PriMera Scientific Engineering
Volume 6 Issue 2 February 2025
DOI: 10.56831/PSEN-06-177
ISSN: 2834-2550

Optimizing AI and Human Expertise Integration in Cybersecurity: Enhancing Operational Efficiency and Collaborative Decision-Making

A Systematic Literature Review of the Symbiotic Relationship Between AI, Automation, and Human Expertise in Cyber Defense Operations

Type: Literature Review
Received: December 11, 2024
Published: January 30, 2025

Citation:
Mehdi Saadallah., et al. "Optimizing AI and Human Expertise Integration in Cybersecurity: Enhancing Operational Efficiency and Collaborative Decision-Making". PriMera Scientific Engineering 6.2 (2025): 03-20.

Mehdi Saadallah*, Abbas Shahim, and Svetlana Khapova

Vrije Universiteit Amsterdam, Amsterdam, Netherlands

***Corresponding Author:** Mehdi Saadallah, Vrije Universiteit Amsterdam, Amsterdam, Netherlands.

Abstract

This systematic literature review draws into multiple theories, such as resource-based view, sociotechnical systems theory, technology acceptance model, dynamic capabilities theory, contingency theory, cybernetic, and human machine interaction Theory, to explore how artificial intelligence, automation, and human expertise can optimize cybersecurity operations through complementary roles and continuous feedback mechanisms. The outcomes of this study introduce two conceptual models that respond to this objective. The symbiotic integration framework, which promotes continuous interaction and ethical oversight between AI systems and human operators, and the symbiotic maturity integration model, which maps the progressive stages of AI-human integration from initial to optimized. This study addresses the literature gaps related to the symbiotic relationship between AI and human expertise in cybersecurity operations, providing a pathway for adaptive, resilient cybersecurity practices that align with organizational values and enhance defensive capabilities in a dynamic threat landscape.

Keywords: Systematic literature review; Automation in Cyber Defense; Artificial Intelligence Integration; AI-Human Interaction; Operational Effectiveness; AI in Threat Detection; Cybersecurity Decision-Making

Introduction

The recent development of cybersecurity threats has raised concerns across sectors, requiring organizations to explore new defensive mechanisms [1, 2]. Although the human-centric approach remains effective in many traditional scenarios, it falls short of addressing the increasing volume and complexity of cyberattacks that require rapid, data-driven responses [3-5]. Recent studies have explored that integrating artificial intelligence (AI) into cybersecurity enhances threat detection, streamlines processes, and supports predictive analysis [6-8]. However, this integration raises challenges in terms of aligning AI systems with human expertise, building trust, efficient collaborative models, and effective decision-making [9, 10]. To address these challenges, our systematic literature review (SLR) addresses the following issues: *How can the integration of AI, automation, and human expertise into cybersecurity be optimized to enhance operational effectiveness and collaborative decision-making across diverse organizational contexts?* This question examines how AI-human tandem can collaborate, adapt, and scale to address cyberattacks [11-13]. The authors drew on multiple theoretical frameworks, such as resource-based view (RBV) [14], sociotechnical systems theory (STS) [15], technology acceptance model (TAM) [16], dynamic capabilities theory (DCT) [17], contingency theory (CT) [18], human-machine interaction (HMI) theory [19], and cybernetic theory [20], to analyze and construct practical models for cybersecurity enhancement that is inclusive of both AI and human expertise. This literature review contributes to the core of the literature using two conceptual models. First, the symbiotic integration framework (SIF), as delineated on Figure 4 structures the feedback loops between AI systems and human operators, fostering adaptive learning and ethical alignment in real-time threat scenarios. The second conceptual model, the symbiotic maturity integration model (SMIM), as delineated on Figure 5 highlight from initial to fully optimized integration the roadmap for organizations to scale AI-human collaboration through progressive maturity stages. These models provide a consolidated view of theoretical and operational best practices, strategies for collaborative decision-making, and scalability challenges in cybersecurity [19, 21]. The study is structured as follows: Section 2 outlines the SLR methodology; Section 3 discusses the theoretical frame-works guiding this analysis; Section 4 details the thematic analysis findings; Section 5 introduces the SIF and SMIM models; Section 6 interprets these findings; and Section 7 concludes with recommendations for future research and practice.

Methodology

Guided by the preferred reporting items for systematic reviews and meta-analyses (PRISMA) framework, this SLR leverages a rigorous and transparent process to analyze the fragmented literature and gaps around the integration of AI, automation, and human expertise into cybersecurity [22-24]. The PRISMA has been applied to manuscripts hosted on major academic databases including IEEE Xplore, Scopus, Web of Science, SpringerLink, and Google Scholar recognized for their comprehensive coverage of AI cybersecurity, and human-computer interaction research [25-29]. A combination of keywords such as “AI in cybersecurity,” “human expertise and automation,” “cybersecurity automation,” and “organizational maturity in AI” was used with a combination of Boolean operators to refine the relevance of the search between 2014 and 2024 to capture recent advancements. We limited our search to English-language articles to avoid translation bias [30]. We prioritize studies that examine AI, automation, and human expertise in cybersecurity operations. As our field of study is nascent, we included theoretical studies related to RBV, STS, TAM, DCT, CT, HMI, and cybernetics in our inclusion criteria. This allowed us to successfully bridge the AI, automation, and human expertise gaps in cybersecurity operations [11, 31]. We excluded studies that were not related to AI, automation, or human expertise in cybersecurity; addressed non-cybersecurity topics; and were published before 2014 unless foundational. This refined PRISMA selection process, documented in Figure 1, started from an initial 1200 studies, in which 850 studies were further reviewed, excluding irrelevant and duplicate papers. 130 articles were shortlisted after applying the inclusion criteria, and 60 articles were selected for in-depth analysis. By examining the references of selected studies, 16 additional articles were added to the dataset. This snowballing technique allowed us to obtain a final dataset of 77 studies. An extract of the standard extraction form is delineated in Table 1, where the inclusion reason of each study is presented. Two conceptual models that provide a structured approach to enhance AI-human collaboration in cybersecurity are developed from the thematic analysis conducted to identify recurring themes, as detailed in section 4. The SIF and SMIM are detailed in section 5 [32-34].

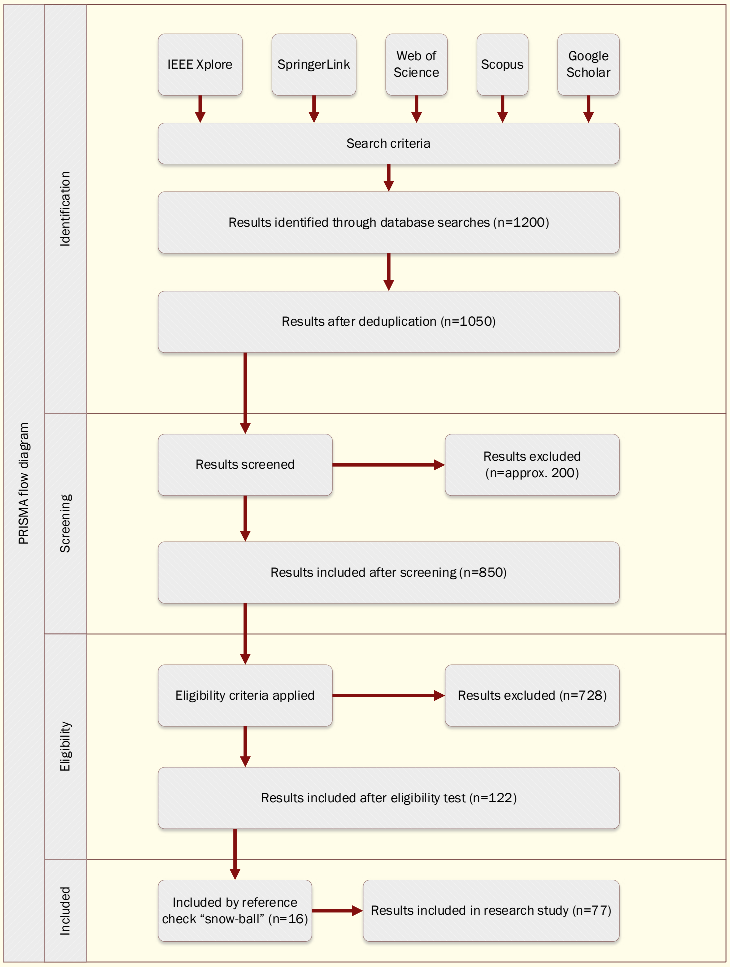

PRISMA flow diagram
Identification
Screening
Eligibility
Included
IEEE Xplore
SpringerLink
Web of Science
Scopus
Google Scholar
Search criteria
Results identified through database searches (n=1200)
Results after deduplication (n=1050)
Results screened
Results excluded (n=approx. 200)
Results included after screening (n=850)
Eligibility criteria applied
Results excluded (n=728)
Results included after eligibility test (n=122)
Included by reference check "snow-ball" (n=16)
Results included in research study (n=77)

Figure 1: Data structure of the PRISMA process.

Reference	***Inclusion reason***
[1]	This study focuses on the state of the art in cybersecurity, highlighting challenges and future directions. This aligns with the literature's aim of exploring how AI and human expertise can optimize cybersecurity operations.
[2]	Discusses theoretical approaches and practical solutions to cybersecurity challenges in the AI era, directly linking to the integration of AI systems and human expertise.
[3]	Covers the design and implementation of cybersecurity operation centers, focusing on the concept of creating resilient and operational frameworks for AI and human collaboration.
[4]	Explores cybersecurity incident response and qualitative themes to provide foundational insights for human-AI collaboration and feedback mechanisms.
[5]	Investigate human factors in cybersecurity, which is an essential component of integrating Sociotechnical Systems Theory into the analysis.
[6]	This study survey machine learning-based intrusion detection, reflecting the importance of AI capabilities in adaptive and resilient cybersecurity practices.
[7]	Focuses on automated, context-aware risk management for vulnerability management, relevant to the study's emphasis on dynamic capabilities and contingency planning.

[8]	The integration of AI into cybersecurity is discussed, directly linking to the symbiotic relationship between AI and human expertise.
[9]	Explores ethical concerns and applications of AI in cybersecurity, which supports the research's emphasis on ethical oversight in the SIF.
[10]	Highlights ethical challenges in applying AI to cybersecurity, providing critical input to the SIF's ethical dimension.
[11]	Emphasizing data-driven intelligence in cybersecurity, which aligns with previous studies' focus on leveraging AI to realize enhanced defensive capabilities.
[12, 13]	Discusses synergies between human expertise, automation, and AI, directly supporting the development of the SMIM model.
[14]	Focuses on cybersecurity resilience, which is relevant to the adaptive and resilient practices highlighted in this review.
[15]	Provides a socio-technical perspective, which is essential for incorporating sociotechnical systems theory into research.
[16]	This study establishes a model for user acceptance of cybersecurity training, directly supporting the exploration of the technology acceptance model (TAM) theory and its application in human-machine interactions in cybersecurity.
[17]	This section discusses the dynamic capabilities theory, which is a core theoretical framework to analyze how AI-human collaboration can adapt and evolve in dynamic cybersecurity environments.
[18]	A contingency framework for cyberattack management that aligns with contingency theory and provides adaptive responses to dynamic threats.
[19]	Examines the effects of human feedback on interactive machine learning are examined, directly supporting the need for continuous feedback mechanisms and trust-building between AI systems and human operators.
[20]	Revisits cybernetics principles to improve safety, quality, and cybersecurity, contributing insights into STS and how AI-human systems can be integrated.
[21]	Explores Human-AI symbiosis in organizational decision-making, a foundational concept for developing the Symbiotic Integration Framework (SIF) to optimize cybersecurity operations.
[22]	Provide updated PRISMA guidance for systematic reviews, ensuring methodological rigor in the review process and aligning with best practices in literature synthesis.
[23-27]	Inspirational literature reviews that leverage a research design similar to that adopted in the current systematic literature review
[28]	Explores maturity models for cybersecurity to support the development of the SMIM.
[29]	Discusses tensions in implementing digital security governance and informing strategies for overcoming integration challenges in AI-human systems.
[30]	Explores knowledge generation at the intersection of AI and cybersecurity, contributing to ethical and strategic oversight in AI-human collaboration.
[31]	In this study, we focus on AI-based quantum-safe cybersecurity and provide insights into advanced AI applications in secure system design.
[32]	Outlines the conceptual design for thematic analysis and supports the development of conceptual models such as the SIF and SMIM.
[33]	Step-by-step thematic analysis for model development, directly applicable to qualitative methodologies used in the research.
[34]	Provides methodological rigor in qualitative research, ensuring robust and credible conceptual frameworks and theme aggregation.
[35]	Highlights the competitive advantage of investing in cybersecurity and reinforces the strategic value of AI-human collaboration.
[36]	Explores behavioral data for adaptive cybersecurity, which is directly linked to the role of AI in augmenting human decision-making.

[37]	The proposed model focuses on agile cybersecurity incident response using real-time analytics, which aligns with the dynamic capabilities highlighted in this SLR.
[38]	Discusses explainable AI in cybersecurity that aligns with the ethical oversight and interpretability emphasized in the SIF.
[39]	This study investigates agile cybersecurity incident response, focusing on the role of big data analytics and dynamic capabilities, directly contributing to the Dynamic Capabilities Theory (DCT) and adaptive security practices discussed in the literature review.
[40]	Explores knowledge management frameworks in AI-driven systems to enhance collaborative decision-making processes.
[41]	Discusses AI applications in cybersecurity and reinforce automation’s role in augmenting human capabilities.
[42]	Examines challenges in implementing AI for IT management, aligning with the research’s focus on scalability and integration challenges.
[43]	Explores dynamic perspective for countering cyber-enabled industrial espionage, aligning with Sociotechnical Systems Theory (STS) and emphasizing the integration of human expertise and artificial intelligence systems in managing sophisticated cyber threats.
[44]	TAM is applied to learning management systems, providing theoretical support for user acceptance in AI-human collaboration.
[45]	A meta-synthesis of dynamic capabilities in cybersecurity intelligence aligns with the review’s objective to identify adaptive and resilient cybersecurity practices, particularly emphasizing the complementarity of human expertise and AI.
[46]	This study focuses on determining system requirements for human-machine integration in cybersecurity incident response, supporting HMI Theory and continuous feedback mechanisms.
[47]	Applies artificial neural networks for cyber threat detection, highlighting the role of predictive analytics in enhancing cybersecurity operations, which is ties to the RBV theory.
[48]	Discusses AI-enhanced incident response and recovery strategies, providing actionable insights into operational efficiency and aligning with the study’s focus on collaborative frameworks.
[49]	Explores continual learning with deep architectures that align with the SIF by emphasizing real-time learning and adaptation in AI systems.
[50]	Focuses on embracing changes in deep neural networks through continual learning, which supports the integration of adaptive AI systems into dynamic cybersecurity environments.
[51]	Investigate data pipelines for AI model development, optimizing efficiency and performance, and directly supports the operational efficiency objectives discussed in this SLR.
[52]	The study examines meta-adaptation strategies in cyberphysical systems, which are essential for understanding adaptive mechanisms and progressive maturity in AI-human collaboration.
[53]	Addresses adaptation timing in self-adaptive systems and provides insights into strategic planning for real-time AI-human collaboration.
[54]	Evaluates cybersecurity platforms and provides practical insights into decision-making frameworks for implementing AI-driven systems.
[55]	Introduces reference-based AI decision support, thereby reinforcing the need for strategic decision-making and human oversight in AI systems.
[56]	Explores computational complexity in human decision-making and highlights the cognitive aspects of human-AI collaboration.
[57]	Discusses how AI complements or supplements the human workforce, supporting HMI Theory and the collaborative environment outlined in the literature.
[58]	Highlights the importance of human oversight in AI governance, directly supporting the ethical dimension of the Symbiotic Integration Framework (SIF).

[59]	Develops an EPIC framework for integrative collaboration, offering insights into the continuous feedback mechanisms required for effective human-AI systems.
[60]	Explores interfaces for interactive machine learning, emphasizing the role of human-AI collaboration and continuous learning systems.
[61]	AI and machine learning applications in redefining cybersecurity and strengthening the operational efficiencies highlighted in this research.
[62]	Develop design principles for scalable AI integration, aligning with the SMIM model's progressive stages of AI-human collaboration maturity.
[63]	Focuses on pilot testing human-work interaction designs, contributing to the iterative development of human-machine integration systems.
[64]	This highlights the need for collaborative intelligence in cybersecurity, which reinforces the review's focus on complementarity between AI and human expertise.
[65]	Investigate trust calibration in AI systems, directly supporting the study's emphasis on ethical oversight and human-AI trust building.
[66]	Explores AI-assisted security alert data analysis, highlighting the integration of imbalanced learning methods into practical cybersecurity applications.
[67]	Opens the black box for AI in medicine, thereby providing transferable insights into transparency and explainability in AI-driven cybersecurity frameworks.
[68]	Focusing on leveraging human factors in cybersecurity, this study provides an integrated methodological approach to STS.
[69]	Discusses building trust in human-machine partnerships, addressing the ethical and trust-building dimensions critical to the Symbiotic Integration Framework.
[70, 71]	Presents the vulnerability management program, which is aligned with contingency planning and adaptive strategies for cybersecurity.
[72]	An AI-driven framework for scalable network slice management is developed, reflecting the scalability objectives of the SMIM model.
[73]	Explores the integration of AI into management information systems, focusing on the efficiency and adaptability that are critical for cybersecurity operations.
[74]	Optimized human inputs for better human-AI interaction, supporting effective collaborative decision-making processes.
[75]	Discusses fairness and accountability in AI systems and contributes to the study's ethical oversight focus.
[76]	Explores explainable AI for IIoT security and provides insights into the interpretability required for ethical and operational AI integration.
[77]	Investigate trust in intrusion detection systems and reinforce the importance of user trust in AI-human collaborative systems.
[78]	Analyzes organizational readiness for AI adoption and SMIM's implementation of the progressive stages.

Table 1: Data structure of the selected dataset.

Theoretical foundations

The focus of this literature review is on the symbiotic relationship between artificial intelligence (AI) and human expertise in cybersecurity operations; thus, we draw into multiple theories, such as the resource-based view (RBV), which emphasizes how organizations can gain competitive advantage from its unique resources in our case the combination of AI, automation, and human expertise to strengthen cybersecurity defenses [14, 35]. This theory further accentuates our SIF model delineated on the figure 5, demonstrating how AI augments human decision-making processes in threat detection and task automation, resulting in an enhanced organizational resilience and strategic advantage [2]. Our analysis using the sociotechnical systems theory (STS) highlights the continuous interaction between AI systems and human operators, where AI handles routine tasks, and humans provide contextual insights for complex decisions, resulting in a win-win situation [13]. These interaction points coupled with a feedback loop form a key building block of the SIF that facilitates learning and adaptation between human and AI systems [15, 36]. The third, fourth, and fifth theories, i.e., the technology acceptance model (TAM), focus on how factors such as perceived usefulness and ease of use, can influence the adoption of AI in cybersecurity. We leverage the dynamic capabilities theory (DCT) mandating organizations to adapt their posture to address the cybersecurity landscape [17, 37]. Contingency theory (CT) highlight that there is no universal approach to organizational structure and that strategies should be tailored to specific circumstances [18]. The SMIM delineated in Figure 5 leverages principles from these three theories and highlights a progressive, flexible, and customized roadmap for adopting a collaborative model between AI and humans, which will result in acceptance of the technology among cybersecurity professionals, simplified workflows, enhanced decision-making, and scaled AI-human integration [16, 38-41]. Lastly, human-machine interaction (HMI) and cybernetics theory principles, such as feedback loops, control systems, and enhanced adaptability and accuracy, are integrated into the SIF [19, 20]. This continuous feedback enables AI to learn from historical data and real-time human interactions, thereby creating a responsive and adaptive cybersecurity framework [42]. The different lenses of each of these theories provide depth to our literature on combining AI capabilities and human expertise to strengthen cybersecurity defenses.

Thematic Analysis

This systematic review identified key themes central to integrating AI, automation, and human expertise in cybersecurity. These themes, informed by theoretical frame-works such as RBV [14, 35], STS [15, 43], TAM [44], DCT [45], and CT [18], reveal patterns that clarify the collaborative dynamics between AI systems and human expertise. The thematic analysis uses first-order concepts, second-order themes, and aggregate dimensions following the Gioia methodology [34] to map these relationships.

Integration and Optimization of AI and Human Expertise

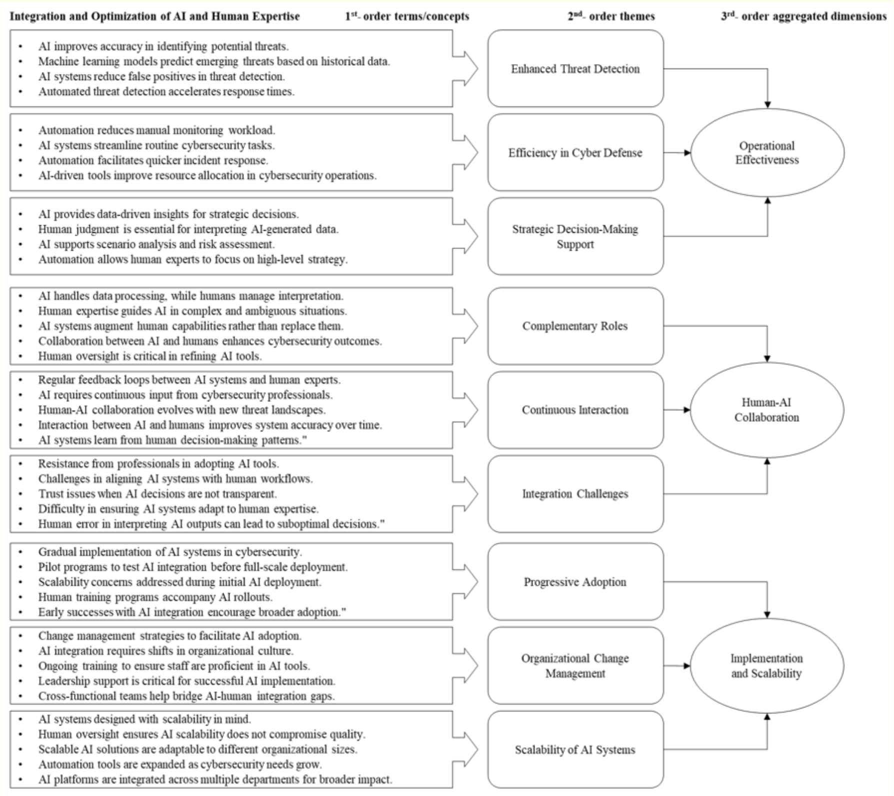
The first theme delineated in the Figure 2 highlights that the integration of AI and human expertise enhances operational effectiveness, collaboration, and scalability. RBV explains how organizations can build the unique competitive advantage through enhanced threat detection, efficiency, and decision-making by combining advanced AI technologies and skilled human expertise. STS complements the RBV perspective and provides a view of the complementary roles that technical systems (AI) and social systems (human expertise) play toward continuous interaction and adaptability. The TAM highlights how criteria such as usefulness and ease of use, influence the cybersecurity professional acceptance of AI systems, which results in successful implementation and scalability in cybersecurity operations.

Operational Effectiveness

The first aggregate is related to the operational effectiveness of the integration of AI and human expertise in cybersecurity in terms of improved threat detection, reduced false positives, and more efficient incident response [6, 7, 46]. We explore this theme through the lens of RBV and STS, where the literature points out that combining AI's ability to process a large amount of security events with human interpretive skills forms a unique resource that strengthens an organization's cybersecurity posture [35]. Lee [47] demonstrated that AI-driven systems improve the accuracy of identifying threats, thereby reducing the likelihood of successful cyberattacks and enabling human experts to focus on complex tasks. Sarker [11] reinforced the STS principles by calling for a balance between technical (AI) and social (human) systems, demonstrating that human oversight helps refine AI outputs, maintain operational goals, and adapt to dynamic security challenges [15].

Human-AI Collaboration

Human–AI collaboration is a recurring theme in the literature. We analyzed this theme through the lens of STS, where the complementary relationship between AI and human expertise provides multiple benefits. For example, Sarker [11] emphasized that continuous interaction between AI and human operators ensures that AI systems benefit from human feedback and remain effective and responsive to emerging threats [15]. HMI theory also applies to this theme, where Jarrahi [21] high-lighted that humans provide


Integration and Optimization of AI and Human Expertise
1st- order terms/concepts
2nd- order themes
3rd- order aggregated dimensions
Enhanced Threat Detection
Efficiency in Cyber Defense
Strategic Decision-Making Support
Operational Effectiveness
Complementary Roles
Continuous Interaction
Integration Challenges
Human-AI Collaboration
Progressive Adoption
Organizational Change Management
Scalability of AI Systems
Implementation and Scalability

- AI improves accuracy in identifying potential threats.
- Machine learning models predict emerging threats based on historical data.
- AI systems reduce false positives in threat detection.
- Automated threat detection accelerates response times.

- Automation reduces manual monitoring workload.
- AI systems streamline routine cybersecurity tasks.
- Automation facilitates quicker incident response.
- AI-driven tools improve resource allocation in cybersecurity operations.

- AI provides data-driven insights for strategic decisions.
- Human judgment is essential for interpreting AI-generated data.
- AI supports scenario analysis and risk assessment.
- Automation allows human experts to focus on high-level strategy.

- AI handles data processing, while humans manage interpretation.
- Human expertise guides AI in complex and ambiguous situations.
- AI systems augment human capabilities rather than replace them.
- Collaboration between AI and humans enhances cybersecurity outcomes.
- Human oversight is critical in refining AI tools.

- Regular feedback loops between AI systems and human experts.
- AI requires continuous input from cybersecurity professionals.
- Human-AI collaboration evolves with new threat landscapes.
- Interaction between AI and humans improves system accuracy over time.
- AI systems learn from human decision-making patterns."

- Resistance from professionals in adopting AI tools.
- Challenges in aligning AI systems with human workflows.
- Trust issues when AI decisions are not transparent.
- Difficulty in ensuring AI systems adapt to human expertise.
- Human error in interpreting AI outputs can lead to suboptimal decisions."

- Gradual implementation of AI systems in cybersecurity.
- Pilot programs to test AI integration before full-scale deployment.
- Scalability concerns addressed during initial AI deployment.
- Human training programs accompany AI rollouts.
- Early successes with AI integration encourage broader adoption."

- Change management strategies to facilitate AI adoption.
- AI integration requires shifts in organizational culture.
- Ongoing training to ensure staff are proficient in AI tools.
- Leadership support is critical for successful AI implementation.
- Cross-functional teams help bridge AI-human integration gaps.

- AI systems designed with scalability in mind.
- Human oversight ensures AI scalability does not compromise quality.
- Scalable AI solutions are adaptable to different organizational sizes.
- Automation tools are expanded as cybersecurity needs grow.
- AI platforms are integrated across multiple departments for broader impact.

Figure 2: Data structure presenting the main theme of the integration and optimization of AI and human expertise.

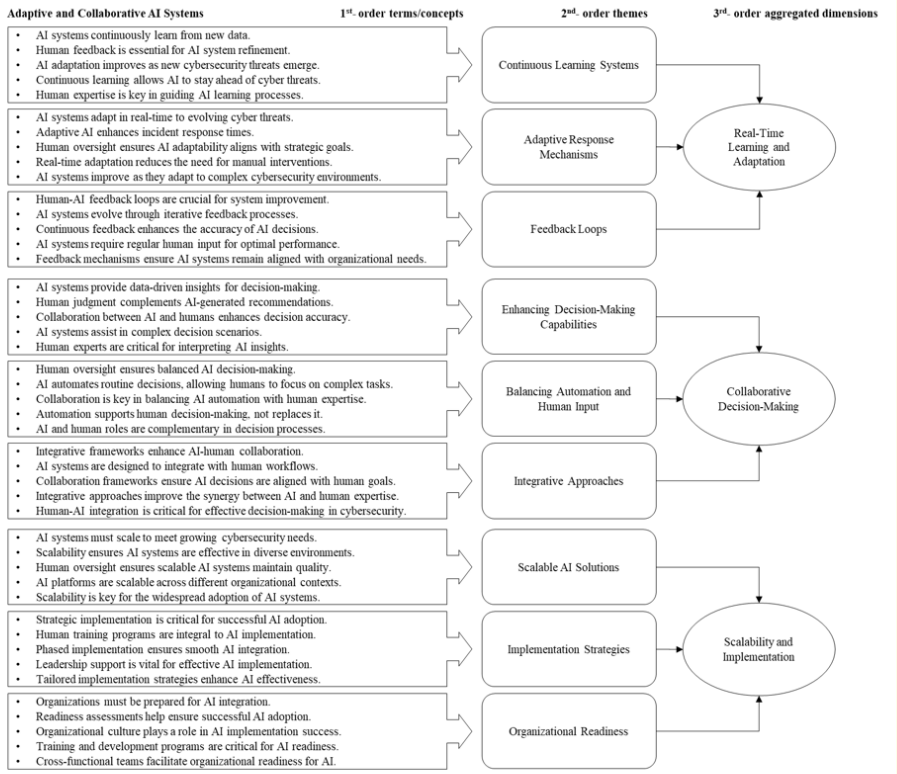
contextual insights that are difficult for AI alone to interpret, and AI enables professionals to leverage AI for strategic decision-making, resulting in better handling of both routine and complex tasks [19].

Implementation and Scalability

This third aggregate addresses the debate in the literature related to the adoption of AI systems in alignment with organizational needs. Both TAM and CT help us navigate how factors such as perceived usefulness and ease of use, are pivotal to ensure that professionals adopt AI in cybersecurity operations [16]. Chahal [48] asserted that resources focus on more valuable tasks when leveraging AI-driven tools, which results in operational efficiency. On the other hand, Das and Sandhane [41] argued that phased AI implementation reduces disruption to the existing organization work-flow, which is in line with the customization required based on the operational needs and maturity levels suggested by CT [18].

Adaptive and Collaborative AI Systems

The second theme delineated in the Figure 3 relies on DCT and CT theories to explore the literature on how AI and human collaboration can contribute to flexible and effective cybersecurity defense [5]. This study explores how human expertise coupled with AI systems can enable organizations to respond dynamically to threats [12]. DCT emphasizes the importance of creating a balanced approach that yields a competitive advantage between AI systems and human inputs to enable organizations to learn, adapt, and respond dynamically to threats [45]. We utilize the CT theory to discuss how the literature points to the necessity of tailoring AI systems to fit each organization's unique context, culture, and operational environment, thereby optimizing the resilience and scalability of cybersecurity operations [18].


Adaptive and Collaborative AI Systems
1st- order terms/concepts
2nd- order themes
3rd- order aggregated dimensions
Continuous Learning Systems
Adaptive Response Mechanisms
Feedback Loops
Real-Time Learning and Adaptation
Enhancing Decision-Making Capabilities
Balancing Automation and Human Input
Integrative Approaches
Collaborative Decision-Making
Scalable AI Solutions
Implementation Strategies
Organizational Readiness
Scalability and Implementation

- AI systems continuously learn from new data.
- Human feedback is essential for AI system refinement.
- AI adaptation improves as new cybersecurity threats emerge.
- Continuous learning allows AI to stay ahead of cyber threats.
- Human expertise is key in guiding AI learning processes.

- AI systems adapt in real-time to evolving cyber threats.
- Adaptive AI enhances incident response times.
- Human oversight ensures AI adaptability aligns with strategic goals.
- Real-time adaptation reduces the need for manual interventions.
- AI systems improve as they adapt to complex cybersecurity environments.

- Human-AI feedback loops are crucial for system improvement.
- AI systems evolve through iterative feedback processes.
- Continuous feedback enhances the accuracy of AI decisions.
- AI systems require regular human input for optimal performance.
- Feedback mechanisms ensure AI systems remain aligned with organizational needs.

- AI systems provide data-driven insights for decision-making.
- Human judgment complements AI-generated recommendations.
- Collaboration between AI and humans enhances decision accuracy.
- AI systems assist in complex decision scenarios.
- Human experts are critical for interpreting AI insights.

- Human oversight ensures balanced AI decision-making.
- AI automates routine decisions, allowing humans to focus on complex tasks.
- Collaboration is key in balancing AI automation with human expertise.
- Automation supports human decision-making, not replaces it.
- AI and human roles are complementary in decision processes.

- Integrative frameworks enhance AI-human collaboration.
- AI systems are designed to integrate with human workflows.
- Collaboration frameworks ensure AI decisions are aligned with human goals.
- Integrative approaches improve the synergy between AI and human expertise.
- Human-AI integration is critical for effective decision-making in cybersecurity.

- AI systems must scale to meet growing cybersecurity needs.
- Scalability ensures AI systems are effective in diverse environments.
- Human oversight ensures scalable AI systems maintain quality.
- AI platforms are scalable across different organizational contexts.
- Scalability is key for the widespread adoption of AI systems.

- Strategic implementation is critical for successful AI adoption.
- Human training programs are integral to AI implementation.
- Phased implementation ensures smooth AI integration.
- Leadership support is vital for effective AI implementation.
- Tailored implementation strategies enhance AI effectiveness.

- Organizations must be prepared for AI integration.
- Readiness assessments help ensure successful AI adoption.
- Organizational culture plays a role in AI implementation success.
- Training and development programs are critical for AI readiness.
- Cross-functional teams facilitate organizational readiness for AI.

Figure 3: Data structure presenting the main theme of adaptive and collaborative AI systems.

Real-Time Learning and Adaptation

The literature emphasizes the importance of adapting AI to the cybersecurity operation environment in which it operates to respond effectively to threats. Real-time learning is a key principle that Lomonaco [49] considered in his study. As novel cyber threats emerge, new data remain relevant for AI systems to learn from. This perspective is further accentuated by DCT principles when considering the need for organizations to reconfigure and adapt their internal and external competencies to maintain a competitive advantage in dynamic environments [45]. This adaptation can be facilitated by AI systems that can self-update based on new threats, thereby providing a proactive defense mechanism [50].

Another form of adaptation comes from feedback loops where human operators provide input that refines AI algorithms over time [51]. This iterative feedback, as highlighted by Honeycutt [19], contributes to a better effective system outcome by enhancing AI decision-making accuracy and decision quality in each feedback cycle. Sarker [11] and Gerostathopoulos [52] reinforced the importance of ongoing collaboration between AI systems and human experts, especially in areas such as incident response, where the result of this collaboration can enable AI systems to respond in real time, thus reducing the need for human manual intervention and freeing them to execute complex strategic decisions [53].

Collaborative Decision-Making

The literature has pointed out that decision-making in cybersecurity operations is an important process where accountability must remain with humans [54-56]. Jarrahi [21] highlighted that AI can collaborate with humans in the decision-making process by executing rapid analysis of large datasets and sharing insights with operators with recommendations on the action to be executed; these insights would be complemented by human judgment aligned with organizational values and strategies. Kapoor and Ghosal [57] emphasized that the insights provided by AI are aimed at augmenting rather than replacing human judgment. Laux [58] highlighted that human over-sight is vital to ensure balanced decision-making and accountability. In addition, Bossaerts [56] encouraged the collaboration between automation, AI, and human expertise because it reinforces AI's role as a supportive tool for decision-making.

Many scholars, such as Sitton and Reich [59], have called for an integrative framework to optimize optimizing AI-human collaboration in decision processes. SIF and SMIM presented in our study contribute to filling the gap in the literature, enabling AI to fit seamlessly into existing workflows [11, 60].

Scalability and Implementation

Scalability, progressive implementation strategies, and organizational readiness have emerged as essential themes to expand AI systems and automation in cybersecurity operations. Several scholars, such as Dhondse and Singh [61], have emphasized that scalability starts from the design phase, where AI solutions are sized to handle increased and decreased workloads, which makes them elastic for deployment in various cybersecurity environments. Soldati [62] stated that embracing adaptability increased the adoption of AI technology [31, 54]. Finally, Chatterjee [40] and Hertzum [63] recommended a phased implementation approach because of its benefits of reducing risk and allowing the organization to adjust the deployment according to their use cases and lessons learned [2].

Conceptual Model Development

Symbiotic Integration Framework (SIF)

The Symbiotic Integration Framework (SIF) delineated in the Figure 4 conceptualizes the structured interaction between AI capabilities and human expertise to optimize decision-making and enhance cybersecurity outcomes. SIF addresses the challenges identified in the literature, such as the necessity for continuous feedback loops between AI systems and human experts and the need for scalability and adaptability in security operations. Rooted primarily in Human-Machine Interaction (HMI) Theory and Cybernetic Theory, the SIF framework bridges the technological and human aspects of cybersecurity, creating a synergistic relationship where AI capabilities in data processing, prediction, and automation are enhanced by human expertise in contextual understanding, ethical judgment, and strategic oversight [21]. This collab-oration supports real-time cooperation, operational efficiencies, adaptive learning, and ethical oversight in cybersecurity [64, 65].

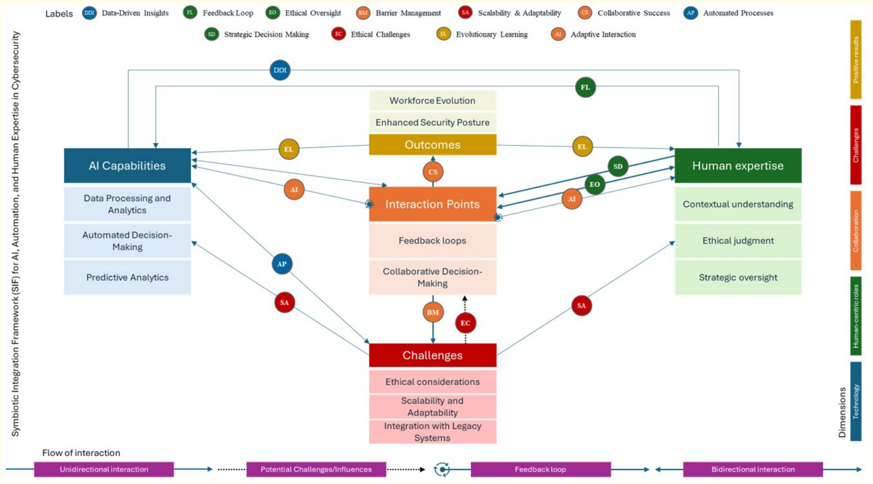


Figure 4: Conceptual model of the symbiotic integration framework (SIF).

Building blocks

The SIF revolve around 5 building blocks. First, the technological building block identifies AI machine learning capabilities to process large datasets and identify meaningful patterns and anomalies. These predictive analytical capabilities leverage historical data to anticipate future threats allow to execute routine tasks, such as log analysis, vulnerability management, and incident response, to be executed to auto-mate decision-making, allowing AI to act on detected threats, triggering pre-programed responses that contain or mitigate security incidents with minimal human intervention resulting into improved threat detection at a scale that is impossible for human operators alone; allowing human operators to focus on more complex and strategic decision-making processes. These capabilities allow organizations to take preventive measures before an attack occurs, transforming cybersecurity operations from being reactive to proactive, which results in operational efficiency in the SIF [66]. The second building block of the SIF is related to human-centric roles in guiding, overseeing, and complementing AI-driven processes. AI requires human ethical over-sight, decision-making, and feedback loops to ensure that these insights are applied in the correct organizational context and that automation errors are mitigated through strategic and ethical considerations [55, 65]. Human expertise complements the analysis that AI systems with judgment on whether those analyses are ethical, free of bias, and fit with organizational goals and security strategies. This constant feedback loop helps AI learn from past decisions and refine algorithms and models, resulting in improvement over time of AI systems, the overall defense mechanism, and the trust in the AI system [21]. Third, the building block deals with the symbiotic collaboration of AI systems and human operators in adaptive interaction, collaborative success, and barrier management, answering the dynamic cybersecurity demands. First, when using AI systems, such as AI prioritized vulnerability management, the human operator can provide real-world feedback to the AI systems so that it can adapt to the context where it operates by gaining better strategic understanding. [21, 64], resulting in enhanced cybersecurity operation. However, this collaboration is prone to fear of job displacement if trust and transparency are not maintained. SIF promotes structured interaction between AI and humans through feedback loops, continuous communication, and shared decision-making resulting in a win-win situation [65]. The fourth building block addresses the challenges that the collaboration between AI and human expertise faces. AI scalability with large datasets, along with ethical challenges, such as transparency and bias, are challenges that impact the success of AI-human integration [31, 62]. Tomsett put into perspective that lack of transparency can lead to trust issues between human operators and AI systems, and bias in AI algorithms can also result in unfair outcomes [65]. By addressing these challenges, SIF ensures that AI-human collaboration remains both scalable and ethically sound [21, 67]. The final building block highlights the positive results that AI and human collaboration can provide in terms of an enhanced security posture, where AI and human operators learn from each other, resulting in a better approach to security risk. This feedback loop leads to a workforce evolution in which the human role evolves toward more strategic tasks that leverage AI's capability to handle large volumes [50].

Value flow and label interactions

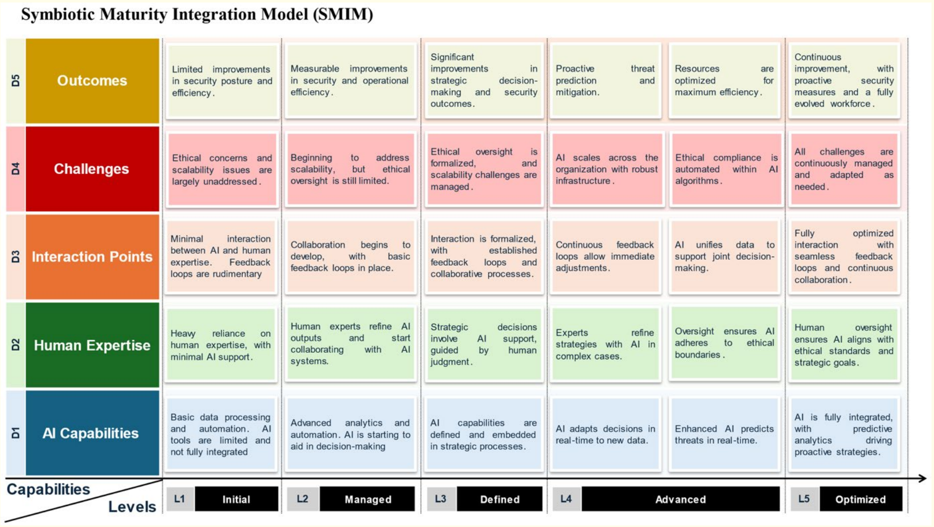
The SIF interactions between human expertise and AI capabilities follow 4 types of interactions. Unidirectional is the first interaction that highlights the data-driven insights produced by AI and reviewed by human operators for interpretation. This interaction highlights the need for contextual understanding when applying professional judgments in line with organizational ethical guidelines. This type of interaction is critical for ensuring that contextual judgment is applied in line with the organization's ethical guidelines [55]. The second interaction presents a use case where continuous bi-directional exchange on cybersecurity threats, vulnerabilities, and potential mitigation allows AI to improve over time based on human input [19]. The feedback loop is a variant of bidirectional interaction that allows an AI system to learn from the feedback shared by human operators in operations such as prioritizing vulnerability or incident response actions, thereby allowing AI systems to predict and respond to threats more effectively over time [11, 51]. Challenges and influence are the last interactions that disrupt the relationship between AI and human operators. The challenges are related to the scalability, ethical concerns, and adaptability of AI systems to the organizational environment, to name a few [21]. We grounded in Table 2 data structure of the connections between the components of the symbiotic integration framework each of the interactions with relevant theories and relevance for the SIF framework in Table 2 data structure of the connections between the components of the symbiotic integration framework, offering insights into how AI and human collaboration can optimize cybersecurity strategies.

Label	***Connection Type***	***Start***	***End***	***Importance of Connection***	***Theories***
Data-Driven Insights (DDI)	Unidirectional Interaction	AI Capabilities	Human Expertise	AI generates insights that human operators can use for decision-making, ensuring informed responses.	HMI: Cybernetic Theory
Feedback Loop (FL)	Feedback Loop	AI Capabilities	Interaction Points	Ensures continuous improvement of AI systems based on human feedback.	HMI: Cybernetic Theory
Ethical Oversight (EO)	Bidirectional Interaction	Human Expertise	AI Capabilities	Allows the integration of ethical frameworks into AI's operational outputs.	HMI Theory and Sociotechnical Systems Theory
Barrier Management (BM)	Unidirectional Interaction	Interaction Points	Challenges	Mitigate risks and ensure system stability in critical cybersecurity processes.	Cybernetic Theory
Scalability and Adaptability (SA)	Potential Challenges/ Influences	AI Capabilities	Challenges	Ensures that the AI system can scale effectively and adapt to changing threat landscapes.	Sociotechnical Systems Theory
Collaborative Success (CS)	Bidirectional Interaction	Interaction Points	Human Expertise	Enables collaboration, which improves decision making and operational efficiency.	HMI Theory
Automated Processes (AP)	Unidirectional Interaction	AI Capabilities	Interaction Points	Automation drives operational efficiency, allowing humans to focus on complex decision-making.	HMI Theory
Adaptive Interaction (AI)	Bidirectional Interaction	Interaction Points	Human Expertise	Human feedback refines AI's adaptive processes, ensuring responsiveness to evolving threats.	HMI Theory
Ethical Challenges (EC)	Potential Challenges/ Influences	Challenges	Interaction Points	Addresses ethical concerns and ensures accountability in AI-human collaboration.	Sociotechnical Systems Theory
Evolutionary Learning (EL)	Feedback Loop	AI Capabilities	Outcomes	Promotes learning and adaptation, ensuring that AI systems evolve in response to new threats.	Cybernetic Theory

Table 2: Data structure of the connections between the components of the symbiotic integration framework.

Symbiotic Maturity Integration Model (SMIM)

Based on the outcomes of the thematic analysis and SIF, the authors realized that achieving a symbiotic relationship between AI and human operators is a progressive exercise requiring a maturity model that would provide a structured roadmap for sophisticating this collaboration. The Figure 5 present the symbiotic maturity integration model (SMIM) conceptual model that will assess and guide the dimensions of the SIF, such as AI capabilities, human expertise, interaction points, challenges, and outcomes; the development of organizational capabilities over time through 5 maturity levels extending the symbiotic integration framework (SIF) from less integrated stages (initial level) to fully optimized collaboration (optimized level), resulting in a mature symbiotic relationship between automation and human oversight. Each of the five maturity levels builds on the previous one, reflecting incremental improvements in both the technological capabilities of AI systems and the depth of human expertise involved in decision-making processes. The proposed model also emphasizes the evolution of collaboration mechanisms, feedback loops, and the ability to handle complex cybersecurity challenges [21, 64, 65].



Symbiotic Maturity Integration Model (SMIM)

Capabilities / Levels	L1 Initial	L2 Managed	L3 Defined	L4 Advanced		L5 Optimized
D5 Outcomes	Limited improvements in security posture and efficiency.	Measurable improvements in security and operational efficiency.	Significant improvements in strategic decision-making and security outcomes.	Proactive threat prediction and mitigation.	Resources are optimized for maximum efficiency.	Continuous improvement, with proactive security measures and a fully evolved workforce.
D4 Challenges	Ethical concerns and scalability issues are largely unaddressed.	Beginning to address scalability, but ethical oversight is still limited.	Ethical oversight is formalized, and scalability challenges are managed.	AI scales across the organization with robust infrastructure.	Ethical compliance is automated within AI algorithms.	All challenges are continuously managed and adapted as needed.
D3 Interaction Points	Minimal interaction between AI and human expertise. Feedback loops are rudimentary	Collaboration begins to develop, with basic feedback loops in place.	Interaction is formalized, with established feedback loops and collaborative processes.	Continuous feedback loops allow immediate adjustments.	AI unifies data to support joint decision-making.	Fully optimized interaction with seamless feedback loops and continuous collaboration.
D2 Human Expertise	Heavy reliance on human expertise, with minimal AI support.	Human experts refine AI outputs and start collaborating with AI systems.	Strategic decisions involve AI support, guided by human judgment.	Experts refine strategies with AI in complex cases.	Oversight ensures AI adheres to ethical boundaries.	Human oversight ensures AI aligns with ethical standards and strategic goals.
D1 AI Capabilities	Basic data processing and automation. AI tools are limited and not fully integrated	Advanced analytics and automation. AI is starting to aid in decision-making	AI capabilities are defined and embedded in strategic processes.	AI adapts decisions in real-time to new data.	Enhanced AI predicts threats in real-time.	AI is fully integrated, with predictive analytics driving proactive strategies.

Figure 5: Conceptual model presenting the symbiotic maturity integration model (SMIM).

Initial and managed levels: Laying foundation

Cybersecurity at the initial level of the SMIM underutilizes AI and relies primarily on human expertise to execute cybersecurity operation. The theme of "Integration and Optimization of AI and Human Expertise" in Figure 2 identified in the thematic analysis allows us to navigate the challenges at this stage; one of them is the recognition of the complementary strengths of AI and humans in cybersecurity operations. The principles of TAM allow the gradual incorporation of AI capabilities and automation into basic cybersecurity processing, such as filtering vulnerabilities and identifying compromise indicators within a large dataset [12]. This incorporation at both the initial and managed levels allows for the early adoption of AI tools as human operators start visualizing AI as a support mechanism in decision-making for routine tasks rather than as a strategic asset [16]. At this stage, the balanced STS approach allows us to navigate the successful transition of other stages as AI tools lack the sophistication to operate autonomously and the feedback loops, while minimal, start to form, laying the groundwork for more advanced integration [32].

Defined Level: Formalized Collaboration and Ethical Oversight

Moving from a managed level to a defined level requires embedding AI capabilities in a strategic decision-making process in which feedback loops become integral [21, 55]. This maturity level is aligned with the analysis of the second theme of our thematic analysis, "Adaptive and Collaborative AI Systems," Figure 3 where principles from cybernetics and DCT theory are essential to navigate adaptive AI-human collaboration. As an example, the cybernetic theory of feedback loops is an essential aspect of cybersecurity operations such as incident prioritization, where AI systems refine classification predictions and responses based on human inputs [19]. As threats involve embracing the adaptability principle with the resources recommended by DCT, organizations can maintain competitive advantages [45]. At this stage, the "interaction points" of the third building block come to life, and principles such as feedback loops, ethical considerations, and contextual oversight are critical in ensuring that AI can inform human decision-makers on why it has taken decisions such as containment of workstations during the cycle of cyber-incidents. Managing at this maturity stage ethical challenges associated with automated cybersecurity decisions remains a significant challenge.

Advanced Level: Robust Collaboration and Real-Time Adaptation

Achieving deep integration between AI and human collaboration is key at the advanced level. The feedback loop principle of cybernetics theory evolved at this stage by enabling AI systems capable of real-time adaptation based on ongoing human input. As an example, an AI system can refine a response playbook based on human inputs by either introducing elements from historical data or elements from other playbooks [20]. This stage demonstrates the realization of the DCT principles by fostering an agile cybersecurity posture that can adapt to complex cybersecurity scenarios [68]. The ethical consideration and scalability principles of the SIF are fully integrated, and organizations can scale their cybersecurity operations without compromising ethical standards or human input.

Optimized Level: Seamless AI-Human Symbiosis and Proactive Security

The final maturity level represents the culmination of AI-human integration in cybersecurity. At an optimized level, AI systems and human expertise work in full harmony to achieve a proactive and resilient security posture, fulfilling all the building blocks of the SIF, allowing AI to operate autonomously in routine tasks, and freeing human experts to focus on strategic and ethical considerations [13]. An organization's cybersecurity posture is fully proactive, leveraging predictive analytics to anticipate and respond to threats before they occur. "Scalability and Implementation" aggregate principles delineated in Figure 3 are embedded in this level, enabling organizations to support large-scale cybersecurity operations across diverse environments. HMI, DCT, and cybernetic theory principles are fulfilled by interaction, enabling continuous adaptation and ethical decision-making that align with long-term organizational goals [21].

Discussion

This systematic literature review contributes to advancing AI-human collaboration in cybersecurity with theoretical and practical insights. The thematic analysis, SIF, and SMIM synthesize the fragmented literature and address gaps in the understanding of how AI capabilities and human expertise can synergistically enhance cybersecurity outcomes [32, 42]. These contributions are grounded in various theories, including RBV [14, 35], STS [15, 43], TAM [44], DCT [45], HMI [19, 20], and CT [18], to enhance our understanding of the complex AI-human collaboration in cybersecurity. The unified relationship covers the gap of studies that predominantly focus on AI as an independent technological asset or emphasize human decision-making in cybersecurity without detailing their integration [1, 48, 61].

The interdependence between technological and social systems, as conceptualized by SIF in the Figure 4, provides a major theoretical contribution that synthesizes the principles of STS, TAM, RBV, and other theories to prove that the symbiotic relationship between AI and humans results in complementary feedback loop forces to achieve optimal cybersecurity outcomes rather than substitutes [36, 69]. SMIM delineated in Figure 5 provides practical contributions by offering a pathway from initial reliance on human expertise to a fully integrated, optimized AI-human collaboration in cybersecurity [16, 27, 71]. The adaptability principles offered through multiple maturity levels allow corporations to adapt their strategy based on the challenges that they face by considering principles such as feedback loops, ethical considerations, and scalability [18]. The SMIM's structured roadmap is particularly valuable for organizations at different stages of technological maturity, from those newly adopting AI tools to those aiming for advanced AI-driven strategies with human oversight [2, 72].

This study has some limitations, starting with the reliance on English-language publications and specific databases that may exclude relevant studies from other languages or cybersecurity priorities [40]. The outcomes of recent developments may not be fully captured, and regular updates in future research are required to incorporate cutting-edge findings [1, 73]. The SIF and SMIM conceptual models require empirical validation in live cybersecurity operations to test the framework's robustness in real-world settings. Future studies could explore the customization and practical utility of the feedback loop and maturity stages based on the industry and size of the organization, offering broader applicability of these frameworks [2, 52, 61].

Conclusions

Through the lens of multiple theoretical frameworks such as RBV, STS, TAM, HMI, DCT, CT, and cybernetics, this study enriches the literature by providing a pathway to optimize the AI-human collaboration and decision-making in cybersecurity environments [20, 21]. Both SIF and SMIM conceptual models have the potential to guide organizations in developing resilient, adaptive, and ethically responsible cybersecurity strategies as their roadmap advances on their maturity journey [28]. This study covers the missing collaborative framework in the literature and offers actionable insights for improving operational effectiveness by ensuring that AI-human-driven decisions are not only efficient but also aligned with ethical standards and organizational goals [74]. Future research should further explore the challenges that AI introduces to specific cybersecurity practices, such as security operation centers and vulnerability management. Future studies could also conduct real-world testing of the SIF and SMIM models across different industries and organizational contexts to assess their scalability, adaptability, and effectiveness in practice and the impact of AI and automation cybersecurity workforce [75-78].

References

1. Admass WS, YY Munaye and A Diro. “Cyber security: State of the art, challenges and future directions”. Cyber Security and Applications (2023): 100031.
2. Familoni BT. “Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions”. Computer Science & IT Research Journal 5.3 (2024): 703-724.
3. DeCusatis C., et al. “Design and implementation of a research and education cybersecurity operations center”. Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments (2019): 287-310.
4. Nyre-Yu M, RS Gutzwiller and BS Caldwell. “Observing Cyber Security Incident Response: Qualitative Themes From Field Research”. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 63 (2019): 437-441.
5. Pollini A., et al. “Leveraging human factors in cybersecurity: an integrated methodological approach”. Cognition, Technology & Work 24.2 (2022): 371-390.
6. Da Costa KA., et al. “Internet of Things: A survey on machine learning-based intrusion detection approaches”. Computer Networks 151 (2019): 147-157.
7. Ahmadi Mehri V, P Arlos and E Casalicchio. “Automated Context-Aware Vulnerability Risk Management for Patch Prioritization”. Electronics 11.21 (2022): 3580.
8. Sadiku MNO, O Fagbohungbe and SM Musa. “Artificial Intelligence in Cyber Security”. International Journal for Research in Applied Science and Engineering Technology (2020).
9. Ali G., et al. “A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns”. Mesopotamian Journal of Computer Science (2024): 71-121.
10. Taddeo M. “Three ethical challenges of applications of artificial intelligence in cybersecurity”. Minds and machines 29 (2019): 187-191.
11. Sarker IH., et al. “Data-Driven Intelligence can Revolutionize Today’s Cybersecurity World: A Position Paper”. ArXiv (2023): abs/2308.05126.
12. Saadallah M, A Shahim and S Khapova. “Synergizing Human Expertise, Automation, and Artificial Intelligence for Vulnerability Management t”. PriMera Scientific Engineering 5.5 (2024): 02-14.
13. Mehdi Saadallah D, A Shahim and S Khapova. “Multi-method Approach to Human Expertise, Automation, and Artificial Intelligence”. in ICT Systems Security and Privacy Protection: 39th IFIP International Conference, SEC 2024, Edinburgh, UK, June 12–14, 2024, Proceedings. Springer Nature (2024).
14. Fernandez de Arroyabe JC., et al. “Cybersecurity Resilience in SMEs. A Machine Learning Approach”. Journal of Computer Information Systems (2023): 1-17.
15. Malatji M, SV Solms and AL Marnewick. “Socio-technical systems cybersecurity framework”. Inf. Comput. Secur 27 (2019): 233-272.

16. Fallatah W, J Kävrestad and S Furnell. “Establishing a Model for the User Acceptance of Cybersecurity Training”. Future Internet 16.8 (2024): 294.
17. Bleady A, AH Ali and SB Ibrahim. “Dynamic capabilities theory: pinning down a shifting concept”. Academy of Accounting and Financial Studies Journal 22.2 (2018): 1-16.
18. Freire FF and VS Padilla. “A Contingency Plan Framework for Cyber-Attacks”. Journal of Information Systems Engineering & Management (2019).
19. Honeycutt DR, M Nourani and ED Ragan. “Soliciting Human-in-the-Loop User Feedback for Interactive Machine Learning Reduces User Trust and Impressions of Model Accuracy”. ArXiv (2020): abs/2008.12735.
20. Cernauskas D and A Kumiega. “Back to the future: Cybernetics for safety, quality and cybersecurity”. Quality Management Journal 29.3 (2022): 183-192.
21. Jarrahi MH. “Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making”. Business Horizons (2018).
22. Page MJ., et al. “PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews”. BMJ (2021): 372.
23. Bolbot V., et al. “Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis”. International Journal of Critical Infrastructure Protection 39 (2022): 100571.
24. Javaheri D., et al. “Cybersecurity threats in FinTech: A systematic review”. Expert Systems with Applications (2023): 122697.
25. Abdullahi M., et al. “Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review”. Electronics 11.2 (2022): 198.
26. Akhtar M and T Feng. “An overview of the applications of Artificial Intelligence in Cybersecurity”. EAI endorsed transactions on creative technologies 8.29 (2021).
27. Albahri O and A AlAmoodi. “Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database”. Mesopotamian Journal of CyberSecurity (2023): 158-169.
28. Le NT and DB Hoang. “Can maturity models support cyber security?”. in 2016 IEEE 35th international performance computing and communications conference (IPCCC). IEEE (2016).
29. Schinagl S, A Shahim and S Khapova. “Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security”. Computers & Security 122 (2022): 102903.
30. Stevens T. “Knowledge in the grey zone: AI and cybersecurity”. Digital War 1.1 (2020): 164-170.
31. Hummelholm A. “AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks”. European Conference on Cyber Warfare and Security (2023).
32. Braun V and V Clarke. “Conceptual and design thinking for thematic analysis”. Qualitative psychology 9.1 (2022): 3.
33. Naeem M., et al. “A step-by-step process of thematic analysis to develop a conceptual model in qualitative research”. International Journal of Qualitative Methods 22 (2023): 16094069231205789.
34. Gioia DA, KG Corley and AL Hamilton. “Seeking qualitative rigor in inductive research: Notes on the Gioia methodology”. Organizational research methods 16.1 (2013): 15-31.
35. Direction S. “Investing in cybersecurity: Gaining a competitive advantage through cybersecurity”. J. Bus. Strat 37 (2021): 19-21.
36. Addae JH., et al. “Exploring user behavioral data for adaptive cybersecurity”. User Modeling and User-Adapted Interaction 29 (2019): 701-750.
37. Naseer H., et al. “Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics”. European Journal of Information Systems 33.2 (2024): 200-220.
38. Capuano N., et al. “Explainable artificial intelligence in cybersecurity: A survey”. IEEE Access 10 (2022): 93575-93600.
39. Naseer A., et al. “Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities”. Computers & Security 135 (2023): 103525.
40. Chatterjee S, SK Ghosh and R Chaudhuri. “Knowledge management in improving business process: an interpretative framework for successful implementation of AI-CRM-KM system in organizations”. Bus. Process. Manag. J 26 (2020): 1261-1281.

41. Das R and R Sandhane. “Artificial Intelligence in Cyber Security”. Journal of Physics: Conference Series (2021): 1964.
42. Ahmadi A. “Implementing Artificial Intelligence in IT Management: Opportunities and Challenges”. Asian Journal of Computer Science and Technology (2023).
43. Sadok M, C Welch and P Bednar. “A socio-technical perspective to counter cyber-enabled industrial espionage”. Security Journal 33.1 (2020): 27-42.
44. Yalcin ME and B Kutlu. “Examination of students’ acceptance of and intention to use learning management systems using extended TAM”. Br. J. Educ. Technol 50 (2019): 2414-2432.
45. Pigola A and PRD Costa. “Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats”. Commun. Assoc. Inf. Syst 53 (2023): 46.
46. Nyre-Yu. Determining System Requirements for Human-Machine Integration in Cyber Security Incident Response (2019).
47. Lee J., et al. “Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles”. IEEE Access 7 (2019): 165607-165626.
48. Chahal S. “AI-Enhanced Cyber Incident Response and Recovery”. International Journal of Science and Research (IJSR) (2023).
49. Lomonaco V. Continual Learning with Deep Architectures (2019).
50. Hadsell R., et al. “Embracing Change: Continual Learning in Deep Neural Networks”. Trends in Cognitive Sciences 24 (2020): 1028-1040.
51. Suryadevara M, S Rangineni and SRCC Venkata. “Optimizing Efficiency and Performance: Investigating Data Pipelines for Artificial Intelligence Model Development and Practical Applications”. International Journal of Science and Research (IJSR) (2023).
52. Gerostathopoulos I., et al. “Strengthening Adaptation in Cyber-Physical Systems via Meta-Adaptation Strategies”. ACM Transactions on Cyber-Physical Systems 1 (2017): 1-25.
53. Moreno GA. Adaptation Timing in Self-Adaptive Systems (2017).
54. Verma R, S Koul and Ajaygopal KV. “Evaluation and Selection of a Cybersecurity Platform — Case of the Power Sector in India”. Decision Making: Applications in Management and Engineering (2023).
55. Lee H-W, T-H Han and T Lee. “Reference-Based AI Decision Support for Cybersecurity”. IEEE Access 11 (2023): 143324-143339.
56. Bossaerts P and C Murawski. “Computational complexity and human decision-making”. Trends in cognitive sciences 21.12 (2017): 917-929.
57. Kapoor R and I Ghosal. “Will Artificial Intelligence Compliment or Supplement Human Workforce in Organizations? A Shift to a Collaborative Human – Machine Environment”. International Journal on Recent Trends in Business and Tourism (2022).
58. Laux J. “Institutionalised Distrust and Human Oversight of Artificial Intelligence: Toward a Democratic Design of AI Governance under the European Union AI Act”. SSRN Electronic Journal (2023).
59. Sitton M and Y Reich. “EPIC framework for enterprise processes integrative collaboration”. Systems Engineering 21 (2018): 30-46.
60. GCS., et al. “Human-AI Collaboration: Exploring interfaces for interactive Machine Learning”. Tuijin Jishu/Journal of Propulsion Technology (2023).
61. Dhondse A and S Singh. “Redefining Cybersecurity with AI and Machine Learning”. International Research Journal of Modernization in Engineering Technology and Science (2023).
62. Soldati P., et al. “Design Principles for Model Generalization and Scalable AI Integration in Radio Access Networks”. IEEE Communications Magazine (2023).
63. Hertzum M., et al. “Pilot Implementation: Testing Human-Work Interaction Designs”. in IFIP TC13 International Conference on Human-Computer Interaction (2021).
64. Martin T. “On the Need for Collaborative Intelligence in Cybersecurity”. in AI-Cybersec@SGAI (2022).
65. Tomsett RJ., et al. “Rapid Trust Calibration through Interpretable and Uncertainty-Aware AI”. Patterns (2020): 1.
66. Ndichu S., et al. “AI-Assisted Security Alert Data Analysis with Imbalanced Learning Methods”. Applied Sciences (2023).
67. Poon AI and JJ Sung. “Opening the black box of AI-Medicine”. Journal of gastroenterology and hepatology 36.3 (2021): 581-584.
68. Pollini A., et al. “Leveraging human factors in cybersecurity: an integrated methodological approach”. Cognition, Technology &

amp; Work 24.2 (2022): 371-390.

69. Canal G., et al. "Building Trust in Human-Machine Partnerships". Comput. Law Secur. Rev 39 (2020): 105489.
70. Haber MJ and B Hibbert. "The Vulnerability Management Program, in Haber 2018 emphasizes the role of vulnerability and compliance management initiatives in securing critical information and demonstrating regulatory compliance". Apress (2018): 111-118.
71. Haber MJ and B Hibbert. The Vulnerability Management Program (2018).
72. Blanco L., et al. "AI-Driven Framework for Scalable Management of Network Slices". IEEE Communications Magazine 61 (2023): 216-222.
73. Bhima B, A Rahmania Az Zahra and T Nurtino. "Enhancing Organizational Efficiency through the Integration of Artificial Intelligence in Management Information Systems". APTISI Transactions on Management (ATM) (2023).
74. Schneider J. "Humans learn too: Better Human-AI Interaction using Optimized Human Inputs". ArXiv (2020): abs/2009.09266.
75. Veale M, M Van Kleek and R Binns. "Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making". in Proceedings of the 2018 chi conference on human factors in computing systems (2018).
76. Zolanvari M., et al. "TRUST XAI: Model-Agnostic Explanations for AI With a Case Study on IIoT Security". IEEE Internet of Things Journal 10 (2022): 2967-2978.
77. Mahbooba B., et al. "Trust in Intrusion Detection Systems: An Investigation of Performance Analysis for Machine Learning and Deep Learning Models". Complex (2021): 5538896.
78. Jöhnk J, M Weißert, and K Wyrtki. "Ready or not, AI comes—an interview study of organizational AI readiness factors". Business & Information Systems Engineering 63.1 (2021): 5-20.