Journal of
Study and Innovation in Education and Development Vol. 6, Issue 3 (2025): 1-27

A Mixed-Methods Cybersecurity Governance Model for the Islamic Republic of Iran in the Ten-Year Horizon

Hossein Jangravi[1], Jamal Aberoumand[2]*, Mohammad Reza Arab Baferani[2]
1. PhD Student in Futures Studies, Imam Hossein University, Tehran, Iran
2. Assistant Professor of Hazrat Wali Asr Aj Research Institute of Imam Hussein University

Received: 14 Jan 2026
Accepted: 15 May 2026
First Available: 09 Jun 2026
Final Publication: 23 Jul 2026

Keywords
Cybersecurity Governance, Interpretive Structural Modeling, MICMAC Analysis, Digital Governance, National Security, Mixed-Methods Approach, Islamic Republic of Iran

ABSTRACT

The present study aimed to design a cybersecurity governance model for the Islamic Republic of Iran in a ten-year horizon using a mixed-methods approach and to identify the structural relationships among its components. This study employed an exploratory mixed-methods design conducted in qualitative and quantitative phases. In the qualitative phase, thematic analysis was applied through semi-structured in-depth interviews with 15 experts in cybersecurity, information technology, public policy, and strategic management to identify the dimensions and components of cybersecurity governance. Participants were selected using purposive and snowball sampling methods, and interviews continued until theoretical saturation was achieved. In the quantitative phase, Interpretive Structural Modeling (ISM) and MICMAC analysis were used to determine the hierarchical structure and interrelationships among the identified components. Quantitative data were collected using pairwise comparison questionnaires, and the relationships among variables were analyzed through the Structural Self-Interaction Matrix, final reachability matrix, and driving-dependence analysis. The qualitative findings revealed four organizing themes: governance experiences in the Islamic Revolution, desirable governance structures and processes, strategic goal-setting in the ten-year horizon, and cybersecurity governance challenges. The ISM results demonstrated a seven-level hierarchical structure in which ideological and theoretical foundations, macro governance structures, state-society relations, and strategic long-term goals were identified as the fundamental driving forces at the highest level. Technological, managerial, cultural, and geopolitical challenges were located at the lowest level and exhibited the highest dependence on other variables. The MICMAC analysis further indicated that structural, institutional, and policy-related variables were positioned in the independent zone, while infrastructural and managerial variables were categorized in the linkage zone. No autonomous variables were identified within the model. The findings indicated that cybersecurity governance in the Islamic Republic of Iran is a multidimensional, networked, and strategic system requiring coordination among ideological foundations, institutional structures, policymaking mechanisms, operational infrastructures, crisis management, and social participation. Accordingly, developing a localized, adaptive, and future-oriented governance model can enhance national cyber resilience and improve the effectiveness of digital governance.

How to cite:
Jangravi, H., Aberoumand, J., & Arab Baferani, M. R. (2026). A Mixed-Methods Cybersecurity Governance Model for the Islamic Republic of Iran in the Ten-Year Horizon. *Study and Innovation in Education and Development*, *6*(3), 1-27.

*** Corresponding Author:**
Jamal Aberoumand
E-mail: j.aberoomand@ihu.ac.ir

EXTENDED ABSTRACT

INTRODUCTION

Cybersecurity governance has emerged as one of the most critical dimensions of contemporary governance systems due to the rapid expansion of cyberspace, digital transformation, artificial intelligence, smart infrastructures, and platform-based economies. In recent decades, cyberspace has evolved from a technical communication environment into a strategic domain intertwined with national security, economic sustainability, political stability, public trust, and social resilience. Consequently, cybersecurity can no longer be understood merely as a technical issue related to information protection; rather, it has become a multidimensional governance challenge involving policy-making, institutional coordination, regulation, crisis management, infrastructure resilience, public participation, and strategic foresight (25, 33, 35).

Recent studies emphasize that cybersecurity governance is increasingly connected to organizational innovation, investor trust, public confidence, digital transformation, and institutional legitimacy. Effective cybersecurity governance frameworks improve organizational resilience and strategic performance while reducing vulnerability to cyber threats (23, 24). Furthermore, the emergence of artificial intelligence and smart governance systems has intensified the need for adaptive and ethical cybersecurity governance capable of addressing evolving technological risks (26-28). Contemporary governance models therefore require a transition from centralized and reactive security approaches toward participatory, networked, and future-oriented governance systems (29).

For countries facing geopolitical pressures, hybrid warfare, sanctions, and information conflicts, cybersecurity governance assumes an even more strategic role. In such contexts, cyber threats are not limited to technical intrusions but may influence social stability, political trust, economic systems, and public order. Studies conducted in the Iranian context indicate that cyberspace has become deeply connected with emerging security threats and social dynamics (30). Therefore, designing a comprehensive cybersecurity governance model aligned with national values, institutional capacities, and strategic priorities is essential for sustainable digital security and national resilience.

Existing literature on cybersecurity governance has explored diverse themes, including governance maturity models, adaptive governance frameworks, cybersecurity policy, digital regulation, and human-centered cybersecurity approaches (31, 36, 45). However, most existing studies focus either on organizational cybersecurity management or on technical dimensions of cybersecurity. Fewer studies have attempted to develop a

comprehensive national cybersecurity governance model integrating ideological, institutional, social, managerial, infrastructural, and geopolitical dimensions simultaneously. Moreover, limited attention has been given to long-term strategic horizons and the structural relationships among governance components.

Theoretical discussions also emphasize the significance of governance quality, institutional coordination, transparency, participation, and leadership in cybersecurity systems (34, 38). Governance in cyberspace increasingly depends on interactions among governments, private organizations, regulatory institutions, technological platforms, and citizens. Consequently, cybersecurity governance must be conceptualized as a dynamic and interconnected governance ecosystem rather than a purely technical security arrangement (29). Human-centered cybersecurity studies further demonstrate that organizational culture, security psychology, cognitive awareness, and public participation significantly influence cybersecurity effectiveness (45, 46).

Despite the growing importance of cybersecurity governance, there remains a significant gap in developing a localized, strategic, and future-oriented governance model for the Islamic Republic of Iran. Addressing this gap requires an integrative methodological approach capable of identifying the key dimensions of cybersecurity governance while also clarifying the hierarchical and structural relationships among them. Accordingly, the present study aimed to design a cybersecurity governance model for the Islamic Republic of Iran in a ten-year horizon using a mixed-methods approach.

METHODS AND MATERIALS

This study employed an exploratory mixed-methods design integrating qualitative and quantitative approaches. The research was conducted in two sequential phases. In the qualitative phase, thematic analysis was used to identify the major dimensions, components, and conceptual relationships of cybersecurity governance. Semi-structured in-depth interviews were conducted with experts in cybersecurity, information technology, governance, public policy, and strategic management. Participants were selected through purposive and snowball sampling methods. The interview process continued until theoretical saturation was achieved, which occurred after 15 interviews.

The qualitative data analysis process included open coding, extraction of concepts, development of basic themes, organizing themes, and overarching themes. The identified themes formed the preliminary conceptual model of cybersecurity governance. To enhance the credibility and reliability of the qualitative findings, expert review, intercoder agreement, and content validation techniques were employed.

In the quantitative phase, Interpretive Structural Modeling (ISM) was used to analyze the structural relationships among the extracted components and determine their hierarchical levels. The same panel of experts participated in the ISM phase. Data were collected using a pairwise comparison questionnaire specifically designed for structural analysis. Experts evaluated the directional relationships among the governance components using the standard ISM symbols V, A, X, and O.

The ISM procedure involved constructing the Structural Self-Interaction Matrix (SSIM), converting it into the initial reachability matrix, developing the final reachability matrix through transitivity analysis, and determining the hierarchical levels of variables. Subsequently, MICMAC analysis was conducted to identify the driving power and dependence power of the variables and classify them into independent, linkage, dependent, and autonomous categories.

FINDINGS

The qualitative findings revealed that the cybersecurity governance model of the Islamic Republic of Iran in the ten-year horizon consisted of four major organizing themes: governance experiences in the Islamic Revolution, desirable structures and processes of cybersecurity governance, strategic goal-setting in the ten-year horizon, and cybersecurity governance challenges.

The first organizing theme included ideological and theoretical foundations, structural and institutional dimensions, governance transformations, managerial dimensions, and state-society relations. The second organizing theme encompassed governance and regulatory institutions, national operational infrastructures, information and data infrastructures, macro governance structures, networked and participatory structures, adaptive governance structures, policy frameworks, evaluation systems, crisis management, and future-oriented prevention mechanisms. The third organizing theme involved strategic goals, mid-term goals, operational goals, and performance evaluation indicators. The fourth organizing theme consisted of structural, technological, managerial, social, cultural, and geopolitical challenges.

The demographic analysis of the expert panel showed that the participants possessed substantial academic and professional expertise in cybersecurity and information technology. Most participants held doctoral degrees and had more than five years of professional experience in academic, governmental, or technological institutions.

The ISM analysis demonstrated that the model had a seven-level hierarchical structure. At the highest level of the hierarchy, ideological and theoretical foundations,

macro governance structures, state-society relations, governance transformations, and strategic ten-year goals were identified as the fundamental driving forces of cybersecurity governance. These variables exhibited the strongest driving power and the lowest dependence.

The sixth level included institutional and managerial structures, governance and regulatory institutions, participatory governance structures, and adaptive governance systems. The fifth level consisted of operational and informational infrastructures. The fourth level contained policy frameworks and evaluation systems. The third level included mid-term goals, crisis management, and future-oriented prevention mechanisms. The second level consisted of operational goals and performance indicators. Finally, the first level included technological, managerial, structural, social, and geopolitical challenges as the most dependent variables in the system.

The MICMAC analysis revealed that ideological foundations, macro governance structures, governance institutions, and policy frameworks were located in the independent zone, indicating strong driving power and weak dependence. Variables such as operational infrastructures, information infrastructures, crisis management, and future-oriented governance were located in the linkage zone, reflecting both high influence and high dependence. Operational goals, evaluation indicators, and cybersecurity challenges were categorized as dependent variables. No variable was located in the autonomous zone, indicating strong structural interconnectedness among all governance components.

DISCUSSION AND CONCLUSION

The findings of this study demonstrate that cybersecurity governance in the Islamic Republic of Iran is a multidimensional and interconnected governance system rather than a purely technical security framework. The placement of ideological foundations, macro governance structures, and state-society relations at the highest level of the ISM hierarchy indicates that cybersecurity governance is deeply embedded within broader political, institutional, and social structures. This finding suggests that sustainable cybersecurity governance cannot be achieved solely through technological development or technical regulation; instead, it requires strategic alignment among governance philosophy, institutional architecture, public trust, and long-term national goals.

The results also highlight the critical role of governance institutions, policy frameworks, and adaptive structures in shaping the effectiveness of cybersecurity governance. The positioning of these variables within the independent and linkage zones of the MICMAC analysis demonstrates that governance quality, institutional coordination,

and strategic policymaking significantly influence the entire cybersecurity ecosystem. In practical terms, weaknesses in institutional coordination or policy integration may eventually manifest as technological vulnerabilities, organizational inefficiencies, or societal cybersecurity challenges.

Another important finding concerns the central role of operational infrastructures, information systems, crisis management, and future-oriented governance mechanisms. These components function as the operational core of cybersecurity governance and serve as the connecting layer between strategic governance principles and practical implementation. Their simultaneous high influence and dependence indicate that cybersecurity governance requires continuous adaptation, coordination, and learning in response to evolving technological and geopolitical conditions.

The findings further suggest that cybersecurity challenges should not be viewed merely as isolated technical problems but rather as outcomes of broader governance conditions. Technological threats, managerial weaknesses, social distrust, and geopolitical vulnerabilities emerge as consequences of governance quality across higher structural and strategic levels. Therefore, addressing cybersecurity challenges requires systemic reforms involving institutional restructuring, policy integration, infrastructure development, strategic foresight, and human-centered governance approaches.

The absence of autonomous variables in the MICMAC analysis confirms the highly interconnected nature of cybersecurity governance. All identified components participate meaningfully within the governance system, indicating that cybersecurity governance functions as a complex adaptive network. Consequently, isolated or fragmented interventions are unlikely to generate sustainable outcomes. Instead, effective cybersecurity governance requires coordinated and integrated policymaking across institutional, technological, social, and strategic dimensions.

Overall, the present study provides a localized, future-oriented, and structurally integrated model for cybersecurity governance in the Islamic Republic of Iran. The proposed model emphasizes the importance of ideological coherence, institutional coordination, adaptive governance, operational infrastructures, strategic foresight, and participatory governance in strengthening national cybersecurity resilience. The findings suggest that future cybersecurity governance strategies should prioritize systemic integration, institutional adaptability, public participation, and long-term strategic planning in order to address the increasingly complex and evolving challenges of cyberspace.

مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله بر مبنای رویکرد آمیخته

حسین جنگروی[۱]، جمال آبرومند[۲*]، محمدرضا عرب بافرانی[۲]

۱. دانشجوی دکتری رشته آینده پژوهی، دانشگاه امام حسین (ع)، تهران، ایران

۲. استادیار پژوهشکده حضرت ولی عصر عج الله دانشگاه جامع امام حسین (ع)، تهران، ایران

تاریخ دریافت: ۱۴۰۴/۱۰/۲۴

تاریخ پذیرش: ۱۴۰۵/۰۲/۲۵

تاریخ چاپ اولیه: ۱۴۰۵/۰۳/۱۹

تاریخ چاپ نهایی: ۱۴۰۵/۰۵/۰۱

چکیده

هدف پژوهش حاضر طراحی مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله بر مبنای رویکرد آمیخته و تبیین روابط ساختاری میان مؤلفه‌های آن بود. پژوهش حاضر از نظر روش، آمیخته اکتشافی بود که در دو بخش کیفی و کمی انجام شد. در بخش کیفی، با استفاده از تحلیل مضمون و انجام مصاحبه‌های نیمه‌ساختاریافته عمیق با ۱۵ نفر از خبرگان حوزه امنیت سایبری، فناوری اطلاعات، سیاست‌گذاری و مدیریت راهبردی، ابعاد و مؤلفه‌های حکمرانی امنیت سایبری شناسایی شد. نمونه‌گیری به‌صورت هدفمند و گلوله‌برفی انجام گرفت و فرایند مصاحبه‌ها تا اشباع نظری ادامه یافت. در بخش کمی، به‌منظور سطح‌بندی و تحلیل روابط میان مؤلفه‌ها، از روش مدل‌سازی ساختاری تفسیری (ISM)و تحلیل MICMAC استفاده شد. داده‌های کمی از طریق پرسشنامه مقایسه زوجی جمع‌آوری و روابط میان متغیرها بر اساس ماتریس خودتعاملی ساختاری، ماتریس دسترسی نهایی و تحلیل قدرت نفوذ–وابستگی بررسی گردید. یافته‌های کیفی نشان داد که مدل حکمرانی امنیت سایبری دارای چهار مضمون سازمان‌دهنده شامل تجربه‌های حکومت‌گرایی در انقلاب اسلامی، اجزا و ساختارهای مطلوب حکمرانی، هدف‌گذاری در افق ده‌ساله و چالش‌های حکمرانی امنیت سایبری است. نتایج ISM نشان داد که مدل دارای ساختاری هفت‌سطحی است که در آن مبانی ایدئولوژیک و نظری، ساختار کلان حکمرانی، نسبت دولت و جامعه و اهداف کلان ده‌ساله به‌عنوان پیشران‌های بنیادین در بالاترین سطح قرار دارند. همچنین، چالش‌های فناورانه، مدیریتی، فرهنگی و ژئوپلیتیکی در پایین‌ترین سطح مدل قرار گرفتند و بیشترین وابستگی را به سایر متغیرها داشتند. تحلیل MICMAC نیز نشان داد که متغیرهای ساختاری، سیاستی و نهادی در ناحیه نفوذی و متغیرهای زیرساختی و مدیریتی در ناحیه پیوندی قرار دارند و هیچ متغیری در ناحیه خودمختار مشاهده نشد. نتایج پژوهش نشان داد که حکمرانی امنیت سایبری در جمهوری اسلامی ایران ماهیتی چندسطحی، شبکه‌ای و راهبردی دارد و تحقق امنیت پایدار سایبری مستلزم هماهنگی میان مبانی نظری، ساختارهای نهادی، سیاست‌گذاری، زیرساخت‌های عملیاتی، مدیریت بحران و مشارکت اجتماعی است. بر این اساس، طراحی یک مدل بومی، انعطاف‌پذیر و آینده‌نگر می‌تواند زمینه ارتقای تاب‌آوری سایبری و کارآمدی حکمرانی دیجیتال کشور را فراهم سازد.

واژگان کلیدی

حکمرانی امنیت سایبری، مدل‌سازی ساختاری تفسیری، تحلیل MICMAC، حکمرانی دیجیتال، امنیت ملی، رویکرد آمیخته، جمهوری اسلامی ایران

شیوه ارجاع‌دهی:

جنگروی، حسین.، آبرومند، جمال.، و عرب بافرانی، محمدرضا. (۱۴۰۵). مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله بر مبنای رویکرد آمیخته. *پژوهش و نوآوری در تربیت و توسعه*، ۶(۳)، ۲۷-۱.

نویسنده مسئول:
جمال آبرومند
پست الکترونیکی: j.aberoomand@ihu.ac.ir

مقدمه

گسترش فضای سایبری در دهه‌های اخیر، مفهوم امنیت ملی را از مرزهای سرزمینی فراتر برده و آن را به عرصه‌ای شبکه‌ای، داده‌محور، فناورانه و چندبازیگری تبدیل کرده است. در چنین شرایطی، امنیت سایبری دیگر صرفاً به حفاظت فنی از سامانه‌ها، شبکه‌ها و داده‌ها محدود نیست، بلکه به مسئله‌ای حکمرانی‌محور تبدیل شده که در آن دولت، نهادهای تنظیم‌گر، بخش خصوصی، جامعه مدنی، سازمان‌های علمی، نهادهای امنیتی و کاربران نهایی در یک نظام پیچیده از نقش‌ها، مسئولیت‌ها و تعاملات قرار می‌گیرند. از این منظر، حکمرانی امنیت سایبری به معنای طراحی، هماهنگی، اجرا و ارزیابی مجموعه‌ای از سیاست‌ها، ساختارها، فرآیندها و ظرفیت‌هاست که بتواند امنیت، تاب‌آوری، اعتماد، حریم خصوصی، نوآوری و منافع ملی را در محیط دیجیتال تضمین کند. ادبیات جدید نشان می‌دهد که حکمرانی امنیت سایبری در سطح ملی و سازمانی با موضوعاتی مانند اعتماد عمومی، ارزش بازار، نوآوری، تاب‌آوری زیرساختی و پایداری عملکردی پیوند مستقیم دارد (23-25).

در سطح جهانی، تحول دیجیتال، هوش مصنوعی، شهرهای هوشمند، اقتصاد پلتفرمی و خدمات عمومی دیجیتال، ضرورت بازاندیشی در مدل‌های سنتی امنیت سایبری را افزایش داده‌اند. با نفوذ هوش مصنوعی در تصمیم‌گیری‌های عمومی، خدمات شهری و فرآیندهای حکمرانی، امنیت سایبری به حوزه‌ای تبدیل شده که هم جنبه فناورانه دارد و هم با مسئولیت‌پذیری، اخلاق، قانون‌گذاری و اعتماد عمومی مرتبط است (26-28). در این وضعیت، سیاست‌گذاری سایبری باید علاوه بر شناسایی تهدیدات، بتواند چارچوبی برای هماهنگی نهادی، پاسخ‌گویی، حفاظت از داده‌ها و انطباق با تغییرات فناورانه فراهم سازد. از سوی دیگر، رشد پلتفرم‌های دیجیتال نشان داده است که حکمرانی در فضای سایبری نه خطی و متمرکز، بلکه شبکه‌ای، چندسطحی و متکی بر تنظیم‌گری پویا است (29). بنابراین، کشورهایی که فاقد مدل حکمرانی منسجم، آینده‌نگر و بومی هستند، در برابر تهدیدات نوظهور، جرائم سایبری، اختلالات زیرساختی و بحران‌های اعتماد عمومی آسیب‌پذیرتر خواهند بود.

حکمرانی امنیت سایبری در سطح ملی، به‌ویژه برای کشورهایی که با فشارهای ژئوپلیتیکی، تحریم، تهدیدات ترکیبی و جنگ شناختی مواجه‌اند، از اهمیت مضاعف برخوردار است. امنیت سایبری در این کشورها فقط به حفاظت از شبکه‌های اطلاعاتی محدود نمی‌شود، بلکه با امنیت سیاسی، امنیت اجتماعی، امنیت اقتصادی و ثبات نهادی نیز پیوند دارد. مطالعه تهدیدات نوین سایبری در ایران، به‌ویژه در زمینه اعتراضات و رخدادهای امنیتی، نشان می‌دهد که فضای سایبری می‌تواند هم بستری برای تعامل اجتماعی و هم ابزاری برای تولید، تشدید و سازمان‌دهی تهدیدات نوین باشد (30). از همین رو، حکمرانی امنیت سایبری در جمهوری اسلامی ایران باید به‌گونه‌ای طراحی شود که ضمن حفظ امنیت ملی و صیانت از زیرساخت‌های حیاتی، امکان مشارکت اجتماعی، شفافیت، اعتماد عمومی و توسعه خدمات دیجیتال را نیز تقویت کند. این ضرورت با توجه به ماهیت متغیر تهدیدات سایبری و تغییر سریع فناوری‌ها، نیازمند مدل‌سازی ده‌ساله و آینده‌نگر است.

یکی از چالش‌های اصلی در حکمرانی امنیت سایبری، نبود یکپارچگی میان سطح سیاست‌گذاری، سطح تنظیم‌گری، سطح اجرایی و سطح ارزیابی است. بسیاری از مدل‌های امنیت سایبری بر بلوغ فنی، کنترل‌های سازمانی یا استانداردهای اطلاعاتی تمرکز دارند، اما در سطح حکمرانی ملی، مسئله فراتر از شاخص‌های فنی است و باید نسبت میان ساختار نهادی، سیاست عمومی، فرهنگ امنیتی، سرمایه انسانی، زیرساخت داده‌ای و ظرفیت پاسخ‌گویی بررسی شود. مقایسه مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات نشان می‌دهد که هرچند این مدل‌ها برای سنجش وضعیت سازمانی مفیدند، اما برای طراحی مدل کلان حکمرانی، باید شاخص‌های مشترک امنیت سایبری با ملاحظات ساختاری، مدیریتی و سیاستی ترکیب شوند (31). همچنین، مدل‌های ارزیابی حکمرانی امنیت سایبری ملی بر این نکته تأکید دارند که بهبود حکمرانی نیازمند سنجش هم‌زمان سیاست‌ها، نقش‌ها، فرآیندها و ظرفیت‌های نهادی است (32).

از منظر نظری، حکمرانی امنیت سایبری ریشه در تحول تاریخی مفهوم حکمرانی سایبری دارد. پیشینه حکمرانی امنیت سایبری نشان می‌دهد که این حوزه در ابتدا بیشتر ذیل مدیریت ریسک، حفاظت از زیرساخت و امنیت اطلاعات تعریف می‌شد، اما به‌تدریج به حوزه‌ای سیاستی، نهادی و اجتماعی تبدیل شد که در آن هماهنگی میان بازیگران و تعیین قواعد تعامل اهمیت محوری یافت (33). این تحول نشان می‌دهد که امنیت سایبری را نمی‌توان صرفاً با ابزارهای فنی یا فرماندهی متمرکز اداره کرد، بلکه نیازمند ترکیبی از رهبری، فرهنگ حفاظتی، آموزش، مشارکت و یادگیری نهادی است. بر همین اساس، رویکردهای جدید بر نقش رهبری انسانی‌محور و فرهنگ سازمانی در ایجاد رفتارهای ایمن و پایدار تأکید دارند (34). در این نگاه، حکمرانی امنیت سایبری زمانی اثربخش است که بتواند ساختارهای رسمی و رفتارهای انسانی را به‌صورت هم‌زمان مدیریت کند.

تحول دیجیتال در خدمات عمومی نیز اهمیت حکمرانی امنیت سایبری را افزایش داده است. دیجیتالی‌شدن خدمات دولتی، دولت الکترونیک و شهرهای هوشمند، حجم عظیمی از داده‌های حساس را در اختیار نهادهای عمومی قرار داده و وابستگی شهروندان به سامانه‌های دیجیتال را افزایش داده است. در چنین وضعیتی، هرگونه ضعف در حکمرانی امنیت سایبری می‌تواند به اختلال در خدمات عمومی، نقض حریم خصوصی، کاهش اعتماد شهروندان و آسیب به مشروعیت نهادی منجر شود. پژوهش‌ها نشان می‌دهند که حکمرانی امنیت سایبری در تحول دیجیتال خدمات عمومی باید با حفاظت از محیط دیجیتال، ارتقای اعتماد و پاسخ‌گویی سازمانی همراه باشد (35). همچنین، در محیط‌های هوشمند، امنیت سایبری با ذی‌نفعان متعددی پیوند می‌خورد و هوش مصنوعی می‌تواند هم به افزایش کارآمدی و هم به خلق ریسک‌های جدید منجر شود (26). بنابراین، مدل مطلوب حکمرانی باید توانایی تنظیم رابطه میان فناوری، سازمان، قانون و جامعه را داشته باشد.

در کنار تحول دیجیتال، موضوع انطباق‌پذیری نیز یکی از مؤلفه‌های کلیدی حکمرانی امنیت سایبری است. تهدیدات سایبری ماهیتی ایستا ندارند و با ظهور فناوری‌های جدید، الگوهای حمله، آسیب‌پذیری‌ها و بازیگران تهدید نیز تغییر می‌کنند. از این رو، چارچوب‌های ثابت و غیرمنعطف نمی‌توانند پاسخ‌گوی پیچیدگی‌های آینده باشند. چارچوب‌های پویا و تطبیقی حکمرانی امنیت سایبری

بر این اصل تأکید دارند که نظام حکمرانی باید بتواند از طریق پایش مستمر، یادگیری نهادی، اصلاح سیاست‌ها و بازطراحی ساختارها با تغییرات محیطی سازگار شود (36). این رویکرد برای افق ده‌ساله اهمیت زیادی دارد؛ زیرا برنامه‌ریزی بلندمدت در فضای سایبری بدون توجه به عدم‌قطعیت، آینده‌نگری و مدیریت سناریو، به سرعت با فرسودگی سیاستی مواجه می‌شود.

یکی دیگر از ابعاد مهم حکمرانی امنیت سایبری، لایه‌بندی فضای سایبری و شناخت ساختار چندسطحی آن است. فضای سایبری را می‌توان متشکل از لایه‌های فیزیکی، منطقی، داده‌ای، خدماتی، شناختی و حکمرانی دانست که هر یک دارای الزامات امنیتی و تنظیم‌گری متفاوت‌اند. مرور مدل‌های لایه‌بندی فضای سایبری نشان می‌دهد که فهم دقیق ساختار لایه‌ای این فضا برای طراحی سیاست‌های امنیتی و حکمرانی ضروری است (37). در سطح ملی، نادیده‌گرفتن پیوند میان لایه‌های زیرساختی، داده‌ای، خدماتی و اجتماعی می‌تواند موجب شود که سیاست‌های امنیتی صرفاً بر بعد فنی تمرکز کنند و از ابعاد فرهنگی، مدیریتی و نهادی غفلت شود. بنابراین، مدل حکمرانی امنیت سایبری جمهوری اسلامی ایران باید بتواند میان لایه‌های مختلف فضای سایبری ارتباط برقرار کند و از نگاه تک‌بعدی به امنیت پرهیز نماید.

ادبیات حکمرانی عمومی نیز برای طراحی مدل حکمرانی امنیت سایبری اهمیت دارد. مفهوم حکمرانی خوب بر اصولی مانند شفافیت، پاسخ‌گویی، مشارکت، اثربخشی، قانون‌مندی و عدالت تأکید می‌کند و این اصول در فضای سایبری نیز قابل بازخوانی هستند. پژوهش‌های مربوط به حکمرانی خوب نشان داده‌اند که شفافیت و پاسخ‌گویی در سازمان‌های سیاست‌گذار می‌تواند به افزایش اعتماد و کاهش ناکارآمدی نهادی کمک کند (38). همچنین، تجربه‌های حکمرانی محلی و سازمانی نشان می‌دهد که کارآمدی حکمرانی وابسته به کیفیت نهادها، مشارکت ذی‌نفعان و قابلیت اجرای سیاست‌هاست (39). در زمینه ایرانی ـ اسلامی نیز مدل حکمرانی مطلوب باید با مبانی ارزشی، عدالت‌محوری، مسئولیت‌پذیری و الگوی پیشرفت بومی سازگار باشد (40). بر این اساس، حکمرانی امنیت سایبری در جمهوری اسلامی ایران نیازمند مدلی است که هم از اصول جهانی حکمرانی کارآمد بهره گیرد و هم با مبانی ارزشی و نهادی کشور سازگار باشد.

حکمرانی امنیت سایبری در سطح سازمانی و اقتصادی نیز پیامدهای مهمی دارد. مطالعات جدید نشان داده‌اند که حکمرانی امنیت سایبری می‌تواند بر ارزش بازار شرکت‌ها، اعتماد سرمایه‌گذاران، اعتماد زنجیره تأمین و نوآوری سازمانی اثر بگذارد (23, 24). این یافته‌ها نشان می‌دهد که امنیت سایبری دیگر هزینه‌ای صرفاً دفاعی نیست، بلکه یک دارایی راهبردی برای توسعه اقتصادی و اعتماد نهادی محسوب می‌شود. در همین راستا، پژوهش‌های حکمرانی شرکتی نیز نشان داده‌اند که ساختارهای حکمرانی مناسب می‌توانند عملکرد مالی و اعتبار سازمانی را بهبود بخشند (41). با این حال، پژوهش‌های حکمرانی و گزارشگری باید به مسائل روش‌شناختی مانند درون‌زایی و روابط علّی پیچیده نیز توجه کنند تا تحلیل‌ها دچار ساده‌سازی نشوند (42). این ملاحظه برای پژوهش حاضر نیز اهمیت دارد؛ زیرا روابط میان مؤلفه‌های حکمرانی امنیت سایبری، خطی و ساده نیستند و باید با رویکردهای ساختاری و تفسیری تحلیل شوند.

در سطح بین‌المللی، حکمرانی امنیت سایبری با مسائل تجارت، حاکمیت داده، جرائم فراملی، حریم خصوصی و امنیت ژئوپلیتیکی پیوند خورده است. معمای تجارت و امنیت سایبری نشان می‌دهد که کشورها در عین نیاز به اتصال و تعامل دیجیتال جهانی، باید از منافع امنیتی و حاکمیتی خود نیز حفاظت کنند (43). همچنین، چالش‌های جرائم سایبری جهانی و حریم خصوصی داده‌ها ضرورت تقویت چارچوب‌های سیاستی و حقوقی را برجسته کرده‌اند (25). از سوی دیگر، سلطه مالی و نهادی در توسعه جهانی نشان می‌دهد که سازوکارهای حکمرانی بین‌المللی همواره بی‌طرف نیستند و می‌توانند بازتاب‌دهنده قدرت‌های ساختاری باشند (44). بنابراین، برای کشوری مانند ایران، حکمرانی امنیت سایبری باید علاوه بر توجه به استانداردهای جهانی، ظرفیت مقاومت، خوداتکایی، استقلال داده‌ای و مدیریت فشارهای بین‌المللی را نیز در نظر بگیرد.

بعد انسانی حکمرانی امنیت سایبری نیز اهمیت بنیادی دارد. بخش قابل توجهی از رخدادهای امنیتی نه صرفاً به ضعف فناوری، بلکه به رفتار کاربران، خطای انسانی، ضعف آموزش، فرهنگ سازمانی نامناسب و نبود درک شناختی از تهدیدات مربوط است. مدل‌های انسان‌محور امنیت سایبری نشان می‌دهند که برای ارتقای وضعیت امنیتی، باید شناخت، نگرش، انگیزش، عادت‌های رفتاری و ظرفیت یادگیری کاربران و مدیران در نظر گرفته شود (45). همچنین، تغییر روان‌شناسی امنیت و وضعیت امنیتی سازمان‌ها در محیط‌هایی مانند تدارکات الکترونیک نشان می‌دهد که حکمرانی امنیت سایبری باید فرهنگ امنیتی را به‌عنوان بخشی از نظام حکمرانی تلقی کند (46). حتی آموزش حکمرانی و سیاست‌گذاری امنیت سایبری با روش‌های نوآورانه مانند محیط‌های بازی‌محور و اتاق فرار سایبری می‌تواند در ارتقای یادگیری سیاستی و آمادگی تصمیم‌گیران نقش داشته باشد (47). بنابراین، مدل ده‌ساله باید به سرمایه انسانی، آموزش، فرهنگ امنیتی و یادگیری نهادی توجه ویژه داشته باشد.

از منظر مشارکت اجتماعی، حکمرانی امنیت سایبری نمی‌تواند صرفاً بر کنترل دولتی و تصمیم‌گیری متمرکز تکیه کند. تجربه‌های حکمرانی مشارکتی و برندسازی اجتماعی نشان می‌دهند که مشارکت ذی‌نفعان، احساس مالکیت اجتماعی و پیوند میان راهبردهای محلی و جهانی می‌تواند کیفیت حکمرانی را افزایش دهد (48). این منطق در فضای سایبری نیز صادق است؛ زیرا امنیت سایبری بدون همکاری کاربران، شرکت‌ها، دانشگاه‌ها، نهادهای مدنی و بخش خصوصی امکان‌پذیر نیست. حکمرانی پلتفرمی نیز نشان می‌دهد که بسیاری از تصمیمات امنیتی در محیط‌هایی اتخاذ می‌شوند که دولت تنها بازیگر اصلی نیست و باید با پلتفرم‌ها، ارائه‌دهندگان خدمات، تولیدکنندگان داده و کاربران وارد تعامل شود (29). از این رو، نسبت دولت و جامعه یکی از محورهای مهم مدل حکمرانی امنیت سایبری در افق ده‌ساله است.

با وجود گسترش مطالعات مربوط به امنیت سایبری، حکمرانی دیجیتال، هوش مصنوعی، حکمرانی شرکتی، مدل‌های بلوغ و حکمرانی خوب، هنوز خلأ مهمی در زمینه طراحی یک مدل بومی، ساختاری، آینده‌نگر و مبتنی بر روش آمیخته برای حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران وجود دارد. بخشی از پژوهش‌ها بر تهدیدات، بخشی بر مدل‌های بلوغ، بخشی بر حکمرانی سازمانی و بخشی بر ابعاد فناورانه متمرکز بوده‌اند، اما کمتر پژوهشی توانسته است این ابعاد را در قالب مدلی منسجم و سطح‌بندی‌شده

برای افق ده‌ساله ترکیب کند. همچنین، با توجه به ماهیت پیچیده و چندسطحی حکمرانی امنیت سایبری، صرف تحلیل نظری یا توصیفی کفایت نمی‌کند و لازم است ابتدا مؤلفه‌ها از طریق تحلیل کیفی شناسایی شوند و سپس روابط ساختاری میان آن‌ها با قضاوت خبرگان و روش‌های ساختاری مانند ISM و MICMAC تحلیل گردد.

بر این اساس، پژوهش حاضر با تمرکز بر ضرورت طراحی الگویی بومی، راهبردی و آینده‌نگر، تلاش می‌کند شکاف موجود میان ادبیات نظری، الزامات سیاستی و نیازهای عملی حکمرانی امنیت سایبری کشور را پوشش دهد. اهمیت این مطالعه از آن جهت است که مدل پیشنهادی می‌تواند برای سیاست‌گذاران، نهادهای تنظیم‌گر، مدیران امنیت سایبری و برنامه‌ریزان کلان کشور، چارچوبی تحلیلی و عملیاتی برای تصمیم‌گیری در افق ده‌ساله فراهم کند. هدف پژوهش حاضر، طراحی مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله بر مبنای رویکرد آمیخته است.

روش پژوهش

پژوهش حاضر از نظر هدف، کاربردی و از حیث ماهیت و شیوه اجرا، مبتنی بر رویکرد آمیخته اکتشافی بود که با ترکیب روش‌های کیفی و کمی به طراحی مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله پرداخت. انتخاب رویکرد آمیخته اکتشافی به دلیل ماهیت پیچیده، چندبعدی و میان‌رشته‌ای موضوع حکمرانی امنیت سایبری صورت گرفت؛ زیرا این حوزه علاوه بر ابعاد فناورانه، دارای مؤلفه‌های سیاسی، حقوقی، مدیریتی، دفاعی، فرهنگی و راهبردی است و تبیین جامع آن نیازمند بهره‌گیری هم‌زمان از تحلیل‌های عمیق کیفی و اعتباربخشی ساختاری کمی است. در این پژوهش ابتدا داده‌های کیفی به‌منظور شناسایی ابعاد، مؤلفه‌ها، شاخص‌ها و روابط مفهومی مرتبط با حکمرانی امنیت سایبری گردآوری و تحلیل شد و سپس یافته‌های حاصل در مرحله کمی، از طریق مدل‌سازی ساختاری تفسیری سطح‌بندی و اعتبارسنجی گردید تا الگوی نهایی پژوهش تدوین شود. اجرای پژوهش در دو مرحله مجزا اما مکمل انجام گرفت و یافته‌های مرحله کیفی مبنای طراحی ابزارها و تحلیل‌های مرحله کمی قرار گرفت.

در بخش کیفی پژوهش، از روش تحلیل مضمون برای استخراج مفاهیم و مؤلفه‌های حکمرانی امنیت سایبری استفاده شد. جامعه مشارکت‌کنندگان در این بخش شامل خبرگان حوزه امنیت سایبری، فناوری اطلاعات، حکمرانی دیجیتال، سیاست‌گذاری عمومی، دفاع سایبری و مدیریت راهبردی بود که دارای سوابق علمی، اجرایی یا مدیریتی مرتبط بودند. نمونه‌گیری به‌صورت هدفمند و با بهره‌گیری از روش گلوله‌برفی انجام شد؛ به این صورت که ابتدا تعدادی از متخصصان شناخته‌شده حوزه شناسایی شدند و سپس از طریق معرفی آنان، سایر خبرگان واجد شرایط انتخاب گردیدند. معیارهای ورود به مطالعه شامل داشتن حداقل مدرک کارشناسی ارشد در حوزه‌های مرتبط، سابقه فعالیت تخصصی یا مدیریتی در حوزه امنیت سایبری یا سیاست‌گذاری فناوری، و آشنایی با ابعاد حکمرانی و امنیت ملی بود. فرایند مصاحبه‌ها تا رسیدن به اشباع نظری ادامه یافت و در نهایت پس از انجام ۱۵ مصاحبه نیمه‌ساختاریافته عمیق،

داده‌های جدید منجر به شکل‌گیری مفهوم یا مضمون تازه‌ای نشد و اشباع نظری حاصل گردید. مدت زمان هر مصاحبه بین ۴۵ تا ۹۰ دقیقه متغیر بود و مصاحبه‌ها پس از اخذ رضایت آگاهانه مشارکت‌کنندگان ضبط و سپس به‌صورت کامل پیاده‌سازی شدند.

در مرحله کمی پژوهش، هدف اصلی تعیین سطح اثرگذاری و اثرپذیری مؤلفه‌های استخراج‌شده و طراحی ساختار نهایی مدل حکمرانی امنیت سایبری بود. روش پژوهش در این بخش توصیفی–پیمایشی و مبتنی بر قضاوت خبرگان بود. جامعه آماری این مرحله شامل همان خبرگان مشارکت‌کننده در بخش کیفی بود که به دلیل تسلط مفهومی بر مؤلفه‌های استخراج‌شده، در فرایند تحلیل ساختاری نیز مشارکت داشتند. مشارکت خبرگان در این مرحله مبتنی بر تکمیل پرسشنامه‌های مقایسه زوجی و ارزیابی روابط میان متغیرها صورت گرفت. انتخاب این گروه به دلیل برخورداری از دانش تخصصی و تجربه اجرایی در حوزه امنیت سایبری و حکمرانی دیجیتال انجام شد تا ساختار نهایی مدل از پشتوانه علمی و عملی کافی برخوردار باشد.

ابزار گردآوری داده‌ها در مرحله کیفی، مصاحبه نیمه‌ساختاریافته عمیق بود که بر اساس مطالعه پیشینه پژوهش، اسناد بالادستی حوزه امنیت سایبری، سیاست‌های کلان فناوری اطلاعات و ادبیات نظری مرتبط با حکمرانی سایبری طراحی شد. سؤالات مصاحبه به‌گونه‌ای تدوین شدند که امکان شناسایی ابعاد کلیدی حکمرانی امنیت سایبری، چالش‌ها، الزامات، پیشران‌ها، موانع، راهبردها و روابط میان مؤلفه‌ها را فراهم سازند. ساختار مصاحبه‌ها انعطاف‌پذیر بود و پژوهشگر تلاش کرد ضمن حفظ چارچوب اصلی، امکان تعمیق مباحث و کشف مفاهیم جدید را نیز فراهم کند. به‌منظور تأمین روایی محتوایی ابزار، سؤالات اولیه در اختیار چند تن از اساتید دانشگاه و متخصصان حوزه امنیت سایبری قرار گرفت و پس از دریافت نظرات اصلاحی، نسخه نهایی مصاحبه تدوین شد.

پس از انجام مصاحبه‌ها، داده‌های کیفی با استفاده از روش تحلیل مضمون مورد بررسی قرار گرفتند. در این فرایند، ابتدا متن مصاحبه‌ها چندین بار مطالعه شد تا درک عمیقی از داده‌ها حاصل شود. سپس کدگذاری اولیه انجام گرفت و مفاهیم کلیدی استخراج شدند. در ادامه، کدهای مشابه در قالب مضامین پایه دسته‌بندی شدند و از تجمیع آن‌ها مضامین سازمان‌دهنده شکل گرفت. در نهایت، با تحلیل روابط میان مضامین، مضامین فراگیر استخراج و مدل مفهومی اولیه پژوهش تدوین شد. برای افزایش اعتبار یافته‌های کیفی، از روش‌هایی نظیر بازبینی مشارکت‌کنندگان، کنترل توسط خبرگان، توافق بین کدگذاران و بررسی روایی محتوایی استفاده شد. همچنین پژوهشگر با ثبت دقیق مراحل تحلیل و مستندسازی فرایند کدگذاری، قابلیت پیگیری و اطمینان‌پذیری تحلیل‌ها را تقویت کرد.

در بخش کمی پژوهش، ابزار اصلی گردآوری داده‌ها پرسشنامه مقایسه زوجی مبتنی بر مدل‌سازی ساختاری تفسیری بود. این پرسشنامه بر اساس مؤلفه‌های استخراج‌شده از مرحله کیفی طراحی شد و هدف آن تعیین نوع و جهت روابط میان متغیرها بود. در این ابزار، خبرگان میزان اثرگذاری هر مؤلفه بر سایر مؤلفه‌ها را بر اساس قضاوت تخصصی خود ارزیابی کردند تا ماتریس خودتعاملی ساختاری شکل گیرد. طراحی پرسشنامه به‌گونه‌ای بود که روابط علی، سلسله‌مراتبی و تعاملی میان مؤلفه‌ها را مشخص سازد. روایی محتوایی پرسشنامه از طریق بررسی و تأیید متخصصان حوزه امنیت سایبری، مدیریت فناوری و روش‌های تصمیم‌گیری ساختاری تأیید

شد و به‌منظور اطمینان از شفافیت و قابلیت فهم گویه‌ها، نسخه اولیه ابزار به‌صورت آزمایشی در اختیار چند نفر از خبرگان قرار گرفت و اصلاحات لازم اعمال شد.

تحلیل داده‌های کیفی با بهره‌گیری از روش تحلیل مضمون انجام شد. در این فرایند، پژوهشگر پس از پیاده‌سازی کامل مصاحبه‌ها، اقدام به کدگذاری باز و استخراج مفاهیم اولیه نمود. سپس مفاهیم مشابه در قالب مضامین پایه طبقه‌بندی شدند و در مرحله بعد، مضامین سازمان‌دهنده و فراگیر شکل گرفتند. تحلیل داده‌ها به‌صورت مستمر و هم‌زمان با فرایند گردآوری اطلاعات انجام شد تا امکان اصلاح و تعمیق مصاحبه‌ها فراهم گردد. در نهایت، بر اساس مضامین استخراج‌شده، مدل مفهومی اولیه حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران طراحی شد. مدیریت و سازمان‌دهی داده‌های کیفی با استفاده از نرم‌افزار MAXQDA انجام گرفت که امکان طبقه‌بندی، کدگذاری و تحلیل نظام‌مند داده‌ها را فراهم ساخت.

در بخش کمی پژوهش، تحلیل داده‌ها بر اساس روش مدل‌سازی ساختاری تفسیری انجام شد. در گام نخست، ماتریس خودتعاملی ساختاری بر مبنای قضاوت خبرگان تشکیل شد و سپس این ماتریس به ماتریس دستیابی اولیه تبدیل گردید. در ادامه، با اعمال قواعد انتقال‌پذیری، ماتریس دستیابی نهایی استخراج شد و سطوح متغیرها تعیین گردید. پس از آن، روابط سلسله‌مراتبی میان مؤلفه‌ها مشخص و مدل ساختاری نهایی پژوهش ترسیم شد. این فرایند امکان شناسایی عوامل زیربنایی، پیوندی، وابسته و مستقل را در ساختار حکمرانی امنیت سایبری فراهم کرد و تصویری نظام‌مند از نحوه تعامل مؤلفه‌ها ارائه داد.

به‌منظور تکمیل تحلیل ساختاری و بررسی میزان نفوذ و وابستگی مؤلفه‌ها، تحلیل MICMAC نیز انجام شد. در این تحلیل، متغیرها بر اساس قدرت اثرگذاری و میزان وابستگی در چهار دسته مستقل، وابسته، پیوندی و خودمختار طبقه‌بندی شدند. نتایج تحلیل MICMAC به پژوهشگر کمک کرد تا مهم‌ترین پیشران‌های حکمرانی امنیت سایبری و عوامل کلیدی اثرگذار بر پایداری و کارآمدی نظام حکمرانی سایبری کشور را شناسایی کند. در مجموع، ترکیب تحلیل مضمون در بخش کیفی و مدل‌سازی ساختاری تفسیری همراه با تحلیل MICMAC در بخش کمی، امکان ارائه الگویی جامع، بومی و آینده‌نگر برای حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله را فراهم ساخت.

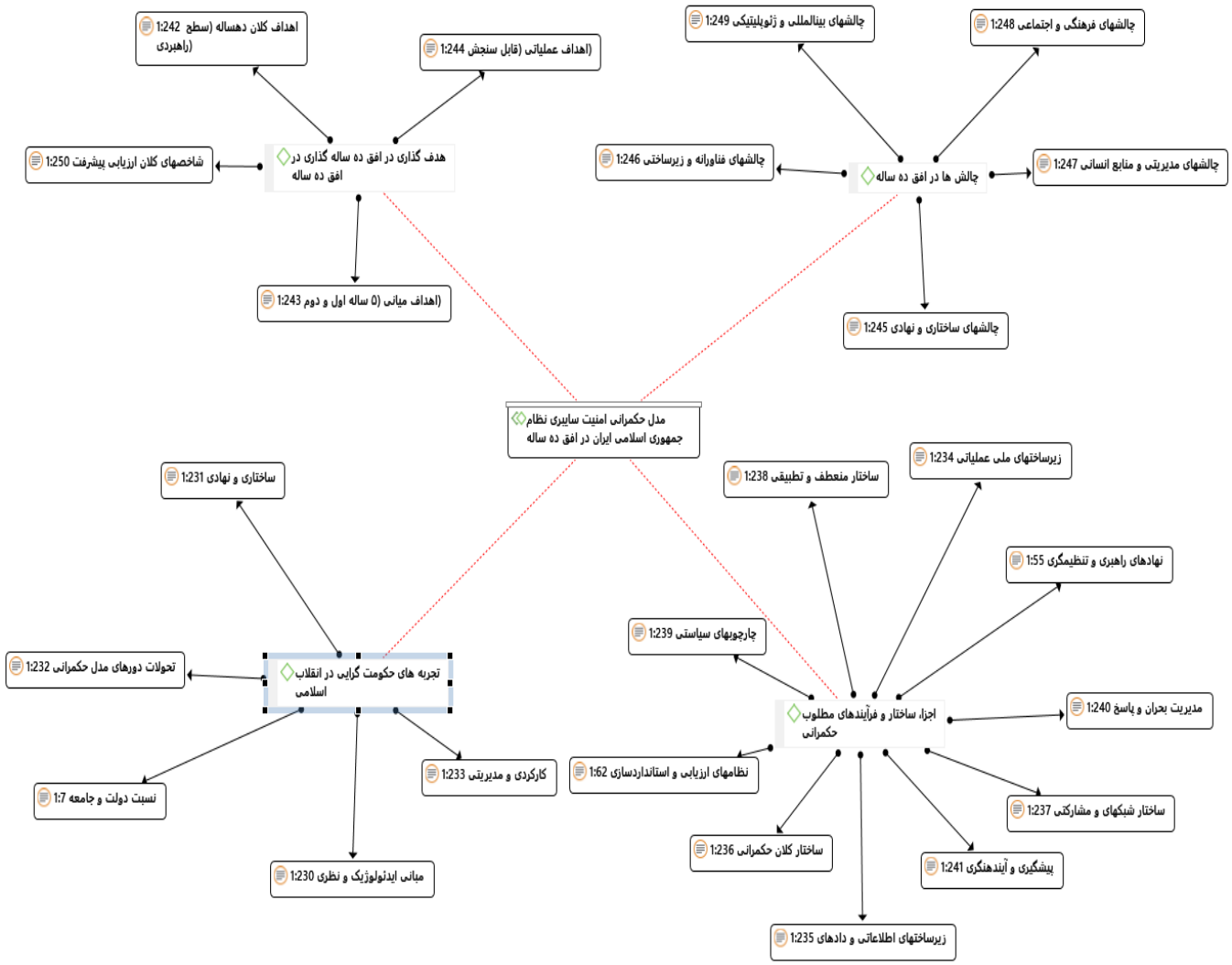
یافته‌ها

در بخش کیفی پژوهش، داده‌های حاصل از مصاحبه‌های نیمه‌ساختاریافته با ۱۵ نفر از خبرگان حوزه فناوری اطلاعات، امنیت سایبری، دانشگاه و سیاست‌گذاری از طریق تحلیل مضمون بررسی شد. فرایند تحلیل ابتدا با کدگذاری اولیه آغاز شد و سپس کدهای هم‌معنا و هم‌پوشان در قالب مفاهیم، مضامین پایه، مضامین سازمان‌دهنده و در نهایت مضامین فراگیر طبقه‌بندی شدند. نتایج تحلیل کیفی نشان داد که مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله دارای چهار مضمون سازمان‌دهنده اصلی

شامل تجربه‌های حکومت‌گرایی در انقلاب اسلامی، اجزا، ساختار و فرآیندهای مطلوب حکمرانی امنیت سایبری، هدف‌گذاری در افق ده‌ساله حکمرانی امنیت سایبری و چالش‌ها در افق ده‌ساله حکمرانی امنیت سایبری است.

جدول ۱. نتایج تحلیل کیفی مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله

شبکه مضامین	مضمون سازمان دهنده	مضمون فراگیر
مبانی ایدئولوژیک و نظری	تجربه‌های حکومت‌گرایی در انقلاب اسلامی	مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده ساله
ساختاری و نهادی		
تحولات دوره‌ای مدل حکمرانی		
کارکردی و مدیریتی		
نسبت دولت و جامعه		
نهادهای راهبری و تنظیم‌گری	اجزا، ساختار و فرآیندهای مطلوب حکمرانی امنیت سایبری	
زیرساخت‌های ملی عملیاتی		
زیرساخت‌های اطلاعاتی و داده‌ای		
ساختار کلان حکمرانی		
ساختار شبکه‌ای و مشارکتی		
ساختار منعطف و تطبیقی		
چارچوب‌های سیاستی		
نظام‌های ارزیابی و استانداردسازی		
مدیریت بحران و پاسخ		
پیشگیری و آینده‌نگری		
اهداف کلان ده‌ساله (سطح راهبردی)	هدف‌گذاری در افق ده‌ساله حکمرانی امنیت سایبری	
اهداف میانی (پنج‌ساله اول و دوم)		
اهداف عملیاتی (قابل سنجش)		
شاخص‌های کلان ارزیابی پیشرفت		
چالش‌های ساختاری و نهادی	چالش‌ها در افق ده‌ساله حکمرانی امنیت سایبری	
چالش‌های فناورانه و زیرساختی		
چالش‌های مدیریتی و منابع انسانی		
چالش‌های فرهنگی و اجتماعی		
چالش‌های بین‌المللی و ژئوپلیتیکی		



شکل ۱. شبکه مضامین مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله

نتایج کیفی نشان داد که حکمرانی امنیت سایبری در افق ده‌ساله صرفاً یک مسئله فنی یا فناورانه نیست، بلکه پدیده‌ای چندلایه و راهبردی است که در پیوند میان مبانی ایدئولوژیک، ساختار نهادی، ظرفیت‌های مدیریتی، زیرساخت‌های عملیاتی، تعامل دولت و جامعه، و چالش‌های محیطی معنا پیدا می‌کند. مضمون سازمان‌دهنده نخست، یعنی تجربه‌های حکومت‌گرایی در انقلاب اسلامی، نشان داد که مدل مطلوب حکمرانی امنیت سایبری باید با مبانی نظری و ارزشی نظام سیاسی، تجربه‌های نهادی جمهوری اسلامی، تحولات دوره‌ای حکمرانی، کارکردهای مدیریتی و الگوی رابطه دولت و جامعه سازگار باشد. مضمون دوم، اجزا و فرآیندهای مطلوب حکمرانی امنیت سایبری، بر ضرورت وجود نهادهای راهبری و تنظیم‌گری، زیرساخت‌های ملی عملیاتی، زیرساخت‌های داده‌ای، ساختار کلان حکمرانی، شبکه مشارکتی، انعطاف‌پذیری نهادی، چارچوب‌های سیاستی، نظام‌های ارزیابی، مدیریت بحران و آینده‌نگری تأکید داشت. مضمون سوم نشان داد که تحقق حکمرانی مطلوب نیازمند هدف‌گذاری مرحله‌ای در افق ده‌ساله است؛ به‌گونه‌ای که اهداف راهبردی، اهداف میانی، اهداف عملیاتی و شاخص‌های ارزیابی پیشرفت به‌صورت منسجم تعریف شوند. مضمون چهارم نیز

بیانگر آن بود که چالش‌های ساختاری، فناورانه، مدیریتی، فرهنگی و بین‌المللی باید نه به‌عنوان عناصر پراکنده، بلکه به‌عنوان پیامدهای مرتبط با کیفیت حکمرانی تحلیل شوند.

در بخش کمی پژوهش، پنل خبرگان شامل ۱۵ نفر بود که از نظر جنسیت، ۱۲ نفر مرد و ۳ نفر زن بودند. از نظر محدوده سنی، ۲ نفر در بازه ۲۵ تا ۳۰ سال، ۵ نفر در بازه ۳۱ تا ۴۰ سال، ۵ نفر در بازه ۴۱ تا ۵۰ سال و ۳ نفر در بازه ۵۱ تا ۶۰ سال قرار داشتند. از نظر سطح تحصیلات، ۴ نفر دارای مدرک کارشناسی‌ارشد و ۱۱ نفر دارای مدرک دکتری بودند. همچنین از نظر حوزه فعالیت، بخشی از خبرگان در حوزه فناوری اطلاعات، بخشی در دانشگاه و بخشی به‌صورت هم‌زمان در حوزه فناوری اطلاعات و دانشگاه فعالیت داشتند. سابقه کاری خبرگان نیز از ۵ سال تا بیش از ۲۰ سال متغیر بود که نشان‌دهنده ترکیب مناسبی از تجربه اجرایی، تخصص علمی و شناخت راهبردی در حوزه امنیت سایبری بود.

در مرحله ISM، ابتدا روابط میان ۲۴ مؤلفه استخراج‌شده از بخش کیفی بر اساس قضاوت خبرگان تعیین شد. برای این منظور، ماتریس خودتعاملی ساختاری با استفاده از نمادهای V، A، X و O تشکیل شد و سپس بر اساس قواعد استاندارد ISM به ماتریس دستیابی اولیه تبدیل گردید. در ادامه، با اعمال قاعده انتقال‌پذیری، ماتریس دسترسی نهایی به دست آمد؛ به این معنا که اگر مؤلفه‌ای بر مؤلفه دوم و مؤلفه دوم بر مؤلفه سوم اثرگذار بود، رابطه استنتاجی مؤلفه اول با مؤلفه سوم نیز در ماتریس نهایی لحاظ شد. روابط استنتاجی در ماتریس با علامت ۱* مشخص شدند تا از روابط مستقیم خبرگانی متمایز باشند.

جدول ۲. ماتریس دسترسی نهایی

i\j	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴
۱	۱	۱*	۱*	۱	۱	۱	۰	۰	۱	۱	۰	۱	۱*	۰	۱	۱	۰	۱	۱	۰	۰	۰	۰	۰
۲	۱	۱	۱	۰	۱*	۱*	۱	۰	۱	۱	۰	۱	۱*	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰
۳	۰	۰	۱	۱	۰	۱	۰	۰	۱	۱*	۰	۰	۱	۰	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰
۴	۰	۱	۱*	۱	۰	۰	۱	۰	۱*	۰	۰	۰	۰	۰	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰
۵	۰	۱	۱*	۰	۱	۱	۰	۰	۱*	۱	۰	۱	۱*	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۶	۰	۰	۰	۰	۰	۱	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۷	۰	۱	۱*	۰	۰	۰	۱	۰	۱*	۰	۰	۱	۱*	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۸	۰	۱	۱	۰	۱	۰	۰	۱	۱*	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۹	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۱۰	۱	۱	۱*	۰	۱	۱	۰	۰	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۱۱	۱	۱	۱*	۰	۱	۱	۰	۰	۱	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۱۲	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۱۳	۰	۱	۱	۰	۱	۰	۱	۰	۱*	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۱۴	۰	۱	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۱۵	۰	۱	۱	۰	۱	۰	۰	۰	۱*	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰
۱۶	۰	۱	۱*	۰	۰	۰	۰	۰	۱*	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰
۱۷	۰	۱	۱	۰	۰	۰	۰	۰	۱*	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰
۱۸	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰
۱۹	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰

۲۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰
۲۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰
۲۲	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰
۲۳	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰
۲۴	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱

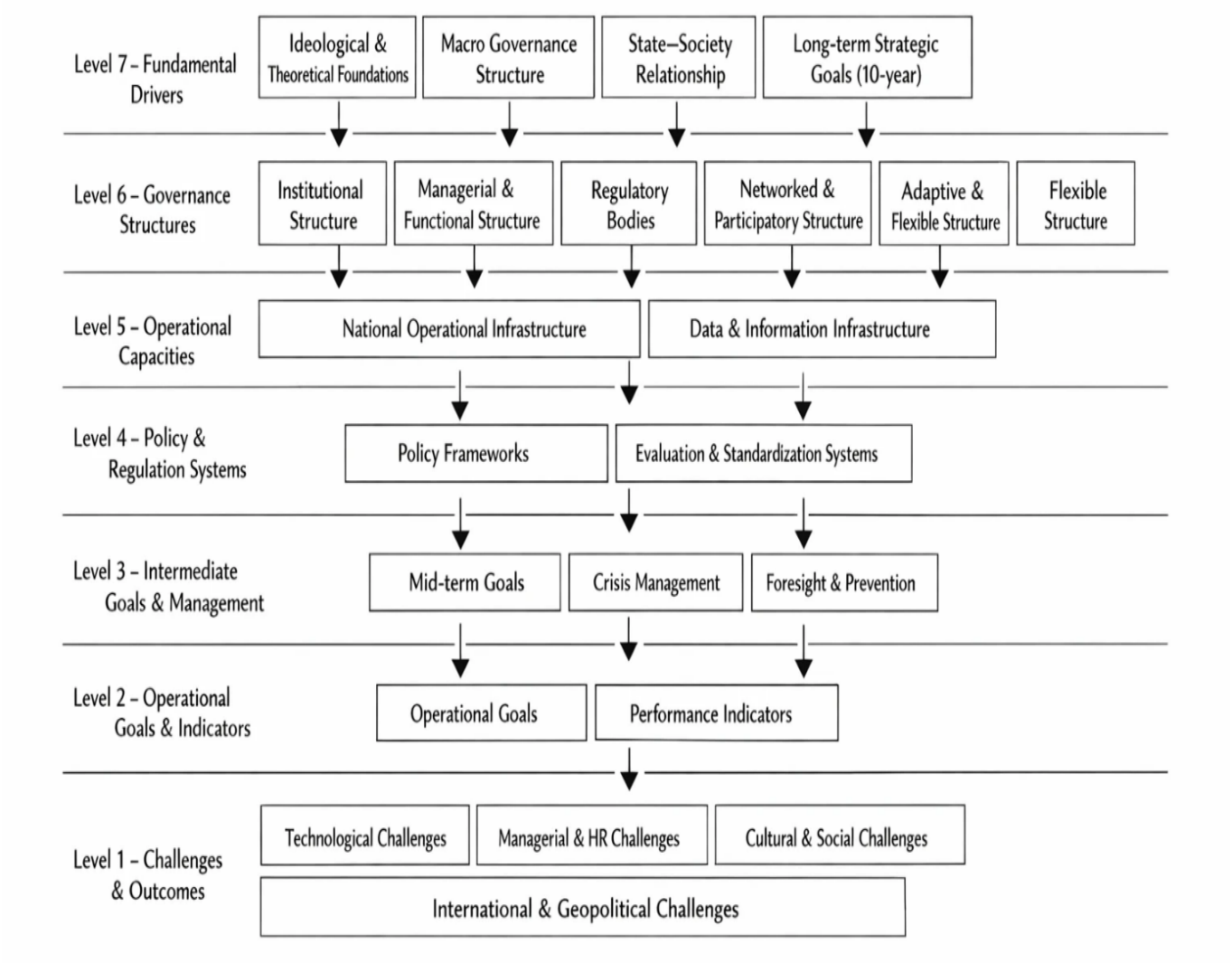
ماتریس دسترسی نهایی نشان می‌دهد که برخی مؤلفه‌ها دارای روابط مستقیم و استنتاجی گسترده‌تری با سایر مؤلفه‌ها هستند و در نتیجه نقش اثرگذارتر و پیشران‌تری در مدل دارند. وجود مقادیر ۱* در ماتریس بیانگر روابط تراگذری است؛ یعنی روابطی که به‌صورت مستقیم توسط خبرگان گزارش نشده‌اند، اما بر اساس منطق ساختاری ISM از روابط میان مؤلفه‌ها استنتاج شده‌اند. بر این اساس، مؤلفه‌هایی مانند مبانی ایدئولوژیک و نظری، ساختار کلان حکمرانی، چارچوب‌های سیاستی، نهادهای راهبری و تنظیم‌گری و نسبت دولت و جامعه در مقایسه با مؤلفه‌های پیامدی، گستره اثرگذاری بیشتری در شبکه روابط دارند. در مقابل، چالش‌های نهایی در ردیف‌های پایانی ماتریس عمدتاً دارای دسترسی محدود به خود هستند و بیشتر به‌عنوان پیامد و خروجی ساختار حکمرانی عمل می‌کنند.

جدول ۳. سطح‌بندی مؤلفه‌های مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله

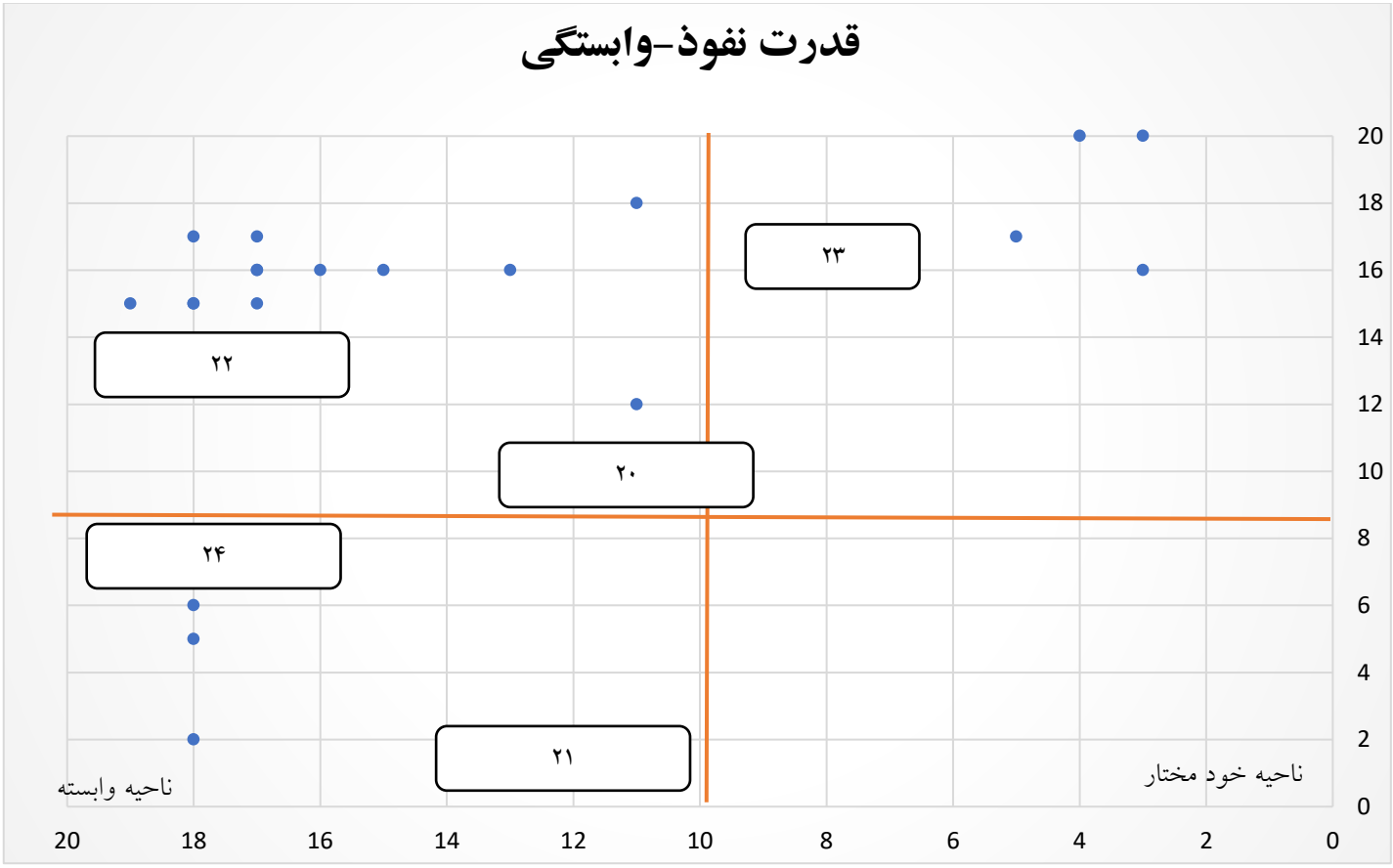
سطح	عنوان سطح	مؤلفه‌ها	تفسیر جایگاه در مدل
سطح ۱	چالش‌ها و پیامدهای نهایی	چالش‌های فناورانه و زیرساختی؛ چالش‌های مدیریتی و منابع انسانی؛ چالش‌های فرهنگی و اجتماعی؛ چالش‌های بین‌المللی و ژئوپلیتیکی؛ چالش‌های ساختاری و نهادی	این مؤلفه‌ها دارای بیشترین وابستگی و کمترین قدرت اثرگذاری هستند و به‌عنوان پیامد نهایی عملکرد نظام حکمرانی ظاهر می‌شوند.
سطح ۲	اهداف عملیاتی و شاخص‌های عملکرد	اهداف عملیاتی قابل سنجش؛ شاخص‌های کلان ارزیابی پیشرفت	این سطح نقش تبدیل‌کننده سیاست‌ها و اهداف کلان به سنجه‌ها و اقدامات قابل ارزیابی را دارد.
سطح ۳	اهداف میانی و مدیریت اجرا	اهداف میانی پنج‌ساله اول و دوم؛ مدیریت بحران و پاسخ؛ پیشگیری و آینده‌نگری	این مؤلفه‌ها لایه اجرایی و مدیریتی مدل را تشکیل داده و موجب اتصال هدف‌گذاری راهبردی به اقدام عملی می‌شوند.
سطح ۴	نظام‌های سیاستی و تنظیم‌گر	چارچوب‌های سیاستی؛ نظام‌های ارزیابی و استانداردسازی	این سطح نقش جهت‌دهنده و تنظیم‌گر دارد و کیفیت سیاست‌گذاری، پایش و اصلاح مسیر حکمرانی را تعیین می‌کند.
سطح ۵	زیرساخت‌ها و ظرفیت‌های عملیاتی	زیرساخت‌های ملی عملیاتی؛ زیرساخت‌های اطلاعاتی و داده‌ای	این مؤلفه‌ها بستر فنی، داده‌ای و عملیاتی لازم برای تحقق سیاست‌ها و اهداف حکمرانی امنیت سایبری را فراهم می‌کنند.
سطح ۶	ساختارهای حکمرانی و نهادی	ساختاری و نهادی؛ کارکردی و مدیریتی؛ نهادهای راهبری و تنظیم‌گری؛ ساختار شبکه‌ای و مشارکتی؛ ساختار منعطف و تطبیقی	این سطح معماری نهادی، مدیریتی و مشارکتی نظام حکمرانی را مشخص می‌کند و بر ظرفیت هماهنگی و انطباق سیستم اثر می‌گذارد.
سطح ۷	پیشران‌های بنیادین و راهبردی	مبانی ایدئولوژیک و نظری؛ ساختار کلان حکمرانی؛ نسبت دولت و جامعه؛ تحولات دوره‌ای مدل حکمرانی؛ اهداف کلان ده‌ساله	این مؤلفه‌ها دارای بیشترین قدرت نفوذ و کمترین وابستگی هستند و جهت‌گیری کلی مدل را تعیین می‌کنند.

نتایج سطح‌بندی نشان داد که مدل حکمرانی امنیت سایبری دارای ساختاری سلسله‌مراتبی و هفت‌سطحی است. در بالاترین سطح، پیشران‌های بنیادین و راهبردی قرار دارند که شامل مبانی ایدئولوژیک و نظری، ساختار کلان حکمرانی، نسبت دولت و جامعه، تحولات دوره‌ای مدل حکمرانی و اهداف کلان ده‌ساله هستند. این عوامل جهت‌گیری اصلی نظام حکمرانی را تعیین کرده و بر سایر

سطوح اثر می‌گذارند. در سطوح میانی، ساختارهای نهادی، ظرفیت‌های زیرساختی، چارچوب‌های سیاستی، نظام‌های ارزیابی، اهداف میانی و سازوکارهای مدیریت بحران قرار دارند که نقش واسط میان مبانی راهبردی و پیامدهای نهایی را ایفا می‌کنند. در پایین‌ترین سطح، چالش‌های ساختاری، فناورانه، مدیریتی، فرهنگی و بین‌المللی قرار گرفته‌اند که بیشترین وابستگی را به کیفیت تصمیمات، سیاست‌ها و ساختارهای سطوح بالاتر دارند. بنابراین، چالش‌های امنیت سایبری در این مدل به‌عنوان علت‌های بنیادین تلقی نمی‌شوند، بلکه پیامدهای ضعف یا قوت در لایه‌های راهبردی، نهادی، سیاستی و عملیاتی حکمرانی محسوب می‌شوند.



شکل ۲. مدل سطح‌بندی ساختاری تفسیری حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله



شکل ۳. نمودار MICMAC مؤلفه‌های مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله

نتایج تحلیل MICMAC نشان داد که مؤلفه‌های مدل از نظر قدرت نفوذ و میزان وابستگی در سه ناحیه اصلی نفوذی، پیوندی و وابسته توزیع شده‌اند و هیچ مؤلفه‌ای در ناحیه خودمختار قرار نگرفته است. نبود متغیر خودمختار نشان می‌دهد که تمامی مؤلفه‌های شناسایی‌شده در شبکه روابط حکمرانی امنیت سایبری نقش معنادار دارند و هیچ عاملی به‌صورت منفصل یا حاشیه‌ای در مدل حضور ندارد. این یافته بیانگر انسجام ساختاری مدل و درهم‌تنیدگی بالای مؤلفه‌های حکمرانی امنیت سایبری است.

در ناحیه نفوذی، متغیرهایی مانند مبانی ایدئولوژیک و نظری، ساختار کلان حکمرانی، نهادهای راهبری و تنظیم‌گری، چارچوب‌های سیاستی، ساختاری و نهادی و نسبت دولت و جامعه قرار گرفتند. این متغیرها از قدرت اثرگذاری بالا و وابستگی پایین برخوردارند و به‌عنوان پیشران‌های اصلی مدل عمل می‌کنند. جایگاه این عوامل نشان می‌دهد که اصلاح پایدار در حکمرانی امنیت سایبری باید از سطح مبانی، معماری نهادی، سیاست‌گذاری کلان و بازتعریف الگوی تعامل دولت و جامعه آغاز شود.

در ناحیه پیوندی، مؤلفه‌هایی مانند کارکردی و مدیریتی، زیرساخت‌های ملی عملیاتی، زیرساخت‌های اطلاعاتی و داده‌ای، مدیریت بحران و پاسخ و پیشگیری و آینده‌نگری قرار گرفتند. این عوامل هم قدرت نفوذ بالا و هم وابستگی بالا دارند؛ بنابراین، ماهیتی حساس و ناپایدار دارند. هرگونه تغییر در این مؤلفه‌ها می‌تواند کل سیستم را تحت تأثیر قرار دهد و در عین حال خود نیز از تغییرات

سایر مؤلفه‌ها اثر بپذیرد. از این رو، این ناحیه نیازمند هماهنگی نهادی، مدیریت مستمر، بازخوردپذیری و ظرفیت تصمیم‌گیری سریع است.

در ناحیه وابسته، اهداف کلان ده‌ساله، اهداف میانی، اهداف عملیاتی، شاخص‌های کلان ارزیابی پیشرفت و مجموعه چالش‌های ساختاری، فناورانه، مدیریتی، فرهنگی و بین‌المللی قرار گرفتند. این متغیرها بیشتر بازتاب‌دهنده وضعیت عملکردی نظام حکمرانی هستند و نسبت به عوامل نفوذی و پیوندی وابستگی بیشتری دارند. به بیان دیگر، بهبود یا تشدید چالش‌های امنیت سایبری مستقیماً تابع کیفیت پیشران‌های راهبردی، ظرفیت‌های نهادی، سیاست‌گذاری، زیرساخت‌های عملیاتی و مدیریت بحران است. بنابراین، نتایج MICMAC تأیید می‌کند که برای دستیابی به مدل مطلوب حکمرانی امنیت سایبری در افق ده‌ساله، تمرکز اصلی باید بر متغیرهای نفوذی و پیوندی قرار گیرد؛ زیرا این متغیرها بیشترین نقش را در شکل‌دهی، تثبیت و اصلاح مسیر حکمرانی امنیت سایبری کشور دارند.

بحث و نتیجه‌گیری

یافته‌های پژوهش حاضر نشان داد که مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله، دارای ساختاری چندسطحی، شبکه‌ای و پویا است که در آن پیشران‌های بنیادین، ساختارهای نهادی، زیرساخت‌های عملیاتی، چارچوب‌های سیاستی، سازوکارهای مدیریتی و چالش‌های محیطی در یک نظام تعاملی و سلسله‌مراتبی به یکدیگر متصل هستند. نتایج تحلیل مضمون نشان داد که حکمرانی امنیت سایبری صرفاً به معنای حفاظت فنی از زیرساخت‌ها نیست، بلکه مفهومی فرابخشی و راهبردی است که ابعاد ایدئولوژیک، نهادی، مدیریتی، اجتماعی، فناورانه و ژئوپلیتیکی را به‌صورت هم‌زمان در بر می‌گیرد. این یافته با دیدگاه‌های جدید حکمرانی امنیت سایبری همسو است که امنیت سایبری را بخشی از نظام حکمرانی دیجیتال و امنیت ملی می‌دانند و بر نقش سیاست‌گذاری، تنظیم‌گری، رهبری و هماهنگی نهادی تأکید می‌کنند (25, 33, 35).

یکی از مهم‌ترین یافته‌های پژوهش، قرار گرفتن «مبانی ایدئولوژیک و نظری»، «ساختار کلان حکمرانی»، «نسبت دولت و جامعه» و «اهداف کلان ده‌ساله» در بالاترین سطح مدل ISM بود. این نتیجه نشان می‌دهد که امنیت سایبری در جمهوری اسلامی ایران ماهیتی صرفاً تکنیکی ندارد و متأثر از فلسفه حکمرانی، الگوی مشروعیت سیاسی، نوع رابطه دولت و جامعه و اهداف کلان توسعه‌ای کشور است. این یافته با پژوهش‌های مرتبط با حکمرانی اسلامی و الگوی بومی پیشرفت همخوانی دارد که بر نقش مبانی ارزشی، عدالت‌محوری و انسجام نهادی در حکمرانی تأکید می‌کنند (40). همچنین، نتایج حاضر با مطالعاتی که امنیت سایبری را به‌عنوان بخشی از حکمرانی کلان و سیاست عمومی تحلیل کرده‌اند همسو است؛ زیرا این مطالعات نیز نشان داده‌اند که ساختار حکمرانی و جهت‌گیری‌های کلان سیاسی می‌توانند نحوه مواجهه با تهدیدات سایبری و کیفیت سیاست‌گذاری دیجیتال را تعیین کنند (29, 43).

نتایج پژوهش همچنین نشان داد که «نهادهای راهبری و تنظیم‌گری»، «ساختارهای نهادی»، «چارچوب‌های سیاستی» و «ساختار شبکه‌ای و مشارکتی» در زمره متغیرهای نفوذی قرار دارند. این یافته بیانگر آن است که کارآمدی حکمرانی امنیت سایبری بیش از هر چیز وابسته به کیفیت معماری نهادی و سازوکارهای هماهنگی میان بازیگران مختلف است. در واقع، بدون وجود نهادهای تنظیم‌گر کارآمد، سیاست‌های هماهنگ و تقسیم نقش شفاف، حتی پیشرفته‌ترین زیرساخت‌های فنی نیز نمی‌توانند امنیت سایبری پایدار ایجاد کنند. این نتیجه با مطالعات مربوط به حکمرانی پلتفرمی و تنظیم‌گری دیجیتال هماهنگ است که بر ضرورت گذار از حکمرانی متمرکز به حکمرانی شبکه‌ای و چندبازیگری تأکید دارند (29). همچنین، یافته حاضر با پژوهش‌هایی که نقش شفافیت، پاسخ‌گویی و هماهنگی نهادی را در ارتقای حکمرانی مؤثر دانسته‌اند همسو است (38, 39).

یکی دیگر از یافته‌های مهم پژوهش، قرار گرفتن «زیرساخت‌های ملی عملیاتی»، «زیرساخت‌های اطلاعاتی و داده‌ای»، «مدیریت بحران و پاسخ» و «پیشگیری و آینده‌نگری» در ناحیه پیوندی نمودار MICMAC بود. این نتیجه نشان می‌دهد که این مؤلفه‌ها دارای وابستگی و نفوذ هم‌زمان هستند و به‌عنوان هسته اجرایی و عملیاتی حکمرانی امنیت سایبری عمل می‌کنند. به بیان دیگر، این متغیرها هم از سطوح بالادستی اثر می‌پذیرند و هم می‌توانند بر کل سیستم تأثیر بگذارند. این یافته با چارچوب‌های تطبیقی حکمرانی امنیت سایبری همخوانی دارد که بر ضرورت انعطاف‌پذیری، یادگیری نهادی و سازگاری مستمر با تهدیدات نوظهور تأکید می‌کنند (36). همچنین، مطالعات مرتبط با تحول دیجیتال خدمات عمومی نشان داده‌اند که بدون زیرساخت‌های داده‌ای، ظرفیت عملیاتی و سازوکارهای پاسخ سریع، امنیت و پایداری خدمات دیجیتال با اختلال مواجه خواهد شد (35).

نتایج تحلیل MICMAC نشان داد که هیچ‌یک از متغیرهای مدل در ناحیه خودمختار قرار نگرفته‌اند. این یافته از منظر روش‌شناختی بیانگر انسجام درونی مدل و از منظر مفهومی نشان‌دهنده ماهیت درهم‌تنیده حکمرانی امنیت سایبری است. در واقع، هیچ عامل مستقلی وجود ندارد که خارج از شبکه تعاملات حکمرانی عمل کند و همه مؤلفه‌ها به‌نوعی در زنجیره سیاست‌گذاری، تنظیم‌گری، اجرا، ارزیابی و پیامدها درگیر هستند. این نتیجه با مطالعات مربوط به پیچیدگی سیستم‌های سایبری و حکمرانی دیجیتال همخوانی دارد که فضای سایبری را محیطی پیچیده، پویا و شبکه‌ای توصیف می‌کنند (29, 37). از این منظر، مدیریت امنیت سایبری نیازمند رویکرد سیستمی و فرابخشی است و تمرکز صرف بر فناوری نمی‌تواند پاسخ‌گوی پیچیدگی‌های حکمرانی باشد.

یافته‌های پژوهش همچنین نشان داد که چالش‌های فناورانه، مدیریتی، فرهنگی و ژئوپلیتیکی در پایین‌ترین سطح مدل قرار دارند و بیشترین وابستگی را به سطوح بالاتر دارند. این نتیجه حاکی از آن است که چالش‌های امنیت سایبری بیشتر پیامد کیفیت حکمرانی هستند تا علت‌های مستقل. به عبارت دیگر، ضعف در سیاست‌گذاری، نبود هماهنگی نهادی، ناکارآمدی ساختار مدیریتی، فقدان آینده‌نگری و ضعف زیرساخت‌ها در نهایت خود را در قالب چالش‌های فناورانه، انسانی و اجتماعی نشان می‌دهد. این یافته با مطالعاتی که تهدیدات سایبری را محصول ضعف در ساختار حکمرانی و سیاست‌گذاری می‌دانند همسو است (25, 30). همچنین،

پژوهش‌های مربوط به تجارت و امنیت سایبری نشان داده‌اند که وابستگی متقابل جهانی، نبود سیاست‌های هماهنگ و ضعف تنظیم‌گری می‌تواند آسیب‌پذیری کشورها را در برابر تهدیدات سایبری افزایش دهد (43).

در بخش کیفی، یافته‌ها نشان داد که نسبت دولت و جامعه یکی از عناصر بنیادین حکمرانی امنیت سایبری در افق ده‌ساله است. این نتیجه بیانگر آن است که امنیت سایبری صرفاً با کنترل دولتی تحقق نمی‌یابد، بلکه نیازمند اعتماد عمومی، مشارکت اجتماعی، فرهنگ امنیتی و همکاری میان نهادهای عمومی و خصوصی است. این یافته با دیدگاه‌های حکمرانی مشارکتی و برندسازی اجتماعی همسو است که بر مشارکت ذی‌نفعان و ایجاد احساس مالکیت جمعی در فرآیند حکمرانی تأکید دارند (48). همچنین، مطالعات مرتبط با فرهنگ امنیتی نشان می‌دهند که رفتار کاربران، نگرش‌های شناختی و روان‌شناسی امنیتی نقش مهمی در موفقیت سیاست‌های امنیت سایبری دارند (45, 46). از این رو، مدل مطلوب حکمرانی امنیت سایبری در ایران باید بتواند میان الزامات امنیت ملی و مشارکت اجتماعی تعادل ایجاد کند.

نتیجه دیگر پژوهش، اهمیت سرمایه انسانی و آموزش در حکمرانی امنیت سایبری بود. قرار گرفتن مؤلفه‌هایی مانند مدیریت بحران، آینده‌نگری و چالش‌های منابع انسانی در ساختار مدل نشان می‌دهد که حکمرانی امنیت سایبری بدون نیروی انسانی متخصص، فرهنگ سازمانی مناسب و آموزش مستمر امکان‌پذیر نیست. این نتیجه با مطالعات جدید درباره نقش رهبری انسانی‌محور و آموزش سیاستی در امنیت سایبری همسو است (34, 47). در واقع، بخش قابل توجهی از تاب‌آوری سایبری وابسته به توانایی تصمیم‌گیران، مدیران و کاربران در درک تهدیدات، واکنش سریع و هماهنگی نهادی است. این موضوع در شرایطی که تهدیدات سایبری ماهیتی ترکیبی و چندلایه پیدا کرده‌اند، اهمیت بیشتری می‌یابد.

یافته‌های پژوهش همچنین نشان داد که حکمرانی امنیت سایبری با توسعه اقتصادی، نوآوری و اعتماد نهادی ارتباط مستقیم دارد. قرار گرفتن اهداف عملیاتی، شاخص‌های ارزیابی و چارچوب‌های سیاستی در سطوح میانی مدل بیانگر آن است که امنیت سایبری بخشی از زیرساخت توسعه دیجیتال کشور محسوب می‌شود. این نتیجه با پژوهش‌هایی که نشان داده‌اند حکمرانی امنیت سایبری می‌تواند بر نوآوری، اعتماد سرمایه‌گذاران و ارزش سازمانی اثر بگذارد همسو است (23, 24). همچنین، یافته حاضر با مطالعات حکمرانی شرکتی که رابطه میان کیفیت حکمرانی و عملکرد اقتصادی را تأیید کرده‌اند نیز همخوانی دارد (41). بنابراین، امنیت سایبری در افق ده‌ساله نباید صرفاً به‌عنوان حوزه‌ای دفاعی دیده شود، بلکه باید بخشی از راهبرد توسعه ملی و تحول دیجیتال کشور تلقی گردد.

از منظر نظری، پژوهش حاضر توانست با ترکیب تحلیل مضمون، مدل‌سازی ساختاری تفسیری و تحلیل MICMAC، تصویری منسجم از ساختار حکمرانی امنیت سایبری ارائه دهد. این رویکرد نشان داد که روابط میان مؤلفه‌های حکمرانی خطی و ساده نیستند و باید در قالب شبکه‌ای از تعاملات متقابل تحلیل شوند. این یافته با ملاحظات روش‌شناختی پژوهش‌های حکمرانی همخوانی دارد که بر پیچیدگی روابط علّی و ضرورت استفاده از مدل‌های ساختاری تأکید می‌کنند (42). در همین راستا، پژوهش حاضر توانست از سطح توصیف مفاهیم عبور کرده و ساختار سلسله‌مراتبی و قدرت نفوذ متغیرها را مشخص سازد.

در مجموع، یافته‌های پژوهش نشان داد که مدل حکمرانی امنیت سایبری نظام جمهوری اسلامی ایران در افق ده‌ساله باید بر پنج محور اصلی استوار باشد: نخست، تقویت پیشران‌های بنیادین شامل مبانی نظری، ساختار کلان و اهداف راهبردی؛ دوم، بازطراحی ساختارهای نهادی و تنظیم‌گری؛ سوم، توسعه زیرساخت‌های عملیاتی و داده‌ای؛ چهارم، تقویت ظرفیت‌های مدیریتی، آینده‌نگری و مدیریت بحران؛ و پنجم، ارتقای فرهنگ امنیتی، مشارکت اجتماعی و سرمایه انسانی. چنین مدلی می‌تواند امکان شکل‌گیری حکمرانی سایبری بومی، منسجم، انعطاف‌پذیر و آینده‌نگر را فراهم کند و کشور را در مواجهه با تهدیدات پیچیده و متغیر فضای سایبری توانمند سازد.

پژوهش حاضر با وجود تلاش برای ارائه مدلی جامع از حکمرانی امنیت سایبری، با محدودیت‌هایی نیز مواجه بود. نخست، جامعه مشارکت‌کنندگان پژوهش محدود به خبرگان دانشگاهی و اجرایی حوزه امنیت سایبری بود و دیدگاه سایر ذی‌نفعان نظیر بخش خصوصی، فعالان جامعه مدنی و کاربران نهایی به‌صورت مستقیم بررسی نشد. دوم، ماهیت کیفی و تفسیری بخشی از داده‌ها ممکن است تحت تأثیر برداشت‌ها و تجربیات فردی خبرگان قرار گرفته باشد. سوم، با توجه به سرعت تحولات فناورانه و تغییر ماهیت تهدیدات سایبری، بخشی از یافته‌ها ممکن است در بازه‌های زمانی آینده نیازمند بازنگری و به‌روزرسانی باشد. همچنین، محدودیت دسترسی به برخی اطلاعات تخصصی و امنیتی می‌توانست بر عمق تحلیل برخی ابعاد حکمرانی سایبری اثر بگذارد.

پیشنهاد می‌شود پژوهش‌های آینده به طراحی مدل‌های کمی و آزمون تجربی روابط میان مؤلفه‌های حکمرانی امنیت سایبری بپردازند و نقش متغیرهایی مانند اعتماد عمومی، سرمایه اجتماعی، فرهنگ امنیتی و حکمرانی داده را با استفاده از مدل‌های علّی و معادلات ساختاری بررسی کنند. همچنین، انجام مطالعات تطبیقی میان مدل حکمرانی امنیت سایبری ایران و سایر کشورها می‌تواند به شناسایی نقاط قوت و ضعف ساختار موجود کمک کند. پیشنهاد دیگر، بررسی تأثیر فناوری‌های نوظهور مانند هوش مصنوعی، بلاکچین، اینترنت اشیا و رایانش کوانتومی بر آینده حکمرانی امنیت سایبری کشور است. علاوه بر این، مطالعه نقش آموزش، سواد سایبری و رفتار کاربران در پایداری امنیت ملی دیجیتال می‌تواند افق‌های جدیدی برای پژوهش‌های آتی فراهم سازد.

از منظر کاربردی، نتایج پژوهش می‌تواند مبنایی برای تدوین سیاست‌های کلان حکمرانی امنیت سایبری کشور قرار گیرد. پیشنهاد می‌شود نهادهای سیاست‌گذار و تنظیم‌گر، سازوکارهای هماهنگی نهادی و شبکه‌ای را تقویت کرده و از تمرکز صرف بر کنترل فنی فاصله بگیرند. همچنین، توسعه زیرساخت‌های داده‌ای و عملیاتی، طراحی نظام‌های ارزیابی و استانداردسازی، تقویت مدیریت بحران سایبری و ارتقای ظرفیت آینده‌نگری باید در اولویت برنامه‌ریزی‌های ملی قرار گیرد. توجه به آموزش تخصصی، فرهنگ‌سازی عمومی، مشارکت دانشگاه‌ها و بخش خصوصی و توسعه سرمایه انسانی نیز می‌تواند تاب‌آوری سایبری کشور را افزایش دهد. در نهایت، طراحی مدل بومی و انعطاف‌پذیر حکمرانی امنیت سایبری می‌تواند زمینه لازم را برای تحقق امنیت پایدار دیجیتال، اعتماد عمومی و توسعه آینده‌محور فضای سایبری در جمهوری اسلامی ایران فراهم سازد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

موازین اخلاقی

در انجام این پژوهش تمامی موازین و اصول اخلاقی رعایت گردیده است.

حامی مالی

این پژوهش حامی مالی نداشته است.

منابع

1. Cowan CP, Cowan PA. When partners become parents: The big life change for couples: Lawrence Erlbaum Associates; 2020.
2. Hetherington EM, Kelly J. For better or for worse: Divorce reconsidered. 2020.
3. Lazarus A, Arun VM. Spiritual involvement, resilience, and positive mindset in adults. World Journal of Advanced Research and Reviews. 2025;26(1):799-806. doi: 10.30574/wjarr.2025.26.1.0951.
4. Cohen K, Baker S, Hoggard L. Religious coping, compassion and resilience in context of adversity. International Journal of Wellbeing. 2025.
5. Pirutinsky S, Cherniak AD, Rosmarin DH. COVID-19, mental health, and religious coping among American Orthodox Jews. Journal of Religion and Health. 2020;59(5):2288-301. doi: 10.1007/s10943-020-01070-z.
6. Chen N, Chen HC. Religion, marriage, and happiness: Evidence from Taiwan. Applied Research in Quality of Life. 2021;16(2):259-99. doi: 10.1007/s11482-019-09797-0.
7. Wheatley I. Religious service attendance and its association with well-being. Journal of Family and Community Studies. 2023;12(3):45-59. doi: 10.1080/12345678.2023.987654.
8. Kasdi A, Saifudin S. Resilience of Muslim families in the pandemic era: Indonesian millennial Muslim community's response against COVID-19. Jurnal Penelitian. 2020:81-94.
9. Fathoni A. Family resilience and implementation of Islamic family jurisprudence on millennial Muslim families in Gresik, Indonesia. Journal of Islamic Law. 2021;2(2):247.
10. Sholeh AN, Saputra N, Haymans A. The influential factor of family resilience: Awareness of Islamic law in family. Journal of Psychology and Education. 2021;38(1):3195-207.
11. Lüscher J, Pauly T, Gerstorf D, Stadler G. Having a good time together: The role of companionship in older couples' everyday life. Gerontology. 2022;68:1428-39.
12. Stadler G, Scholz U, Bolger N, Shrout PE, Knoll N, Lüscher J. How is companionship related to romantic partners' affect, relationship satisfaction, and health behavior? Using a longitudinal dyadic score model to understand daily and couple-level effects of a dyadic predictor. 2022. doi: 10.1111/aphw.12450.
13. Tong JPS, Lu S, Sing CY, Sze LCY, Lum TYS, Tse S. It was the deepest level of companionship: Peer-to-peer experience of supporting community-dwelling older people with depression: A qualitative study. BMC Geriatrics. 2022;22:443. doi: 10.1186/s12877-022-03121-4.

14. Boateng G, editor Towards real-time multimodal emotion recognition among couples. Proceedings of the 2020 International Conference on Multimodal Interaction; 2020.
15. Boateng G, Zurich E, Hilpert P, Bodenmann G, Neysari M, Kowatsch T. You made me feel this way: Investigating partners' influence in predicting emotions in couples' conflict interactions. 2021.
16. Koçak TM, Dibek BC, Polat EN, Kafesçioğlu N, Demiroğlu C. Automatic detection of attachment style in married couples through conversation analysis. EURASIP Journal on Audio, Speech, and Music Processing. 2023:26. doi: 10.1186/s13636-023-00291-w.
17. Birni G, Eryilmaz A. Enhancing well-being of the married: Investigating marital satisfaction, self-compassion and happiness increasing strategies. Turkish Psychological Counseling and Guidance Journal. 2022;12(67):650-68.
18. Carreno DF, Eisenbeck N, Greville J, Wong PTP. Cross-cultural psychometric analysis of the Mature Happiness Scale-Revised: Mature happiness, psychological inflexibility, and the PERMA model. Journal of Happiness Studies. 2023;24:1075-99.
19. Sattarzadeh Jahdi N, Hakimi S, Shakbaeifar M. The effect of sexual assertiveness training on marital satisfaction and happiness of Azari women: A semi-experimental study. Medical Journal of Tabriz University of Medical Sciences. 2024;46(2):188-98. doi: 10.34172/mj.2024.025.
20. Pudjiati SRR, Reksodiputro SHD, Purwono RU. Family resilience model: The influence of cultural identity, coping, family strain, socioeconomic status, and community support on family resilience among the Batak Toba ethnic group. Makara Human Behavior Studies in Asia. 2021;25(2):153-69. doi: 10.7454/hubs.asia.1131121.
21. Nurdin R, Ridwansyah M, Iskandar Z. Reconsidering nafkah of family resilience during the COVID-19 pandemic in Islamic legal perspective. Journal Ilmu-Ilmu Keislaman. 2021;45(1).
22. Hidayati TW, Susilawati U, Sriani E. Dynamics of family fiqh: The multiple roles of women in realizing family resilience. Wacana Hukum Islam dan Kemanusiaan. 2022;22(2):219-38.
23. Tan W, Guo B, Zhang Q. Cybersecurity Governance and Corporate Market Value: Perspectives from Investor Trust and Supply Chain Trust. Pacific-Basin Finance Journal. 2025;90:102646.
24. Xu J. Cybersecurity Governance and Corporate Innovation: Evidence from China. Finance Research Letters. 2025;82:107619.
25. Qudus L. Cybersecurity Governance: Strengthening Policy Frameworks to Address Global Cybercrime and Data Privacy Challenges. International Journal of Science and Research Archive. 2025;14(1):1146-63.
26. Bokhari SAA, Myeong S. The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective. IEEE Access. 2023.
27. Adaji C, Bello A, Ukatu C, Okika N, Agboola O, Amomo CG. AI-Powered Cybersecurity Governance: The Role of Business Analysts in Ethical AI Deployment. International Journal of Innovative Science and Research Technology. 2025;10(3):1384-96.
28. Martínez EM, Castro SV, Buenaño JEJ, Meléndez MCE, Armas DGA, Portero RN. An Approach to Artificial Intelligence Tools and the Legal Basis for Cybersecurity Governance. Intelligent Sustainable Systems: Selected Papers of WorldS4 2025, Volume 3. 32026. p. 63.
29. Pan Q, Luo W, Liu Z, Zhang JZ. Digital Platform Governance: Literature Review and Research Outlook. Journal of Organizational Computing and Electronic Commerce. 2025;35(4):407-31.
30. Abyati A, Ahmadi M, editors. Emerging Security Threats in Cyberspace: A Case Study of the 2019 Protests. Specialized Conference on Monitoring Emerging Military Threats in the Second Step of the Islamic Revolution; 2021; Qom.
31. Akhtari K, Mousavi SAA. A Comparative Comparison of Cybersecurity and Information Security Maturity Models and Identification of Common Cybersecurity Indicators. Passive Defense Quarterly. 2023;13(4):21-38.
32. Tatar U, Karabacak B, Gheorghe A. An Assessment Model to Improve National Cyber Security Governance. 11th International Conference on Cyber Warfare and Security: ICCWS20162016. p. 312.
33. Fidler B. Cybersecurity Governance: A Prehistory and Its Implications. Digital Policy, Regulation and Governance. 2017;19(6):449-65.
34. Singh M, Srivastava S, Mahanandia R. Leadership and Cybersecurity Governance: Building a Human-Centric Protective Culture in the Digital Age. The Human Dimension of Cybersecurity: Cultivating a Protective Organizational Culture: IGI Global Scientific Publishing; 2026. p. 1-28.
35. Mijwil M, Filali Y, Aljanabi M, Bounabi M, Al-Shahwani H. The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. Mesopotamian Journal of Cybersecurity. 2023;2023:1-6.
36. Melaku HM. A Dynamic and Adaptive Cybersecurity Governance Framework. Journal of Cybersecurity and Privacy. 2023;3(3):327-50.
37. Khoshhalpour E. A Review of Cyberspace Layering Models and the Proposal of a New Model. Science and Technology Policy Letter. 2025;15(2):96-114.
38. Sepehrnia R, Alborzi M, Kermanshah A, Azar A, Sepehrnia R. A Creative Model of Good Governance Transparency for Policy-Making Organizations in Iran. Innovation and Creativity in Human Sciences. 2019;9(2):77-102.

39. Ambarwati R, Mudjib AW, Lestariana FF, Handiwibowo GA. The Implications of Good Governance of Village Government Office in Sidoarjo. Binus Business Review. 2019;10(3):147-58.
40. Montazeri M, Bahmani A, Fathizadeh A. The Model of Good Governance from the Perspective of Nahj al-Balagha: A Step toward Explaining the Islamic-Iranian Model of Progress. Islamic-Iranian Progress Model. 2018;6(11):133-55.
41. Kyere M, Ausloos M. Corporate Governance and Firms Financial Performance in the United Kingdom. International Journal of Finance & Economics. 2021;26(2):1871-85.
42. Khatib SF. An Assessment of Methods to Deal with Endogeneity in Corporate Governance and Reporting Research. Corporate Governance: The International Journal of Business in Society. 2025;25(3):606-30.
43. Mishra N. The Trade: (Cyber) Security Dilemma and Its Impact on Global Cybersecurity Governance. Journal of World Trade. 2020;54(4).
44. Jomo KS, Chowdhury A. World Bank Financializing Development. Development. 2019;62(1):147-53.
45. Talebi, Taghavi, Rahmati. A Human-Centered Cognitive Model of Cybersecurity. Defense Human Capital Management. 2022;2(2).
46. Gani ABD, Fernando Y. The Cybersecurity Governance in Changing the Security Psychology and Security Posture: Insights into E-Procurement. International Journal of Procurement Management. 2021;14(3):308-27.
47. Hasan KF, Hughes W, Rahman Tory A, Campbell C, Turkay S. Game On: A Developmental Approach to UNSW Cyber Escape Room for Cybersecurity Governance and Policy Education. Education Sciences. 2026;16(1):133.
48. Della Spina L. Community Branding and Participatory Governance: A Glocal Strategy for Heritage Enhancement. Heritage. 2025;8(6):188.