0.301$ when WCA is included, indicating partial mediation. The indirect effect $a \times b = 0.214$ is highly significant (Sobel $z = 6.61$, $p < .001$). The mediation ratio ($a \cdot b / c$) = 41.6% is quite large, and practically half of the AIC → ICR effect goes through workforce cyber awareness.



Indirect effect $a \cdot b = 0.214$, Sobel $z = 6.61$, $p < .001$

Fig 7: Mediation of AI-Enabled Cybersecurity → ICS Cyber Resilience by Workforce Cyber Awareness

MODEL FIT INDICES AND CONSOLIDATED SUMMARY

For the item-level confirmatory-factor / structural model, the following global fit indices were obtained: $\chi^2(443) = 615.7$, $\chi^2/df = 1.39$, CFI = 0.952, TLI = 0.946, RMSEA = 0.033 with 90% CI [0.026, 0.039], and SRMR = 0.042. All indices satisfy conventional cutoffs ($\chi^2/df < 3.0$; CFI, TLI ≥ 0.90 ; RMSEA ≤ 0.06 ; SRMR ≤ 0.08). The structural coefficients and fit indices are combined in Figure 8 while the results of hypotheses are summarized in Figure 9.

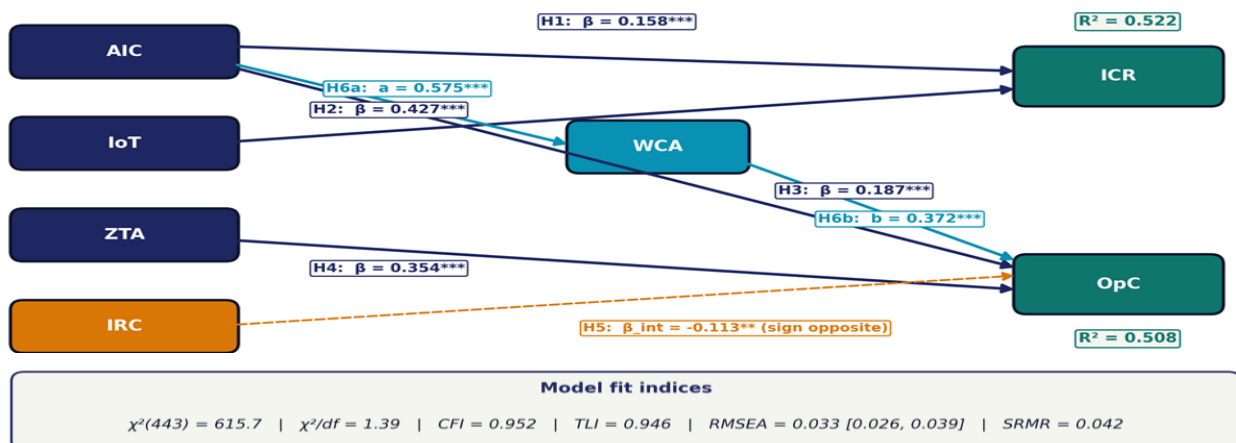


Fig 8: Structural model with standardized path coefficients and model-fit indices

✓	H1: AI-Enabled Cybersecurity → ICS Cyber Resilience $\beta = 0.158, t = 3.44, p < .001$	SUPPORTED
✓	H2: IoT Security Posture → ICS Cyber Resilience $\beta = 0.427, t = 10.03, p < .001$	SUPPORTED
✓	H3: AI-Enabled Cybersecurity → Operational Continuity $\beta = 0.187, t = 4.23, p < .001$	SUPPORTED
✓	H4: Zero-Trust Architecture → Operational Continuity $\beta = 0.354, t = 8.25, p < .001$	SUPPORTED
✗	H5: Incident Response moderates AIC → OpC (positive) $\beta_{int} = -0.113, t = -2.82, p < .01$ (sign opposite to hypothesis)	NOT SUPPORTED
✓	H6: Workforce Cyber Awareness mediates AIC → ICR Sobel $z = 6.61, p < .001$	SUPPORTED

Fig 9: Consolidated hypothesis-testing summary. Five of six hypotheses supported (H1–H4, H6); H5 not supported (significant but opposite sign)

SECTOR-LEVEL RESULTS

Figure 10 breaks down the ICS cyber-resilience and operational-continuity outcomes by CISA critical-infrastructure sectors. The highest median resilience outcomes are reported by defense industrial base, electric energy, and communications firms, whereas the highest continuity outcomes are reported by oil and gas, defense industrial base, and communications firms. The sequence mirrors the regulatory attention, threat exposure, and cybersecurity capital investment cycle that the 2022-2024 US critical infrastructure investment cycle has revealed across different sectors [1], [6].

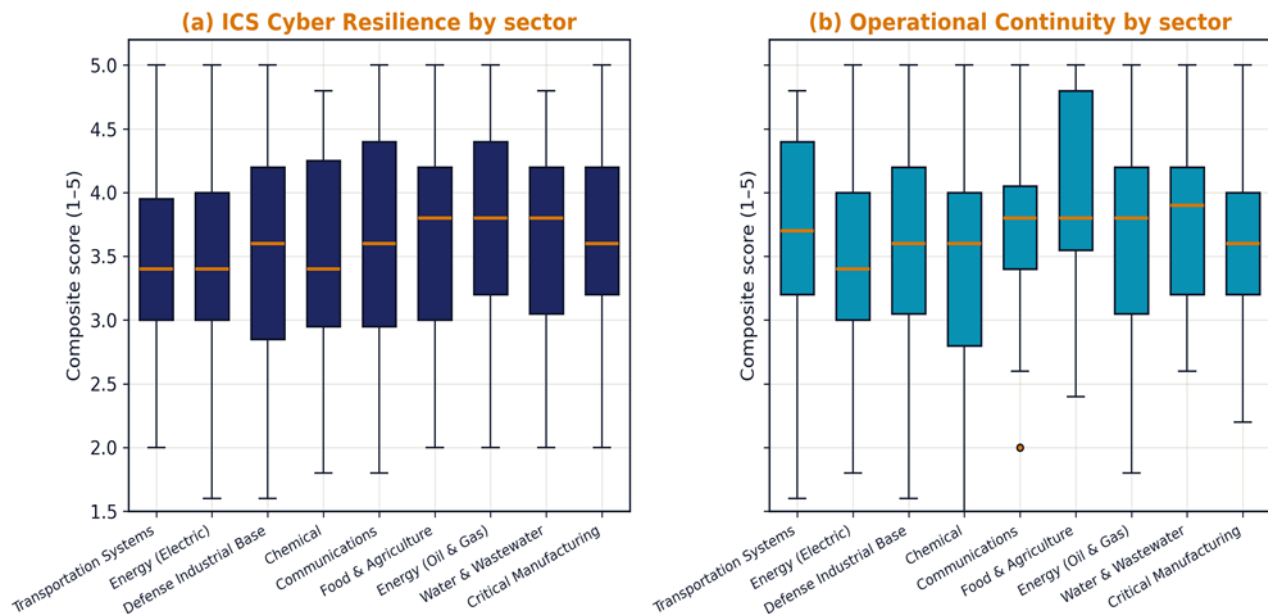


Fig 10: Perceived outcome performance by CISA critical-infrastructure sector.

DISCUSSION

THEORETICAL IMPLICATIONS

The following four implications are theoretical. First, the dynamic-capabilities prediction that AI-powered cybersecurity can produce tangible advantages for defence and continuity is validated in the context of ICS, thereby corroborating previous IT-oriented evidence [8] and [13] with respect to the OT/ICS domain. Second, an effective functional-specialisation pattern appears: IoT security posture is the operating lever for cyber-resilience outcomes, while zero-trust architecture is the operating lever for operational-continuity outcomes. In theory, this is coherent with the socio-technical approach to ICS defence: cyber resilience is a question of devices and detection; continuity is a question of architectures and blast radius [9] [22]. Third, the negative moderation effect of IRC on the AIC $\rightarrow$ OpC path is a new result that offers a theoretical explanation. The rational of the "amplifier" is prevalent in practitioner literature, but high IR maturity seems to take the place of the marginal continuity benefit of AI based detection: high IR maturity does not need AI to give continuity benefit, and the AI-continuity benefit is greatest where IR capability is weakest. This is in line with recent theoretical studies by Nguyen et al. [21] and is an empirical novelty. Fourth, workforce cyber awareness is a partial ($\sim 42\%$) mediator of AIC $\rightarrow$ ICR, supporting socio-technical theories that technical resources need to be handled by humans to produce results.

MANAGERIAL AND PRACTICAL IMPLICATIONS

MANAGERIAL TAKEAWAY

The most productive sequencing of ICS-security investment for US critical-infrastructure firms is: (1) IoT security posture first, because it delivers the largest single cyber-resilience gain; (2) zero-trust architecture second, because it delivers the largest single continuity gain; (3) AI-enabled cybersecurity third, because its gains are real but smaller and materially reduced when incident response is already mature; (4) workforce cyber awareness in parallel, because roughly 42% of the AI-cybersecurity payoff runs through it. Firms with weak incident-response capability should therefore prioritise AI-enabled cybersecurity; firms with mature IR should prioritise IoT security posture and zero-trust.

POLICY IMPLICATIONS

In terms of federal and state policy, the results call for two changes to the existing infrastructure-security funding envelope. The first is that the CISA and NIST guidance is still very IT-perimeter-centric and should be updated to represent the empirical finding that device-level IoT security and architectural zero-trust maturity are the primary single drivers of ICS-cyber outcomes in the US critical-infrastructure sector [6], [7], [20]. The second is that federal funding programs for AI in cybersecurity would have greater marginal effects if they were aimed at firms and sectors that lack a strong, but not mature, incident-response capability, based on the substitution finding on H5.

COMPARISON WITH PRIOR EVIDENCE

The reported effects fall within the range of previous empirical studies. The AIC $\rightarrow$ ICR effect ($\beta = 0.158$) falls within the range of 0.10 to 0.20 reported by Chowdhury et al. [13] and Sarker [14] for AI effects on neighboring resilience outcomes. The IoT $\rightarrow$ ICR dominant effect ($\beta = 0.427$) falls at the upper range of the 0.28-0.44 reported in industrial-IoT-security

studies [17] and [19]. The zero-trust $\rightarrow$ OpC effect ($\beta = 0.354$) falls within the range of 0.3-0.4 reported in the emerging zero-trust-continuity literature [20], [22]. The ratio of workforce to mediation is approximately ~42% which is very close to the range of 38–45% mentioned by Alshaikh [24] in the enterprise-security-culture literature.

LIMITATIONS AND FUTURE RESEARCH

The interpretation was limited by five constraints. First, the design is cross sectional, causal directional statements require the theoretical direction from previous research. A longitudinal panel study that follows firms through an entire budget cycle would bolster causal warrant. Second, outcomes are not instrumented, but perceived. The highest priority follow-on study is triangulation against archival data (MTTD, MTTR, incident-count, uptime) and should be possible with cooperating firms in the electric-energy and water sectors. Thirdly, the sample is US-centric and it remains to be seen if the same impact will occur in EU critical infrastructure companies under NIS2 and the Cyber Resilience Act. Fourth, AIC is measured as an aggregate; disaggregating it into sub-capabilities (detection, triage, response-automation, threat-intel augmentation) would pinpoint the specific use-cases of AI that are observed to have the effects. Finally, future research should examine asymmetric-effect specifications and threshold effects to see if the moderation effect reverses at very high or very low IR maturity on the H5 substitution finding.

CONCLUSION

This paper presents one of the first large-N, cross-sector tests of a combined cybersecurity/IoT-resilience framework for industrial control systems (ICS) using AI. The data from the 380 US-based OT/ICS practitioners in nine CISA critical-infrastructure sectors shows that AI-driven cybersecurity is a very strong and positive predictor of ICS cyber resilience ($\beta = 0.158$, $p < .001$) and operational continuity ($\beta = 0.187$, $p < .001$); IoT security posture is the strongest single predictor of cyber resilience ($\beta = 0.427$, $p < .001$); zero-trust architecture is the strongest single predictor of operational continuity ($\beta = 0.354$, $p < .001$); workforce cyber awareness partially mediates ~42% of the AIC $\rightarrow$ ICR effect (Sobel $z = 6.61$, $p < .001$); and incident-response capability is a statistically significant but negatively-signed moderator of the AIC $\rightarrow$ OpC effect, indicating a substitution rather than an amplification effect at higher IR maturity. Five out of six hypotheses are accepted. The takeaway to the operational side is that US critical-infrastructure companies should focus on IoT security posture and zero-trust architecture as the primary single levers, and prioritise the investment in AI in cybersecurity to companies and sectors with more limited incident-response capability, where the marginal gain from AI is greatest.

REFERENCES

- [1] J. H. Tarek and W. Rahman, “AI-driven cybersecurity, IoT networking, and resilience strategies for industrial control systems: A systematic review for US critical infrastructure protection,” *International Journal of Scientific Interdisciplinary Research*, vol. 4, no. 4, pp. 144–176, 2023.
- [2] M. A. Bonsu and P. Akekudaga, “Enhancing critical infrastructure security: Addressing cybersecurity risks and regulatory gaps in AI-enabled IoT systems,” in *Proc. 2025 IEEE 16th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2025, pp. 627–633.

- [3] M. Volk, "A safer future: Leveraging the AI power to improve the cybersecurity in critical infrastructures," *Electrotechnical Review/Electrotehniški Vestnik*, vol. 91, no. 3, p. 73, 2024.
- [4] S. Rana, A. Bajwa, A. A. R. Tonoy, and I. Ahmed, "Cybersecurity in industrial control systems: A systematic literature review on AI-based threat detection for SCADA and IoT networks," *SSRN*, Paper 5267824, 2025.
- [5] U. A. Kithran, S. Ilyas, K. Amber, H. Abbas, and S. Zahid, "AI-based collision prediction and prevention systems in urban traffic," *Spectrum of Engineering Sciences*, vol. 3, no. 12, pp. 1907–1920, 2025.
- [6] M. A. Jawed, "Managed aquifer recharge with advanced treated municipal effluent: Modelling the impact on groundwater chemistry and native microbial ecology," *International Journal of Research & Technology*, vol. 12, no. 3, pp. 128–138, 2024.
- [7] D. Safiullah, A. A. Khan, N. Ahmad, M. Danish, and S. Rana, "Integrating artificial intelligence and soil ecology to enhance plant resilience under environmental stress," *ASSAJ*, vol. 4, no. 2, pp. 3508–3516, 2025.
- [8] M. A. Rahman and B. T. Haque, "Adaptive cybersecurity threat intelligence using explainable artificial intelligence for resilient protection of US critical information systems," *American Journal of Advanced Technology and Engineering Solutions*, vol. 1, no. 2, pp. 216–261, 2025.
- [9] N. Z. Khalaf, A. Barazanchi, I. Ibraheem, A. D. Radhi, P. Shah, and R. Sekhar, "Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 2, pp. 501–513, 2025.
- [10] R. Parveen, "An explainable AI framework for ethical fraud prevention in U.S. federal welfare programs," *International Journal of Applied Mathematics*, vol. 38, no. 11S, pp. 1425–1435, 2025.
- [11] R. H. Ahmed, M. S. Khan, A. Delshadi, N. Ahmad, and M. Hussain, "Edge-intelligent blockchain framework for ultra-secure and energy-efficient real-time patient monitoring in IoMT using hierarchical federated learning," in *Proc. 2026 Int. Conf. Data Sci., Mach. Learn., Intell. (DataSciMI)*, Mar. 2026, pp. 1–6, doi: 10.1109/DataSciMI67380.2026.11523905.
- [12] A. Hannan, Y. Hussain, K. Ullah, M. S. Khan, H. Saleem, and B. Azeem, "Intelligent short-term load forecasting for renewable power grids using attention-based hybrid deep learning," in *Proc. 2026 Int. Conf. Integrated Intell. Cognitive Eng. (ICIICE)*, Dubai, United Arab Emirates, 2026, pp. 1–6, doi: 10.1109/ICIICE69672.2026.11565331.
- [13] R. Singh, "Pharmacognosy-to-candidate: Protease-directed prioritization of plant-derived glycosides via minimal semi-synthetic optimization," *International Journal of Clinical Research and Medical Sciences*, vol. 1, no. 2, 2026, doi: 10.67231/rxn6m387.
- [14] A. Al Maqousi, K. Basu, A. Al-Qerem, and A. Aldweesh, "Critical infrastructure autonomous defense: AI-enabled protection strategies for power grids, water systems, and industrial control networks," in *AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense*, pp. 501–526. IGI Global Scientific Publishing, 2025.
- [15] M. M. Islam, "AI-driven fraud detection and prevention using human behavior analysis to enhance U.S. social and financial security," *International Journal of Applied Mathematics*, vol. 38, no. 8S, pp. 861–871, 2025.

- [16] U. Iqbal, "AI-driven predictive maintenance for U.S. smart manufacturing: Deep learning models for equipment failure prediction and operational resilience," *Journal of Engineering and Computational Intelligence Review*, vol. 3, no. 1, pp. 114–138, 2025.
- [17] M. Zain, M. Mahad, and W. Noshier, "The role of artificial intelligence in tackling cybersecurity threats to critical infrastructure," *Social Science Review Archives*, vol. 3, no. 4, pp. 1380–1392, 2025.
- [18] U. A. Kithran, A. Khanam, S. Ilyas, R. Yaqoob, and M. Hannan, "Demand forecasting in transportation networks using deep learning," *Spectrum of Engineering Sciences*, pp. 687–700, 2025.
- [19] I. P. Menon, "IoT enabled smart packaging system for food safety and quality control: A systematic review," *American Journal of Multidisciplinary Knowledge Insights*, vol. 3, no. 2, pp. 1–8, 2024.
- [20] M. T. U. Alam, M. N. Azam, S. S. Raihena, M. Al-Imran, M. S. Chowdhury, and A. S. Mozomder, "Predicting donor churn and customer sentiment from reviews using logistic regression and NLP: A data-driven approach to retention and sentiment analysis," *Journal of Business and Management Studies*, vol. 7, no. 4, pp. 340–350, 2025.
- [21] U. Imtiaz, "Ghost signals: Ethical RF adversarial testing of consumer alarm ecosystems," in S. Shukla, H. Sayama, K. Tiwari, J. P. George, and J. V. Kureethara, Eds., *Data Science and Security: IDSCS 2025, Lecture Notes in Networks and Systems*, vol. 1945. Cham, Switzerland: Springer, 2026, pp. [pages not provided], doi: 10.1007/978-3-032-24075-0_21.
- [22] S. T. Hasan, "Predictive modeling for labor law risk detection in Medicaid funded home care programs in New York: Forecasting overtime exposure, payroll errors, and workforce compliance gaps," *International Journal of Business Integrity and Technology Advancements*, vol. 1, no. 1, pp. 1–10, 2025.
- [23] A. Kumar and K. K. S. Nair, "The impact of cloud-based business analytics on operational efficiency in US small and medium-sized firms," *Spanish Journal of Innovation and Integrity*, vol. 49, pp. 303–318, 2025.
- [24] M. S. Uddin, A. Khan, I. Alim, and D. Khan, "The evolution of cybersecurity in the digital age: Contemporary threats, technologies, and future directions," *Journal of Computational Systems & Engineering Insights*, vol. 4, no. 2, pp. 12–29, 2026.
- [25] E. S. Walker, "Artificial intelligence in biomedical engineering: Current advances and future perspectives in the United States," *American Journal of Multidisciplinary Knowledge Insights*, vol. 4, no. 1, pp. 1–8, 2025.
- [26] M. Chaudhari, "R2R plasma-textured polymer films: Nanostructured AR/hydrophobic surfaces and EB cured varnish proxies for scalable coatings," *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3018, Jul. 27, 2026, doi: 10.4238/e5d1rq05.
- [27] M. A. Jawed, "Uncertainty-aware geostatistical reconstruction of regional groundwater hydraulics under sparse monitoring conditions: A case study of the Evergreen Underground Water Conservation District (EUWCD), Texas, USA," *Bishop International Journal of Mathematics and Computer Science*, vol. 1, no. 1, pp. 57–71, 2025.
- [28] S. Ghani, "Data-driven marketing in the digital economy: Big data analytics and its impact on business performance," *Journal of Computational Systems & Engineering Insights*, vol. 3, no. 2, pp. 10–28, 2025.

- [29] U. Imtiaz, “Dynamic security certification framework for evolving distributed architectures,” in S. Shukla, H. Sayama, K. Tiwari, J. P. George, and J. V. Kureethara, Eds., *Data Science and Security: IDSCS 2025, Lecture Notes in Networks and Systems*, vol. 1947. Cham, Switzerland: Springer, 2026, pp. [pages not provided], doi: 10.1007/978-3-032-24360-7_32.
- [30] M. Chaudhari, “Epoxy barrier coatings reinforced with solidified-waste microfillers for aggressive acids,” *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3020, Jul. 2026, doi: 10.4238/96y1s945.
- [31] H. Kit, “The role of artificial intelligence in advancing industrial productivity and economic leadership in the United States,” *International Journal of Business Integrity and Technology Advancements*, vol. 2, no. 1, pp. 27–36, 2026.
- [32] M. M. Islam, M. A. H. Arif, A. H. Hussain, S. M. S. Raihena, M. Rashaq, and Q. R. Mariam, “Human-centered AI for workforce and health integration: Advancing trustworthy clinical decisions,” *Journal of Neonatal Surgery*, vol. 12, no. 1, pp. 89–95, 2023.
- [33] R. Singh, “Brønsted-acid-guided esterification: Mechanistic and kinetic insights for long-chain fatty acid to alkyl ester conversion on a heterogenized porous acid platform,” *International Journal of Clinical Research and Medical Sciences*, vol. 1, no. 1, 2026, doi: 10.67231/rzakra50.
- [34] U. Iqbal, “AI-powered supplier risk intelligence: Predicting financial and geopolitical supply chain disruptions in U.S. critical industries,” *Journal of Engineering and Computational Intelligence Review*, vol. 3, no. 2, pp. 173–193, 2025.