RAIS Journal for Social Sciences | VOL. 9, No. 2, 2025
ISSN 2574-0245 (Print) | ISSN 2574-1179 (Online) | DOI: 10.5281/zenodo.17670119

Interoperability as a Decision Variable in Cyber Threat Intelligence Adoption: A Conceptual Synthesis of Technology Adoption Models

Marlon TAYLOR

Marymount University, United States, m0t78249@marymount.edu

Abstract: Cyber Threat Intelligence (CTI) adoption is essential for strengthening organizational cybersecurity, yet decision-makers continue to struggle with selecting and integrating CTI solutions that ensure effective interoperability. This narrative literature review synthesizes current research across decision-making theory, interoperability studies, technology adoption models, and CTI-sharing frameworks to identify the factors shaping CTI adoption in practice. Findings show that bounded rationality and cognitive overload influence how organizations evaluate CTI technologies, while compatibility and integration feasibility consistently emerge as dominant adoption determinants. A comparative analysis of DOI, TOE, TAM, TTF, and UTAUT indicates that these models provide valuable but incomplete perspectives on CTI contexts, particularly in addressing interoperability's central role. The review highlights critical gaps in existing theoretical frameworks and offers targeted directions for future qualitative research to better understand how interoperability informs cybersecurity decision-making and CTI implementation.

Keywords: Cyber Threat Intelligence (CTI), Interoperability, Decision-Making, Bounded Rationality, Technology Adoption, Diffusion Of Innovation (DOI), Technology–Organization–Environment (TOE), Technology Acceptance Model (TAM), Unified Theory Of Acceptance And Use Of Technology (UTAUT), Task–Technology Fit (TTF), Cybersecurity, Information Systems

Problem Statement

Despite the expanding body of research on decision-making, interoperability, and cybersecurity, the intersection of these domains remains conceptually fragmented and empirically underexplored. Prior studies have established that decision-making within organizational and technological systems is influenced by bounded rationality, contextual pressures, and information asymmetries (Sharma & Sharma, 2024; Simon, 1978). Likewise, scholarship on technology adoption has shown that compatibility—often a proxy for interoperability—is a decisive factor in whether organizations adopt new systems (Herath et al., 2020; Russo, 2024). However, few studies have systematically examined how interoperability functions as a *decision variable* within the process of adopting CTI solutions, even though such systems inherently depend on interconnectivity, data exchange, and shared intelligence. This gap limits both theoretical clarity and practical guidance for organizations seeking to enhance cybersecurity resilience through interoperable CTI architectures.

The existing literature also reveals a disjunction between theoretical models and real-world cybersecurity practices. While frameworks such as the Diffusion of Innovation

(DOI), Technology–Organization–Environment (TOE), and Technology Acceptance Model (TAM) offer valuable insights into adoption behavior, they inadequately account for the multidimensional role of interoperability in cybersecurity decision-making. The result is a persistent gap in understanding how technical, organizational, and cognitive factors interact when decision-makers evaluate CTI solutions. Without a unified conceptual framework, organizations risk adopting CTI technologies that optimize individual system performance but fail to support collective intelligence sharing, thereby undermining both operational efficiency and strategic defense coordination.

Purpose Statement

The purpose of this study is to examine the role of interoperability in organizational decision-making related to the adoption of Cyber Threat Intelligence (CTI) technologies. By synthesizing theories of decision-making and technology adoption—including DOI, TOE, TAM, the Task–Technology Fit (TTF) model, and the Unified Theory of Acceptance and Use of Technology (UTAUT)—this study aims to construct an integrative framework that captures how interoperability influences both the rationale and the process of CTI adoption. The study seeks to illuminate how decision-makers balance competing priorities such as security, efficiency, and collaboration when evaluating CTI systems that require interorganizational data exchange and technical compatibility.

This research further aims to bridge the divide between theoretical models and operational cybersecurity practice. Specifically, it seeks to identify how interoperability mediates the relationship between organizational readiness, environmental pressure, and perceived technological value in CTI adoption decisions. Through this conceptual synthesis, the study intends to contribute both to the scholarly understanding of cybersecurity adoption behavior and to the practical design of interoperable, decision-aligned CTI frameworks that enhance intelligence-sharing effectiveness and collective defense capability.

Significance Statement

This study holds theoretical significance by addressing a critical gap in the integration of decision-making and technology adoption theories within the cybersecurity context. By positioning interoperability as a central mediating construct, the research advances existing models such as DOI and TOE, which traditionally treat compatibility as a peripheral technical factor. The proposed framework extends these theories by explaining how interoperability influences organizational cognition, strategic judgment, and technology evaluation processes in CTI adoption. This reconceptualization deepens understanding of how decision-making operates under the unique pressures of cybersecurity environments characterized by high uncertainty, rapid innovation, and shared vulnerability.

Practically, the study provides actionable insights for policymakers, cybersecurity managers, and system architects seeking to design and implement interoperable CTI infrastructures. By clarifying how decision-makers evaluate interoperability trade-offs—balancing openness against security and efficiency against control—the research offers a roadmap for improving coordination among organizations engaged in threat intelligence sharing. Ultimately, the study contributes to the development of cybersecurity ecosystems that are not only technologically robust but also cognitively and organizationally aligned, fostering resilience through informed, interoperable decision-making.

Nature of the Study

The nature of this study is conceptual and exploratory, grounded in a synthesis of existing empirical and theoretical research. Drawing upon interdisciplinary perspectives from information systems, organizational theory, and cybersecurity studies, the analysis integrates behavioral decision-making theories with technology adoption frameworks to examine the mediating role of interoperability. This approach allows for a comprehensive understanding of CTI adoption as a multifactorial process shaped by cognitive biases, organizational contexts, and systemic dependencies. By combining insights from diverse literatures, the study identifies the conceptual mechanisms through which interoperability influences decision-making and adoption outcomes.

Methodologically, the research adopts a qualitative, theory-building orientation rather than an empirical testing model. Through critical synthesis and comparative analysis of existing models—specifically DOI, TOE, TAM, TTF, and UTAUT—the study develops an integrative conceptual framework applicable to cybersecurity environments. This framework not only refines theoretical constructs but also provides a foundation for subsequent empirical studies that can test, validate, and extend its propositions across different organizational contexts.

Relevant Studies

Recent scholarship has increasingly emphasized the interrelated dynamics of decision-making, interoperability, and cybersecurity—three domains that collectively underpin the effectiveness of contemporary organizational and technological systems. This section critically examines current research across these intersecting areas to elucidate their relevance to the present study. By synthesizing and contrasting existing empirical and conceptual contributions, the discussion identifies key points of convergence and divergence between prior scholarship and the focus of this investigation. In doing so, it highlights persistent gaps in the literature—particularly those concerning the integration of secure, interoperable infrastructures with evidence-based decision processes—and delineates opportunities for advancing both theoretical understanding and practical application in these domains.

Decision Making

Decision-making research has long sought to understand how individuals and organizations make choices under uncertainty, especially when faced with complex information environments. Building on the foundational work of Herbert A. Simon (1978), who introduced the notion of *bounded rationality*—the idea that decision-makers satisfice rather than optimize due to cognitive and informational constraints—contemporary scholars have extended these principles into domains such as consumer behavior, organizational management, and information systems. Recent work by Sharma and Sharma (2024) provides a particularly comprehensive account of these dynamics through a systematic review of paradoxes in consumer decision-making. Their study reviewed 233 publications spanning five decades (1972–2023), employing a co-citation cluster analysis and inferential synthesis to identify influential works and emergent research streams.

Sharma and Sharma (2024) identified two enduring paradoxes in the decision-making literature: the *paradox of rational choice* and the *paradox of variety*. The paradox of rational choice underscores that decision-makers frequently deviate from value-maximization principles due to contextual and environmental factors—an observation that resonates with Simon's theory of bounded rationality. Preference reversals, framing effects, and other violations of rationality demonstrate how real-world decisions often depend on

heuristics, social cues, and situational constraints rather than on stable preference structures. The paradox of variety, on the other hand, captures the tension between the human desire for diverse options and the cognitive overload that excessive choice can induce. Sharma and Sharma organized this paradox into three interrelated themes: variety-seeking behavior, choice overload, and the mechanisms by which decision-makers attempt to reconcile these opposing forces.

Although Sharma and Sharma's synthesis is rooted in consumer decision-making, its implications extend meaningfully into organizational and technological contexts. In cybersecurity decision-making—particularly within CTI adoption—professionals face analogous cognitive dilemmas. For instance, security analysts routinely experience "choice overload" when evaluating competing CTI platforms, threat feeds, or analytic models, each offering distinct capabilities but also introducing integration challenges. Similarly, "preference reversals" can occur when organizations initially prioritize advanced analytic capabilities but later favor interoperability or regulatory compliance once implementation risks become salient. These behaviors mirror the paradoxes outlined by Sharma and Sharma and reveal that bounded rationality operates not only at the consumer level but also within institutional decision environments.

By drawing these parallels, Sharma and Sharma's work contributes a valuable theoretical lens for understanding how decision-making processes influence technology adoption and cybersecurity strategy. Their findings underscore that decision outcomes are shaped as much by context and cognitive limitation as by rational evaluation of alternatives. This perspective is particularly relevant to CTI adoption, where interoperability constraints, information asymmetries, and time-sensitive pressures compel decision-makers to balance analytical rigor with expedient action. The paradoxes identified in consumer behavior thus offer a conceptual scaffold for analyzing the interplay between rationality, cognitive load, and organizational priorities in cybersecurity decision-making—a theme that recurs throughout subsequent sections of this study.

Technology Adoption and Organizational Factors

Technology adoption in cybersecurity-intensive environments is shaped not only by the technical attributes of innovations but also by the organizational and behavioral conditions under which decision-makers operate. Within this domain, Herath et al. (2020) and Russo (2024) provide complementary perspectives that, when examined together, illuminate how organizational dynamics, individual cognition, and system interoperability collectively influence adoption outcomes. Herath et al. (2020) advanced an integrative model grounded in Diffusion of Innovation (DOI) theory and the Technology–Organization–Environment (TOE) framework to examine the determinants of information-security-solution (ISS) adoption. Their model incorporated four innovation characteristics—compatibility, complexity, cost, and perceived gain—alongside organizational and environmental factors such as readiness, managerial support, external pressure, and visibility. Survey data from 368 information-systems managers across North American firms demonstrated that organizational and environmental factors exert greater influence on adoption than the intrinsic technological properties of the ISS itself. In particular, compatibility, conceptually analogous to interoperability, emerged as a critical adoption driver. These findings suggest that cybersecurity adoption decisions are embedded in broader organizational ecosystems of resources, culture, and regulatory expectation. For example, a firm's decision to implement a new endpoint-detection platform may hinge less on algorithmic sophistication and more on how seamlessly it integrates with existing monitoring infrastructure and compliance frameworks.

Expanding the discussion to the behavioral and perceptual level, Russo (2024) examined the adoption of generative-AI tools in software engineering using a mixed-methods design informed by the Technology Acceptance Model (TAM) and DOI theory. Russo found that compatibility with existing workflows was the predominant factor driving adoption, outweighing traditionally emphasized constructs such as perceived usefulness and social influence. This finding challenges core TAM assumptions by indicating that technological alignment with established routines and systems supersedes subjective utility perceptions in determining user acceptance. Translating this insight to cybersecurity contexts, particularly CTI adoption, suggests that decision-makers prioritize *interoperability* and *integration feasibility* over novelty or perceived innovativeness. For instance, an organization may favor a CTI platform that interfaces effortlessly with its current SIEM architecture and incident-response processes—even if competing tools promise greater analytic power—because interoperability reduces operational friction and cognitive uncertainty.

Taken together, Herath et al. (2020) and Russo (2024) underscore that technology adoption is not a linear function of perceived usefulness or technical merit but a strategic negotiation among organizational context, behavioral disposition, and systemic compatibility. Herath et al. illuminate the structural and environmental contingencies that frame adoption decisions, while Russo reveals the micro-cognitive mechanisms that privilege interoperability in user acceptance. Their combined insights point to a crucial theoretical implication: interoperability—long treated as a peripheral technical characteristic—functions as a central decision variable that links organizational readiness, task alignment, and individual trust in technology. This conceptual convergence directly informs the forthcoming analysis of how interoperability mediates decision-making in CTI adoption, serving as both a determinant of adoption success and a foundation for cross-organizational collaboration in cybersecurity ecosystems.

Interoperability and Platform Studies

Interoperability has emerged as a critical determinant of technological and organizational success in digitally networked environments. Defined broadly as the capacity of systems, applications, and organizational processes to exchange and meaningfully use information, interoperability underpins collaboration, innovation diffusion, and ecosystem stability across industries. Within information systems research, it is increasingly recognized as a multidimensional construct—encompassing technical (data and protocol compatibility), semantic (shared meaning and standards), and organizational (process and governance alignment) layers. These dimensions are not merely technical attributes but strategic enablers that shape decision-making, competitive positioning, and collective resilience in interconnected technology ecosystems.

Spaeth and Niederhöfer (2022) advanced this discussion by examining how platform sponsors determine compatibility strategies in multi-platform environments. Using a novel dataset of 157 platforms within the smart-home market, they employed a network-analytic approach based on an exponential random graph model to capture the structural processes influencing compatibility promotion. Their results revealed that platform-to-platform compatibility decisions are far from arbitrary; they are the outcome of deliberate strategic selection shaped by industry structure, market dominance, and standard complementarity. Specifically, platform sponsors tend to promote compatibility with dissimilar industry sectors and ecosystem niches to broaden market reach, while simultaneously maintaining alignment with shared open standards to preserve technical coherence. The majority of endorsements were directed toward giant platforms, allowing smaller actors to benefit from established network effects but also constraining openness at the technology level.

From a strategic perspective, Spaeth and Niederhöfer's findings illustrate that interoperability and openness are not synonymous; rather, organizations must balance collaborative integration with competitive differentiation. Their work reveals a duality in interoperability: it can expand network value and innovation potential, yet excessive dependence on dominant platforms can lead to structural rigidity and vulnerability concentration. These insights are highly relevant to cybersecurity and, by extension, to CTI ecosystems, which operate under comparable interdependencies. Just as smart-home platforms decide with whom to interconnect, cybersecurity actors—such as managed security providers, threat-intelligence vendors, and governmental agencies—must decide how to interoperate within shared intelligence networks. In the CTI context, interoperability decisions influence not only technical efficiency but also trust, control, and risk exposure. For example, an organization that integrates its CTI platform with a widely used external data-exchange standard such as STIX or TAXII benefits from enhanced situational awareness and collaborative detection capabilities, yet simultaneously assumes the security liabilities and dependency risks associated with that shared framework. Thus, the trade-offs identified by Spaeth and Niederhöfer resonate strongly in cybersecurity environments: maximizing interoperability promotes collective defense, but it may also propagate vulnerabilities across interconnected systems.

Viewed through this lens, interoperability emerges as a strategic decision variable at both micro- and macro-levels. At the organizational level, it determines how seamlessly technologies integrate into internal infrastructures; at the ecosystem level, it dictates how effectively platforms coordinate, compete, and share intelligence. When combined with the behavioral insights of decision-making research (Section 3.1) and the organizational adoption determinants identified by Herath et al. (2020) and Russo (2024) (Section 3.2), Spaeth and Niederhöfer's findings emphasize that interoperability is simultaneously a technical construct, a managerial concern, and a governance mechanism. This multifaceted understanding provides the conceptual foundation for the subsequent comparative analysis, which examines how decision-making frameworks and technology-adoption models collectively illuminate the role of interoperability in CTI solution adoption and cybersecurity resilience.

Cyber Threat Intelligence (CTI) Sharing and Adoption

Cyber Threat Intelligence (CTI) has become a cornerstone of modern cybersecurity strategy, enabling organizations to transition from reactive defense postures to proactive threat anticipation and mitigation. CTI refers to the systematic collection, analysis, and dissemination of data about adversaries, vulnerabilities, and attack patterns to enhance situational awareness and inform strategic and operational decision-making. The growing sophistication of cyber threats has prompted organizations to increasingly rely on CTI sharing frameworks and platforms, which facilitate the exchange of actionable intelligence across sectors and jurisdictions. However, as Alaeifar et al. (2024) emphasize, the effectiveness of CTI sharing is deeply contingent upon the degree of interoperability among technical systems, organizational processes, and policy environments.

Alaeifar et al. (2024) provided one of the most comprehensive contemporary analyses of CTI sharing, offering a taxonomy of CTI architectures, including centralized, federated, and hybrid models. Their study systematically examined the foundations of CTI, the mechanisms through which intelligence is exchanged, and the structural and operational challenges that impede sharing effectiveness. Among the key insights was the recognition that interoperability is both a *technical prerequisite* and a *strategic barrier* to efficient intelligence exchange. Differences in data standards, communication protocols, and trust governance frameworks often hinder seamless CTI integration across organizations. For

example, inconsistencies in structured data languages (e.g., STIX versions) or transfer protocols (e.g., TAXII implementations) can cause intelligence latency, duplication, or misinterpretation, reducing the value of shared data.

Alaeifar et al. also highlighted how CTI sharing intersects with organizational decision-making, noting that the value of intelligence depends not only on its accuracy or timeliness but also on how decision-makers interpret and operationalize it within their institutional contexts. Yet, while their research mapped the technical and managerial contours of CTI interoperability, it stopped short of analyzing *how* decision-makers weigh interoperability considerations when selecting or implementing CTI solutions. For instance, organizations frequently face trade-offs between maintaining control over sensitive threat data and participating in federated CTI networks that require higher levels of openness. The decision to adopt a particular CTI model therefore involves balancing the desire for interoperability-driven collaboration with the need for information sovereignty and security assurance.

The omission of explicit analysis on interoperability as a *decision-making variable* exposes an important gap in the CTI literature. As the findings of Herath et al. (2020) and Russo (2024) suggest in other technological contexts, compatibility and integration capabilities play a decisive role in adoption success—yet few CTI studies have systematically explored how these considerations are evaluated during technology selection and implementation. For example, a security operations center (SOC) might prefer a CTI platform that supports open exchange formats (e.g., STIX/TAXII) to enhance collaboration but may ultimately select a proprietary system that aligns better with internal infrastructure and governance requirements. Such decisions reflect bounded rationality and contextual prioritization similar to those observed by Sharma and Sharma (2024) in decision-making paradoxes.

In synthesizing these insights, Alaeifar et al.'s (2024) work affirms that CTI sharing is both a technological and a sociotechnical phenomenon—dependent not only on the interoperability of systems but also on the cognitive, organizational, and environmental factors that govern adoption behavior. Interoperability thus emerges as the *connective tissue* linking technical design with human judgment and institutional trust. This conceptual recognition sets the stage for the comparative analysis that follows, which examines how major technology adoption models—such as DOI, TOE, TAM, TTF, and UTAUT—can be applied to CTI contexts to explain how interoperability mediates the relationship between decision-making and cybersecurity innovation adoption.

Conceptual Synthesis

The preceding review reveals that decision-making, technology adoption, interoperability, and cybersecurity are conceptually intertwined through both behavioral and structural mechanisms. Across the literature, decision-making is characterized by bounded rationality, contextual sensitivity, and the persistent tension between analytical rigor and practical constraint (Sharma & Sharma, 2024). Within this cognitive framework, individuals and organizations often navigate competing priorities—such as efficiency, control, and security—under conditions of incomplete information. In cybersecurity contexts, these dynamics are amplified: analysts and organizational leaders must make rapid, high-stakes decisions amid volatile threat landscapes, information asymmetry, and systemic complexity. The result is a decision environment where rational optimization yields to satisficing—an equilibrium of feasible, timely, and risk-adjusted choices.

At the organizational level, technology adoption theories such as DOI, TOE, and TAM reinforce this behavioral complexity by identifying compatibility, complexity, and contextual pressures as key determinants of adoption (Herath et al., 2020). Russo (2024)

expanded this understanding by demonstrating that *compatibility*—conceptually aligned with interoperability—outweighs traditional predictors such as perceived usefulness or social influence. Collectively, these findings highlight that organizations adopt technologies not solely because they offer new capabilities, but because they integrate effectively into existing infrastructures and workflows. This insight reframes interoperability from a technical consideration to a behavioral determinant that shapes confidence, trust, and perceived feasibility in the decision-making process.

At the ecosystem level, interoperability emerges as both a strategic asset and a systemic constraint. Spaeth and Niederhöfer (2022) showed that organizations within interconnected technological ecosystems make compatibility decisions strategically, balancing openness with control to maximize network value while mitigating dependency risks. Their findings demonstrate that interoperability simultaneously enables collaboration and introduces new vulnerabilities—a duality mirrored in cybersecurity ecosystems where interdependence among platforms can amplify both collective defense and shared exposure. Within CTI sharing networks, as discussed by Alaeifar et al. (2024), this trade-off manifests through technical and organizational barriers to information exchange. Variations in data standards, trust frameworks, and architectural models (centralized, federated, hybrid) require decision-makers to continually negotiate between interoperability, security assurance, and operational autonomy.

Synthesizing these perspectives across cognitive, organizational, and systemic levels suggests that interoperability functions as the conceptual nexus linking decision-making and technology adoption in cybersecurity. It simultaneously constrains and enables rational action, shaping how decision-makers assess risk, value, and feasibility in adopting CTI solutions. Decision-making theories explain the *how* of these choices—the bounded rationality and trade-offs at play—while technology adoption models explain the *why*—the contextual and structural conditions under which adoption occurs. Yet existing frameworks insufficiently capture interoperability's dual role as both a *determinant* and *outcome* of adoption. This synthesis therefore identifies a critical theoretical gap: the need for an integrative model that positions interoperability as a mediating construct that aligns human reasoning, organizational strategy, and systemic integration.

In practical terms, this synthesis implies that the success of CTI adoption—and by extension, organizational cybersecurity resilience—depends on the organization's ability to institutionalize interoperability as both a design principle and a decision criterion. By conceptualizing interoperability as a dynamic interaction among technical capability, human cognition, and organizational context, future research can develop more predictive and adaptive models of technology adoption in cybersecurity ecosystems. This insight provides the intellectual foundation for the forthcoming Comparative Analysis, which evaluates how major technology adoption frameworks collectively elucidate the role of interoperability and decision-making in CTI adoption.

Comparative Analysis of Technology Adoption Models in CTI Contexts

Understanding Cyber Threat Intelligence (CTI) adoption requires a careful examination of how existing technology adoption models explain, support, or fail to capture the distinctive challenges that characterize cybersecurity environments. Although frameworks such as the Diffusion of Innovation (DOI) theory, the Technology–Organization–Environment (TOE) framework, the Technology Acceptance Model (TAM), the Task–Technology Fit (TTF) model, and the Unified Theory of Acceptance and Use of Technology (UTAUT) offer important conceptual tools, their explanatory power varies substantially when applied to the context of CTI. CTI adoption is shaped by dynamic threat conditions, interorganizational dependencies, the need for interoperable data-sharing infrastructures, and heightened

decision-making pressures—conditions that extend beyond the scope of traditional adoption settings. Thus, a comparative analysis of these models reveals not only their contributions but also the conceptual limitations that persist when they are applied to high-stakes cybersecurity technologies.

The Diffusion of Innovation (DOI) theory (Rogers, 2003) provides one of the earliest and most widely applied frameworks for understanding innovation uptake, emphasizing attributes such as relative advantage, compatibility, complexity, trialability, and observability. In CTI contexts, *compatibility* is particularly salient because organizations rely on seamless integration with existing security tools, standardized data formats (e.g., STIX), and trusted information-exchange protocols (e.g., TAXII). While DOI offers a valuable lens for assessing how these innovation characteristics shape adoption intent, it lacks the organizational and ecosystem-level nuance needed to account for regulatory pressures, threat intelligence consortia, and cross-organizational coordination demands. As a result, DOI partially explains CTI adoption but does not fully address the strategic and cooperative aspects integral to CTI ecosystems.

The Technology–Organization–Environment (TOE) framework (Tornatzky & Fleischer, 1990) adds an important contextual dimension by incorporating organizational readiness, environmental pressures, and institutional drivers. TOE is especially relevant for CTI adoption because organizations often face external mandates—such as compliance requirements, industry standards, or participation in Information Sharing and Analysis Centers (ISACs)—that compel interoperability and coordinated threat intelligence sharing. TOE also captures internal determinants such as resource allocation, leadership commitment, and the ability to absorb and apply complex intelligence data. However, despite its strengths, TOE treats compatibility largely as a technical factor rather than as a determinant of collaborative capability or security governance, thereby overlooking the sociotechnical interdependencies central to CTI.

The Technology Acceptance Model (TAM) (Davis, 1989) shifts focus to individual perceptions by highlighting the roles of perceived usefulness and perceived ease of use. These constructs are important in CTI adoption because analysts and security teams must trust that a CTI platform enhances situational awareness and supports efficient decision-making under time pressure. Yet empirical evidence, such as that presented in Russo (2024), suggests that compatibility and integration feasibility frequently outweigh perceived usefulness in complex technological environments. TAM therefore provides insights into cognitive evaluations but underestimates the organizational and ecosystemic requirements of CTI adoption—particularly the critical role of interoperability in shaping user perceptions of system value.

The Task–Technology Fit (TTF) model (Goodhue & Thompson, 1995) introduces a functional perspective, proposing that technology is adopted when it aligns well with the tasks users must perform. In CTI contexts, task fit includes the platform's ability to synthesize heterogeneous threat data, support collaborative analytics, and generate actionable intelligence in real time. Interoperability enhances task–technology fit by enabling CTI systems to connect with security information and event management (SIEM) platforms, vulnerability scanners, and automated response tools. However, TTF does not explicitly address the external interdependencies or governance structures that shape CTI use, limiting its explanatory scope.

Finally, the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003) integrates several earlier models and introduces the constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions. UTAUT offers particular value in CTI settings due to its focus on social influence, which aligns with the way CTI adoption often diffuses through trust-based networks and shared-sector norms. For instance, when a major federal agency or sector-leading institution adopts

a particular CTI protocol, peer organizations may follow suit to ensure data compatibility and maintain operational alignment. Nevertheless, while UTAUT captures some collaborative and institutional dynamics, it does not explicitly account for interoperability's dual role as both a precondition of successful CTI adoption and a driver of ecosystem cohesion. Taken together, the comparative analysis reveals that while each adoption framework contributes meaningful insights, none fully encapsulates the interplay between decision-making, interoperability, and CTI adoption. DOI and TOE address contextual and structural factors; TAM and UTAUT emphasize cognitive and behavioral determinants; TTF clarifies alignment between CTI tasks and system capabilities. Yet interoperability—central to CTI's value proposition—remains under-theorized across all models. As a result, these frameworks must be synthesized and extended to better reflect the sociotechnical complexity, interorganizational dependencies, and real-time decision pressures inherent to cybersecurity environments. This analysis underscores the need for future research to explore how interoperability operates not simply as a technical requirement but as a foundational construct influencing technology adoption and cybersecurity decision-making.

Conclusion

The synthesis of prior research confirms that decision-making, interoperability, and cybersecurity adoption are deeply interdependent constructs. Across cognitive, organizational, and ecosystem levels, the literature demonstrates that decisions concerning technology adoption are not purely rational but are shaped by bounded rationality, contextual constraints, and perceptions of interoperability. Compatibility and integration feasibility consistently emerge as pivotal factors influencing adoption intent and success, underscoring that organizations adopt technologies not solely for innovation value but for their ability to interconnect and co-function within larger information ecosystems.

The analysis also reveals that existing adoption models provide valuable but incomplete explanations for CTI adoption behavior. While frameworks such as DOI and TOE capture contextual influences, and TAM and UTAUT highlight individual perceptions, none fully address interoperability's dual role as both a determinant and outcome of adoption. Consequently, this study concludes that future theoretical development must explicitly incorporate interoperability as a central construct—one that mediates between cognitive decision processes and technological implementation—to more accurately reflect the realities of cybersecurity innovation and intelligence sharing.

Recommendations for Future Research

Future research should empirically investigate how decision-makers assess and prioritize interoperability when adopting CTI solutions. A Qualitative Case Study approach would be particularly valuable for exploring how different organizations conceptualize interoperability in their cybersecurity strategies and how contextual factors—such as organizational culture, regulatory mandates, and resource availability—shape these decisions. Case studies could yield nuanced insights into the lived decision-making experiences of cybersecurity professionals, revealing how interoperability considerations evolve during technology selection, integration, and performance evaluation.

Alternatively, a Modified Delphi Study or Focus Group Qualitative Research design could be employed to achieve consensus among experts on the critical dimensions and metrics of interoperability in CTI adoption. The Delphi method would allow researchers to systematically capture expert judgment across diverse sectors, refining conceptual frameworks through iterative feedback. Focus groups, by contrast, would facilitate dynamic dialogue among practitioners, uncovering the tacit reasoning, challenges, and heuristics that guide decision-making under uncertainty. Additionally, an Action Research approach could

be used to collaboratively design and test interoperability strategies within organizations, linking theoretical insight with applied improvement in real-world cybersecurity practices. Together, these approaches would strengthen both the theoretical robustness and the practical applicability of future CTI interoperability research.

References

Alaeifar, S., Radanliev, P., & De Roure, D. (2024). Cyber threat intelligence sharing: Architectures, challenges, and future directions. *Computers & Security, 139,* 103690.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly, 19*(2), 213–236.

Herath, T., Chen, R., Wang, J., Banjanovic, A., & Rao, H. R. (2020). Adoption of information security solutions: An integrative model. *Decision Support Systems, 131*, 113248.

Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.

Russo, M. (2024). Adoption of generative artificial intelligence tools in software engineering: Examining individual, technological, and social factors. *Information Systems Frontiers*, Advance online publication.

Sharma, A., & Sharma, S. (2024). Paradoxes in consumer decision making: A systematic review and research agenda. *Journal of Business Research, 172*, 114086.

Simon, H. A. (1978). Rationality as process and as product of thought. *American Economic Review, 68*(2), 1–16.

Spaeth, S., & Niederhöfer, A. (2022). Platform compatibility and standardization strategies in the smart home ecosystem: A network analysis approach. *Technological Forecasting & Social Change, 185*, 122099.

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

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.