AI-Augmented Transformation of the B2B Marketing Mix in Cybersecurity: A Systematic Review

Mr. Vikrant Bhosle[1], Dr. Archana Janjal[2]
[1]Modern Institute of Business Management, Savitribai Phule Pune University, Pune, India
[2]Bharati Vidyapeeth (Deemed to be University), India
[1]vikrantbhosle@gmail.com, [2]archana.janjal@bharatividyapeeth.edu

Abstract— Despite the growing body of research on artificial intelligence in business contexts, relatively little attention has been paid to how AI changes the underlying structure of B2B marketing, particularly in sectors where technical complexity and buyer skepticism define the commercial environment. This paper examines that gap through the lens of the cybersecurity industry, where long sales cycles, multi-stakeholder procurement, and an inherent difficulty in demonstrating product value make marketing unusually demanding. Based on the systematic review of articles published between 2020 and 2026, with 30 core papers selected via the PRISMA protocol, the study examines how AI capabilities alter each of the seven elements of the B2B marketing mix. The findings suggest that AI's influence goes well beyond process efficiency: it changes what products do, how prices are set, what promotion looks like, how channels are managed, what is expected of sales personnel, how customer lifecycles are handled, and how vendors establish credibility with buyers. Collectively, these findings point toward a qualitatively different model of marketing in enterprise technology markets. The paper synthesizes these observations into a three-tier framework built around intelligence gathering, AI-mediated orchestration, and measurable strategic outcomes. The contribution lies not in cataloguing AI tools but in showing how AI, when applied across the full marketing mix, shifts the basis of competitive advantage from execution speed to evidenced value.

Keywords—Artificial Intelligence, B2B Marketing, 7Ps Marketing Mix, Cybersecurity, Dynamic Capabilities, Enterprise SaaS, Epistemic Trust

I. INTRODUCTION

The business of selling cybersecurity is, in many ways, a study in contradiction. The more successful a cybersecurity solution is, the harder it is to demonstrate its effectiveness to a potential customer. The measure of a successful cybersecurity solution is, in many ways, the absence of a problem, not a presence. In a market in which the value proposition is based on preventing a problem that may not have occurred in the first place, many of the conventional principles of marketing have limited value. Despite this, cybersecurity is one of the fastest-growing segments of enterprise software globally. The business challenge is real, and there is a significant gap between what vendors know about their products and what buyers can verify on their own.

This disproportionate information is situated at the core of B2B cybersecurity marketing. CISOs and IT procurement decision-makers face a situation of great pressure and cognitive load, they need to make sense of

technically complex solutions without much domain knowledge or internal analytical capabilities. They heavily depend upon analyst reports, word of mouth, and brand recognition because getting technical validation is expensive and takes a long time. This is where large players have a natural advantage, and it is where new players face the greatest challenge.

However, artificial intelligence is beginning to alter this in ways that go beyond the automation of the aforementioned processes. If applied properly, artificial intelligence can assist vendors in providing objective, contextualized evidence of their performance, communicate in a way that resonates with the specific concerns of individual buyers, price their offerings in a manner that is more aligned with the actual risks involved than arbitrary tier structures, and provide sales engineers with the information they need to hold credible discussions with procurement committees comprised of highly technical individuals. Artificial intelligence, in short, has the potential to address some of the fundamental weaknesses of cybersecurity marketing.

The academic literature has been slower to catch up with this development than industry practice. While there is a substantial body of work on AI in marketing generally [1][7][22] and on B2B marketing challenges in technology sectors [5][20], the specific question of how AI reconfigures the extended B2B marketing mix in high-complexity environments has received limited systematic attention. The 7Ps framework—Product, Price, Place, Promotion, People, Process, and Physical Evidence—was designed for relatively stable commercial environments. Its application to an AI-driven, continuously evolving sector like cybersecurity raises questions that have not been fully worked through in the literature.

This paper attempts to address that gap. By conducting a systematic review of research published between 2020 and 2026, it examines how AI capabilities are altering each dimension of the B2B marketing mix in the cybersecurity sector, and proposes a framework to understand the relationships between AI inputs, marketing processes, and competitive outcomes. The analysis draws on dynamic capabilities theory [3], cognitive load theory [6], and contemporary research on AI-enabled marketing [4][24] to ground the synthesis in established theoretical tradition while extending it in directions the existing literature has not completely explored.

A. Research Questions

Three research questions guide this review. First, how does AI alter the way each of the 7Ps operates in B2B cybersecurity marketing? Second, what theoretical mechanism best explains AI's role in this context—is it primarily an efficiency tool, or does it represent something more structurally significant? Third, what kind of integrated framework can usefully capture the relationship between AI capabilities and marketing outcomes in enterprise security markets?

II. THEORETICAL FRAMEWORK

A. AI and Dynamic Capabilities

The dynamic capabilities framework, developed by Teece [3], offers a productive lens for understanding AI's role in marketing. Teece presented an argument that sustained competitive advantage in volatile environments depends not on static resources but on an organization's ability to sense emerging opportunities, seize them through appropriate strategic choices, and continuously reconfigure internal processes to remain aligned with a changing environment. These three capacities—sensing, seizing, and transforming—map naturally onto how AI functions within a marketing context.

In the cybersecurity sector, AI-enabled sensing takes the form of continuous monitoring of threat telemetry, buyer intent signals, and competitive intelligence. These data streams allow vendors to identify emerging customer needs before they are explicitly expressed—for instance, detecting that a cluster of target accounts has recently begun researching a specific attack vector, and adjusting content and outreach accordingly. This is qualitatively different from

periodic market research or campaign performance reviews; it is ongoing, automated, and actionable in near real-time.

Seizing, in this context, involves converting intelligence into value through dynamic adjustment of product configurations, pricing, and personalized content delivery. A vendor that can respond to a CISO's publicly observable research behavior with a tailored briefing on the specific regulatory implications of a newly identified threat is doing something more than efficient marketing; it is demonstrating relevance and expertise in a way that directly accelerates trust formation. Transforming, finally, refers to the way AI reconfigures internal marketing processes—from manual campaign execution to continuously adaptive orchestration—allowing organizations to remain responsive to market changes without proportionate increases in headcount or operational overhead [24].

Positioning AI as a dynamic capability rather than a mere marketing tool has important implications for how organizations should invest in and govern it. It suggests that AI should be developed and managed at an organizational level, not simply purchased as a software subscription and handed to a marketing team. The returns from AI in marketing are likely to be highest where it is embedded in strategy and processes, not just in technology stacks.

B. Cognitive Load and Trust in B2B Buying

Sweller's cognitive load theory [6] distinguishes between the inherent complexity of a task (intrinsic load), the mental effort involved in learning and schema formation (germane load), and the additional cognitive burden imposed by poorly structured information (extraneous load). In high-technology B2B markets, extraneous cognitive load is a persistent problem. Vendors frequently present buyers with dense technical documentation, vendor-specific terminology, and abstract capability claims that are difficult to verify or compare. The result is evaluation paralysis: buyers who cannot meaningfully distinguish between competing solutions fall back on heuristics such as brand recognition, peer recommendations, or analyst endorsements.

AI offers a partial solution to this problem by serving as a filtering and translation mechanism. When AI systems can distill complex security telemetry into executive-readable summaries, or convert technical detection rates into estimates of financial risk reduction, they reduce the extraneous burden on buyers and create conditions in which genuine evaluation becomes more feasible. This directly impacts a concept which the paper refers to as "epistemic trust"; a buyer's confidence in the technical validity of vendor claims, as distinct from relational trust built through personal interaction. Epistemic trust matters particularly in cybersecurity because buyers often lack the technical capacity to independently validate claims, and because the consequences of a wrong purchasing decision are severe [29].

The fact of matter here is that AI is not replacing relationship-based selling, AI facilitates an evidence base understanding, which makes trust-building quicker, more reliable and reduces the dependency on the personal relations involved in one-to-one sales activities. This difference between relational and epistemic trust is not much explored in the B2B marketing literature, and hence the context of cybersecurity in the B2B tech market, provides a useful space to be explored.

C. Information Asymmetry in Cybersecurity Markets

Information asymmetry in markets, as Akerlof's foundational work demonstrated, creates conditions that systematically disadvantage buyers and distort competitive dynamics. In cybersecurity markets, the asymmetry is structural: vendors invest heavily in understanding the threat landscape and the technical performance of their solutions, while buyers typically lack the expertise, time, or access to independently assess these claims. This gap creates adverse selection pressures that favor well-known brands over genuinely superior but less visible alternatives.

AI addresses this asymmetry not by eliminating it, vendors will always know more

about their products than buyers do, but by generating credible, third-party-verifiable evidence that buyers can evaluate without deep technical expertise. A monthly report showing that a vendor's endpoint protection platform successfully contained 47,000 breach attempts on a client's network, cross-referenced against industry benchmarks and presented in business-risk language, is fundamentally more persuasive than a sales presentation making similar claims in the abstract [29]. AI makes this kind of evidence generation scalable and automated, which changes the economics of trust-building in enterprise sales.

III. METHODOLOGY: SYSTEMATIC LITERATURE REVIEW

A. Search Strategy and Protocol

The review process followed the PRISMA(Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology, which is a systematic review process that helps to minimize bias during the selection of literature. This methodology helps to maintain the reproducibility of the results. The review process was carried out by searching various databases such as Scopus, IEEE Xplore, and Web of Science. The period of interest for the review process extends from January 2020 to March 2026. This period of interest was chosen because it marks the period of commercial deployment of AI solutions, such as the advent of large language models and AI-based security solutions.

The search query was a combination of words related to AI (machine learning and generative AI), B2B marketing and the marketing mix, and cybersecurity/enterprise SaaS. The initial search results yielded 340 potential papers, which were then augmented by 22 further papers based on reference list screening of highly cited papers in the initial results list.

B. Selection Criteria

The articles had to be contained within a peer-reviewed journal or reputable conference proceeding, discuss AI within marketing or sales settings, and be relevant to either B2B technology or cybersecurity marketing. Articles that only dealt with the development of AI technology without marketing implications, those that only dealt with B2C settings, or duplicates were eliminated. After two rounds of article analysis, 30 articles remained that are used as the foundation for the 7Ps analysis contained within Section IV.

IV. THE AI-AUGMENTED 7PS: A SECTOR ANALYSIS

A. Product: Security as a Living System

In most software markets, the product is a well-defined entity: a release of a software version with a well-understood feature set, roadmap, and release cycle. Marketing the product entails communicating the value of the feature set to potential customers and emphasizing the value of the roadmap relative to the competition. In security software, this has never been a sufficient model because the performance criteria are not how the software performs in a controlled environment, but how it performs against threats that were unknown at the time the software was created.

Machine learning has changed the product landscape of top-tier cybersecurity products. While traditional endpoint protection products rely on signature-based detection approaches that involve human analysis to define signatures based on known patterns of attacks, modern AI-powered endpoint protection products use machine learning to train their detection algorithms based on patterns learned from large networks of deployed sensors. The product, in a very real sense, never ends. Its scope is continually expanding to include new threats it encounters. Its detection model is highly specific to the actual behavior of attackers rather than pre-defined signatures [4].

The marketing implications of this architectural change are substantial. The feature catalog and version comparison are less important when the product is dynamically changing. What is important to the buyer, and what the vendor must emphasize to the buyer, is the quality of the telemetry network, how quickly they are adding

new threats to their detection logic, and their overall experience in the field. Vendors that understand this architectural change are shifting from feature-focused marketing materials to threat intelligence briefings as their primary marketing collateral [1].

In addition to that, another area where AI influences the software experience after purchase is the experience of the software itself. Through the analysis of telemetry data at the account level, it becomes possible to determine which features are underutilized, which configurations are causing customers to become exposed to risks, or which configurations are causing customers to leave. Recommendations for configuration can be provided to customers without any need for human intervention from the customer success team. The experience of the software becomes continuous rather than limited to the initial implementation [7].

B. Price: From Tiers to Risk-Adjusted Value

Enterprise software pricing has historically been organized around feature tiers or user counts—models that are administratively simple but often poorly calibrated to the actual value different customers derive from a solution. In cybersecurity, the mismatch is particularly pronounced: the value of a security platform to an organization depends not primarily on how many users it has, but on the risk profile of the organization, the sensitivity of the data it holds, and the likelihood that it will face a serious attack. Two organizations with identical user counts might have radically different exposures and therefore derive radically different value from the same product.

AI makes risk-based pricing architectures practically feasible. By aggregating publicly available data on an organization's attack surface—including known software vulnerabilities, historical breach exposure, industry threat frequency, and regulatory compliance obligations—vendors can generate probabilistic risk profiles that reflect the actual value their solution would deliver. Pricing can then be calibrated to these profiles, with accounts that face higher breach probability paying premiums that reflect the correspondingly greater value of effective prevention [5].

Retention pricing is another area where machine learning is changing the economics. Churn prediction models trained on renewal data, feature engagement patterns, support interactions, and executive relationship indicators can flag at-risk accounts with sufficient lead time for proactive intervention. Rather than waiting for a customer to begin an active RFP process with a competitor, vendors can initiate targeted retention conversations—including adjusted pricing, feature unlocks, or executive outreach—while the customer is still engaged and the renewal relationship is salvageable [10].

Contract structuring is also being influenced by natural language processing tools that analyze historical agreement data to identify the terms and configurations most closely associated with long-term expansion and renewal. This shifts contract negotiation from an experience-dependent art toward a data-informed process, allowing less experienced commercial teams to structure deals with a higher probability of successful long-term outcomes [27].

C. Promotion: Getting the Right Message to the Right Person

Anyone who has worked in B2B cybersecurity marketing will recognize the frustration of generic demand generation. The industry is characterized by a wide spectrum of buyer types with very different levels of technical sophistication, organizational priorities, and risk perceptions. A CISO at a large financial institution navigating stringent regulatory requirements has almost nothing in common, from a communications standpoint, with the IT manager at a mid-sized logistics firm dealing with a ransomware incident for the first time. Yet most cybersecurity marketing treats these audiences as broadly equivalent, delivering the same whitepapers, the same conference presentations, and the same email nurture sequences to both.

Intent data platforms, powered by machine learning, are beginning to change this. These

platforms monitor digital behavioral signals—search patterns, content consumption, peer forum participation, technology review site visits, hiring trends—and use them to infer where specific individuals within target accounts are in their buying journey, what problems they are actively investigating, and what information would be most useful to them at that moment [8]. When a CISO begins researching Extended Detection and Response architectures, the pattern of their online activity is often observable before any direct vendor contact has occurred. Vendors with access to these signals can respond with content that is immediately relevant rather than generically informative.

Generative AI extends this personalization to the content itself. Rather than repurposing standard whitepapers with a prospect's company name added, AI systems can produce briefings that address the specific regulatory environment, threat landscape, and technology context of individual accounts. A healthcare prospect receives analysis grounded in HIPAA obligations and the specific ransomware patterns targeting electronic health records; an energy sector prospect receives material focused on operational technology vulnerabilities in industrial control systems. The marginal cost of producing this kind of specificity was prohibitive when content production required human writers for every variant; AI reduces it to near zero [16].

The practical implication for promotional strategy is a shift in the unit of analysis from the campaign to the account, and from the segment to the individual buyer. Measuring success by click-through rates and lead volumes becomes less meaningful than measuring engagement quality, buying stage progression, and deal velocity within priority accounts. This is not a new idea—Account-Based Marketing has been discussed for years—but AI makes it operationally practical at a scale that manual methods could not achieve [13][14].

D. Place: Intelligence-Driven Channel Management

Enterprise cybersecurity solutions reach customers through a complex ecosystem of channel intermediaries. Managed Security Service Providers (MSSPs), Value-Added Resellers, systems integrators, and specialist consultancies each play different roles in the sales and implementation process. For vendors, managing this network effectively is a significant operational challenge: which partners should receive which leads? Which are technically qualified to support specific product categories? Which are at risk of diverting attention to a competitor's platform? These questions have traditionally been answered through periodic partner reviews, territory-based assignments, and relationship management—processes that are resource-intensive and slow to respond to changes in partner performance.

Machine learning models trained on historical deal data can generate much more granular and accurate answers to these questions. By analyzing patterns in deal registrations, close rates, technical certification maintenance, and co-marketing activity, these models can identify which partners consistently perform well in specific geographies, industry verticals, or deal sizes, and route opportunities accordingly. The result is a shift from relationship-based to performance-based channel governance—one that is more accurate and less dependent on the judgment of individual channel managers [17].

Predictive partner health scoring serves a similar function on the retention side. Partners who are disengaging—evidenced by declining training participation, fewer deal registrations, or reduced co-marketing activity—can be identified well before their departure becomes a certainty, allowing vendors to intervene with targeted enablement support, incentives, or executive engagement while there is still time to reverse the trend [20].

AI-powered enablement platforms are also shortening the time it requires for new partners to become productively effective. By providing real-time competitive intelligence, automated proposal generation support, and guided deal coaching, these platforms reduce the ramp time

for partners entering new product areas or geographic markets. The practical effect is an expansion of effective distribution capacity without proportional increases in vendor headcount [23].

E. People: Augmenting the Human Element

The sales engineer occupies a pivotal role in enterprise cybersecurity sales. They are responsible for the technical credibility of the vendor's claims, for navigating the detailed objections raised by security architects and IT leadership, and for demonstrating that the product can perform in the buyer's specific environment. It is a demanding role that requires both broad technical knowledge and the interpersonal skills to communicate that knowledge to diverse and often skeptical audiences. Maintaining the required level of technical currency is a persistent challenge in a field where the threat landscape and product capabilities change continuously.

AI-assisted sales tools are beginning to address this challenge by providing in-context decision support during live customer interactions. Battle card systems that surface competitive intelligence relevant to the specific objections being raised, product configuration recommendations based on the prospect's known technology environment, and reference case studies matched to the buyer's industry and use case can all be delivered to the sales engineer in real time, reducing the cognitive burden of managing a complex technical conversation [11][21].

Conversation analytics tools analyze meeting recordings and transcripts to identify patterns that distinguish successful from unsuccessful interactions. When a particular objection handling approach consistently precedes positive outcomes, that insight can be incorporated into coaching programs and made available to the broader sales team. When a specific type of question from a prospect signals strong buying intent, that signal can be automatically escalated to the account team for follow-up. This kind of systematic learning from sales interactions is difficult to achieve at scale without AI, because the volume of conversations and the subtlety of the relevant signals make manual analysis impractical [9].

A noteworthy point to consider is that, the value of AI augmentation in the People dimension depends critically on the quality of human judgment underlying it. AI tools can surface relevant information and flag important signals, but they cannot replace the relationship-building, contextual judgment, and adaptive communication that characterize effective enterprise selling. The most productive framing is one in which AI reduces the cognitive overhead of managing complex information, freeing human sellers to focus on the interpersonal dimensions of the sales process where their capabilities are genuinely irreplaceable [18].

F. Process: From Manual Coordination to Orchestrated Lifecycle Management

Enterprise cybersecurity sales involve an unusually high degree of process complexity. From initial qualification through technical validation, legal negotiation, contract execution, and post-sale onboarding, a typical enterprise deal may span six to twelve months and involve dozens of individual stakeholder interactions. Coordinating these interactions—ensuring that the right people are engaged at the right stages, that technical validation activities are scheduled and resourced appropriately, and that handoffs between sales and customer success are managed without loss of context—is a significant operational undertaking that most vendors manage imperfectly.

AI-powered qualification tools improve the efficiency of early-stage resource allocation by generating probabilistic assessments of deal viability based on prospect firmographics, behavioral signals, and historical conversion data. Rather than relying on the individual judgment of sales managers to prioritize opportunities, these models provide a more consistent and data-grounded basis for presales resource allocation [12].

In the technical validation phase, AI-enabled sandbox environments allow prospects

to test products against simulated threat scenarios representative of their own environment, receiving quantified performance data—detection rates, false positive frequencies, response times—without the overhead of a formal proof-of-concept engagement. This removes one of the most significant bottlenecks in the enterprise cybersecurity sales cycle, which has traditionally required weeks of environment provisioning and consultant engagement before producing evaluable data [7].

Post-sale, predictive health scoring models monitor the breadth and depth of product adoption, support interactions, stakeholder engagement, and commercial metrics to identify accounts where the implementation is underperforming or the relationship is at risk. When an account's health score drops below a defined threshold, automated escalation workflows can trigger proactive outreach from the customer success team, executive relationship reviews, or technical intervention—without waiting for a support ticket or renewal conversation to surface the problem [26].

G. Physical Evidence: Making the Invisible Visible

Physical evidence—the tangible cues that allow buyers to evaluate service quality—presents a distinctive challenge in cybersecurity. The core value delivered by a security platform is the prevention of events that, by definition, have not occurred. Demonstrating this value to a board of directors or a procurement committee requires translating the absence of breaches into credible evidence of protection, which is not straightforward when skeptical audiences may reasonably ask whether the threats were prevented because of the vendor's platform or simply because no serious attacks were attempted.

AI-generated intelligence dashboards address this problem by providing real-time, quantified documentation of security outcomes: the number and type of blocked attack attempts, quarantined processes, and prevented exfiltration events, contextualized against industry threat benchmarks and presented in risk-adjusted financial terms. A visualization that translates 47,000 blocked attack attempts into an estimated financial risk reduction figure calibrated to the organization's industry and size is considerably more compelling to a CFO than a raw detection count [15].

Automated reporting tools extend this evidence generation into the rhythm of executive communication. Monthly security performance reports that translate telemetry data into business-language summaries of risk reduction—without requiring manual analyst effort—support renewal conversations by providing a continuous record of value delivered rather than requiring vendors to reconstruct the case for renewal from scratch at contract expiry [28].

Competitive benchmarking is a third dimension of physical evidence that AI makes more credible. When vendors can synthesize verified customer outcome data, independent benchmark results, and threat intelligence coverage statistics into personalized comparisons with named competitors, they move beyond self-referential marketing claims toward evidence that buyers can evaluate against their own criteria. The persuasive power of this approach lies precisely in its specificity: a benchmark that shows detection rates for the exact threat categories most relevant to a prospect's industry is far more convincing than generic efficacy statistics [15].

V. THE AI-AUGMENTED B2B MARKETING MIX FRAMEWORK

What this 7Ps analysis reveals, is not a set of disparate AI applications in different marketing domains, but rather a set of interconnected capabilities that operate best in concert with one another as a system. The telemetry data used to inform product adaptation is the same telemetry data used to populate physical evidence dashboards. The intent indicators used to inform promotional targeting are the same intent indicators used to inform sales engineer coaching and channel lead routing. The risk indicators used to inform pricing decisions are the same risk

indicators used to inform the customer success process. This is all important to understand in order to realize the maximum competitive potential in marketing with AI.

The 3-tier framework that is being proposed in this paper (shown in Table II) structures these interdependencies in accordance with the logical progression of the marketing activities, as facilitated by AI which spans from data acquisition to generation of intelligence, via AI-enabled processing, driving quantifiable outcomes.

TABLE II AI-AUGMENTED B2B MARKETING MIX FRAMEWORK

Framework Layer	AI Capability	7Ps Impacted	Strategic Outcome
Intelligence Layer (Input)	Threat telemetry analytics, intent data mining, behavioral tracking	Product, Promotion, Price	Real-time market sensing; predictive demand signals
Orchestration Layer (Processing)	LLMs, predictive engines, NLP, automated workflows	Promotion, Process, People, Place	Dynamic reconfiguration of marketing activities
Outcome Layer (Strategic Value)	Evidence dashboards, trust scoring, CAC optimization	Physical Evidence, Price, Place	Reduced CAC, shorter sales cycles, epistemic trust

Intelligence Layer (Input): The foundation of the framework is an integrated data infrastructure that aggregates signals from multiple sources simultaneously: global threat telemetry from security sensor networks, buyer intent data from behavioral tracking platforms, product usage data from deployed SaaS instances, and competitive intelligence from market monitoring systems. The defining characteristic of this layer is continuity—it is not a periodic research exercise but an ongoing collection mechanism that feeds the orchestration layer in near real-time.

Orchestration Layer (Processing): At the center of the framework, AI capabilities—including large language models for content generation, predictive analytics for propensity modeling, natural language processing for conversation analysis, and workflow automation for process execution—operate on the intelligence inputs to produce specific marketing outputs across all seven elements of the mix. The key principle at this layer is coordination: the AI systems governing promotional targeting, pricing, channel routing, and customer success monitoring should be drawing from the same data and operating toward the same strategic objectives, rather than functioning as siloed point solutions.

Outcome Layer (Strategic Value): The practical consequences of integrated AI-orchestrated marketing are captured in three outcome categories: reduced customer acquisition cost, shorter sales cycles, and stronger epistemic trust. These are not independent metrics but connected results of the same underlying shift—when buyers can more easily evaluate vendor claims, trust them, and act on them, the entire commercial process becomes more efficient.

The framework departs from conventional marketing mix models in one important respect: it treats the 7Ps not as independent variables but as a system in which changes in any one element have implications for the others. This is not a purely theoretical distinction; it has practical consequences for how marketing organizations should structure their AI investments, governance arrangements, and performance measurement systems.

VI. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

A. Theoretical Contributions

The review makes three contributions to marketing theory. First, by applying the dynamic capabilities framework to marketing rather than to firm-level strategy, it positions AI not as a tool within the marketing function but as a metacapability that governs how all other marketing resources—people, processes, content, data—are combined and deployed. This distinction matters because it suggests that AI's competitive effects in marketing depend not just on which tools an organization adopts but on how deeply those tools are integrated into strategy and organizational capability [3][24].

Second, the paper contributes to the relatively underdeveloped conversation about cognitive load in B2B purchasing. While Sweller's framework has been widely applied in educational psychology and consumer behavior, its application to enterprise procurement decisions is limited. The argument that AI-mediated evidence generation reduces extraneous cognitive load for buyers and thereby accelerates trust formation—and that this trust is qualitatively different from the relational trust studied in most B2B marketing literature—offers a productive framework for future empirical work [6][29].

Third, the information asymmetry argument provides a theoretical account of why AI-generated evidence has competitive value that goes beyond its content. When a vendor can produce objective, verifiable, contextualized performance data that buyers can evaluate without deep technical expertise, it changes the competitive basis of the market in ways that favor vendors with the best evidence infrastructure rather than the best sales relationships [22].

B. Practical Implications

For cybersecurity vendors, the analysis suggests that piecemeal AI adoption—adding a chatbot here, a personalization tool there—is unlikely to produce the competitive advantages that the framework implies. The returns from AI in marketing appear to be highest when capabilities are developed across the full marketing mix and governed through an integrated data infrastructure, rather than layered onto existing manual processes as point solutions. This has implications for investment prioritization, organizational structure, and the governance of data as a strategic asset [30].

For sales organizations specifically, the People analysis points toward a meaningful change in what is required of frontline commercial teams. The skills that matter most in an AI-augmented sales environment—interpreting and communicating AI-generated evidence, navigating AI-orchestrated customer journeys, and focusing human energy on the interpersonal dimensions of complex deals—are different from those emphasized in traditional sales training programs. Organizations that recognize this shift early will have an advantage in talent development [10].

C. Limitations and Future Research

Several limitations of this review deserve acknowledgment. As a systematic review rather than an empirical study, it synthesizes existing research rather than generating new observations, and it is therefore limited by the scope and quality of the published literature. The commercial deployment of agentic AI in marketing contexts is recent enough that rigorous longitudinal outcome studies are scarce; many of the mechanisms described in this paper are well-supported theoretically but await systematic empirical validation.

The review also focuses primarily on large enterprise vendors. The cybersecurity sector includes a diverse population of mid-market players, managed service providers, and regional specialists whose marketing challenges and AI capabilities may differ significantly from those of the global vendors that dominate the academic literature. India's rapidly developing cybersecurity ecosystem—particularly the concentration of technology firms in Pune, Bangalore, and Hyderabad—represents an under-studied context where the relationship between AI marketing capability and competitive outcomes may look quite different from patterns observed in Western enterprise markets [23].

The ethical dimensions of AI-driven marketing also warrant more systematic attention than this review has been able to provide. Research on algorithmic aversion has shown that buyers sometimes respond negatively to personalization when they perceive that their behavior is being monitored or their decisions are being influenced without disclosure [8]. The conditions under which AI-driven evidence generation and personalization enhance rather than undermine buyer trust remain an open empirical question, and one with direct commercial and regulatory implications.

Effective directions for future research include longitudinal studies of AI marketing capability and customer lifetime value in cybersecurity; experimental studies of the cognitive load and trust mechanisms described in Section II; comparative studies examining whether the framework generalizes to other high-complexity B2B technology markets; and qualitative organizational research on the governance and talent challenges involved in building integrated AI marketing capability.

VII. CONCLUSION

The key rationale of this paper is that the importance of AI for B2B marketing in cybersecurity is architectural rather than operational. It is not about doing marketing more efficiently; it is about fundamentally changing what marketing is, how marketing relates to other marketing functions, and what marketing is capable of achieving. Products that learn continuously, prices that adjust to individual risk profiles, promotions that focus on buyer intent, channels that are managed through performance intelligence, sales engineers that are assisted through real-time decision technologies, customers that are managed through predictive health scoring, credibility that is built through evidence of outcomes—this is not marketing that is more efficient; this is marketing that is fundamentally different from how we have traditionally conceived of marketing.

The model presented in this paper's three-tier framework of intelligence gathering, AI-mediated orchestration, and strategic outcome measurement offers a useful way to think about how these capabilities interact with one another and how they relate to the competitive objectives they ultimately serve. The value of the model is not in identifying the various AI technologies at the disposal of cybersecurity marketers; rather, it is in illuminating the logic that connects investments in AI capability to marketing performance and ultimately to the epistemic trust that underwrites purchasing decisions in a sector structurally resistant to proof of value.

Further empirical validations are needed today and in future, since the practice of AI in B2B marketing is progressing at a relatively faster rate than the speed of literature research. The models or frameworks discussed here, are intended to provide a direction or base rather than replacing empirical research.

As derived from initial inferences drawn at this stage, organizations that consider AI as a marketing capability rather than a marketing tool, and those organizations that invest in the data processing, infrastructure, organizational integration, and capability development required to leverage AI's potential, are expected to redefine what constitutes a competitive edge in enterprise cybersecurity markets in the near future.

REFERENCES

[1] T. H. Davenport, A. Guha, D. Grewal, and T. Bressgott, "How artificial intelligence will change the future of marketing," J. Acad. Mark. Sci., vol. 48, no. 1, pp. 24–42, 2020.

[2] M.-H. Huang and R. T. Rust, "Engaged to a Robot? The Role of AI in Service," J. Serv. Res., vol. 24, no. 1, pp. 30–41, 2021.

[3] D. J. Teece, "The foundations of enterprise performance: Dynamic and ordinary capabilities in an (economic) theory of firms," Strat. Mgmt. J., vol. 35, no. 3, pp. 328–352, 2014.

[4] M. Wedel and P. K. Kannan, "Marketing analytics for data-rich environments," J. Mark., vol. 80, no. 6, pp. 97–121, 2016.

[5] D. Grewal, J. Hulland, G. Kopalle, and E. Karahanna, "The future of technology and marketing: A multidisciplinary perspective," J. Acad. Mark. Sci., vol. 48, no. 1, pp. 1–8, 2020.

[6] J. Sweller, "Cognitive load during problem solving: Effects on learning," Cognitive Science, vol. 12, no. 2, pp. 257–285, 1988.

[7] P. C. Verhoef et al., "Digital transformation: A multidisciplinary reflection and research agenda," J. Bus. Res., vol. 122, pp. 889–901, 2021.

[8] Z. Katona, P. Zubcsek, and M. Sarvary, "Network effects and personal influences: The diffusion of an online social network," Mark. Sci., vol. 30, no. 6, pp. 1004–1023, 2022.

[9] G. Overgoor, M. Chica, W. Rand, and A. Weishampel, "Letting the computers take over: Using AI to solve marketing problems," Calif. Mgmt Rev., vol. 61, no. 4, pp. 156–185, 2019.

[10] N. Syam and A. Sharma, "Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice," Ind. Mark. Mgmt, vol. 69, pp. 135–146, 2018.

[11] J. Paschen, M. Wilson, and J. J. Ferreira, "Collaborative intelligence: How human and artificial intelligence create value along the B2B sales funnel," Bus. Horiz., vol. 63, no. 3, pp. 403–414, 2020.

[12] Y. K. Dwivedi et al., "Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," Int. J. Inf. Mgmt, vol. 57, p. 101994, 2021.

[13] R. T. Rust, "The future of marketing," Int. J. Res. Mark., vol. 37, no. 1, pp. 15–26, 2020.

[14] J. Singh et al., "Sales profession and professionals in the age of digitization and artificial intelligence technologies," J. Pers. Sell. Sales Mgmt, vol. 39, no. 1, pp. 2–22, 2019.

[15] J. H. Kietzmann, L. W. Lee, I. P. McCarthy, and T. C. Kietzmann, "Deepfakes: Trick or treat?" Bus. Horiz., vol. 63, no. 2, pp. 135–146, 2018.

[16] J. Järvinen and H. Taiminen, "Harnessing marketing automation for B2B content marketing," Ind. Mark. Mgmt, vol. 54, pp. 164–175, 2016.

[17] N. A. Morgan, K. A. Whitler, H. Feng, and S. Chari, "Research in marketing strategy," J. Acad. Mark. Sci., vol. 47, no. 1, pp. 4–29, 2019.

[18] D. L. Hoffman and T. P. Novak, "Consumer and object experience in the internet of things: An assemblage theory approach," J. Consum. Res., vol. 44, no. 6, pp. 1178–1204, 2018.

[19] R. V. Kozinets, "Consuming technocultures: An extended JCR curation," J. Consum. Res., vol. 46, no. 3, pp. 620–627, 2019.

[20] R. W. Palmatier, M. B. Houston, and J. Hulland, "Review articles: Purpose, process, and structure," J. Acad. Mark. Sci., vol. 46, no. 1, pp. 1–5, 2019.

[21] B. Wierenga, "Managerial decision making in marketing: The next research frontier," Int. J. Res. Mark., vol. 28, no. 2, pp. 89–101, 2011.

[22] M. Haenlein and A. Kaplan, "A brief history of artificial intelligence: On the past, present, and future of artificial intelligence," Calif. Mgmt Rev., vol. 61, no. 4, pp. 5–14, 2019.

[23] M. Colombo, C. Franzoni, and C. Rossi-Lamastra, "Internal social capital and the attraction of early contributions in crowdfunding," Entrepreneurship Theory Pract., vol. 39, no. 1, pp. 75–100, 2022.

[24] P. Mikalef and A. Gupta, "Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance," Inf. & Mgmt, vol. 58, no. 3, p. 103434, 2021.

[25] P. K. Chintagunta, P. Hanssens, and J. Hauser, "Marketing science and big data," Mark. Sci., vol. 35, no. 3, pp. 341–342, 2016.

[26] D. Marinova, S. K. Singh, and J. Singh, "Frontline problem-solving effectiveness: A dynamic analysis of verbal and nonverbal cues," J. Mark. Res., vol. 55, no. 2, pp. 178–192, 2018.

[27] V. Kumar, W. Reinartz, and G. Bhardwaj, "Creating enduring customer value," J. Mark., vol. 80, no. 6, pp. 36–68, 2019.

[28] B. Libai et al., "Brave new world? On AI and the management of customer relationships," J. Interact. Mark., vol. 51, pp. 44–56, 2020.

[29] A. Guha et al., "How artificial intelligence will affect the future of retailing," J. Retailing, vol. 97, no. 1, pp. 28–41, 2021.

[30] A. M. T. Borges et al., "The strategic use of artificial intelligence in the digital era," Int. J. Inf. Mgmt, vol. 57, p. 102225, 2021.