SOCIAL PRISM

Volume 3(5), 2026, 323-335
Online ISSN: 3006-8886
Print ISSN: 3006-8878

AI Cybersecurity Capabilities and IoT Resilience: A Moderated Serial Mediation Model of Threat Detection Effectiveness and Incident Response Agility

Bilal Qureshi[1], Mian Haseeb Mushtaq[2], Muhammad Shozab Mehdi[3], Sarfaraz Ahmed[4]

[1]*Independent Researcher, Pakistan, Email: bilalqureshi991188@gmail.com*
[2] *Department of Computer Science, Lahore Garrison University, Pakistan, Email: haseebmuhstaq@gmail.com*
[3]*FAST School of Computing, National University of Computer & Emerging Sciences (NUCES), Karachi, Pakistan, Email: shozabmehdi89@gmail.com*
[4]*Department of Computer Science, University of the People, California, USA, Email: space.sarfaraz216@gmail.com*

Abstract

While strategically deploying Artificial Intelligence (AI) is critical for the security of Internet of Things (IoT) ecosystems, organizations often face challenges in converting their AI investments into operational resilience. This study investigates a moderated serial mediation model, shedding light on how AI Cybersecurity Capabilities contribute to achieving IoT Resilience. Based on Resilience Engineering and Dynamic Capabilities theory, we hypothesize that AI Cybersecurity Capabilities as a reflective-formative higher-order construct consisting of Sensing, Learning, Automation, and Decision-Support can increase IoT Resilience by first supporting the operation of the Threat Detection Effectiveness (TDE) and then the Incident Response Agility (IRA) capabilities. Moreover, we hypothesize that Cybersecurity Governance (CSG) is a meta-capability with a unique moderating effect on each phase of the process. The results support the serial mediation pathway ($\beta = 0.10$, $p < 0.001$, 95% CI [0.06, 0.15]) based on the survey data obtained from 327 senior cybersecurity executives in critical infrastructure sectors and analyzed using the Partial Least Squares Structural Equation Modeling (PLS-SEM) with repeated indicators approach. Importantly, CSG moderates the indirect effect, and the serial mediation has a significant stronger effect in high-governance contexts (Index of Moderated Serial Mediation = 0.08, CI [0.04, 0.13]). This research provides a granular process-based cybersecurity value realization model, with suggestions and insights for Security Operations Centers and security governance committees at the board level.

Keywords: AI Cybersecurity Capabilities, Incident Response Agility, IoT Resilience, Threat Detection Effectiveness, Cybersecurity Governance, Serial Mediation, PLS-SEM, Higher-Order Construct.

Introduction

With the increasing proliferation of the Internet of Things (IoT), organizations' operations have been revolutionized, and at the same time, the number of attack surfaces of the Internet has increased exponentially. With the advent of heterogeneous, resource-constrained IoT devices and

Received 30 May 2026; Revised 08 July 2026; Accepted 17 July 2026; Published (online) 25 July 2026

Corresponding Author Email: haseebmuhstaq@gmail.com
DOI: https://doi.org/10.69671/ socialprism.3.5.2026.139

Online ISSN: 3006-8886
Print ISSN: 3006-8878

the unprecedented security challenges in critical infrastructure sectors such as energy, healthcare, manufacturing, and smart cities, the need to secure these new and evolving systems has never been greater. Industry reports have shown significant growth in the attack surface area of the IoT sector and signature-based defenses are becoming ineffective against emerging threats from multiple vectors (Cisco, 2024).

In response, organisations are taking a proactive approach to improving their cyber security posture by implementing Artificial Intelligence (AI). With AI-powered solutions that incorporate machine learning, deep learning, and predictive analytics, they provide much more than just a set of rules: real-time anomaly detection, behavioral analysis, and automated threat response. Research has shown that the Mean Time to Detect (MTTD) can be significantly decreased and the overall accuracy of threat detection can be enhanced with the inclusion of AI (Ahmed et al., 2024; Sarker et al., 2024). A disconcerting disconnect remains, however: even the most sophisticated AI-powered companies have subpar IoT resiliency, routinely subjected to extended periods of downtime despite early warning.

Research Gap

Although there has been an emerging interest in examining AI in cybersecurity, there are several gaps in the literature. First, current studies have tended to take a narrower focus on technical performance indicators like detection accuracy, false positive rates, and reaction times, without exploring how organizational mechanisms facilitate the creation of resilience outcomes from the AI capabilities.First, current research has tended to be more focused on the technical performance indicators of the AI capabilities, such as detection accuracy, false positive rates, and response times, rather than on the organizational mechanisms that enable the creation of resilience outcomes from the capabilities. While there is research on the adoption and effectiveness of AI tools, little is known about how AI investments lead to operational resilience.Research has focused on the adoption and effectiveness of AI tools, but the link between AI investments and operational resilience remains poorly theorized. Second, although threat detection has been recognized as playing a crucial role, the mediating effect of Threat Detection Effectiveness between AI and IoT resilience has not been analyzed systematically in order to examine the role of Threat Detection Effectiveness in the relationship between AI and IoT resilience. Third, although Cybersecurity Governance is often touted as an important factor in determining the effectiveness of investment in AI tools for cybersecurity, it has, to date, not been tested empirically in its ability to influence the effectiveness of investment in AI tools, specifically its effects on the cybersecurity detection and response capabilities (De Haes & Van Grembergen, 2022; NIST, 2023). Fourth, existing research has focused primarily on the capabilities of AI as a single entity without accounting for the complexities of how these capabilities are applied in the field of cybersecurity (Mikalef et al., 2022). Fifth, limited attention has been devoted to the empirical basis of the interplay between detection and response two functionally distinct, yet interdependent operations in security (Johnston et al., 2023; Naseer et al., 2023).

In order to tackle these gaps, we pose the following research questions:

RQ1: Do Threat Detection Effectiveness and Incident Response Agility sequentially mediate the relationship between AI Cybersecurity Capabilities and IoT Resilience?

RQ2: Is Cybersecurity Governance an intervening mediator in this serial mediation pathway?

Online ISSN: 3006-8886
Print ISSN: 3006-8878

This research work has three main contributions. First, we enrich the cyber security literature by introducing a cycle of “AI-performance” with a “serialized” view and elucidating why “perfect” detection accuracy does not necessarily lead to “resilience.” Second, we propose a new meta-dynamic capability Cybersecurity Governance and differential moderating effects, following the call for studying "cybersecurity orchestration" (Sarker et al., 2024). Third, we combine Resilience Engineering dimensions to the Resource Based View, thus establishing a comprehensive framework that brings together the technical detection and the organizational recovery.

Literature Review

The theoretical framework used is based on Dynamic Capabilities theory (Teece 2007) of how organizations recognize new threats, capitalize on opportunities to withstand those threats, and change their security stance in response to changes. In our model, AI Cybersecurity Capabilities are the strategic resource base, Threat Detection Effectiveness an operationalization of the ‘sensing' capability (the organizational process of detecting threats), and Incident Response Agility an operationalization of the ‘seizing' capability (the organizational process of mobilizing resources to contain and recover from threats). The conceptual framework of Resilience Engineering (Hollnagel, 2021) is used to understand the outcome: IoT Resilience is not just the lack of failures, it's the capacity to anticipate, monitor, respond, and learn from failures. The Resource-Based View (Barney, 1991) serves as the background justification for the fact that AI can be viewed as a VRIN resource, from which cybersecurity advantage is drawn.

Cybersecurity Governance is an organizational mechanism which creates the environment in which the deployment and impact of these cybersecurity dynamic capabilities are carried out. Governance provides the organizational frameworks, strategies and monitoring systems that make sensing and seizing effective and continuously improve. Governance is not a dynamic capability, but a means to achieve effective operation of dynamic capabilities, including the validation of AI deployments, coordination between detection and response functions, and pre-allocation of recovery resources. Our model is based on a hierarchical logic resources, in which processes lead to outcomes, and governance orchestrates the process chain.

AI Cybersecurity Capabilities as a Reflective-Formative Higher-Order Construct

AI Cybersecurity Capabilities (AIC) are defined as a more complex organizational capability that indicates an organization's capability to use AI technologies as a means of security. This will be modeled as a reflective-formative (Type II) higher-order construct based on the guidelines of hierarchical latent variable modeling of PLS-SEM (Becker et al., 2012; Hair et al., 2022). This specification is theoretically suitable since the four dimensions – Sensing, Learning, Automation and Decision-Support – are conceptually separate aspects that combine to give the total latent capability, and are not synonymous with a single underlying ability. The three dimensions each represent a specific operational need within the cybersecurity value chain, and collectively represent strategic AI proficiency (Mikalef et al., 2022). The key difference between the Type II (as opposed to reflective-reflective – Type I) is that dimensions are not only reflections of a common underlying factor but also are independent factors that describe the capability. It is also primarily preferred over formative-formative (Type IV) since the lower order components are measured reflectively and have common variance. The four dimensions are based on the consensus in the AI capabilities literature, and Mikalef et al. (2022) found that the key dimensions of the AI capabili-

Online ISSN: 3006-8886
Print ISSN: 3006-8878

ties were sensing, learning, and automation, while decision-support was a later discovery from research on human-AI teaming in a security environment. These four dimensions are not only different from conceptualizations of alternative models, but they directly correspond to the cybersecurity value chain: sensing - detection, learning - adaptation, automation - rapid response, and decision-support - human-AI collaboration. In the repeated-indicators approach, the higher-order construct is estimated while keeping the second-order dimensions in the model, incorporating the theoretical relationship among them and providing a single unified model estimation (Becker et al., 2012; Hair et al., 2022). The two-stage approach has some advantages in terms of Fisher consistency (Ringle et al., 2012), but the repeated indicators approach was chosen because it provides a single unified model that estimates all paths simultaneously, maintaining the nomological network, it is more efficient for predictive models in which the HOC is a cause of the LOCs, and it is more appropriate for the formative specification, in which the LOCs are considered as distinct facets which combine to form the overall capability (Hair et al., 2022). Both methods are found to have similar results in a well-specified model in simulation studies (Becker et al., 2012). AI Sensing Capability is the ability to use pattern recognition and anomaly detection algorithms to extract threat information from a heterogenous IoT network traffic; AI Learning Capability is the capacity to adaptively retrain algorithms to prevent new forms of adversarial tactics, zero-day exploits, and new attack vectors; AI Automation Capability is the degree to which the AI algorithm can trigger predefined containment protocols without the need for human intervention, thereby minimizing response latency; and AI Decision-Support Capability is the ability for the AI algorithm to provide prioritized, contextualized, actionable intelligence to the human SOC analyst, thereby reducing cognitive load and decision fatigue. These dimensions collectively encapsulate the complexity of AI proficiency in cybersecurity settings, offering a thorough framework for our empirical study.

IoT Resilience: From survival to adaptation

Based on Resilience Engineering, we define IoT Resilience (RES), as the systemic capability of an organization to perform four critical functions (Duchek, 2020): Anticipate (proactively predict attack vectors), Withstand (absorb the first impact of an attack without cascading effects of critical failures), Recover (restore degraded functions to operational baselines), Adapt (evolve defensive posture, architecture, and procedures through post-incident forensic learning). We operationalize IoT Resilience as a reflective-formative second-order construct because the four dimensions are conceptually different patterns and/or components that come together to form the overall IoT Resilience capability, and are not interchangeable measures of a single underlying factor. This specification aligns with resiliency as measured in organizational settings in which organizations might have varying profiles of anticipation, withstanding, recovery, and adaptation capacities (Duchek, 2020).

Construct Boundaries

In order to keep the concepts clear, we clearly separate the four model constructs. AI Cybersecurity Capabilities are the organizational capabilities to deploy and use AI-enabled cybersecurity technologies. Threat Detection Effectiveness is an indicator of true operational performance, showing the accuracy, speed, and extent of threat detection capabilities enabled by artificial intelligence. Incident Response Agility is an organizational execution capability that is represented by the ability to mobilize, coordinate and quickly and effectively execute incident response activ-

Online ISSN: 3006-8886
Print ISSN: 3006-8878

ities including containment, eradication and coordination. Organizational IoT Resilience is an outcome of a systemic state that the organizational capability has in anticipation, resisting, recovering, and adapting to cyber incidents. This distinction capacity: performance: execution: outcome is a clear conceptual sequence without overlap of constructs.

Hypothesis Development

In this study, we propose the following nine hypotheses under an umbrella of the theoretical framework and conceptual model developed in this study:

H1As AI Cybersecurity Capabilities increase, IoT Resilience increases.

H2: The impact of AI Cybersecurity Capabilities on Threat Detection Effectiveness is positive.

H3:The Threat Detection Effectiveness has a positive relationship with Incident Response Agility.

H4: Incident Response Agility has positive influence on IoT Resilience.

H5:The relationships between AI Cybersecurity Capabilities and IoT Resilience (AI → TDE → IRA → RES) are mediated by Threat Detection Effectiveness and Incident Response Agility in succession.

H6: The relationship between AI Capabilities and Threat Detection Effectiveness is a positive one that is moderated by Cybersecurity Governance, with the interaction being stronger when Cybersecurity Governance is in its higher dimension.

H7: The relationship between Threat Detection Effectiveness and Incident Response Agility is positive and is different between low and high levels of Cybersecurity Governance.

H8:The relationship between Incident Response Agility and IoT Resilience is moderated positively by Cybersecurity Governance, meaning that this relationship is stronger and more valuable when Cybersecurity Governance is high.

H9: The serial indirect effect of AI Cybersecurity Capabilities on IoT Resilience through Threat Detection Effectiveness and Incident Response Agility is stronger as Cybersecurity Governance is higher.

Methodology

Research Design and Sampling

A quantitative cross sectional survey design was used, surveying organizations that have extensive deployments in Manufacturing, Healthcare and Utilities/Smart Cities. We sent 1,500 invites to senior security executives using a purposive sampling approach via the Cybersecurity Insiders panel. Of the screened questionnaires, 327 were rejected as valid responses (21.8% effective rate). This sample size is larger than the minimum recommended for PLS-SEM with complex moderation and higher order constructs (Hair et al., 2022). Senior cybersecurity executives (CISOs, IT Directors, Senior SOC Managers) were chosen as key informants because they have

Online ISSN: 3006-8886
Print ISSN: 3006-8878

broad, strategic responsibilities for overseeing cybersecurity and a deep understanding of organizational cybersecurity capabilities.

Table 1: Sample Demographics

Characteristic	Category	Frequency	Percentage
Industry Sector	Manufacturing	147	44.9%
	Healthcare	98	30.0%
	Utilities/Smart Cities	82	25.1%
Organization Size	< 500 employees	62	19.0%
	500–2,500 employees	128	39.1%
	2,501–10,000 employees	89	27.2%
	> 10,000 employees	48	14.7%
Respondent Role	CISO	108	33.0%
	IT Director	96	29.4%
	Senior SOC Manager	77	23.5%
	VP/Head of Security	46	14.1%

Instrument Development

The survey instrument has been designed based on guidelines established (DeVellis, 2017). The initial pool of 45 items was judged by five experts. The final instrument consisted of 32 items in five constructs. The constructs were all scaled from 1 = Strongly Disagree to 5 = Strongly Agree on multi-item scales.

AI Cybersecurity Capabilities (AIC): Eight items operationalized as a reflective-formative higher-order construct that has four dimensions (two items each), adapted from Mikalef et al. (2022).

Threat Detection Effectiveness (TDE): Five items adapted from Goode et al. (2022) that are related to detection accuracy, false positives, coverage, and timeliness.

Adopted from Naseer et al. (2023) and Johnston et al. (2023), Incident Response Agility (IRA): 5 items measuring containment speed, eradication effectiveness and recovery velocity.

Cybersecurity Governance (CSG): Six items from De Haes & Van Grembergen (2022) and NIST CSF 2.0 that cover strategic oversight, policy adherence, resource allocation, and accountability.

IoT Resilience (RES): This second order construct was measured as a reflective construct based on four core dimensions of Resilience Engineering (Anticipate, Withstand, Recover, Adapt) as developed by Duchek (2020).

Control Variables: Organization Size, Organizational Age, IT Infrastructure Age, Cybersecurity Budget, IoT Deployment Maturity, Industry Sector, Cybersecurity Maturity, AI Adoption Experience and Organization Type.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Analytical Procedures

We used two-step Partial Least Squares (PLS) Structural Equation Modeling (SEM) with the help of SmartPLS 4.0. The PLS-SEM is well suited for this complex model as it allows for the handling of higher-order constructs, moderation, and prediction orientation (Hair et al., 2022).

For the reflective-formative HOC (AIC), we used the Repeated Indicators Approach (RIA) developed by Becker et al. (2012) and Hair et al. (2022) which allows for the estimation of a single unified model while maintaining the nomological network.

Step 1 – Measurement Model Assessment: Internal consistency reliability (Cronbach's α and CR > 0.70), convergent validity (AVE > 0.50), and discriminant validity (HTMT < 0.85) were assessed. Model fit was assessed using SRMR (< 0.08) and NFI (> 0.90).

Step 2 – Structural Model Assessment: Bootstrapping (5,000 times resample) was used to assess the path coefficients. The Index of Moderated Mediation (Hayes, 2022) was used to test H9. The predictive power was evaluated by R^2, Q^2, f^2 and PLSpredict.

Common Method Bias: We used procedural measures such as anonymity, distinct scale anchors and statistical tests like Harman's single-factor test, full collinearity VIF, common latent factor, marker-variable approach.

Results

Measurement Model Assessment

The results of the measurement model are shown in Table 2. Each of the constructs have good psychometric attributes. Cronbach's α values ranged from 0.82 to 0.91, CR values from 0.86 to 0.93, and AVE values from 0.62 to 0.78. Good model fit was suggested by the SRMR = 0.062 and NFI = 0.91.

Table 2: Measurement Model: Reliability and Convergent Validity

Construct	Items	Cronbach's α	Composite Reliability	AVE
AI Cybersecurity Capabilities (HOC)	8	0.89	0.92	0.66
Sensing (LOC)	2	0.84	0.88	0.72
Learning (LOC)	2	0.86	0.89	0.74
Automation (LOC)	2	0.82	0.86	0.68
Decision-Support (LOC)	2	0.85	0.88	0.71
Threat Detection Effectiveness	5	0.88	0.91	0.69
Incident Response Agility	5	0.87	0.90	0.67
Cybersecurity Governance	6	0.91	0.93	0.72
IoT Resilience (Reflective SOC)	8	0.90	0.92	0.65

Discriminant Validity: Table 3 presents HTMT ratios. All values were below 0.85 (highest HTMT = 0.72), confirming adequate discriminant validity.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Table 3: Discriminant Validity (HTMT Ratios)

Construct	1	2	3	4	5
1. AI Cybersecurity Capabilities					
2. Threat Detection Effectiveness	0.72				
3. Incident Response Agility	0.68	0.71			
4. Cybersecurity Governance	0.58	0.62	0.65		
5. IoT Resilience	0.64	0.69	0.73	0.60	

Higher-Order Construct Validation: Table 4 presents outer weights, loadings, VIF values, and redundancy analysis. All four dimensions contributed significantly to AIC formation (Automation: 0.34, Sensing: 0.31, Learning: 0.28, Decision-Support: 0.22). All VIF values were below 3.3, indicating no multicollinearity.

Table 4: Higher-Order Construct Validation

Dimension	Weight	t-value	p-value	VIF	Loading	R^2
Sensing	0.31	5.82	< 0.001	2.14	0.84	0.71
Learning	0.28	5.14	< 0.001	2.08	0.82	0.67
Automation	0.34	6.21	< 0.001	2.31	0.86	0.74
Decision-Support	0.22	4.03	< 0.001	1.95	0.79	0.62
HOC (Formative)						**0.78**

Common Method Bias Assessment

Harman's single-factor test (28.4% variance), full collinearity VIF (1.42–2.87), common latent factor (average change < 0.03), and marker-variable approach (non-significant correlations) collectively indicated that common method bias is not a significant concern.

Structural Model Assessment

Table 5 presents direct path coefficients. The model explained substantial variance: R^2 for TDE = 0.43, IRA = 0.51, RES = 0.56. Q^2 values exceeded zero (TDE: 0.31, IRA: 0.38, RES: 0.42).

Table 5: Structural Model: Path Coefficients

Hypothesis	Path	β	t-value	p-value	f^2	Supported
H1	AIC → RES	0.28	4.56	< 0.001	0.12	Yes
H2	AIC → TDE	0.52	8.94	< 0.001	0.28	Yes
H3	TDE → IRA	0.48	7.82	< 0.001	0.22	Yes
H4	IRA → RES	0.41	6.73	< 0.001	0.18	Yes

Mediation Analysis (H5)

Table 6 presents the direct, indirect, and total effects for the serial mediation model. Given the structural model specified in Table 5 — in which TDE and IRA are linked only through the sequential path AIC → TDE → IRA → RES — the serial pathway constitutes the sole indirect route by which AIC influences RES. This indirect effect was significant (β = 0.10, CI [0.06, 0.15]), confirming H5. Accordingly, the Total Indirect Effect is equal to this specific indirect ef-

Online ISSN: 3006-8886
Print ISSN: 3006-8878

fect (β = 0.10), and the Total Effect of AIC on RES is the sum of the direct effect (β = 0.28) and this indirect effect, yielding β = 0.38. The serial pathway accounted for 26.3% of the total effect (VAF = 0.10/0.38), indicating partial mediation.

Table 6: Serial Mediation: Direct, Indirect, and Total Effects

Effect	β	t-value	95% CI	p-value	VAF
Total Effect (AIC → RES)	0.38	8.21	[0.28, 0.48]	< 0.001	—
Direct Effect (AIC → RES)	0.28	4.56	[0.16, 0.40]	< 0.001	73.7%
Total Indirect Effect	0.10	4.87	[0.06, 0.15]	< 0.001	26.3%
Specific Indirect: AIC → TDE → IRA → RES	0.10	4.87	[0.06, 0.15]	< 0.001	26.3%

Note: The total indirect effect (0.10) equals the specific serial indirect effect (AIC → TDE → IRA → RES = 0.52 × 0.48 × 0.41 = 0.10). This represents the only indirect pathway from AIC to RES given the structural model specified in Table 5. The total effect (0.38) is the sum of the direct effect (0.28) and the total indirect effect (0.10).

Moderation Analysis (H6, H7, H8)

Table 7 presents moderation results. All three interaction terms were significant, with H7 (TDE × CSG → IRA) being the strongest ($f^2 = 0.11$).

Table 7: Moderation Effects

Hypothesis	Interaction	β	t-value	p-value	f^2	Supported
H6	AIC × CSG → TDE	0.22	3.84	< 0.001	0.08	Yes
H7	TDE × CSG → IRA	0.27	4.56	< 0.001	0.11	Yes
H8	IRA × CSG → RES	0.19	3.21	< 0.01	0.05	Yes

Moderated Serial Mediation (H9)

Table 8 presents conditional indirect effects. The Index of Moderated Serial Mediation was significant (Index = 0.08, CI [0.04, 0.13]), confirming H9. The serial indirect effect was significantly stronger under high CSG (β = 0.16) compared to low CSG (β = 0.06).

Table 8: Conditional Indirect Effects (Moderated Serial Mediation)

CSG Level	Conditional Indirect Effect	SE	95% CI	p-value
Low CSG (μ - 1σ)	0.06	0.02	[0.02, 0.11]	< 0.01
Mean CSG	0.10	0.03	[0.06, 0.15]	< 0.001
High CSG (μ + 1σ)	0.16	0.04	[0.10, 0.23]	< 0.001
Index of Moderated Serial Mediation	**0.08**	**0.02**	**[0.04, 0.13]**	**< 0.001**

PLS predict and IPMA

PLS predict confirmed predictive relevance (PLS-SEM RMSE < LM RMSE). IPMA revealed TDE (importance: 0.38, performance: 72.4) and IRA (importance: 0.31, performance: 68.9) as the most critical drivers of IoT Resilience.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

Discussion

Summary of Findings

This study empirically tested a moderated serial mediation model examining how AI Cybersecurity Capabilities translate into IoT Resilience. Our findings support all nine hypotheses. First, AI Cybersecurity Capabilities have a significant direct positive effect on IoT Resilience (H1: $\beta = 0.28$, $p < 0.001$). Second, TDE and IRA sequentially mediate the AI-Resilience relationship (H5: $\beta = 0.10$, $p < 0.001$, 20.4% VAF). Third, Cybersecurity Governance significantly moderates all three pathways, with the strongest effect on TDE → IRA (H7: $\beta = 0.27$, $f^2 = 0.11$). Fourth, the moderated serial mediation effect was confirmed (H9: Index = 0.08, CI [0.04, 0.13]), with the serial indirect effect being substantially stronger under high CSG.

Explanation of Findings

The observed relationships can be understood through organizational information processing theory and socio-technical systems theory. AI enhances information processing capacity, but this must be channeled through organizational routines (TDE) and response mechanisms (IRA) to produce resilience. The direct effect of AI on resilience ($\beta = 0.28$) suggests AI also serves a symbolic and strategic function. The strong moderation of governance on TDE→IRA ($f^2 = 0.11$) reflects the concept of organizational ambidexterity governance structures facilitate the transition between exploration (detection) and exploitation (response). The weaker moderation effects on H6 ($f^2 = 0.08$) and H8 ($f^2 = 0.05$) suggest governance is most critical at organizational interfaces rather than within single functions.

Comparison with Prior Studies

Our findings extend prior research by demonstrating that AI-resilience relationship operates through a serialized process in cybersecurity contexts (Mikalef et al., 2022). We complement Naseer et al. (2023) by showing response agility is enabled by detection effectiveness and amplified by governance. We extend De Haes & Van Grembergen (2022) by identifying governance as a strategic enabler with distinct mechanisms validation, coordination, and resource allocation.

Theoretical Contributions

First, we extend RBV and Dynamic Capabilities by disaggregating the "black box" of AI security value creation through a serialized process (AI → TDE → IRA → RES). Second, we propose Cybersecurity Governance as a meta-dynamic capability that has differential moderating effects, namely validation, coordination, and resource allocation. Thirdly, we combine Resilience Engineering dimensions along with RBV and Dynamic Capabilities, forming a holistic model that creates a bridge between the socio-technical domains.

Practical Implications

There are several implications for the action in this study for different organizational stakeholders. The results highlight the critical need for CISOs and SOC Managers to invest in “detection-to-action” pipelines, since purchasing advanced AI capabilities is not enough if they lack the investment necessary to support response capabilities. Organisations should regularly run "purple team" exercises with detection and response teams working together, with the high fidelity alerts

Online ISSN: 3006-8886
Print ISSN: 3006-8878

converting to the quickest possible containment. These results indicate that the detection and response capabilities are complementary and not substitutes, and when dealing with SOC best practice, SOC managers should concentrate on the delay between the detection alert and the action of the response being initiated, since this is where the value is most likely being lost. The IPMA results show that Threat Detection Effectiveness (0.38) is most important with regard to resilience, and Incident Response Agility (0.31) comes second. This implies that investments in Threat Detection Effectiveness and Incident Response Agility will provide the greatest return for resilience. The findings confirm that Cybersecurity Governance is neither a burden nor an expense – it is an enabler that can magnify the impact of investing in AI security. Boards should have clear escalation procedures between detection and response teams, have pre-approved budgets for emergency response resources, have regular tabletop exercises with technical and executive stakeholders, and review performance metrics at the board level. The differential moderation effects suggest that boards should focus especially on the detection-response interface because governance has the highest modulating effect ($f^2 = 0.11$), while the IPMA results reveal that governance performance (65.2) could be enhanced when compared with TDE (72.4) and IRA (68.9). The results underscore the importance of including "governance dashboards" in AI security tools that provide real-time reporting and transparency about detection success rate and false-positive metrics for use by governance committees to monitor tools and pinpoint inefficiencies in the detection-to-response process. For Policymakers and Regulators, the findings indicate that policy needs to focus on the management of the AI security lifecycle, not just implementation, and that there should be rules for the board to review the cybersecurity function, regular risk assessments, and rehearsals of incident responses. Finally, for Organizational Leaders, the findings indicate that resilience is a property of the organization as a whole and is dependent on coordinating activities across technical, operational and governance levels – for leadership, fostering a culture where detection and response teams work collaboratively on a continuous basis and governance structures support, rather than impede, rapid action.

Limitations and Future Research

The present study has certain limitations which require mention and be addressed in future studies. The first is the cross-sectional nature of the study, which doesn't allow us to draw causal inferences; although our endogeneity analysis uncovered no serious issues, future research should focus on longitudinal studies to see how AI capabilities, TDE, IRA, and governance have developed over time. Second, perceptual measures provided by a single informant were used, and future studies should include objective measures of performance, such as actual MTTD logs, false positive rates and the time to respond to incidents, as well as multiple informant designs to increase the validity of the measures. Third, we focus our sample on organizations in manufacturing, healthcare, and utilities, and results may not be generalizable to other sectors or organizations that are smaller. This raises the question of the need for cross-sectoral and cross-cultural studies. Fourth, we studied a small number of moderators and future studies might focus on other contextual factors like the organizational culture, the characteristics of the threat landscape, and national cybersecurity maturity. Finally, we proposed AI Cybersecurity Capabilities as a reflective-formative higher-order construct, and future studies might investigate other higher-order constructs for studying these effects or employ alternative factors for the construct, such as the individual AI dimensions (Automation: 0.34, Sensing: 0.31, Learning: 0.28, Decision-Support: 0.22) on resilience outcomes. As a future extension, a fourth mediator, Cyber Learning Capabil-

Online ISSN: 3006-8886
Print ISSN: 3006-8878

ity (CLC) would capture the organization's capability of turning the outcomes of incidents into improved defenses, thereby completing the Resilience Engineering lifecycle of Detect → Respond → Learn → Adapt, into a serial quadruple mediation (AI → TDE → IRA → CLC → RES). Furthermore, future studies might use qualitative approaches to study the micro-foundations of the detection-response hand-off in order to gain greater insight into the mechanisms of governance that enable or impede agility.

Conclusion

As cyber threats grow more complex and rapidly evolve against IoT ecosystems, there is no longer enough time for organizations to allow threat detection and incident response to be disconnected and separate tasks. This study has empirically proven that IoT Resilience is not just created by single investments in the AI technology — it is built across an integrated chain of organizational capabilities from the detection to agile response and supported by good governance structures that connect these capabilities. The results support our hypothesis that AI Cybersecurity Capabilities influence IoT Resilience directly, as well as indirectly. The indirect influence is mediated by Threat Detection Effectiveness and Incident Response Agility and accounts for 20.4% of the overall influence of AI Cybersecurity Capabilities. Most importantly, Cybersecurity Governance comes as a meta-capability that strongly moderates this entire process, and the serial indirect effect is significantly stronger (166% increase) in high-governance contexts than in low-governance contexts. The differential moderation effects suggest that the marginal benefits of governance is at the detection-response interface ($f^2 = 0.11$), at which point governance enables the "hand-off" between detecting and responding through the facilitation of co-ordination arrangements that overcome organisational silos. These results have three important implications for the cybersecurity literature: First, we break down the monolithic linkage of AI and performance into a series of steps that reveal why organizations with high accuracy in cybersecurity detection may not be able to become resilient; Second, we introduce a new capability, termed Cybersecurity Governance, for the cybersecurity literature that is defined by a series of validation, coordination, and resource allocation mechanisms; and Third, we create a framework to integrate the dimensions of Resilience Engineering with the Resource Based View and Dynamic Capabilities theory to help close the socio-technical gap in the cybersecurity literature. In the case of practitioners, the need is obvious: optimize algorithms, SOC processes, and boardroom oversight. In addition to the investments in AI, detection processes, agile response capabilities, and governance frameworks must all be in place to ensure detection intelligence is quickly followed by action.

References

1. Ahmed, M., Khan, S. A., & Lee, J. (2024). AI-driven reductions in mean time to detect for critical infrastructure. *Computers & Security*, 138, 103654.
2. Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99-120.
3. Becker, J. M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM. *Long Range Planning*, 45(5-6), 359-394.
4. Cisco. (2024). *Cybersecurity readiness index: IoT threat landscape*. Cisco Annual Security Report.

Online ISSN: 3006-8886
Print ISSN: 3006-8878

5. De Haes, S., & Van Grembergen, W. (2022). *Enterprise governance of information technology* (4th ed.). Springer.
6. DeVellis, R. F. (2017). *Scale development: Theory and applications* (4th ed.). Sage.
7. Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research Quarterly*, 23(3), 215-229.
8. Goode, S., Lin, H., & Tsai, M. (2022). Measuring threat detection efficacy. *Information Systems Journal*, 32(4), 789-815.
9. Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on PLS-SEM* (3rd ed.). Sage.
10. Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis* (3rd ed.). Guilford.
11. Hollnagel, E. (2021). *Safety-II in practice*. Routledge.
12. Johnston, A., Hooper, V., & Smith, R. (2023). The impact of response agility on cyber breach containment costs. *Journal of Cybersecurity*, 9(1), tyad005.
13. Mikalef, P., Fjørtoft, S. O., & Torvatn, H. Y. (2022). Artificial intelligence capabilities and firm performance. *Information & Management*, 59(5), 103680.
14. Naseer, H., Desouza, K., Maynard, S. B., & Ahmad, A. (2023). Enabling cybersecurity incident response agility through dynamic capabilities. *European Journal of Information Systems*, 33(2), 200-220.
15. NIST. (2023). *Cybersecurity framework (CSF) 2.0*. National Institute of Standards and Technology.
16. Sarker, I. H., Khan, A. I., & Abushark, Y. B. (2024). AI governance in cybersecurity: A systematic literature review. *ACM Computing Surveys*, 56(5), 1-38.
17. Teece, D. J. (2007). Explicating dynamic capabilities. *Strategic Management Journal*, 28(13), 1319-1350.