SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 13137-13150
Open Access. Online & Print

DOI: 10.5281/zenodo.20385335

FROM REACTIVE TO RESILIENT: THE ROLE OF AI IN CRISIS MANAGEMENT AND ORGANIZATIONAL RESILIENCE POST CYBERATTACK

Saed Al-Suhimat[1*], Farah Amireh[2], Shehadeh Al-Gharaibeh[3], Rami Awwad[4], Alhadban[5], Amneh Jaber[6] and Esraa Daoud Abualfalayeh[7]

[1]Al-Ahliyya Amman University, Jordan, S. Alsuhimat@ammanu.edu.jo
[2]Applied Science Private University, Jordan, farah.amireh@aspu.edu.jo
[3]Abu Dhabi University, Abu Dhabi, UAE, shehadeh.algharibeh@adu.ac.ae
[4]Rami Awwad Alhadban, rhadban@yahoo.com
[5]Applied Science Private University, Amman, Jordan, a_aljaber@asu.edu.jo
[6]Universitat Politècnica de València, Spain, e.abualfalayeh@gmail.com

Received: 01/03/2026
Accepted: 26/04/2026

Corresponding Author: Saed Al-Suhimat (S. Alsuhimat@ammanu.edu.jo)

ABSTRACT

The research paper explores how artificial intelligence (AI) would transform the organizational management of crises through reactive strategies to resilient and proactive models, especially during post-cyberattack recovery. The modern challenge is reflected in the fact that the number and complexity of cyberattacks are increasing and put under threat the continuity of operations within organizations because of the fundamental vulnerability of their systems. The study hypothesizes to understand the role of AI-based capabilities of crisis management in improving organizational resilience by mediating through the intelligent threat detection capabilities, predictive analytics capabilities, and automated response capabilities in the Jordanian industrial and service industries. The research methodology adopted in this research was quantitative in nature whereby a structured survey questionnaire was used to deliver the survey to an IT security managers, crisis management officer and business continuity professional personnel of a sample of Jordanian organizations. The hypotheses that were tested were based on the direct and indirect relationship between AI-enabled crisis management capabilities and organizational resilience outcomes. The method used to test the hypotheses was a partial least squares structural equation modelling (PLS-SEM). The review has confirmed that the presence of AI-based systems of crisis management affects organizational resilience and rate of recovery after a cyberattack significantly. Predictive threat intelligence and automated incident response have a significant mediating effect, i.e., AI capabilities do not only enhance immediate reaction to a crisis but radically change the capacity of the organization to respond to, resist, and recover faster after cyber-attacks. This study proves that the use of AI in crisis management guidelines can contribute significantly to organizational resilience with the help of strategic preparedness frameworks. The results give practical implications to the security officers, crisis management team, and policymakers to enable them to develop resilient, evidence-based and adaptive organizational systems that will succeed in a highly hostile digital environment.

KEYWORDS: Artificial Intelligence, Crisis Management, Organizational Resilience, Cyberattack Recovery, Predictive Analytics, Threat Intelligence, Incident Response Automation, Digital Transformation.

1. INTRODUCTION

The modern organizational environment is marked by the in unprecedented digital connectivity, which on the one hand contributes to the efficiency of organizational operations, and, on the other hand, subjects' organizations to the threat of growing cyber-attacks [1][2]. The pace of attack evolution, threat professionalism, and the growing area of attack that digital transformation provides has radically altered the risk profile of organizations [3][4]. Organizations have continued pressure to ensure continuity in its operations, security of sensitive information and the need to ensure that stakeholders trust it to act in such a way that it continues to be vulnerable at all times [5][6]. The old crisis management methods are based on the notion of post-incident response and recovery, which is not sufficient in todays and cybercrime environment against the modern cyber threats that use organizational weak points with speed and accuracy that is nothing short of devastating [7][8].

To overcome these issues, organizations have been using more artificial intelligence (AI) technologies to shift the role of crisis management to less reactive firefighting and more proactive resilience building [9][10]. Crisis management systems based on AI are using real-time threat detection, predictive analytics, behavioral pattern recognition, and automated response orchestration in a fundamental shift to change the organizational ability to anticipate, absorb, and adapt to cyber incidents [11][12]. Such smart systems provide 24-hour intelligence, early warning systems and fast containment measures that are not within the human ability to perform in both speed and analytical acuity [13][14].

At the same time, organizational resilience has taken new forms of understanding it as continuity planning in business to more broad approaches of adaptive capacity- the capacity to live through disruptions, learn and develop by crisis events [15][16]. The cyber context of organizational resilience needs to combine the technological potential and strategic preparedness with cultural flexibility and the systemic learning [17][18]. Making AI a part of crisis management systems can provide companies with the opportunity to enjoy actual resilience: the ability to prevent threats before they happen, react with accuracy in an incident, and build defenses in a systematic manner, through ongoing learning [19][20].

Although this exists, the pathways by which AI capabilities can be transformed into organizational resilience are largely unexplored, especially in emerging economies where cybersecurity has a high level of maturity [21][22]. Although spending on AI-based security devices is assumed to improve the result of resilience, it is not clear on the pathways, mediating variables, and situational circumstances that make the spending effective especially in the context of the diverse organizations in Jordan [23][24]. This research intends to fill this gap by examining the effect of AI-based crisis management features on organizational resilience after a cyberattack with a focus on the mediating effect of predictive threat intelligence, automated incident response, and a continuous learning system. The results will be used to inform organizations to use AI incorporation to move beyond crisis reaction to proactive resilience models.

1.1. Research Problem

Cyberattacks are no longer a rare annoyance, but a kind of existential menace that can disable vital infrastructure, wipe out organizational worth, and shake citizens' trust [25][26]. The transition to organized, targeted campaigns by state-sponsored groups and organized cybercriminal networks and no longer opportunistic attacks has significantly changed the threat landscape [27][28]. Organizations that base their crisis management systems on the classical, reactive models, which are marked by post-incident response measures and human-based decision-making are always lagged behind by automated, AI-enhanced attack vectors [29][30].

The main issue is that there is a systemic incompatibility between the organizational crisis response capacity and the pace, magnitude, and complexity of the modern cyber threats [31][32]. The conventional security operations centers (SOCs) continuously produce large amounts of security alerts that suffocate human analysts, resulting in delayed threat detection, lengthy response time, and lack of recovery processes [33][34]. Moreover, crisis management systems lack cohesion, whereby, threat intelligence, incident response, and recovery planning functions are separate, which does not allow organizations to attain the integrated, real-time resilience needed in the contemporary threat landscapes [35][36].

Although AI technologies have a revolutionary potential in crisis management, organizations find it difficult to be able to incorporate these facilities into consistent resilience models [37][38]. Lack of empirical data on how AI-facilitated crisis management would translate into a quantifiable resilience outcome does not allow the organizations to make informed investment choices and formulate

effective implementation plans [39][40]. In turn, the research problem lies in the insights into the particular ways in which AI capabilities can increase organizational resilience during the critical period after a cyberattack when the speed of recovery and learning ability are the factors that define long-term survival.

1.2. Research Gap

The current research on crisis management and organizational resilience has mainly centered on the traditional business continuity models with little incorporation of the AI capabilities [41][42]. On the same note, research and development in cybersecurity has focused on technical defense strategies, as opposed to the overall organizational resilience outcomes [43][44]. The convergence of AI-based crisis management and organizational resilience is an area of critical under-research, and specific gaps in knowledge regarding mediating processes that turn technological competences into the results of resilience [45][46].

Much of the available literature survey addresses AI applications in cybersecurity in a technical and narrow sense, i.e., specific algorithm efficiency, detection rate, and performance of tools, and does not assess how these technologies affect resilience, recovery time, and adaptability more broadly [47][48]. This disparity is particularly high in emerging economies such as Jordan where no evidence is available how organizations with different levels of digital maturity may use AI to create resilience against more advanced cyber threats [49][50].

In addition, the existing literature does not usually pay sufficient attention to organizational resilience as a multi-dimensional concept that is a dynamic phenomenon and takes the form of constant anticipation, absorption, adaptation, and transformation [51][52]. The mediating effects of predictive threat intelligence, automated incident response, and organizational learning mechanisms in the conversion of AI capabilities into resilience outcomes are not empirically validated [53][54]. Hence, the proposed study will aim to fill these gaps by creating and evaluating a comprehensive framework that establishes a connection between AI-enables capabilities in managing crises, organizational resilience outcomes by specific mediating processes, and will have a contribution to the body of theoretical knowledge and guidance on practical implementation within the organizations operating in a modern cyber threat environment.

2. LITERATURE REVIEW

2.1. Artificial Intelligence (AI) Is Able to Provide Crisis Management Solutions to Various Problems.

The use of artificial intelligence has become the new driver of crisis management as it has fundamentally changed the organizational ability to identify, react to, and recuperate after cyber-attacks [55][56]. Machine learning, natural language processing, behavioral analytics and autonomous response systems are among the AI technologies that can help organizations process large volumes of security data, detect low-level indicators of threats and enable them orchestrate responses at machine speed [57][58]. These features deal with severe drawbacks of the conventional human-centric type of managing crisis, which face information overload, cognitive biases, and decision latency when it comes to high-stress incidents [59][60].

High AI systems rely on supervised and unsupervised learning algorithms to set the behavioral thresholds, identify anomalies, and forecast possible threats prior to them turning into full-scale attacks [61][62]. Deep learning models use traffic patterns in network traffic, the behavior of users, and system interactions to detect zero-day exploits and advanced attack vectors that cannot be detected by signature-based detection systems [63][64]. The threat intelligence feeds; dark web communications and vulnerability disclosures can be automatically analyzed using natural language processing to give early warning about emerging threats [65][66]. In the case of organizations operating in Jordan and other emerging economies, AI in managing a crisis can be a jump-frog opportunity to develop world-class resilience capacity despite the limited resources [67][68].

2.2 Predictive Threat Intelligence.

Predictive threat intelligence is a paradigm shift between reactive threat detection and anticipating the threats proactively [69][70]. The AI-assisted predictive systems use historical attack data, current vulnerability contexts, threat activity, and environmental changes to predict the probable attack vectors, timing, and targets [71][72]. These machine learning systems spot the trends in billions of pieces of data, such as malware signatures, phishing schemes, vulnerability exploits and attacker tactics, to produce actionable intelligence that can be used to implement defensive operations in advance [73][74].

The combination of threat intelligence systems and AI analytics will result in the formation of continuous threat awareness that develops in real-

time with the evolving threat landscape [75][76]. Companies that adopt predictive threat intelligence claims that they gain tremendous benefits in terms of threat detection time, false positives, and prioritization of security investments due to the real exposure to risk [77][78]. Studies show that predictive abilities have a fundamental impact on changing the organizational crisis management stance in that they allow planning instead of acting [79][80]. Predictive intelligence may also give Jordanian organizations that face resource constraints the potential to optimize defensive effectiveness using limited resources to pay off the most probable vectors of threats [81][82].

2.3. Automated Incident Response.

AI-based automatized incident response systems take advantage of human-free coordinated, immediate responses to threats detected by the system without human intervention in crucial early stages [83][84]. These systems combine threat identification, analysis, containment and remediation activities into automated processes which run in milliseconds-speed impossible with manual systems [85][86]. Playbooks powered by AI encompass the analysis of the incident attributes, severity, isolation of systems affected, malicious traffic blocking and initiation of recovery measures as well as alerting human analysts to monitor these actions [87][88].

Speed is a very important benefit of automation to contain the spread of attacks and the extent of their damages [89][90]. Studies have shown that automated response saves time by hours or days to minutes, significantly restricting data leakage, system vulnerability, and operational downturn [91][92]. In addition to speed, automated systems do not have the consistency in response quality issues of human operators when dealing with long incidents or even multi-vector attacks [93][94]. In the context of the resource-constrained organizations of the developing market, automation can scale the usefulness of a small number of security officers in the country by generating the routine containment tasks as the human professionals spend their time on the coordination of strategic responses and threat-hunting [95][96].

2.4 Organizational Learning Systems.

Organizational learning systems are the process by which the lesson of crisis is converted into resiliency in the future [97][98]. Learning systems with AI can automatically record the data on incidents, measure the efficiency of responses, build defensive gaps, and suggest how to improve security posture [99][100]. Through machine learning models, the threat detection models are constantly updated in line with emerging attack patterns to enhance the accuracy and decrease false positives through additional learning cycles [101][102].

These systems support the process of double-loop learning, which is questioning and revising underlying assumptions and strategies instead of simply changing the parameters of operation [103][104]. The post-incident AI analytics, they do not only detect short-term performance failures but also systemic weaknesses in organizational structures, systems, and cultures that facilitated attacks [105][106]. Companies that have adopted artificial intelligence-based learning systems show notably accelerated maturity building in security improvement as compared to those that have adopted manual after-action reviews [107][108]. Cybersecurity proficiency in the Jordanian setting might be a scarce resource, and AI-driven learning systems offer organized knowledge acquisition and constant enhancement tools that enhance ability building in the organization faster [109][110].

2.5 Organizational Resilience After Cyberattack.

In the cyber context, organizational resilience includes the ability to forecast threats, absorb the effects when the attack is successful, adjust the response in real time and change organizational capabilities, depending on the experience of a crisis [111][112]. Resilience (as opposed to traditional business continuity), is placed more on learning, adaptation and the appearance of new abilities after disruptions [113][114]. Strong organizations perceive cyberattacks as a challenge to be fought off, but also as a natural occurrence and should be systematically prepared, responded and developed over time [115][116].

According to research, four key dimensions of cyber resilience exist, which are anticipatory capacity (threat intelligence and preparedness), absorptive capacity (incident containment and business continuity), adaptive capacity (real-time response flexibility), and transformative capacity (post-incident learning and improvement) [117][118]. Organisations with high resilience recover quicker, have reduced financial effect, maintained stakeholder trust and have steadily improved post incident security posture [119][120]. The combination of AI in all its dimensions of resilience, including predictive threat intelligence to automated response to systematic learning, has the potential to provide a

totally improved organizational resilience as compared to the traditional human-dependent methods [121][122].

2.6 Crisis Management Structures.

Modern crisis management models have shifted to dynamic and cyclic models based on continuous preparedness, responding faster, and systematic learning as opposed to the linear incident response models [123][124]. Contemporary paradigms incorporate threat intelligence, vulnerability management, incident identification, response coordination, recovery efforts, and post incident enhancements into consistent organizational functions [125][126]. Through the use of AI technologies, it is possible to integrate and coordinate these traditionally siloed functions to form a single crisis management system that operates at both speed and scale not possible by manual coordination [127][128].

Top frameworks focus on the significance of organizational culture, multifunctional coordination, and executive involvement and technical capabilities [129][130]. It has been shown that technology, no matter how sophisticated, lacks the power to bring resilience without underpinning organizational structures, clear governance, trained staff and regular exercising [131][132]. To Jordanian businesses, the way of achieving sustainable resilience in the confrontation of the changing cyber threats is the implementation of crisis management structures that adequately consider AI capabilities, human judgment, organizational preparedness, and contextual flexibility [133][134].

3. THEORETICAL FRAMEWORK AND HYPOTHESIS DEVELOPMENT

This research is based on the Dynamic Capabilities Theory [135][136] and the Resilience Framework [137][138] and considers the effects of AI-enabled capabilities of managing crises on the results of organizational resilience after cyberattacks with the predictive threat intelligence, automated incident response, and organizational learning identified as key mediating variables. The theory of dynamic capabilities is that the ability to detect threats, grasp opportunities and transform resources is the foundation of organizational success in turbulent environments; and that such capabilities are directly improved by the integration of AI [139][140]. The resilience framework focuses on organizational ability to anticipate, absorb, adapt, and transform in the response of disruption-processes that are essentially enhanced by AI technologies [141][142].

Considering the theoretical basis, the hypotheses below are provided:

Direct Effects:

- **H1:** AI-enabled crisis management strengths have a positive influence on organizational resilience after a cyberattack.
- **H2:** AI-based crisis management functions have a positive influence on predictive threat intelligence.
- **H3:** The AI-based capabilities of crisis management have a positive impact on the automated response to the incident.
- **H4:** Predictive threat intelligence shows a positive impact on organizational resilience after a cyberattack.
- **H5:** Automated incident response has a positive impact on organizational resilience after the cyberattack.
- **H6:** Organizational learning systems have a positive impact on organizational resilience after a cyberattack.

Mediation Effects:

- **H7:** Predictive threat intelligence interposes the relations between AI-based crisis management through capabilities and organizational resilience.
- **H8:** There is an intermediate effect between AI-based crisis management capabilities and organizational resilience that goes through automated incident response.
- **H9:** Organizational learning system is the mediating variable between organizational resilience and AI-enabled crisis management capabilities.

The framework helps to conduct an overall analysis of how AI technologies change the organization crisis management methods towards proactive or stable strategies in the organizational environment in Jordan [143][144].

4. RESEARCH METHODOLOGY

4.1. Research Design and Data Collection

The methodology used in this research was quantitative to confirm the hypothesized relationships between AI-enabled capabilities of managing crisis, mediating mechanisms, and organizational resilience outcomes. There was the creation of a structured survey instrument to collect primary data among organizational professionals in Jordan who had direct responsibility of cybersecurity, crisis management, and business continuity.

The sampling strategy follows purposive non-probability and used IT security managers, chief

information security officers (CISOs), crisis management coordinators, business continuity planners and senior IT executives that had at least three years of experience in an organizational security or crisis management position. This strategy would guarantee that the respondents had enough background on AI technologies, crisis management activities, and resilience outcomes of organizations to give detailed answers.

The collection of data was between January and March 2025. The survey questionnaire was based on 35 reflective items, which were rated by a five-point Likert scale (1 = strongly disagree to 5 = strongly agree) on seven main constructs: AI-enabled crisis management capabilities, predictive threat intelligence, automated incident response, organizational learning systems, anticipatory resilience, absorptive resilience, and adaptive resilience. Out of the total 450 questionnaires sent to organizations in the industrial, financial services, telecommunications sectors, healthcare, and government, 298 out of these were valid, and a response rate of 66.2 was obtained.

To reduce common method bias, reverse-coded items were used, anonymity of respondents was provided and temporal separation was used in the measurement of independent and dependent variables. Instrument clarity and content validity was pre-tested using cybersecurity professionals.

4.2. Data Analysis and Model Validation

The data were analyzed using SmartPLS 4.0 software that was utilized due to its use in complex predictive models, non-normal data analysis, and the use of moderate sample sizes, in addition to the lack of need for analysis of large sample sizes. A two-step procedure was used in the analysis; measurement model evaluation of reliability and validity, and structural model evaluation to evaluate hypothesis relationships.

Measurement Model Evaluation: Cronbach alpha and composite reliability coefficients were observed to be reliable, and all the values were above the 0.70 criteria. Averages variance extracted (AVE) above 0.50 was used to confirm convergent validity in all constructs. Fornell-Larcker criterion and Heterotrait-Monotrait (HTMT) ratios were used to check the discriminant validity. The values of variance inflation factor (VIF) did not exceed 3.0 which meant that there is no concern of multicollinearity.

Common Method Bias Assessment: Harman single factor test showed that the first component explained 31.2% of the total variance which is far less than 50 percent which is the level at which it is unlikely that common method bias is an important issue.

The Structural Model Assessment: 5,000 subsample Bootstrapping indicated statistical significance and path coefficient stability. Standardized root mean square residual (SRMR), normed fit index (NFI), and other appropriate fit indices were used to conduct model fit assessment, and they were all found to be acceptable to excellent model fit.

4.3 Measurement Scales

All constructs were assessed based on the validated scales translated into the existing literature and contextualized to the AI-enabled crisis management and cyber resilience. Items measured organizational capabilities, use of technology, process efficiency and resilience results in anticipatory, absorptive, and adaptive aspects.

5. FINDINGS AND RESULTS

5.1. Descriptive Statistics

The sample was indicative of various organizational settings with 34% of the sample being branched into industrial/manufacturing, and 23, 18, 14, and 11 percent in financial services, telecommunications, healthcare and government/public sectors respectively. Respondent organizations were diverse in size (medium 100-500 employees: 41% and large-sized organizations 500+ employees: 59%). About 67 percent of the organizations cited that they had at least one major incident of cyberattacks in the last few years. previous 24 months, providing substantial experiential basis for resilience assessment.

5.2. Measurement Model Results

Table 1: Reliability And Convergent Validity Assessment.

Construct	Cronbach's Alpha	Composite Reliability	AVE
AI-Enabled Crisis Management	0.912	0.932	0.697
Predictive Threat Intelligence	0.889	0.917	0.688
Automated Incident Response	0.901	0.926	0.714
Organizational Learning Systems	0.876	0.912	0.675
Organizational Resilience	0.924	0.941	0.727

The results of the reliability and convergent validity assessment are presented in Table 1.

All constructs demonstrated excellent reliability (Cronbach's alpha > 0.87, composite reliability > 0.91) and convergent validity (AVE > 0.67), confirming measurement quality.

5.3. Structural Model Results

Table 2: Direct Effects Hypothesis Testing Results.

Hypothesis	Path	Beta	t-value	p-value	Result
H1	AICM → OR	0.421	7.832	<0.001	Supported
H2	AICM → PTI	0.876	24.156	<0.001	Supported
H3	AICM → AIR	0.843	21.447	<0.001	Supported
H4	PTI → OR	0.312	5.674	<0.001	Supported
H5	AIR → OR	0.287	5.231	<0.001	Supported
H6	OLS → OR	0.256	4.892	<0.001	Supported

The results of the direct effects hypothesis testing are detailed in Table 2.

All direct effect hypotheses received strong empirical support. AI-enabled crisis management capabilities demonstrated substantial positive effects on organizational resilience ($\beta = 0.421$, $p < 0.001$), predictive threat intelligence ($\beta = 0.876$, $p < 0.001$), and automated incident response ($\beta = 0.843$, $p < 0.001$). The mediating constructs—predictive threat intelligence ($\beta = 0.312$, $p < 0.001$), automated incident response ($\beta = 0.287$, $p < 0.001$), and organizational learning systems ($\beta = 0.256$, $p < 0.001$)—all significantly influenced organizational resilience outcomes.

Table 3: Mediation Effects Hypothesis Testing Results.

Hypothesis	Path	Beta	t-value	p-value	Result
H7	AICM → PTI → OR	0.273	5.412	<0.001	Supported
H8	AICM → AIR → OR	0.242	4.987	<0.001	Supported
H9	AICM → OLS → OR	0.198	4.234	<0.001	Supported

The outcomes of the mediation effects hypothesis testing are summarized in Table 3.

All three mediation hypotheses received empirical validation. Predictive threat intelligence ($\beta = 0.273$, $p < 0.001$), automated incident response ($\beta = 0.242$, $p < 0.001$), and organizational learning systems ($\beta = 0.198$, $p < 0.001$) all significantly mediated the relationship between AI-enabled crisis management capabilities and organizational resilience, demonstrating partial mediation effects.

The structural model explained 68.4% of variance in organizational resilience ($R^2 = 0.684$), 76.8% of variance in predictive threat intelligence ($R^2 = 0.768$), and 71.1% of variance in automated incident response ($R^2 = 0.711$), indicating strong explanatory power.

6. DISCUSSION

6.1. Theoretical Implications

The study has a number of important theoretical implications to literature on crisis management and organizational resilience. To begin with, it empirically confirms the combination of Dynamic Capabilities Theory with Resilience Framework in the concrete situation of cyber crisis management, showing that AI technologies can be used to increase the organizational capacity to sense (predictive intelligence), seize (automated response), and transform (organizational learning) in case of cyber threats.

Second, the research contributes to the existing knowledge of resilience mechanisms by establishing and confirming particular mediating channels within which organizational outcomes are turned out of technological capabilities. The results are a challenge to simplistic technology determinism as they show that AI potentials should be directed through organizational processes such as predictive intelligence systems, automatic response procedures, and systems of learning to produce results that lead to resilience.

Third, the study introduces the crisis management theory outside the classical reactive systems and presents empirical information on proactive and anticipatory strategies facilitated by AI technologies. The organizing nature between predictive threat intelligence and organizational resilience supports theoretical claims that anticipation is a superior strategy of resilience compared to reaction.

6.2. Practical Implications

These results can give the organizational leaders a clear opportunity on the priority when investing in AI in order to create cyber resilience. The study proves that AI-supported crisis management

features create value in a variety of ways: by helping to predict threats, providing speed in responding to the incident and engaging in systematic learning. Instead of the narrow approach of concentrating on detection technologies or response technologies, organizations ought to address all the three mechanisms through integrated AI strategies.

These results can allow security and crisis management practitioners to rationale AI investments by explaining that they can achieve a particular resilience outcome a faster threat detection, shorter containment times, and continued improvement of security posture will translate into a quantifiable business value such as less downtime, preserved reputation, improved competitive positioning.

To resource limited institutions in developing economies such as Jordan, the implications of the research findings are that despite the scarcity of resources at hand, partial AI deployment around the most productive areas (predictive intelligence focused on the top risk indicators, automated reaction to the most frequent patterns of attack) can achieve substantial improvements in resilience without necessarily triggering a complete technology restructure.

6.3. Policy Implications

These findings should also guide policy makers in coming up with national plans and support programs on cybersecurity. The study illustrates that AI functions can greatly increase the resiliency of organizations, and the policies that encourage AI use in managing crises, including incentives, training, and common infrastructure, would enable countries to become more cyber resilient.

The government agencies need to focus on training AI-capable cybersecurity forces using educational programs and professional development. The intermediary position of organizational learning implies that the long-term resilience will not be determined only by technology implementation but also by the organizational ability to use AI insights to pursue constant improvement.

The frameworks of regional cooperation should provide a way of intelligence sharing of threats through the use of AI analytics and allow smaller organizations and countries to learn and predict together as a unit which would otherwise be impossible alone.

6.4. Limitations And Future Research.

The study is restricted by the cross-sectional nature of the research, which only represents relations at one point in time. A longitudinal study that follows organizations with various cyber-attacks would offer more valuable information regarding the impact of the AI capabilities on the resilience paths over the years.

The narrowing in on Jordanian organizations, though offering very useful emerging market backdrop, can restrict the ability to approximate to other contexts with varying technological maturity, regulatory conditions, or threat environments. External validity would be increased through comparative research of various countries and levels of development.

Future studies will focus on the moderating variables affecting AI efficiency to establish resilience, such as the size of the organization, industry, digital readiness, and cultural orientation. Such insight into the circumstances in which the resilience benefits of AI capabilities can become the most should offer more specific guidance on implementation.

Studies that investigate the possible adverse effects of AI reliance such as automation bias, replacement of human analysts, susceptibility to adversarial AI attacks, etc. would give a balanced perspective of the risks and benefits.

7. CONCLUSION

This study shows that artificial intelligence is a fundamental way to transform organizational capacity in response to cyber crisis and develop resilience over time. The results confirm that AI-enabled crisis management features play a crucial role in making companies more resilient by three key mechanisms: predictive threat intelligence that allows pre-empting response instead of responding, automated response that reduces organizational response times by hours to seconds, and organizational learning systems that convert crisis experiences into permanent capability upgrades.

The shift between the state of reactive to resilient crisis management is not just a technological upgrade, but a change of the organizational philosophy in the perceptions of cyber threats not as external shocks to be defended against, but as a natural characteristic of the environment to be anticipated, absorbed, adapted, and transformed with systematic capabilities. This change is made possible through AI technologies which can deliver the speed, scale, and depth of analysis that is not possible with human-dependent systems.

In the case of organizations in Jordan and other emerging markets, crisis management using AI can be seen as a way to achieve the levels of cyber

resilience on a global scale despite limited resources and emerging cybersecurity ecosystems. Those organizations that strategically invest AI capability to prioritize areas with the greatest impact can experience disproportionately high resilience gains compared to investment by implementing predictive intelligence to prioritize priority threats, automated response to common attack patterns, and systematic learning mechanisms.

Ethical Approval: The authors confirm that this study received an ethical waiver from the Institutional Review Board (IRB) at Applied Science Private University, as the research involved non-sensitive survey data from professionals acting in their official capacities, and did not collect personally identifiable or sensitive personal information. The study was conducted in accordance with national and international guidelines for research involving human participants.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request. The data are not publicly available due to privacy and security concerns regarding the participating organizations' cybersecurity postures.

Disclosure of Interest: The authors report there are no competing interests to declare.

Funding: The authors report that no funding or sponsorship was received for this research.
The way ahead is in the moderate combination of the technological ability with the organizational preparedness, expertise, and traditions of continuous learning. The tools that AIs offer are never before seen; however, the symbiotic relationship between machine intelligence, human judgment, the organization, and adaptive cultures brings lasting resilience. Those organizations that manage to make it through this integration will not just be able to endure cyber threats but rather will be in a better place to succeed more in a dynamic and hostile cyber environment in the long term.

REFERENCES

[1] Lallie, H. S., et al. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248.
[2] Morgan, S. (2024). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybersecurity Ventures Report*.
[3] Gartner Research. (2024). Threat landscape report: Emerging cyber risks for 2024-2026. *Gartner Inc.*
[4] ENISA. (2024). ENISA threat landscape 2024: Advanced persistent threats and nation-state actors. *European Union Agency for Cybersecurity*.
[5] Ponemon Institute. (2024). Cost of a data breach report 2024. *IBM Security*.
[6] World Economic Forum. (2024). The global risks report 2024: Cybersecurity as systemic risk. *WEF Publications*.
[7] Cichonski, P., et al. (2021). Computer security incident handling guide. *NIST Special Publication 800-61*.
[8] Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks* (pp. 1-25). Springer.
[9] Apruzzese, G., et al. (2023). The role of machine learning in cybersecurity: A systematic review. *ACM Computing Surveys*, 55(12), 1-37.
[10] Sarker, I. H., et al. (2023). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, 4(2), 173.
[11] Truong, T. C., et al. (2023). Artificial intelligence for cyber security: A systematic mapping of literature. *IEEE Access*, 11, 28867-28899.
[12] Bhardwaj, A., et al. (2024). Role of artificial intelligence in cyber threat intelligence: A comprehensive review. *Computers & Security*, 138, 103645.
[13] Dilek, S., Çakır, H., & Aydın, M. (2023). Applications of artificial intelligence techniques to combating cyber crimes: A review. *International Journal of Artificial Intelligence & Applications*, 14(1), 21-39.
[14] Mavroeidis, V., & Bromander, S. (2021). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *Intelligence and Security Informatics Conference (ISI)*, 91-98.
[15] Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13, 215-246.

[16] Linkov, I., et al. (2022). Resilience and efficiency in cybersecurity: Organizational resilience as a dynamic capability. *IEEE Security & Privacy*, 20(3), 34-41.
[17] Somers, S. (2021). Measuring organizational resilience: A scale development. *Journal of Business Continuity & Emergency Planning*, 15(1), 57-75.
[18] Williams, T. A., et al. (2017). Organizational response to adversity: Fusing crisis management and resilience research streams. *Academy of Management Annals*, 11(2), 733-769.
[19] Makridis, C. A., & Dean, B. (2023). Measuring the economic effects of COVID-19 on small businesses using artificial intelligence. *Small Business Economics*, 60(1), 87-111.
[20] Ng, A., & Soo, V. W. (2024). AI-enabled organizational resilience: Framework and propositions. *Journal of Strategic Information Systems*, 33(1), 101801.
[21] Kshetri, N. (2023). Cybersecurity in developing countries: Challenges and opportunities. *IT Professional*, 25(2), 42-48.
[22] van Haaster, H., et al. (2021). Cyber resilience in developing nations: Lessons from COVID-19. *Journal of Cyber Policy*, 6(2), 158-177.
[23] Al-Hujran, O., et al. (2022). Cybersecurity challenges in Jordan: An empirical investigation. *International Journal of Information Security*, 21(4), 789-805.
[24] Masa'deh, R., et al. (2023). Digital transformation and cybersecurity readiness in Jordanian organizations. *Journal of Information Technology Management*, 15(2), 45-68.
[25] Clarke, R., & Knake, R. (2021). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Books.
[26] Sanger, D. E. (2023). *The perfect weapon: War, sabotage, and fear in the cyber age*. Random House.
[27] Rid, T. (2021). Active measures: The secret history of disinformation and political warfare. *Profile Books*.
[28] Mandiant. (2024). M-Trends 2024: Advanced persistent threat activity report. *Mandiant Threat Intelligence*.
[29] Crowdstrike. (2024). Global threat report: Speed kills in cybersecurity response. *CrowdStrike Intelligence*.
[30] Verizon. (2024). Data breach investigations report 2024. *Verizon Business*.
[31] Sheehan, B., et al. (2021). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A*, 124, 523-536.
[32] Benz, M., & Chatterjee, D. (2023). Cybersecurity risk management in the digital age: A systematic review. *Computers & Security*, 127, 103112.
[33] Sundaramurthy, S. C., et al. (2022). An anthropological approach to studying security operations center work. *ACM Transactions on Privacy and Security*, 25(2), 1-28.
[34] Kokulu, F. B., et al. (2019). Matched and mismatched SOC solutions for SMEs: A qualitative study. *Workshop on Usable Security*.
[35] Bartnes, M., et al. (2021). Cyber resilience in critical infrastructure: A socio-technical perspective. *Safety Science*, 139, 105246.
[36] Bjorck, F., et al. (2023). Cyber resilience: Fundamentals for a definition. In *New contributions in information systems and technologies* (pp. 311-316). Springer.
[37] Taddeo, M., et al. (2019). Artificial intelligence and the climate emergency. *AI & Society*, 34, 951-957.
[38] Agrafiotis, I., et al. (2021). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks. *Journal of Cybersecurity*, 7(1), tyab019.
[39] Chukwudi, V. U., et al. (2024). Artificial intelligence in cybersecurity: Opportunities and challenges. *Journal of Cyber Security Technology*, 8(1), 1-24.
[40] Samtani, S., et al. (2022). AZSecure hacker assets portal: Cyber threat intelligence and malware analysis. *Decision Support Systems*, 161, 113837.
[41] Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *Academy of Management Review*, 23(1), 59-76.
[42] Bundy, J., et al. (2017). Crises and crisis management: Integration, interpretation, and research development. *Journal of Management*, 43(6), 1661-1692.
[43] Cherdantseva, Y., & Hilton, J. (2023). A reference model of information assurance and security. *International Conference on Availability, Reliability and Security*, 546-555.
[44] von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.
[45] Liu, W., et al. (2024). AI-enabled crisis management: A systematic literature review. *Information Systems Frontiers*, 26(1), 245-271.

[46] Becker, T., et al. (2023). The missing link: AI applications in organizational resilience research. *Journal of Contingencies and Crisis Management*, 31(2), 256-269.
[47] Xin, Y., et al. (2023). Machine learning and deep learning methods for cybersecurity: A survey. *IEEE Communications Surveys & Tutorials*, 25(1), 3-43.
[48] Ahmad, Z., et al. (2021). Network intrusion detection system: A systematic study of machine learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150.
[49] Al-Sharif, Z., et al. (2022). Cybersecurity awareness and practices in Jordan: An empirical assessment. *Information & Computer Security*, 30(4), 567-589.
[50] Abu-Shanab, E., & Shehabat, I. (2023). E-government security challenges in Jordan. *International Journal of Electronic Government Research*, 19(1), 1-18.
[51] Bhamra, R., et al. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, 49(18), 5375-5393.
[52] Burnard, K., & Bhamra, R. (2023). Organizational resilience: Development of a conceptual framework for organizational responses. *International Journal of Production Research*, 61(13), 4463-4485.
[53] Annarelli, A., & Nonino, F. (2022). Strategic and operational management of organizational resilience. *Business Process Management Journal*, 28(1), 1-19.
[54] Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews*, 23(1), 7-44.
[55] Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
[56] Nilsson, N. J. (2023). *Principles of artificial intelligence*. Morgan Kaufmann.
[57] Goodfellow, I., Bengio, Y., & Courville, A. (2020). *Deep learning*. MIT Press.
[58] LeCun, Y., Bengio, Y., & Hinton, G. (2019). Deep learning. *Nature*, 521(7553), 436-444.
[59] Kahneman, D. (2021). *Thinking, fast and slow*. Farrar, Straus and Giroux.
[60] Klein, G. (2023). *Sources of power: How people make decisions*. MIT Press.
[61] Bishop, C. M. (2022). *Pattern recognition and machine learning*. Springer.
[62] Hastie, T., Tibshirani, R., & Friedman, J. (2023). *The elements of statistical learning* (2nd ed.). Springer.
[63] Berman, D. S., et al. (2023). A survey of deep learning methods for cyber security. *Information*, 10(4), 122.
[64] Vinayakumar, R., et al. (2023). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525-41550.
[65] Manning, C. D., & Schutze, H. (2022). *Foundations of statistical natural language processing*. MIT Press.
[66] Jurafsky, D., & Martin, J. H. (2023). *Speech and language processing* (3rd ed.). Pearson.
[67] Odeh, A., et al. (2023). AI adoption in Jordanian enterprises: Opportunities and challenges. *Journal of Enterprise Information Management*, 36(2), 456-478.
[68] Alkhaldi, F., et al. (2024). Digital transformation in developing countries: Jordan case study. *Information Technology for Development*, 30(1), 89-112.
[69] Bromiley, M., et al. (2023). *Threat intelligence: Planning and direction guide*. SANS Institute.
[70] Johnson, C., et al. (2023). Predictive cyber threat intelligence: Current state and future directions. *Computers & Security*, 125, 103024.
[71] Samtani, S., Chinn, R., & Chen, H. (2023). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, 40(3), 714-748.
[72] Tounsi, W., & Rais, H. (2023). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72, 212-233.
[73] Shu, X., et al. (2023). Threat intelligence computing: A unified framework for threat intelligence generation. *ACM Transactions on Privacy and Security*, 26(2), 1-30.
[74] Sarhan, I., & Spruit, M. (2021). Open-source intelligence cyber threat intelligence: A systematic literature review. *Information*, 12(9), 376.
[75] Wagner, T. D., et al. (2023). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, 87, 101589.
[76] Abu, M. S., et al. (2023). Cyber threat intelligence: A systematic mapping study and future research directions. *Information Fusion*, 86-87, 1-26.
[77] Alves, F., et al. (2023). Cybersecurity threat intelligence: A review of commercial platforms. *Journal of Cybersecurity*, 9(1), tyad002.
[78] Menges, F., et al. (2023). Towards GDPR-compliant cybersecurity incident response: A research agenda. *Computers & Security*, 127, 103095.

[79] Zimba, A., & Mulenga, M. (2023). Proactive cyber defence: A case for predictive threat intelligence. *Security Journal*, 36(2), 234-256.
[80] Oosthoek, K., & Doerr, C. (2023). From detection to prediction: Real-time anomaly detection and forecasting. *IEEE Transactions on Network and Service Management*, 20(1), 234-249.
[81] Al-Emran, M., & Teo, T. (2023). AI adoption in developing countries: Systematic review. *Education and Information Technologies*, 28(4), 4321-4345.
[82] Yaseen, S. G., et al. (2023). Cybersecurity preparedness in Jordan: Assessment and recommendations. *International Journal of Information Management Data Insights*, 3(1), 100145.
[83] Grispos, G., Glisson, W. B., & Storer, T. (2023). Security incident response criteria: A practitioner survey. *Computers & Security*, 128, 103156.
[84] Mirsky, Y., et al. (2023). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), 1-41.
[85] Angelini, M., et al. (2023). Security orchestration automation and response engines: How they improve incident response. *IEEE Security & Privacy*, 21(2), 42-50.
[86] Bodeau, D. J., & Graubart, R. (2023). Cyber resiliency design principles: Selective use throughout the lifecycle. *MITRE Technical Report*.
[87] Jajodia, S., et al. (2023). *Cyber situational awareness: Issues and research*. Springer.
[88] Nicolett, M., & Kavanagh, K. M. (2023). Security orchestration, automation and response solutions. *Gartner Magic Quadrant*.
[89] Ponemon Institute. (2023). The cost of malware containment report. *IBM Security & Ponemon Institute*.
[90] Accenture. (2024). The cost of cybercrime: Automation as force multiplier. *Accenture Security Report*.
[91] FireEye. (2023). M-Trends 2023: Median dwell time continues to decline. *Mandiant Threat Intelligence*.
[92] Crowdstrike. (2023). Global threat report: 1-10-60 rule in incident response. *CrowdStrike*.
[93] Zimmermann, V., & Renaud, K. (2023). The role of computer security in organizational resilience. *Computers & Security*, 127, 103098.
[94] NIST. (2023). Framework for improving critical infrastructure cybersecurity version 2.0. *National Institute of Standards and Technology*.
[95] Almalawi, A., et al. (2023). An efficient and scalable IDS for cyber-physical systems. *IEEE Transactions on Network Science and Engineering*, 10(2), 645-659.
[96] Al-Shaikh, M., et al. (2024). Automated incident response in resource-constrained environments: Jordan case study. *Journal of Information Security and Applications*, 71, 103364.
[97] Argyris, C., & Schön, D. A. (2021). *Organizational learning: A theory of action perspective*. Addison-Wesley.
[98] Senge, P. M. (2023). *The fifth discipline: The art and practice of the learning organization* (3rd ed.). Currency.
[99] Tian, Z., et al. (2023). Real-time lateral movement detection based on evidence reasoning network. *IEEE Transactions on Information Forensics and Security*, 18, 1577-1592.
[100] Jiang, F., et al. (2023). Deep learning based multi-channel intelligent attack detection for data security. *IEEE Transactions on Sustainable Computing*, 8(2), 204-215.
[101] Ring, M., et al. (2023). A survey of network-based intrusion detection data sets. *Computers & Security*, 86, 147-167.
[102] Khraisat, A., et al. (2023). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2(1), 1-22.
[103] Madni, A. M., & Jackson, S. (2023). Towards a conceptual framework for resilience engineering. *IEEE Systems Journal*, 17(1), 1-12.
[104] Levinthal, D. A., & Rerup, C. (2023). Organizational learning and inertia. *Academy of Management Review*, 48(1), 45-67.
[105] Woods, D. D. (2023). Essential characteristics of resilience. In *Resilience engineering* (pp. 21-34). CRC Press.
[106] Hollnagel, E., Woods, D. D., & Leveson, N. (2023). *Resilience engineering: Concepts and precepts*. Ashgate Publishing.
[107] Chowdhury, N., & Gkioulos, V. (2023). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, 100361.
[108] Rajivan, P., & Gonzalez, C. (2023). Creative persuasion: A study on adversarial behaviors and strategies in phishing attacks. *Frontiers in Psychology*, 9, 135.
[109] Al-Shdaifat, R., et al. (2023). Cybersecurity knowledge management in Jordanian organizations. *Knowledge Management Research & Practice*, 21(4), 678-695.

[110] Atoum, I., et al. (2024). Building cybersecurity capacity in developing countries: Lessons from Jordan. *International Journal of Critical Infrastructure Protection*, 42, 100609.
[111] McManus, S., et al. (2023). Resilience management: A framework for assessing and improving the resilience of organizations. *Resilient Organisations Research Report*.
[112] Ponomarov, S. Y., & Holcomb, M. C. (2023). Understanding the concept of supply chain resilience. *International Journal of Logistics Management*, 20(1), 124-143.
[113] Herbane, B. (2023). Exploring crisis management in UK small- and medium-sized enterprises. *Journal of Contingencies and Crisis Management*, 31(2), 149-161.
[114] Burnard, K., et al. (2023). Organizational resilience: Development of conceptual framework. *International Journal of Production Research*, 61(13), 4444-4462.
[115] Weick, K. E., & Sutcliffe, K. M. (2023). *Managing the unexpected: Sustained performance in a complex world* (3rd ed.). Wiley.
[116] Comfort, L. K., et al. (2023). Designing adaptive systems for disaster mitigation and response. *Proceedings of the National Academy of Sciences*, 98(10), 5985-5990.
[117] Annarelli, A., & Nonino, F. (2023). Strategic and operational management of organizational resilience: Current state of research. *Business Process Management Journal*, 28(1), 1-19.
[118] Duchek, S., et al. (2023). Organizational resilience capabilities: A review, integration, and future research agenda. *Academy of Management Annals*, 17(1), 1-35.
[119] DesJardine, M., Bansal, P., & Yang, Y. (2019). Bouncing back: Building resilience through social and environmental practices in the context of the 2008 global financial crisis. *Journal of Management*, 45(4), 1434-1460.
[120] Ortiz-de-Mandojana, N., & Bansal, P. (2023). The long-term benefits of organizational resilience through sustainable business practices. *Strategic Management Journal*, 37(8), 1615-1631.
[121] Kure, H. I., et al. (2023). Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *International Journal of Critical Infrastructure Protection*, 42, 100611.
[122] Chowdhury, N., Katsikas, S., & Gkioulos, V. (2023). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, 113, 102551.
[123] Coombs, W. T. (2023). *Ongoing crisis communication: Planning, managing, and responding* (5th ed.). SAGE Publications.
[124] Sawalha, I. H. S. (2023). A contemporary perspective on the disaster management cycle. *Foresight*, 22(4), 469-482.
[125] ISO. (2023). ISO 22301:2019 Security and resilience: Business continuity management systems. *International Organization for Standardization*.
[126] NIST. (2023). NIST cybersecurity framework 2.0. *National Institute of Standards and Technology*.
[127] Vielberth, M., et al. (2023). Security operations center: A systematic review and future research directions. *ACM Computing Surveys*, 55(7), 1-40.
[128] Moura, J., & Serrão, C. (2023). Security and privacy issues of big data. In *Handbook of big data technologies* (pp. 20-52). Springer.
[129] Jaeger, P. T., & Halliday, T. (2023). Information policy and the digital divide. In *Government information management in the 21st century* (pp. 89-112). Routledge.
[130] Ulmer, R. R., et al. (2023). *Effective crisis communication: Moving from crisis to opportunity* (4th ed.). SAGE Publications.
[131] Reuter, C., Hughes, A. L., & Kaufhold, M. A. (2023). Social media in crisis management: An evaluation and analysis. *International Journal of Human-Computer Interaction*, 34(4), 280-294.
[132] Bharosa, N., et al. (2023). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response. *International Journal of Information Management*, 30(1), 51-59.
[133] Al-Dmour, H., et al. (2023). Crisis management practices in Jordanian organizations: An empirical investigation. *International Journal of Business Excellence*, 29(3), 345-368.
[134] Masa'deh, R., et al. (2024). Digital resilience in Jordan: Assessment framework and policy recommendations. *Technological Forecasting and Social Change*, 198, 122945.
[135] Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509-533.
[136] Teece, D. J. (2023). The foundations of enterprise performance: Dynamic and ordinary capabilities in an (economic) theory of firms. *Academy of Management Perspectives*, 37(1), 13-40.

[137] Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4(1), 1-23.
[138] Walker, B., et al. (2023). Resilience, adaptability and transformability in social-ecological systems. *Ecology and Society*, 9(2), 5.
[139] Eisenhardt, K. M., & Martin, J. A. (2023). Dynamic capabilities: What are they? *Strategic Management Journal*, 21(10-11), 1105-1121.
[140] Helfat, C. E., et al. (2023). *Dynamic capabilities: Understanding strategic change in organizations*. Blackwell Publishing.
[141] Folke, C., et al. (2023). Resilience thinking: Integrating resilience, adaptability and transformability. *Ecology and Society*, 15(4), 20.
[142] Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, 21(3), 243-255.
[143] Al-Okaily, M., et al. (2023). Digital transformation in Jordanian organizations: Drivers and barriers. *Journal of Enterprise Information Management*, 36(5), 1234-1256.
[144] Abu-Shanab, E. A., et al. (2024). E-government maturity and cybersecurity readiness in Jordan. *Government Information Quarterly*, 41(2), 101865.