The Eastasouth Journal of Information System and Computer Science
Vol. 1, No. 02, December, pp. 194-214

AI-Driven Cyber Threat Intelligence as a Management Information System: Integrating Cybersecurity Governance and IT Project Management for Organizational Resilience

Shuchona Malek Orthi[1], Partha Chakraborty[2], Md Abubokor Siam[3], Ahmed Shan-A-Alahi[4], Abdullah Al Zaiem[5], Syed Nazmul Hasan[6], Jobanpreet Kaur[7], Foysal Mahmud[8], Mohammad Abdul Goffer[9]

[1] College of Business, Westcliff University, Irvine, CA 92614, USA
[2] School of Business, International American University, Los Angeles, CA 90010, USA
[3] College of Business, Westcliff University, Irvine, CA 92614, USA
[4] Department of Information Technology, Washington University of Science and Technology, Virginia, USA
[5] Department of Information Technology, Washington University of Science and Technology, Virginia, USA
[6] College of Technology & Engineering, Westcliff University, Irvine, CA 92614, USA
[7] College of Technology & Engineering, Westcliff University, Irvine, CA 92614, USA
[8] College of Business, Westcliff University, Irvine, CA 92614, USA
[9] School of Business, International American University, Los Angeles, CA 90010, USA

Article Info

Article history:

Received Dec, 2023
Revised Dec, 2023
Accepted Dec, 2023

Keywords:

Artificial Intelligence;
Cyber Threat Intelligence;
Cybersecurity Governance;
Decision Support Systems;
IT Project Management;
Management Information Systems;
Organizational Resilience

ABSTRACT

As organizations quickly become increasingly digital, they are experiencing escalating, complex cyber threats. These challenges make cybersecurity an important area for managers and governance, and not just a technical problem. Even if you are a heavy investor in security tech, it still happens to many companies to suffer from cyber. The reasons are broken information flows, a lack of clear visibility among managers, and misalignment between the security operations and the overall decision-making. This research rethinks Artificial Intelligence (AI) based Cyber Threat Intelligence (CTI) as a Management Information System (MIS). It combines the approach of cybersecurity governance and IT project management to increase the resilience of organizations. Using MIS theory, cybersecurity governance models, and studies of IT project management, the paper derives one cohesive model for translating raw threat data into useful managerial insight. Through a design science methodology, the research chooses a lot of scholarly sources and demonstrates a layered AI-enabled CTI-MIS architecture. This is good architecture for strategic oversight, risk-based governance, and flexible project execution. The paper extends the theory of MIS to Artificial Intelligence (AI) driven cybersecurity intelligence and provides practical knowledge for companies seeking to achieve resilient digital transformation in a time of evolving cyber threats.

Corresponding Author:

Name: Md Abubokor Siam
Institution: College of Business, Westcliff University, Irvine, CA 92614, USA
Email: m.siam.263@westcliff.edu

1. INTRODUCTION

Digital technologies have become an integral part of modern organization and are fundamentally changing the way companies operate, innovate, and compete. Cloud computing, enterprise information systems, mobile platforms and data-driven analytics enhance efficiency and strategic agility and increase organizational attack surface [1], [2]. As firms are becoming more interconnected and dependent on data, cyber threats are increasingly systemic and extend beyond the technical damage to operational disruption as they cause strategic, financial and reputational damage.

High-profile cyber-attacks in the healthcare, finance, manufacturing and public infrastructure sectors indicate that threats are no longer isolated events but enterprise-wide crises that would compromise resilience [3], [4]. Ransomware attacks cripple mission-critical services, supply chain attacks spread risk across borders and data breaches destroy trust for stakeholders and regulatory compliance [5]. These realities reveal the limitations of approaches to security that pursue narrow views on perimeter defense and incident response.

Cyber Threat Intelligence (CTI) has emerged as a vital capability to gain business understanding of adversary behavior to inform defense. CTI gathers and evaluates information for attacker tactics, techniques, procedures, indicators of compromise and contextual risk data [6]. In theory, CTI helps support proactive security; that is, allowing organizations to anticipate threats rather than react only. In practice, however, it is still restricted to mostly technical teams and Security Operations Centers, which restricts its strategic value [7].

At the same time, the developments in artificial intelligence (AI) and machine learning have revolutionized cybersecurity Analytics. AI-driven techniques help perform automated anomaly detection, threat correlation and predictive analysis from huge amounts of heterogeneous data. These capabilities result in improved detection speed and accuracy but are not inherently present in the improved decision-making process. Without integration in managerial information flows, AI-enablement of CTI runs the danger of becoming yet another detached technical subsystem.

Management Information Systems (MIS) studies emphasize the contribution of information systems in the areas of planning, coordinating and controlling [8]. Traditional MIS had as its focus the need for structured reporting, and internal control but modern MIS includes analytics and decision support to solve problems of uncertainty and complexity (Sharda et al., 2020). Despite such evolution, cybersecurity intelligence is hardly considered as a core part of MIS. Instead, security information is usually separated from the enterprise decision-making systems, with consequences of inadequate executive awareness and ad hoc governance [9].

Cybersecurity governance frameworks including ISO/IEC 27001 and COBIT emphasize aligning cybersecurity practices to organizational goals and accountability structures [10], [11]. However, governance mechanisms tend to rely on periodic typing and static reporting which do not reflect on the dynamic nature of threats through cyber. Scholars note that the governance of things is proper if information about cyber risks and their connection to business and project is available in time and relevant to the decision [12].

IT project management is another critical integrated point. Most cybersecurity initiatives - such as infrastructure modernization, security architecture redesign and compliance implementation - are done as IT projects with scope, cost, and schedule constraints [13]. Yet cybersecurity risks are often discovered late in project lifecycles, driving up rework, cost overruns and failure rates [5]. The lack of continuous threat intelligence in project planning and execution results in flawed project success as well as organizational resilience.

Organizational resilience means the ability of an organization to anticipate, absorb, adapt, and recover from disruptive events. In the cyber domain, resilience does not just need strong technical controls but also needs to be supported by sound governance, informed managerial decision-making, and adaptive project execution underpinned by timely intelligence. Reframing AI-driven CTI as a Management Information System could provide a way to achieve this integration.

In view of the above, this research work aims to answer the following research question: How can AI-free cyber threat intelligence be thought of as a management information system that integrates cybersecurity governance and IT project management to conduct an organization more resiliently?

To respond to this question, the paper has been carried out by following the design science research and process to create conceptual AI driven CTI-MIS framework based wholly on literature. The study contributes to the MIS research by extending its dimension into AI enabled cybersecurity intelligence, advances the cybersecurity governance by operationalizing the intelligence driven cybersecurity governance, and offers practica guide to integrating CTI into IT project management to support resilient digital transformation.

2. LITERATURE REVIEW

2.1 *Management Information Systems as Decision-Support Infrastructure*

Management Information Systems (MIS) had been defined initially as integrated systems to collect, process, and distribute information, to aid in managerial planning, control and decision-making [8]. Early research focused on structured reporting and operation efficiency. The scope also was widened in later scholarship toward strategic alignment and executive support in decision making [11]. As organizations struggled with more and more uncertainty, MIS became decision support systems (DSS) and executive information systems (EIS). These systems integrate complicated data into the drives for action [2]. The contemporary research focuses on analytics, dashboards, and predicting models for pro-active control and strategic foresight. They are particularly useful in high-risk environments in which uncertainty and time sensitivity are paramount in decision-making. Despite this evolution, the information related to cybersecurity has very often been on the periphery of enterprise MIS architectures. [9] suggest that many organizations stabilize the security as a technical protection and not as strategic information resource. This separation results in reduced visibility of cyber risks by the executives and prevents coordination between the levels of the organization in taking necessary decisions. [14] write that managerial involvement in information security is often reactive driving at incidents to occur rather than systematic support to information. This hostile attitude further undermines the inclusion of cyber risk considerations in managerial processes: MIS scholars are increasingly stressing on the need to incorporate risk-related information in core information systems to facilitate enterprise-wide governance and resilience [15]. From this point of view, cyber threat intelligence is a key type of managerial information that is poorly exploited and is quite compatible with the objectives of MIS.

2.2 *Cyber Threat Intelligence: Concepts and Practice*

Cyber Threat Intelligence (CTI) refers to the process of systematically collecting, analyzing, and distributing intelligence on cyber threats for making decisions about defense and strategic countermeasures [6]. CTI is structured into four intelligence levels, i.e., strategic, tactical, operational, and technical intell methodologies developed for different audiences of the organization [16]. Strategic CTI looks at long term trends found in threats and adversary motivations and is used to assist executives and the board in making informed decisions. Tactical and operational CTI aid security teams in the discovery and response to incidents. Technical CTI provides indicators of compromise and signatures for automated defense machines. Together, these levels form a proactive approach to cybersecurity because organizations can anticipate the risk of attack and efficiently allocate resources. Yet, in reality, CTI is not really integrated. The majority of the outputs can be seen coming from the technical teams, and a minimal amount is converted into business-relevant insights [7]. As a result, executives and project managers frequently lack timely intelligence on emerging threats to organizations and their potential effect on organizational objectives. Traditional CTI is based on manual analysis and static threat feeds that find it difficult to stay abreast of the volume, pace and complexity of modern cyber threats [3]. These challenges make clear the need for automated and advanced analytics to make CTI more effective and relevant throughout the organization.

2.3 *Artificial Intelligence in Cybersecurity Intelligence*

AI has brought dramatic changes in cybersecurity analytics like automating cyber threat detection and classification and forecasting them. Machine learning identifies unusual network traffic and identifies variants of malware, and the events in various systems are all linked together. Deep-learning models go even further in their accuracy by detecting complex patterns in large datasets of multi-dimensional data [17]. Within Cyber threat Intelligence (CTI), AI assists to prioritize threats and assign scores for their risks and future occurrences, moving the firms from a reactive response to pro-active defense [18]. Natural - language processing - used for the analysis of unstructured sources, such as threat reports, vulnerability disclosures, and online forums extending the scope of collected intelligence [19]. However, most AI focused cybersecurity research is focused on metrics such as detection accuracy, false positive rates, and computation efficiency. Few studies examine the incorporation of intelligence generated by AI in organizational decision-making. This gap points towards a larger issue: taking technical knowledge and making it into operational management knowledge. Management Information Systems (MIS) theory, driven by the point that AI's real benefit is not only automation, but augmenting human decision-making through comprehensible flows of information and interpretable outputs, [20]. If AI-powered CTI is not embedded in MIS frame wings, it can build up silos and lack success in driving organization-wide strength and resilience.

2.4 *Cybersecurity Governance and Information Alignment*

Cybersecurity governance refers to the structures, policies and processes that are used to guide and control an organization's cybersecurity activities to align with its strategic goals [4]. Standards such as ISO/IEC 27001 and COIT are orientated towards accountability, risk management, compliance and continuous improvement [10], [11]. Good governance requires information to be timely, accurate and of use for decision making. Yet studies show that many organizations still rely on periodic audits to compliance reports and a static risk assessment which misses the fast-changing threat environment [12]. Scholars state that governance requires the use of real-time intelligence in order for the risks to be proactively managed and investment decisions made more informed [21]. Adding CTI to governance can provide members of the board with better visibility, bring cyber initiatives into line with strategy, and drive accountability in every business unit. Although the relevance of CTI is obvious, documents are rarely found to explain how it should be implemented in the context of enterprise information systems. This deficiency indicates that there is a need for a method based on MIS to integrate intelligence directly into governance processes.

2.5 *IT Project Management and Cybersecurity Risk*

IT project management is the primary manner in which cybersecurity strategies and governance directives are implemented [13]. Projects such as modernizing security architecture, migrations, and compliance are projects that carry massive investments and high risk. Cybersecurity risks are revealed late in a project and can cause additional rework, delays, and cost overruns [5], studies reveal. Risk assessments are often only conducted at the beginning of a project and there continues to be no update as conditions of threats change. Adding CTI to project management enhances risk identification, enables adaptive planning and the ability to continuously monitor the entire lifecycle [22]. AI -driven CTI can support feasibility reviews, choices of controls, and support in real-time changes while conducting. However, the overlap between CTI and ITPM is still poorly examined. Current research tends to treat cybersecurity almost exclusively as a technical limitation, not as a fluid interpretive managerial factor when making project decisions [3].

2.6 *Research Gap and Synthesis*

Existing research points out to a major gap at the intersection of the areas of Management Information System (MIS), Artificial Intelligence (AI)-based Cyber Threat Intelligence (CTI), cybersecurity governance, and IT project management. While each field has evolved independently, there has been little work that brings them together into a broader framework as a way to enhance the resilience of an organization. In particular, CTI has not been systematically framed as an MIS that can translate the insights from AI into decisions, both at a governance and a project level.

3. RESEARCH METHODOLOGY: DESIGN SCIENCE RESEARCH

3.1 *Research Paradigm and Methodological Rationale*

This study employs Design Science Research that is termed as DSR to examine the possibility of shaping a Cyber Threat Intelligence (CTI) characterized by AI during Cyber Security into the form of a Management Information System (MIS). The idea is to integrate governance for cybersecurity with IT project management to make the organization more resilient. DSR is suitable, as it generates and tests system artifacts that solve real business problems and contribute to theoretical knowledge [23], [24]. Whereas purely explanatory or predictive approaches rely mainly on the interpretation of research information, DSR pays special attention to relevance, innovations and rigorous evaluation. This makes it ideal for addressing the interdisciplinary combination of MIS, cyber security, and management [25]. CTI is currently treated separately in the different areas of technical, governance, and project management, which provides a complex socio technical challenge. Dealing with this problem involves consolidating and codifying knowledge into a clear, structured conceptual artifact and this is not the portion of the problem that empirical observation alone can fulfill. DSR has a long history in MIS research, where it supports the creation of decision support systems, governing framework and analytics architecture linking technical tools and managerial process [23]. Following this tradition, this study designs a conceptual AI and CTI MIS framework based on the known theory and verifies the framework through analytical evaluation.

3.2 *Design Science Research Process*

The research is based on the canonical DSR process by [26]. It consists of six activities that need to be carried out in an iterative manner: problem identification, objective definition, design and development, demonstration, evaluation, and communication.

Problem Identification and Motivation: This study addresses the existing gap in the production of cyber threat intelligence (CTI) and its use in managerial decisions, governance oversight and IT project execution. Earlier works show that CTI is most used at the technical level that has limited strategic impact and CTI contribution to organizational resilience [7], [9]. That fragmentation creates the need for a one sized MIS - oriented solution.

Definition of Objectives: We want to establish a conceptual framework with AI-driven CTI as a management information system. The system should be able to support cybersecurity governance and IT project management. It has to translate technical threat data into decision-ready intelligence that is aligned to the organization's goals, risk appetite, and project constraints [11].

Design and Development: The Main artifact is a layered AI-driven CTI-MIS framework. It combines data recording, AI analysis, information processing, administrative mechanisms, and workflows for management and project administration. The design is based on the MIS theory, cybersecurity governance requirements and project management best practices to maintain coherence and practicability [10], [13].

Demonstration: We demonstrate the framework over typical governance, project management scenarios, like risk-based decision making, investing in cybersecurity, and adjusting project controls. These examples illustrate how the framework can be applied in any type of organization, and it doesn't have to be in a specific industry or have a specific tech stack.

Evaluation: We evaluate the artifact by comparing it to established theories and frameworks. Criteria: Relevance, internal consistency, completeness and explanatory power, according to DSR evaluation principles [23], [25].

Communication: The findings are communicated in a clear academic narrative that provides value to the field of MIS, Cybersecurity governance, and IT project management literature.

3.3 *Knowledge Base and Theoretical Foundations*

DSR necessitates that artefacts are based upon a solid knowledge base with theories, frameworks and empirical evidence [23]. In this research study, we synthesize three theoretical core streams that create that knowledge base. First, MIS theory provides basic principles for information processing, decision support and strategic alignment [2], [8]. By emphasizing the quality of information, managerial relevance of information, and timeliness of decision, MIS theory is useful in shaping CTI output into useful MIS artifacts. Second, cybersecurity governance literature is a guide to how CTI is in line with accountability structures, risk-management processes and compliance requirements [4], [21]. Its principles of governance are such that the framework is conducive to oversight, enforcement of policy and strategic prioritization. Third, the IT project-management theory allows for a lifecycle-based structure to integrate CTI into the project stages: initiation, planning, execution, monitoring and closure [13]. Through this integration, cybersecurity intelligence is used to inform decision making at every stage of the digital transformation initiative.

3.4 *Artifact Description: Conceptual AI-Driven CTI-MIS Framework*

This study describes a conceptual CTI-MIS framework that is AI driven and is developed as its main artefacts. In MIS design science, conceptual artifacts are often employed in solving complex organizational problems that need to be integrated theoretically as opposed to a system immediately built out [25]. The framework represents CTI as more than a technical tool; CTI is an enterprise information system converting threat data into management information. It makes visible the interplay between AI analytics, information presentation, modes of governance and project workflows, creating a link between how cybersecurity is carried out day by day and as a strategic operation. By making these relationships explicit, the artifact gives leaders of the organization clear, practical guidance for putting CTI in its current context of MIS architectures and governance structures.

3.5 *Evaluation Strategy and Rigor*

Given the conceptual nature of the proposed artifact, an analytical approach to evaluation is adopted in this study instead of an empirical approach of testing the hypothesis. Analytical evaluation is utilized to determine if the artifact exhibits logical coherence, theoretical foundation and ability to solve the identified research problem, based on accepted design science research principles [23]. The evaluation focuses on establishing the framework's relevance to filling a well-documented void in the MIS and cybersecurity literature, on its alignment with defined principles of MIS, cybersecurity governance and IT project management and on its comprehensiveness in enabling strategic, tactical and operational decision-making levels of support. Additionally, the utility of the framework is evaluated based on the ability to provide actionable information for integrating cyber threat intelligence in governance and project management processes. This evaluative framework is consistent with previous MIS design science research [24], [25] which calls for such conceptual rigor and attachment to theory in the development of governance and decision support-oriented artifacts.

3.6 *Research Validity and Limitations*

While the DSR approach ensures theoretical rigor and relevance, the study has inherent limitations. As a conceptual design, the framework has not yet been empirically validated through case studies or quantitative testing. However, conceptual rigor and analytical evaluation are appropriate at this stage of theory development [23]. Future research may extend this work by empirically evaluating the framework in organizational settings or by developing prototype implementations to assess performance and usability.

4. AI-DRIVEN CYBER THREAT INTELLIGENCE AS A MANAGEMENT INFORMATION SYSTEM: CONCEPTUAL FRAMEWORK

The central premise of this study is that AI-driven Cyber Threat Intelligence (CTI) should be considered not only a technical tool, but as a Management Information System (MIS) for supporting the decision-making process of managers, governors and IT projects. This section identifies a framework we developed and how AI-enabled CTI is used to transform raw cyber data into actionable intelligence to support organizational resilience.

4.1 *Reframing Cyber Threat Intelligence as an MIS Artifact*

Traditional cybersecurity architecture uses CTI as an op input to detection and response. While this approach works technically, it restricts the organizational value of CTI in terms of intelligence being isolated to Security Operation Centers (SOC) and being pushed outside managerial information flows [7], [9]. In contrast, MIS theory focuses on the transformation of data into information and knowledge that is used in planning, control and strategic decision-making [8].

Reframing CTI as an MIS artifact consists of three basic ways. First, outputs of CTIs needs to be decision-wise and should be oriented to some risk implications, priorities and tradeoffs but not technical indicators. Second, CTI must be integrated with existing organizational information systems which must ensure visibility across manager levels. Third, CTI needs to be institutionalized in governance and project management processes in order to facilitate accountability and adaptive control [11].

AI technologies are playing an important role in facilitating this transformation. By automating data analysis, pattern recognition and prediction, AI enables CTI systems to run at the scale and speed needed to facilitate managerial decision-making in dynamic threat environments [18]. However, the use of AI alone does not create an MIS as it is the structured integration of the AI outputs in the managerial workflows that create strategic value.

4.2 *Overview of the AI-Driven CTI-MIS Framework*

The proposed framework conceptualizes AI-driven CTI as a **layered management information system** that bridges technical cybersecurity operations and organizational decision-making. The framework consists of four interdependent layers:

1. Data Acquisition
2. AI Analytics and Intelligence Generation
3. MIS Integration and Decision Support, and
4. Governance and IT Project Management Alignment

This layered structure is a reflection of MIS principles of information processing and control. It ensures that the intelligence is flowing upwards from the systems of technical to the managerial decision points while the feedback is flowing downward through the mechanisms of governance and project execution [2].

4.3 *Data Acquisition Layer: Cyber Intelligence Inputs*

The Data Acquisition Layer is used for collecting raw cybersecurity data from both internal and external sources, including network logs, endpoint telemetry, intrusion detection systems, vulnerability scanners, cloud, and open-source intelligence feeds [6]. It additionally incorporates the contextual info about organizational assets, enterprise processes and the surroundings for projects.

From an MIS point of view, data quality is important. Inconsistent, incomplete or delayed data impairs decision support and creates more uncertainty [27]. Therefore, the framework emphasizes standardizing data collection, integration and preprocessing in order to achieve data accuracy, timeliness and relevance. By bringing together different data sources in the Data Acquisition Layer, a comprehensive situational awareness base is created for providing support to advanced analytics and managerial insight.

4.4 *AI Analytics and Intelligence Generation Layer*

The AI Analytics Layer represents the backbone of the CTI-MIS system's intelligence with machine learning, deep learning and statistical modelling used to translate raw data into viable threat intelligence. Its functions include Anomaly detection, Attack pattern recognition, Threat correlation, Risk scoring and Predictive analysis [17], [28].

Crucially, the framework focuses not only on technical performance, but further, it emphasizes interpretability and relevance. MIS research has shown that decision support systems must present information that is easy to understand and believable by managers [20]. Accordingly, the results of the AI analytics are designed to provide explanatory information, such as likelihood of threat, potential business impact and confidence levels, rather than to provide an obscure classification.

By creating forward-looking intelligence, this layer supports anticipatory risk management and enables organizations to anticipate emerging known threats and make strategies accordingly. This capability is in line with the MIS objectives of backing strategic foresight and adaptive control in uncertain environments [15].

4.5 *MIS Integration and Decision Support Layer*

The MIS Integration Layeraks integrates the intelligence generated by AI into managerial information artifacts, such as dashboards, key risk indicators, performance metrics and scenario analyses. By providing alignment of the presentation of information in relation to a managerial role and the context of decision making, this layer operationalizes fundamental MIS principles [8].

Strategic dashboards offer summary views of the risks, trend analyses, and alignment of organizational objectives to senior executives and boards. Tactical dashboards, on the other hand, are useful for resource allocation, prioritization and control decisions for the middle managers and project leaders. By providing CTI outputs as an integral part of enterprise MIS platforms, this layer will ensure that cybersecurity intelligence is part of the routine of managerial decision-making, not an ad hoc report.

The integration also creates feedback loops that allow managers to assess their cybersecurity investments and governance choices over time to see whether those choices are effective. Such feedback mechanisms are vital to MIS based control systems and foster organizational learning [29].

4.6 *Governance and IT Project Management Alignment Layer*

The final layer of the architecture includes the outputs from CTI-MIS as part of the areas of cybersecurity governance and IT project management. Through this integration, governance mechanisms use the insights gained from CTI on policy enforcement, understanding of risk appetite, compliance and accountability [4], [21].

At the project level, CTI-MIS provides transition of risk-informed decision-making throughout the entire IT project lifecycle. During the initiation and planning stages, intelligence is used to provide information about feasibility and about specifying security needs. During the execution and monitoring of the activities, real-time intelligence facilitates adaptive control actions and risk mitigation of emerging risks. In the closure phase, post-project intelligence enables learning and promotes process improvement [13].

By integrating CTI into the governance frameworks as well as the project workflow, the framework ensures intelligence is not only used as an informant of decisions, it also ensures coordination of organizational action. This collision merges the current definition of cybersecurity as an element of merely response and reassignment to a strategic enabler of organizational resilience.

4.7 *Contribution to Organizational Resilience*

Organizational resilience involves the ability to anticipate disruptions, adapt to changing conditions, and recover effectively. The AI-driven CTI-MIS framework is the contribution to resilience by improving anticipatory awareness, facilitating adaptive governance, and project-level continuous risk management.

In contrast to siloed security systems, the proposed framework embeds intelligence into the organizational fabric, which is an important step in ensuring that cyber risks are understood, controlled and managed as enterprise-wide concerns. This holistic integration is not untrue to the basic mis objective of not calling for aligning information systems with the organization's strategy and performance.

5. INTEGRATING AI-DRIVEN CTI-MIS WITH CYBERSECURITY GOVERNANCE

Effective cybersecurity governance alone does not rely on technical safeguards, nor does it require them as part of its governance; it is dependent upon structured decision rights, accountability mechanisms and information flows that give alignment between cybersecurity activities and organizational strategy and risk appetite [4], [11]. This part discusses how the proposed use of Artificial Intelligence (AI)-enabled Cyber Threat Intelligence as a Management Information System (CTI - MIS) operationalizes cybersecurity governance by incorporating intelligence into oversight, risk management, and accountability processes.

5.1 Cybersecurity Governance as a Managerial Control Function

Cybersecurity governance is a subdomain of corporate governance and ensures that information security is consistent with organizational objectives and is responsible for the effective management of cyber risks [4]. Key concepts in governance frameworks include strategic alignment, risk management, resource optimization and the measurement of performance [10]. From the MIS viewpoint, governance is an information issue; decision-makers need timely, accurate and sufficient information to exercise control and accountability [8].

Nonetheless, empirical investigations have repeatedly confirmed the disparity between the intention of governance and governance reality. Board and senior executives often rely on periodic mechanisms for compliance reporting and aggregated risk assessments that do not help illustrate the dynamic nature of cyber threats [12]. The fallout of such informational lagging defeats proactive governance & leads to mad rush decision-making after security incidents.

The AI-driven CTI-MIS framework helps close this gap by deriving incorrect geo-information of cyber intelligence in real-time, which is also relevant for governance. By incorporating the outputs of CTI into managerial dashboards and reporting systems, the framework fits the cybersecurity governance principles with the MIS principles of continuous monitoring and feedback [29].

5.2 Intelligence-Driven Risk Governance

Risk management at the heart of cybersecurity governance. Conventional risk analyses are based on static threat scenarios and insufficient reviews that do not keep up with the rapidly evolving cyber world [9]. Researchers say that real-time intelligence is required to assess the probability of a threat, the effect that the threat might be capable of causing, and the effectiveness of controls [21].

In the model of the CTI-MIS, AI generates threat information that goes directly into the risk management process within the organization. Scores, trend analyses and predictive indicators allow decision makers to continuously update risk exposure and concentrate on the most important risk mitigation actions. Such a data-driven approach enables firms to comprehend the allocation of resources where they will supply the most resilience benefits [14].

Additionally, CTI-MIS places technical threats in the context of business processes, key assets, and to ongoing projects. That contextualization ensures the risk information will be more relevant to stakeholders. Executives can review cyber risks in addition to financial, operational, and strategic risks, thus contributing to integrated enterprise governance [11].

5.3 Policy Enforcement and Compliance Monitoring

Governance frameworks in cybersecurity deal with developing, enforcing, and monitoring policies to control risk [10]. Yet many organizations are still looking at compliance retroactively, through audits that (in many cases) find violations only after the fact the damage has been done.

CTI-MIS assumes threat intelligence directly tied to policy controls, which allows for the ongoing contextual monitoring of compliance. Its Artificial intelligence analytics identifies deviations from policies, anomalous behaviors and informs the governance stakeholders almost instantly [18]. This proactiveness suits well with MIS-based control systems that emphasize real-time monitoring as well as prompt corrective action [2].

When compliance metrics are displayed in the governance dashboards, CTI-MIS increases transparency and accountability. Decision makers can track how effectively policies operate, identify gaps in systems and adjust controls based on newly emergent threat intelligence. In such a way, compliance changes from being a static obligation towards an active and dynamic control instrument [21].

5.4 *Accountability and Role Clarity*

Clear accountability is one of the basic principles of good governance. Cybersecurity governance frameworks emphasize the importance of well-defined roles and responsibilities in the management of cyber risks and across organizational levels [4]. Yet ambiguity still remains at the practical level, particularly in organizations that consider cybersecurity as an IT security matter rather than an enterprise issue.

The CTI-MIS framework contributes to accountability by tying the outputs of intelligence to units of organizations, business processes, and IT projects. By linking threats and risks to responsible owners, the system allows readiness governance stakeholders to make explicit ownership and enable monitoring of performance over time [11].

From an MIS perspective, such linkage is helpful for management control because it offers measurable outputs in terms of responsibility and performance [29]. Executives can assess the performance of various units in handling cyber risks and address obsolete performance below acceptable levels.

5.5 *Board-Level Oversight and Strategic Alignment*

Board oversight of is now considered mandatory with cybersecurity governance. Researchers say that boards should move beyond technical briefings and participate in strategic conversations on cyber risk and resilience [12]. Yet on boards, the information systems are often not in place to make oversight knowledgeable.

CTI -MIS addresses this problem by providing board-oriented views of strategic intelligence. It offers aggregated threat trends but also provides risk heat maps and scenario analysis so that boards have an understanding of the implications of cyber threats without having technical know-how. This approach is in line with MIS research that emphasizes the need for role-specific information [8].

By historicizing the intelligence on cybersecurity into enterprise performance reports, CTI-MIS links cyber efforts with organizational strategy. This integration makes cybersecurity part of the strategic enabler rather than a cost and improves long-term resilience [15].

5.6 *Governance Maturity and Continuous Improvement*

Governance is not a static concept but a dynamic capability that grows by an iterative learning process [20] through feedback and experiential learning. The CTI-MIS framework promotes the development of governance by allowing continued evaluation of the efficacy of cybersecurity. Intelligence-driven feedback loops empower organizations to assess the role that governance decisions play in shaping the outcomes of threats and in turn to change strategies as needed.

This continuous improvement mechanism is in line with both MIS and cybersecurity governance doctrines and emphasizes learning, adaptation, and resiliency. In the long run it is possible for organizations to optimize governance structures, policies and investment portfolios by relying on empirical intelligence, and not just intuition or some compliance to policies.

6. INTEGRATING AI-DRIVEN CTI-MIS WITH IT PROJECT MANAGEMENT

IT project management (ITPM) is the key organizational process by which cybersecurity strategies and governance directions are operationalized.

As organizations engage in digital transformation initiatives, such as cloud migration, enterprise system integration, and security architecture modernization, cybersecurity risks play a bigger role in driving project success and organizational fulfillment [13].

This section explores how the proposed AI-based Cyber Threat Intelligence as a Management Information System (CTI-MIS) can be integrated into the IT project management processes for risk-informed planning, adaptive execution, and resilient end results.

6.1 Cybersecurity Risk in IT Project Management

Cybersecurity risk is a critical but underappreciated component of the information technology project risk. Traditional project risk management focuses on the uncertainty of scope, cost and schedule and cybersecurity is usually just a technical obligation for compliance, not a dynamic risk factor [5]. Consequently, security considerations are usually handled in the later stages of project lifecycles, leading to expensive reworking, delays and vulnerabilities in deployed systems.

Research shows that project failures often occur due to poor risk identification at the initiation and planning stage [22]. In the case of cybersecurity-intensive projects, static risk assessments simply prove to be insufficient, since threat situations keep changing with time. Therefore, effective project management is dependent upon access to intelligence-driven and timely insights that mirror both instantly existing and up-and-coming cyber threats.

The CTI-MIS framework helps in fulfilling this need by integrating cyber threat intelligence into project risk management processes. By treating CTI as a managerial information resource, project managers have continuous visibility of threat landscapes relevant to project assets, project technologies and timelines.

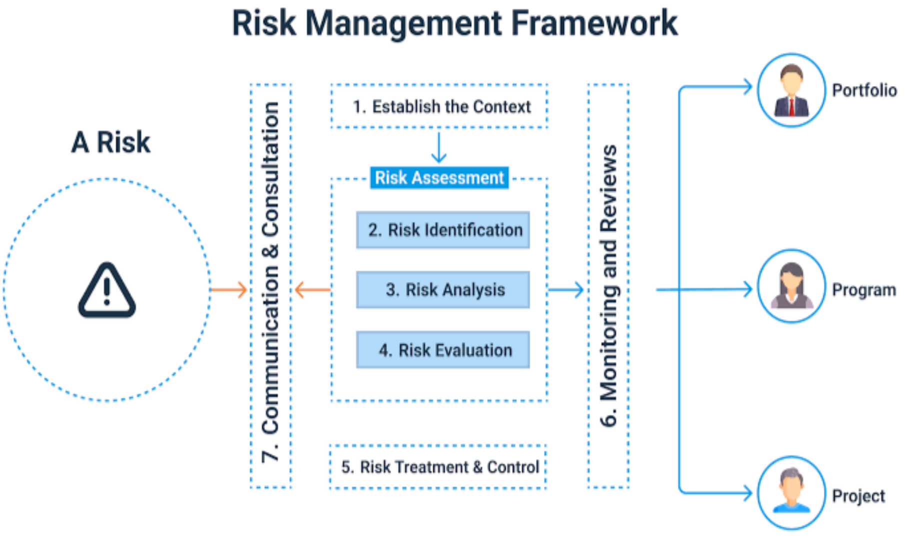

Figure 1. Risk Management Framework Integrating Governance and Portfolio–Program–Project Decision Levels

6.2 *CTI-MIS Integration Across the Project Lifecycle*

The integration of CTI-MIS into IT project management can be conceptualized across the standard project lifecycle, that is, initiation, planning, execution, monitoring and control, and closure [13].

Project Initiation: During initiation, feasibility analysis, and project justification, CTI-MIS provides intelligence about the threat exposure associated with proposed technologies and architectures. AI-empowered risk assessments can help decision-makers decide whether the expected benefits outweigh cybersecurity risks and can help them decide appropriate levels of governance oversight [14].

Project Planning: In the planning phase, CTI-MIS provides information for the identification and prioritization of cybersecurity risks. Intelligence-driven insights are used to make the decision-making process of security controls, resources, and scheduling decisions. By fusing threat intelligence into planning artifacts such as risk registers and work breakdown structures, CTI passant - miembros (2003) of the industry (Institute of Management Development, 2010) and resilience is enhanced in planning.

Project Execution: With execution, CTI-MIS offers continuous tracking of threat conditions that affect project assets and environments. AI-powered alerts and dashboards make project managers have near real-time intelligence to support adaptive responses to risks arising. This capability is in line with the principles of MIS of real-time control and feedback [8].

Monitoring and Control: Gamma CTI is a system that integrates cybersecurity performance metrics into project control mechanisms (CTI-MIS). Key risk indicators, security milestones and compliance status are monitored in addition to the traditional project performance indicators. This integrated monitoring is useful in supporting informed decision-making and corrective action [29].

Project Closure: At closure, CTI-MIS supports post project evaluation through capture of intelligence regarding residual risks, control effectiveness and incident results. This information contributes towards organizational learning and continuous improvement towards resilience of projects in the future [20].

6.3 *Risk-Informed Decision-Making and Adaptive Control*

One of the main contributions of CTI-MIS to information technology project management is the facilitation of risk-informed decision-making. Conventional project management is known to rely on static risk matrices that are unaware of the dynamic nature of evolving threat conditions. In comparison, AI-based threat intelligence provides dynamic risk assessments, which constantly adapt to changes in the threat landscape [18].

By placing these assessments inside project dashboards and in decision support tools, CTI-MIS can help project managers assess margin trade-offs among security, cost and schedule in near real-time. Given that it creates a capacity for adaptive control, this increases the resiliency of projects by allowing timely interventions before risks reach a stage where project failures may occur [27].

From the standpoint of management information systems, this integration constitutes a case of decision augmentation, in which information systems augment management judgment, rather than replacing it. Project managers do not hand off the accountability of decisions, but maintain their responsibility and CTI-MIS provides the required intelligence for effective performance in a complex risk environment.

6.4 *Alignment with Governance and Organizational Objectives*

IT projects do not exist in an isolated context and are integrated into larger governance structures and strategic goals. The CTI-MIS framework helps the organization to ensure a match between the decisions that are made at a project level and the organization's cybersecurity governance policies by linking the project risks to the enterprise risk management processes [11].

Governance bodies may use CTI-MIS outputs to manage risks of projects, prioritize important initiatives, and allocate resources across project portfolios. This alignment reinforces the accountability processes and ensures that project choices contribute to organizational resilience objectives against optimization (quantitative metric) choices that may only optimize isolated performance metrics [4].

6.5 *Enhancing Project Success and Organizational Resilience*

Success is more than delivering on schedule or working within budget. It also requires that the systems you deliver are secure, compliant, and resilient. CTI (cyber threat intelligence) in project management helps to mitigate post-deployment vulnerabilities and incidents that will help build long-term value. The CTI-MIS framework resiliency capability incorporates intelligence-centric risk management into project execution. It makes projects into adaptive processes that can respond to changes in threats to improve the organization's capacity to withstand and recover from cyber disruptions.

6.6 *Challenges and Implementation Considerations*

Integrating CTI-MIS into IT project management brings numerous benefits to the business, but on the other hand, it also raises some challenges. Project managers are also not always well-versed in cybersecurity, and with too much detailed intelligence, it is a lot to process, and it can overwhelm decision makers. MIS research shows that presenting information in accordance with each of the roles reduces overload [8]. The effectiveness of CTI-MIS also depends on the culture of the organization and how mature its governance is. In order to be implemented successfully, organizations require executive support, clarity of responsibility, and integration of the security and project management teams [11].

7. ORGANIZATIONAL RESILIENCE AND STRATEGIC IMPLICATIONS

Organizational resilience has become a central concept in management and information systems literature and refers to organizational capability to anticipate, absorb, adapt to, and recover from disruptive events [30]. In digitally contingent contexts, cyber threats are a constant and evolving area of disarray that compromises traditional resilience mechanisms. The present writing investigates the contribution that the proposed AI-driven Cyber Threat Intelligence as a Management Information System (CTI - MIS) can make in building organizational resilience and outlines the wide strategic ramifications.

7.1 *Conceptualizing Organizational Resilience in Cyber Contexts*

Resilience goes beyond the concept of robustness or resistance to disruption in order to include learning, adapting and transforming in response to adversity [31]. From the information systems perspective, resilience requires the availability of sufficient, timely, relevant and actionable information so that organizations can sense changes in the environment and make effective responses [15].

Cyber disruptions differ from traditional operational disruptions in a number of respects. They are frequently invisible before impacts become visible, travel quickly through disparate interconnected systems, and change constantly as toughened sedentary foes evolve (until they vanish from sight as they invest in and develop all kinds of business armaments, tactics, and techniques to boost their probability of survival and well-being). Consequently, resilience in the cyber context requires those intelligence-driven capabilities that support anticipation and adaptation instead of static protection.

The CTI - MIS framework is consistent with this way of thinking by making cyber threat intelligence a part of the information flows within organizations, allowing emerging risks to be identified early and strategic responses made. By addressing CTI as a managerial information resource, organizations become more capable of sensing and interpreting cyber threats as they form a portion of the overall risk environment.

7.2 *Anticipatory Capability and Situational Awareness*

Anticipation forms an inherent part of the dimension of organizational resilience, referring to the ability to anticipate possible disruptions and to prepare for them [30]. Conventional paradigms of cybersecurity are focused on detection and response, usually after the event. On the other hand, CTI-MIS focuses on the anticipatory intelligence, where the intelligence is driven by artificial intelligence (AI) analytics to identify the trends of treating threats, behaviors of adversaries, and vulnerabilities (if they emerge) [18].

From the point of view of Management information systems, readiness for anticipation is dependent on the awareness of the situation, which is supported by integrated information systems [2]. CTI-MIS is used to augment situation awareness through the use of data from heterogeneous threat research and its contextualization within organizational processes, assets, and projects. This synthesis makes it possible for the managers to identify weak signals and assess the strategic status of such signals.

Robust anticipation is the basis of proactive governance decisions, such as the recalibration of risk appetite, prioritization of investment portfolios, or restructuring of project portfolios. These actions contribute toward resilience as they reduce exposure to high-risk cyber risks before the problematic manifestation of cyber disruptions.

7.3 *Adaptive Capacity and Decision Flexibility*

Adaptation refers to an organization's ability to change its structures, processes and strategies in response to changing transforming conditions [31]. In cyber environments, such adaptation requires expeditious decision-making with an intelligence underpinning it. Static policies and inflexible control structures make it harder to adapt and, thus, increase vulnerability to changing threats.

The CTI-MIS framework promotes adaptive capacity by integrating intelligence (real-time) into governance and project management processes. By providing constant feedback to the condition of the threats and how effectively controls are working, CTI-MIS gives managers the ability to dynamically modify decisions. This corresponds with information systems research, which emphasizes feedback loops and control systems as key enablers of organizational learning and adaptation [29].

Adaptive decision flexibility is especially relevant in the domain of IT project portfolios, for which emergent threats may demand changes in prioritization, scope, or reallocation of resources. CTI- MIS manages such adaptations by having the intelligence enable direct connection to project-level decision points, thereby contributing to an increased resilience across the portfolio.

7.4 *Recovery, Learning, and Knowledge Integration*

Recovery is a critical component of organizational resilience, which describes the ability to recover and establish operational continuity and to learn lessons from disruptive events [30]. Cyber incidents often provide valuable intelligence about the vulnerabilities of systems and their attack methods, as well as the effectiveness of responding to the incident. Nevertheless, in the absence of some form of systematic incorporation into knowledge management systems, such lessons are in danger of not being retained.

Management information systems theory emphasizes the integral role of information systems in processes that support the creation of organizational learning and knowledge [20]. The CTI -- MIS framework encourages learning by institutionalizing post-incident intelligence and embedding it in review of governance and in project retrospectives. Such institutionalization of learning enables organizations to continuously revise policies, controls and decision-making processes.

Through the embedding of learning mechanisms into MIS architecture, the CTI thinking in the MIS architecture, or simply known as CTI-MIS, metamorphoses cyber incidents from being an isolated failure into an opportunity for resilience enhancement. Remaining for a period of time, this accumulated learning contributes to increased governing maturity and better strategic alignment.

7.5 *Strategic Alignment and Competitive Implications*

The strategic implications of resilience are more than just a risk mitigation approach. Academic scholarship argues that organizations that express resilience are more likely to have a sustainable competitive advantage in a volatile environment [30]. Specifically, cyber resilience has an impact on the trust of the stakeholders, regulatory compliance, and continuity of operation.

The CTI-MIS framework enhances strategic alignment through the alignment of cybersecurity intelligence in strategic planning and investment decisions. Through the integration of CTI into MIS, organizations make cybersecurity initiatives fit into large-scale strategic objectives and, in so doing, avoid the temptation of reclassifying them as cost centers [11].

Such alignment promotes the balancing of security investments to innovation and growth goals, which would further enable sustainable competitive positioning. Consequently, the CTI-MIS framework is part of resilience, strategic agility, and the development of long-term value.

7.6 *Enterprise-Wide Integration and Cultural Implications*

Organizational resilience has been affected by culture, leadership, and common understanding of risk [32]. Siloed cybersecurity practices do not support resilience because intelligence and cross-functional coordination are restricted. CTI-MIS fosters enterprise-wide integration through opening up cyber intelligence to and relevant to multiple stakeholders such as executives, project managers, and business leaders.

By institutionalizing CTI through MIS, small organizations cultivate a culture of decisions based on well-transformed information and common responsibility for cyber risk. As such, this cultural shift lends itself to resilience to support proactive engagement with cyber threats (as opposed to reactive behavioral compliance with cyber threats) [21].

8. DISCUSSION AND THEORETICAL CONTRIBUTIONS

This section synthesizes empirical results and outlines the theoretical and practical implications for the area of Management Information Systems (MIS), cybersecurity governance, and IT project management (ITPM).

By redefining AI-driven Cyber Threat Intelligence (CTI) as a Management Information System, the study leads to a better understanding of how cybersecurity intelligence can be integrated within the organizational decision-making structures in order to improve resilience.

8.1 *Advancing MIS Theory Through Cyber Threat Intelligence*

One of the principal theoretical contributions in this work is the extension of MIS theory to encompass AI-induced cybersecurity intelligence as an integral managerial information resource. Traditional MIS scholarship is focused on the study of operational efficiency, decision support, and strategic alignment [2], [8]. While these principles have been implemented in the areas of finance, supply chain management and healthcare, the same cannot be said for cybersecurity intelligence, which was largely confined to the conceptual boundaries of MIS.

This study challenges that boundary by establishing CTI as a type of managerial intelligence, just like financial or operational analytics. By conceptualizing CTI as an MIS artifact, the research brings cybersecurity intelligence within the goals of the core MIS function in foreseeability and versatility: supporting decision making, planning, and control during uncertainty [27]. This reconceptualization solves a long-standing gap that was identified by [9], who noted the marginalization of security information in managerial decision processes.

Furthermore, the study adds to the theory of MIS, for the emphasis is on augmenting rather than automating decisions. AI-driven CTI is not the kind to appear as replacing the power of managerial judgment, but instead increasing its value by providing contextualized intelligence created in real time. This view is consistent with the work by MIS in the field of analytics-enabled decision support in emphasizing the need for interpretability, relevance and human supervision [2], [20].

8.2 *Contributions to Cybersecurity Governance Research*

The study also contributes to cybersecurity governance literature by operationalizing the principles of governance through an intelligence-driven MIS framework. Existing governance frameworks have a strong focus on accountability, risk management and strategic alignment, but offer little pointers as to how real-time intelligence can support governance decisions [4], [10].

By introducing CTI in the governance processes, the proposed framework helps mitigate an information asymmetry that typically plagues the process of cybersecurity oversight. Board and executives often do not have access to intelligence that is ready for decision-making, leading to reactive governance and dominance in compliance [12]. CTI-MIS here overcomes this hurdle by translating technical threat data into metrics enjoyable to gauge (governance) and make into strategic information.

This integration helps support a move from compliance-oriented governance towards risk-based governance where decisions are made in the context of dynamic assessments of the likelihood and impact of threats [21] . The research, therefore, adds to the theory of governance by showing one way in which MIS architecture can be made to deploy continuous oversight and adaptive control in volatile cyber environments.

8.3 *Extending IT Project Management Theory*

IT project management literature has long recognized the importance of risk management, yet cybersecurity risks are often treated as static or peripheral concerns [13]. This study extends ITPM theory by conceptualizing cybersecurity intelligence as a dynamic managerial input that informs project decisions throughout the lifecycle.

By integrating CTI-MIS into project initiation, planning, execution, monitoring, and closure, the framework advances understanding of adaptive project control. Traditional project management emphasizes baseline planning and variance control, whereas CTI-MIS enables continuous risk reassessment and flexible response to emerging threats [5].

This contribution aligns with calls for more adaptive and learning-oriented project management approaches in complex environments [22]. By linking project-level decisions to enterprise intelligence and governance structures, the study bridges a critical gap between project management and organizational resilience research.

8.4 *Organizational Resilience as an Integrative Outcome*

The study highlights that organizational resilience is achieved through the combination of MIS-enabled governance and project management. Earlier research describes resilience as a multi-D capability that includes anticipation, adaptation and recovery [30]. The CTI-MIS framework puts these dimensions into practice by integrating intelligence into the decision-making process at all levels of organizations.

From an MIS perspective, resilience increases with information systems to deliver situational awareness, feedback, and learning [15]. The new framework shows how CTI-MIS supports these functions with a capability for continuous intelligence and adaptive governance, and puts learning from cyber incidents into the regular operation of the organization.

This integrated view adds to resilience theory, demonstrating the power of information system architecture to influence the capacity to treat cyber disruptions as strategic challenges, rather than isolated technical problems, to be brushed under the rug in an organization.

8.5 *Practical Implications for Managers and Practitioners*

The research offers practical insights for managers, governance bodies and IT project leaders. It stresses out that CTI should be treated as an important information resource and not just a technical tool. Organizations that are interested in being resilient should design CTI in their existing Management Information Systems, rather than maintain separate security tools.

Secondly, the framework demonstrates the need for customized information presentation. Executives, governance, and project managers need various levels of details and context to make their decisions appropriately [8]. Designing CTI- MIS dashboards and reports according to these needs leads to greater usability and impact.

Thirdly, the study emphasizes the importance of organizational culture and leadership. Without executive sponsorship and clear accountability, intelligence-driven systems are also likely to be underused. For organizations to succeed, they need to align incentives, governance structures and project practices [11].

8.6 *Limitations and Directions for Future Research*

While there is much to learn from the study, it also has its limitations, and these limitations indicate future research. The framework is at the conceptual stage and has not been tested with case studies and quantitative data. Future studies should examine the effectiveness of CTI-MIS implementation in different industries with regard to performance, usability, and resilience.

Further research must also examine the ethical and organizational dimensions of intelligence through artificial intelligence, including the issues of transparency, bias, and trust. As the impact of AI on managerial decision-making continues to grow, this understanding of the governance implications of AI is a viable research priority.

9. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Cyber threats are growing in frequency, increasing in sophistication and have more strategic impact. As such, cybersecurity is no longer a technical or operational matter, but a matter that impacts all aspects of an organization. Threats can compromise strategic objectives, impact day-to-day operations, threaten regulatory compliance and damage stakeholder trust. Traditional approaches to cybersecurity which focus on the technical aspect are no longer sufficient. This study addresses the gap by re-imagining the AI-driven Cyber Threat Intelligence (CTI) as a Management Information System (MIS). The MIS framework is a combination of cybersecurity governance and IT project management practices aimed at building greater organizational resilience. The research developed an overall conceptual framework based on MIS theory, cybersecurity governance principles and IT project management practices. By using a design science research methodology, the study synthesized existing knowledge to create an integrated artefact to address a well - documented literature gap: the lack of managerial integration for cyber threat intelligence.

9.1 Summary of Key Findings

The study indicates that this perspective of treating CTI as a managerial information resource rather than a technical output can play a significant role in enhancing the capability to make better decisions as well as increasing the resilience of an organization. The proposed AI-driven CTI-MIS framework is a system for converting raw cyber data into decision-ready intelligence, in alignment with the needs of managers. Embedding this intelligence across governance structures and project management processes supports the transition for organizations from reactive cybersecurity practices to proactive intelligence-driven resilience.

At the governance level, CTI-MIS offers dynamic risk management oversight, constant continuous compliance monitoring and decision support at the board level. These capabilities cover some of the old problems, such as information asymmetry, delayed reporting, and compliance-driven behavior [4], [12]. By providing shop owners with real-time, contextualized intelligence, CTI-MIS puts the principles of governance into practice in a simple, operational approach.

At the project level, the framework demonstrates the ways that CTI can be applied to inform IT project management across the lifecycle. By effectively incorporating threat intelligence into the initiation, planning, execution, monitoring, and closure of projects, the risks will be identified earlier, controls will remain agile, and lessons will be retained. This approach is used to update the project management theory by considering cybersecurity intelligence not as a restrainer but as a dynamic managerial input [5], [13].

Together, these integrations increase an organization's resilience by increasing anticipatory capability, adaptive capacity and recovery mechanisms. The study confirms that resilience is not only a technical attribute but also an organizational capability that comes from effective information systems and governance [15], [30].

9.2 Contributions to Theory

This study contributes to making a number of significant theoretical contributions. On the one hand, it expands the MIS theory by formally introducing AI-based cybersecurity intelligence into the realm of management information systems. The existing state of earlier research in MIS focused on analytics and decision support and did not include cybersecurity intelligence as a central conceptual focal point. This study increases the scope of MIS scholarship by establishing CTI as an MIS artifact, which solves one of the riskiest areas that contemporary organizations face.

Second, the research contributes to the development of the cybersecurity governance theory by illustrating how the principles of governance can be implemented and realized by using intelligence-based information systems. The framework focuses on constant supervision and dynamic decision-making with real-time intelligence instead of regarding governance as a set of controls and policies.

Third, the research will add to the literature on IT project management by bringing about CTI in project life cycle management. This integration emphasizes how dynamic risk intelligence is significant in project environments that are dynamic and contributes to the demand to implement more dynamic and learning-based project management practices.

9.3 Practical Implications

To practitioners, the results indicate that more expensive AI-driven CTI technologies will not bring much value when they are not embedded within organizational MIS architectures and decision-making processes. Instead of focusing on the technical intelligence translation to managerial intelligence, organizations need to focus on providing governance and project decisions.

An alternative viewpoint that the top executives and boards ought to take towards CTI-MIS is that it is a strategic capability that increases visibility, accountability, and resilience. With CTI being integrated into enterprise dashboards and performance reporting, leaders would have a more effective way of aligning cybersecurity programs with organizational goals.

Continuous risk assessment and adaptive control of IT projects life cycles should rely on CTI-MIS by IT project managers. This will help minimize security project failure risks and make digital transformation projects more resilient.

9.4 Limitations

This study is as a conceptual study of design science and thus limited. The framework proposed has not been empirically tested either by a case study or quantitative analysis. Although analytic assessment guarantees theoretical rigor and relevance, empirical analysis must be conducted to determine difficulties in implementation, performance results, and acceptance of it by the user in the real-world setting.

Also, the research fails to discuss ethical and legal issues related to AI-based intelligence systems, including transparency, bias, and accountability. The problems must be given close attention since AI continues to affect managerial decisions.

9.5 Future Research Directions

This work can be further developed in a number of ways in future research. The research question that could be addressed by empirical studies is the implementation of CTI-MIS in various industries to investigate its role in measuring governance effectiveness, project performance, and resilience in organizations. Longitudinal case studies would be a special asset in determining the role of intelligence-motivated systems in learning and maturity in governance.

Depending on quantitative research, measurement models can be constructed and tested to connect CTI-MIS capabilities with resilience outcomes, and statistical evidence on the developed framework is obtained. Besides, another possible research topic in the future is the ethical management of AI-led CTI, such as transparency and human control.

9.6 Concluding Remarks

To sum up, this paper argues that AI-based cyber threat intelligence must cease as a technical operational role, but rather a core element of the management information system.

With the alignment of CTI and cybersecurity governance and information technology project management, organizations can significantly enhance their ability to predict, adapt to, and recover from cyber disruptions.

The suggested CTI-MIS concept thus provides a rationally grounded and pragmatically relevant way towards a healthy digital transformation of a more hostile cyberspace.

REFERENCES

[1] A. Bharadwaj, O. A. El Sawy, P. A. Pavlou, and N. Venkatraman, "Digital business strategy," *MIS Q.*, vol. 37, no. 2, pp. 471–482, 2013, [Online]. Available: https://doi.org/10.25300/MISQ/2013/37.2.09

[2] H. Chen, R. H. L. Chiang, and V. C. Storey, "Business intelligence and analytics," *MIS Q.*, vol. 36, no. 4, pp. 1165–1188, 2012, [Online]. Available: https://doi.org/10.2307/41703503

[3] A. Behl and K. Behl, "Cyberwar: The next threat to national security," *Int. J. Bus. Contin. Risk Manag.*, vol. 7, no. 1, pp. 31–45, 2017, [Online]. Available: https://doi.org/10.1504/IJBCRM.2017.082972

[4] R. Von Solms and B. Von Solms, "From policies to culture," *Comput. Secur.*, vol. 23, no. 4, pp. 275–279, 2004, [Online]. Available: https://doi.org/10.1016/S0167-4048(04)00071-1

[5] F. Farahmand, S. B. Navathe, G. P. Sharp, and P. H. Enslow, "Managing vulnerability of information systems," *Inf. Syst. Res.*, vol. 14, no. 3, pp. 247–267, 2003, [Online]. Available: https://doi.org/10.1287/isre.14.3.247.16560

[6] S. Jajodia, P. Liu, V. Swarup, and C. Wang, "Cyber situational awareness," *Springer*, 2011.

[7] E. Karanja and M. A. Rosso, "Stakeholder involvement in information systems security," *Inf. Syst. J.*, vol. 27, no. 5, pp. 243–255, 2017, [Online]. Available: https://doi.org/10.1111/isj.12132

[8] I. Benbasat and R. W. Zmud, "The identity crisis within the IS discipline," *MIS Q.*, vol. 27, no. 2, pp. 183–194, 2003, [Online]. Available: https://doi.org/10.2307/30036520

[9] D. W. Straub and R. J. Welke, "Coping with systems risk," *MIS Q.*, vol. 22, no. 4, pp. 441–469, 1998, [Online]. Available: https://doi.org/10.2307/249551

[10] ISO/IEC, "ISO/IEC 27001: Information security management systems," 2018.

[11] P. Weill and J. W. Ross, "IT governance," *Harvard Bus. Sch. Press*, 2004.

[12] M. Alshaikh, "Cybersecurity governance: A component of corporate governance," *Comput. Secur.*, vol. 93, p. 101773, 2020, [Online]. Available: https://doi.org/10.1016/j.cose.2020.101773

[13] PMI, *PMBOK® Guide*, 7th ed. Project Management Institute, 2021.

[14] A. Dutta and K. McCrohan, "Management's role in information security," *Calif. Manage. Rev.*, vol. 45, no. 1, pp. 67–87, 2002, [Online]. Available: https://doi.org/10.2307/41166164

[15] S. Sarker, S. Chatterjee, X. Xiao, and A. Elbanna, "The sociotechnical axis of IS development," *MIS Q.*, vol. 46, no. 5, pp. 695–720, 2019, [Online]. Available: https://doi.org/10.25300/MISQ/2019/13780

[16] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, "State of the practice of CSIRTs," *SEI*, 2003.

[17] P. Wang, "On defining artificial intelligence," *J. Artif. Intell. Res.*, vol. 63, pp. 1–37, 2021, [Online]. Available: https://doi.org/10.1613/jair.1.12295

[18] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cybersecurity intrusion detection," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, [Online]. Available: https://doi.org/10.1109/COMST.2015.2494502

[19] Z. Tufekci, "Algorithmic harms beyond Facebook and Google," *Color. Technol. Law J.*, vol. 13, pp. 203–218, 2015, [Online]. Available: https://doi.org/10.2139/ssrn.2464111

[20] I. Nonaka, "A dynamic theory of organizational knowledge creation," *Organ. Sci.*, vol. 5, no. 1, pp. 14–37, 1994, [Online]. Available: https://doi.org/10.1287/orsc.5.1.14

[21] M. Siponen and R. Willison, "Information security management standards," *Inf. Manag.*, vol. 43, no. 5, pp. 267–270, 2009, [Online]. Available: https://doi.org/10.1016/j.im.2008.12.007

[22] R. K. Yin, "Case study research and applications," *Sage*, 2018.

[23] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004, [Online]. Available: https://doi.org/10.2307/25148625

[24] R. J. Wieringa, "Design science methodology for information systems," *Springer*, 2014.

[25] S. Gregor and A. R. Hevner, "Positioning and presenting design science research," *MIS Q.*, vol. 37, no. 2, pp. 337–355, 2013, [Online]. Available: https://doi.org/10.25300/MISQ/2013/37.2.01

[26] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007.

[27] R. Sharda, D. Delen, and E. Turban, "Analytics, data science, & artificial intelligence," *Pearson*, 2020.

[28] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[29] R. S. Kaplan and D. P. Norton, "The balanced scorecard," *Harvard Bus. Sch. Press*, 1996.

[30] C. A. Lengnick-Hall, T. E. Beck, and M. L. Lengnick-Hall, "Developing a capacity for organizational resilience," *Hum. Resour. Manag. Rev.*, vol. 21, no. 3, pp. 243–255, 2011, [Online]. Available: https://doi.org/10.1016/j.hrmr.2010.07.001

[31] E. Hollnagel, D. D. Woods, and N. Leveson, "Resilience engineering," *Ashgate*, 2006.

[32] E. H. Schein, "Organizational culture and leadership," *Jossey-Bass*, 2010.