Quarterly journal of strategic management attitude
Vol 2, No 3(7), Autumn2024
https://pmr.sndu.ac.ir

Type of Article: Reseach

Governance model of cyber security industry of the Islamic Republic of Iran

Mojtaba Karimi Kalimani*[1]، Ebrahim Mahmodzadeh[2]، Reza taghipor[3]، Alireza Boshehri[4]

Received: 2024/04/30 **PP: 127-152** **Accepted:** 2024/09/11

Abstract

The current situation in achieving the mission in the cyber security industry in the public sector, maintaining and increasing the profits of the shareholders in the private sector, has made them far from strategic planning. Defining a framework for the country's cyber security industry that includes standards, strategies and measures to localize effective equipment in order to improve the protection of critical infrastructure and increase national power, for industries that have research and production activities to achieve security products and services. It is necessary to have cyber. This framework includes determining the playing field, actors, passing rules and guidelines, as well as control, evaluation and feedback, which he refers to as governance.

In the beginning, this research was designed by providing related definitions and theoretical foundations in the library method and studying many countries, the initial conceptual model and six dimensions of the governance model of the cyber security industry of the Islamic Republic of Iran, and in order to continue the work, the initial model was examined by some experts. took Then, with the field tools of interviews and qualitative analysis of the data obtained with the foundation data method, the dimensions, components and indicators of the model were determined. In the following, with the approach of applying the quantitative method, the design, distribution and collection of 93 items of the questionnaire were carried out, and with the help of SPSS and LISREL software, the relationship between the dimensions, components, and indicators was obtained, and at the end, by using the Dimtel Fuzzy method, the prioritization and the impact of each was done. They were determined from the dimensions. The model obtained in this research includes 6 dimensions, 22 components and 107 indicators.

KeyWords: industrial revolution, industry, cyber security, governance.

Reference: Karimi kalimani, M. , Mahmodzadeh, E. , taghipor, R. & Boshehri, A. (2024). Governance model of cyber security industry of the Islamic Republic of Iran. Strategic management attitude, 2(3), 127-152.https://dor.isc.ac/dor/20.1001.1.30605865.1403.2.3.5.7

[1] Correspondence author :Doctoral student, Strategic Management,Higher National Defense University (mojtaba.kalimani.313@gmail.com)
[2] Professor ,PhD in strategic management ,Malik Ashtar University.Tehran,Iran.
[3] PhD - Advanced Management Sciences - Higher National Defense University, Tehran,Iran
[4] Associate Professor - PhD in industrial engineering - Malik Ashtar University, Tehran,Iran.

فصلنامه نگرش مدیریت راهبردی
سال ۲/ شماره ۳(۷)/ پاییز ۱۴۰۳
https://pmr.sndu.ac.ir/

نوع مقاله: پژوهشی

الگوی حکمرانی صنعت امنیت سایبری جمهوری اسلامی ایران

مجتبی کریمی کلیمانی[۱]، ابراهیم محمودزاده[۲]، رضا تقی‌پور[۳] و علیرضا بوشهری[۴]

دریافت: ۱۴۰۳/۰۲/۱۱ صص: ۱۲۷-۱۵۲ پذیرش: ۱۴۰۳/۰۶/۲۱

چکیده

حفظ وضعیت موجود در تحقق مأموریت صنعت امنیت سایبری در بخش دولتی و افزایش سود سهامداران در بخش خصوصی، آنها را از برنامه‌ریزی راهبردی و جامع برای این صنعت دور می‌سازد. تعریف یک چارچوب برای صنعت امنیت سایبری کشور که شامل استانداردها، راهبردها و اقداماتی برای بومی‌سازی تجهیزات مؤثر به‌منظور بهبود حفاظت از زیرساخت‌های حیاتی و افزایش قدرت ملی باشد، برای آن دسته از صنایعی که فعالیت های تحقیقاتی و تولیدی به منظور دستیابی به محصولات و خدمات امنیت سایبری را دارند، ضروری است. این چارچوب شامل تعیین زمین بازی، بازیگران، تصویب قوانین و دستورالعمل‌ها و نیز کنترل، ارزیابی و بازخوردهاست که از آن به‌عنوان حکمرانی یاد می‌شود.

این پژوهش در ابتدا با ارائه تعاریف مرتبط و مبانی نظری به روش کتابخانه‌ای و مطالعه کشورهای متعدد، الگوی مفهومی اولیه و شش بُعد الگوی حکمرانی صنعت امنیت سایبری جمهوری اسلامی طراحی شد و برای پی ریزی ادامه کار، الگوی اولیه مورد بررسی برخی از خبرگان قرار گرفت. سپس با ابزار میدانی مصاحبه و تحلیل کیفی داده‌های به‌دست‌آمده با روش داده‌بنیاد، ابعاد، مؤلفه‌ها و شاخص های الگو مشخص شدند. در ادامه و با رویکرد به کارگیری روش کمی، اقدامات طراحی، توزیع و جمع‌آوری ۹۳ فقره پرسش‌نامه انجام شد و با نرم‌افزارهای SPSS و LISREL ارتباط بین ابعاد، مؤلفه‌ها و شاخص‌های به‌دست آمد و در انتها نیز با استفاده از روش دیمتل فازی، اولویت‌بندی و تأثیر هر کدام از ابعاد مشخص شدند. الگوی به‌دست‌آمده در این تحقیق شامل ۶ بُعد، ۲۲ مؤلفه و ۱۰۷ شاخص می‌باشد.

کلیدواژه‌ها: انقلاب صنعتی، صنعت، امنیت سایبری، حکمرانی.

استناددهی(APA): کریمی کلیمانی، مجتبی، محمودزاده، ابراهیم، تقی‌پور، رضا و بوشهری، علیرضا(۱۴۰۳). الگوی حکمرانی صنعت امنیت سایبری جمهوری اسلامی ایران. ***فصلنامه نگرش مدیریت راهبردی***،۲(۳)، ۱۲۷-۱۵۲.
https://dor.isc.ac/dor/20.1001.1.30605865.1403.2.3.5.7

[۱]. دانشجوی دکتری مدیریت راهبردی، دانشگاه عالی دفاع ملی، تهران، ایران.(mojtaba.kalimani.313@gmail.com)
[۲]. دکتری مدیریت راهبردی، دانشگاه مالک اشتر، تهران، ایران.
[۳]. دکتری علوم پیشرفته مدیریت، دانشگاه عالی دفاع ملی، تهران، ایران.
[۴]. دکتری مهندسی صنایع، دانشگاه مالک اشتر، تهران، ایران.

مقدمه

امروزه به‌دلیل افزایش جرائم اینترنتی، تولید وصف‌ناپذیر داده و نیز اطلاعات، شدت و تنوع حملات سایبری، ورودی زیاد کارخانجات و صنایع و کمبود تجربه امنیت سایبری و پیچیده بودن محیط، یافتن راه‌حل مناسب به‌منظور حفظ یا ارتقای امنیت پایدار، حوزه امنیت داده را با مخاطراتی روبه‌رو ساخته است. علت عمده آن در کشور، عدم اطلاع از الزامات و ویژگی‌های صنعت و واحدهای تحقیق و توسعه و تولید تجهیزات امنیت سایبری است.

محصولات، خدمات و حوزه‌هایی ازقبیل راه‌کارهای مدیریت وقایع و امنیت اطلاعات (SIEM)، مدیریت یکپارچه تهدیدات، امن‌سازی شبکه، گواهی الکترونیکی و PKI، فایروال برنامه‌های تحت وب، سیستم مدیریت امنیت اطلاعات، انواع فایروال‌ها، مرکز عملیات امنیت، سوییچ و روتر امن، سخت‌افزارهای خاص منظوره، فناوری‌های احراز هویت، خدمات فنی و عملیاتی، تست نفوذ، خدمات مشاوره و مدیریت، خدمات فرهنگ‌سازی و آموزش، خدمات آزمایشگاهی و اعتبارسنجی و مراکزی همانند مراکز آپای دانشگاهی و مراکز ارزیابی امنیتی و ... که به‌طور مشخص برای اهداف نظام اسلامی و سیاست‌های بالادستی باید هم‌راستا باشند، نتوانسته‌اند مزیتی درخور صنعت امنیت سایبری ایران اسلامی را رقم بزنند.

تهدیدات سایبری از اتصال‌پذیری و پیچیدگی فزاینده سامانه‌های زیرساختی حیاتی نشئت می‌گیرد و امنیت ملی، سلامت و ایمنی عمومی را به‌خطر می‌اندازد. همانند مخاطرات نظامی، اقتصادی و اجتماعی، مخاطرات امنیت سایبری نیز بر بقای شرکت‌ها تأثیرگذار خواهد بود. تهدیدات سایبری می‌تواند هزینه‌ها را بالا ببرد و درآمد را کاهش دهد. تهدیدات سایبری می‌تواند بر توانایی شرکت‌ها در نوآوری، کسب‌وکار و حفظ مشتریانشان آسیب وارد کند. یکی از دلایل اینکه امنیت سایبری در ایران آنچنان که باید جدی گرفته نشده، این است که این حوزه بسیار دیرتر از فناوری در دنیا مطرح شده و موضوع جدیدتری به‌شُمار می‌رود و سرعت ما در ساخت محصولات موردنظر با دنیا فاصله دارد که ناشی از عدم هم‌افزایی شرکت‌های مشغول در این حوزه می‌باشد. امنیت سایبری در سال‌های اولیه که فضای مجازی ایجاد شد، آنقدرها هم مهم نبود.

اکنون با وجود حملات پی در پی سایبری، هکرهای گسترده در سطح جهانی و افزایش روزافزون بدافزارها، امنیت سایبری به امری بسیار جدی و مهم تبدیل شده است. براین اساس ما نیز باید به ابزارهای کشف و شناسایی، مقابله، دفع و حتی سلاح‌هایی برای واکنش و مقابله به‌مثل مجهز باشیم. به‌اصطلاح دستمان در صنعت سازنده این نیازمندی‌ها پُر باشد.

با وجود اقدامات سازنده و مؤثر در حوزه امنیت سایبری به‌ویژه در سال‌های اخیر، اما همچنان ضعف در تحقق مأموریت صنعت امنیت سایبری در بخش دولتی و حفظ و افزایش سود سهامداران در بخش خصوصی و نبود یکپارچگی و هم‌افزایی طراحان و تولیدکنندگان محصولات و تجهیزات امنیت سایبری، آنها را از برنامه‌ریزی راهبردی، جامع و آینده‌نگر در مقیاس ملی دور ساخته که مهم‌ترین آسیب آن اتلاف منابع، ایجاد ضعف در بازدارندگی، اثربخش نبودن سبد محصولات و خدمات و طولانی‌بودن زمان ایده تا محصول در کشور را به‌دنبال داشته است. یکی از دلایلی که فعالیت‌های جزیره‌ای و عدم‌یکپارچگی، مسئله‌ساز شده، این است که کمتر می‌توانیم در لحظه در همه ابعاد مقابله با تهدیدات سایبری، واکنش مطمئن نشان دهیم یا پیشگیری به‌موقع داشته باشیم، زیرا هنوز متولی تولید نرم‌افزارها و سخت‌افزارها برای مقابله با تهدیدات مشخص نیست. تاکنون آمار شفافی از پروژه‌های تحقیقاتی امنیت سایبری و سهم اثربخشی آنها در بازدارندگی، قدرت ملی و مقاوم‌سازی اقتصادی دردسترس نیست. چیستی فرایند ثبت شرکت و نبود شرح وظایف آنها و حتی کافی‌نبودن نشریات خاص صنعت امنیت سایبری برای به‌اشتراک‌گذاری دانش و دستاوردها از دیگر مسائل می‌باشد. اینکه صنعت امنیت سایبری در محیط پیچیده امروز چه تصمیماتی اتخاذ باید بکند که درراستای اهداف و استقلال انقلاب اسلامی باشد و بقا و رشد این صنعت را به همراه داشته باشد، خود ابهام دیگری بر وجود این مسئله می‌باشد.

از سوی دیگر میزان فعلی توزیع جغرافیایی این صنعت در سطح کشور نیز می‌تواند تهدیدی برای واکنش سریع یا یک سوءمدیریت در شناسایی استعدادهای انسانی در حوزه سایبر و فناوری اطلاعات باشد. در حال حاضر به‌درستی نمی‌دانیم که کدام صنعت یا خط تولید در حوزه امنیت سایبری چه توانمندی دارد، که در صورت ضرورت به‌کار گرفته شود. برای نمونه کدام فرد، گروه یا واحد، سابقه و تجربه و دانش کافی را در

شناسایی و جمع‌آوری و کدام یک در مقابله با نفوذ و حملات، توانایی لازم را دارد یا اینکه کدام واحد می‌تواند یک مرکز عملیات سایبری اثربخش یا یک سامانه مدیریت وقایع و امنیت اطلاعات باشد. هم‌اکنون یکی از نیازهای کوچک اما جدی در سطح کشور و نیروهای مسلح، نبود تلفن همراه امن (هم به لحاظ سخت‌افزاری، هم به لحاظ نرم‌افزاری یعنی سیستم عامل و امنیت آن) است که می‌تواند مسئله این تحقیق باشد. جایگاه پشتیبان‌کننده صنعت در حوزه عملیات زمینی، هوایی، دریایی، فضایی و شهری با رویکرد رزم سایبری و سایبر در رزم با توجه به نقاط بهبود پیش‌گفته، فقط از طریق تدوین و تحقق الگوی حکمرانی برای این صنعت محقق می‌شود.

اهمیت و ضرورت پژوهش:

۱. محیط پیچیده و رشد فناوری از یک سو و تهدیدات سایبری و نیز دشمنی استکبار با انقلاب اسلامی از سوی دیگر و همچنین عدم توجه به یکپارچه‌سازی و مدیریت صنایع کوچک و بزرگ در حوزه تحقیقات و تولید و تأمین تجهیزات امنیت فاوا و سایبری، سه ضلع از مثلثی هستند که اهمیت و ضرورت این پژوهش را نشان می‌دهد.

اهمیت پژوهش (دیدگاه ایجابی)

۱. ارتقاء قدرت تصمیم‌سازی در حوزه برنامه‌ریزی برای صنعت امنیت سایبری کشور؛

۲. بهره‌مندی از فرایندها، روش‌ها و برنامه‌های مبتنی‌بر توسعه فناوری برای ارتقاء صنعت امنیت سایبری؛

۳. یکپارچه‌سازی اقدامات و برنامه‌ها برای حرکت یکپارچه و توسعه‌بخش در حوزه صنعت امنیت سایبری؛

۴. توسعه قدرت صادرات و کسب درآمد در سطح ملی برای این صنعت درراستای کمک به امنیت سایبری کشورهای دوست و مسلمان.

ضرورت پژوهش (دیدگاه سلبی)

۱. پراکندگی و بی‌برنامگی در استفاده از نیروی انسانی متخصص حوزه امنیت سایبری؛

۲. ایجاد موضع انفعالی و غافلگیری راهبردی در حوزه امنیت سایبری؛

۳. انجام اقدامات موازی در ایجاد سکوهای مشترک در حوزه صنعت امنیت سایبری؛

۴. ایجاد بی‌برنامگی در حوزه هم‌افزایی بین عوامل علمی و عملیاتی مرتبط با صنعت.

اهداف تحقیق:

هدف اصلی

دستیابی به الگوی حکمرانی صنعت امنیت سایبری در کشور

اهداف فرعی

۱. تبیین ابعاد، مؤلفه‌ها و شاخص‌های الگوی حکمرانی صنعت امنیت سایبری کشور؛

۲. شناسایی ارتباط بین ابعاد، مؤلفه‌ها و شاخص‌های الگوی حکمرانی صنعت امنیت سایبری کشور؛

۳. تبیین رویکرد مدیریت یکپارچه و هم‌افزا در صنعت امنیت سایبری کشور.

پیشینه و مبانی نظری

در بسیاری از پژوهش‌ها و تحقیقات عبارت امنیت سایبری و امنیت ملی، دفاع سایبری، امنیت سایبری ملی و از این دست عبارات به چشم می‌خورد، اما بر اساس بررسی‌ها، تحقیق قابل‌توجهی که عبارت صنعت امنیت سایبری و توسعه این صنعت را مدنظر قرار دهد، وجود ندارد.

جدول ۱. اهم تحقیقات پیشین

ردیف	عنوان	نویسندگان	سال و محل انتشار	نتیجه
۱	کتاب نظام مدیریت فضای سایبری رژیم صیهونیستی	شرکت صنعت امنیت فضای تبادل اطلاعات صا ایران	زمستان ۱۳۹۷ انتشارات انستیتو ایزایران	به‌طور کلی دلایل تبدیل‌شدن رژیم صهیونیستی به یک مرکز جهانی امنیت سایبری را می‌توان در موارد زیر خلاصه کرد: ۱. شناخته‌شدن رژیم صهیونیستی به‌عنوان یک رژیم نظامی و امنیتی، ۲. دولت به‌عنوان هماهنگ‌کننده و کاتالیزور کسب‌وکار، ۳. تبدیل ارتش به یک شتاب‌دهنده و مرکز رشد برای استارتاپ‌ها، ۴. سرمایه‌گذاری بر روی نیروی انسانی، ۵. ورود زودهنگام و قدرتمند استارتاپ‌های رژیم صهیونیستی به بازار جهانی و ۶.

ردیف	عنوان	نویسندگان	سال و محل انتشار	نتیجه
				تسهیل‌گری و مذاکره نهادهای دولتی برای توسعه همکاری‌های بین‌المللی
۲	کتاب نظام مدیریت فضای سایبری انگلیس	شرکت صنعت امنیت فضای تبادل اطلاعات صا ایران	زمستان ۱۳۹۷، انتشارات انستیتو ایزایران	اقدامات دولت انگلستان برای رشد امنیت سایبری شامل موارد زیر است: ایجاد دو مرکز نوآوری، اختصاص بودجه به نوآوری‌های سایبری و دفاعی، فراهم کردن تجهیزات تست و ارزیابی برای شرکت‌ها، خرید محصولات امنیت سایبر توسط دولت
۳	نقش حیاتی صنعت در امنیت ملی سایبری	انتشارات دانشگاه هوایی – جیمز پی فارول	فصلنامه مطالعات راهبردی- زمستان ۲۰۱۴	یک رویکرد همسو موردنیاز است تا موانع قانونی را برای امنیت سایبری قوی‌تر از بین ببرد، مشارکت‌های قوی بین بخش‌های دولتی و خصوصی ایجاد کند و خطررا در زنجیره تأمین جهانی بهتر مدیریت کند.
۴	الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران	رضا تقی‌پور، حمیدرضا لشکریان و رحیم یزدانی چهاربرج	فصلنامه علمی امنیت ملی، سال ۹، شماره سی‌وچهارم، زمستان ۱۳۹۸	درواقع این پژوهش نشان داد که الگوی راهبردی حفاظت سایبری، دارای ۴ بُعد، ۱۸ مؤلفه و ۱۳۱ زیرمؤلفه است که سیاست‌گذاری، ظرفیت‌سازی، راهبری، دیپلماسی سایبری و نگاشت نهادی از مهم‌ترین مؤلفه‌ها در بُعد حکمروائی است.
۵	صنعت امنیت سایبری شمال غرب ۲۰۱۶	دانشگاه لنکستر	دانشگاه لنکستر - ۲۰۱۶	کسب‌وکارهای امنیت سایبری در شمال غربی انگلستان، صنعتی را تشکیل می‌دهند که در حال رشد است. شناسایی و تحلیل صنعت امنیت سایبری شمال غرب و توانایی این صنعت برای صادرات از اهداف این تحقیق بود.

در هیچ‌کدام از تحقیقات انجام‌شده داخلی در رابطه با موضوع، صنعت امنیت سایبر به صورت راهبردی مورد بررسی قرار نگرفته است. همچنین مفهوم‌سازی صنعت امنیت

سایبر، به‌عنوان مهم‌ترین حوزه قدرت سایبری در قرن معاصر به صورت کامل انجام نشده است. ازآنجایی‌که امنیت فضای سایبر با انقلاب اسلامی از دیدگاه مقام معظم رهبری(مدظله‌العالی) هم سطح است، به راهبردی بودن و مشارکت همه اجزای نظام جمهوری اسلامی اشاره دارد. امری که از طرف توسعه‌دهندگان فضای سایبر نیز به‌درستی درک شده است، بنابراین راهبردهای ملی خود را منطبق بر فضای سایبر قرار داده‌اند.

مفهوم‌شناسی

امنیت سایبری: امنیت سایبری، حفاظت از سیستم‌های متصل به اینترنت مانند سخت‌افزار، نرم‌افزار و داده‌ها در برابر تهدیدات سایبری است. این عمل توسط افراد و شرکت‌ها برای محافظت در برابر دسترسی غیرمجاز به مراکز داده و سایر سیستم‌های رایانه‌ای استفاده می‌شود. یک راهبرد امنیت سایبری قوی می‌تواند موقعیت امنیتی خوبی در برابر حملات مخرب ایجاد کند که برای دسترسی، تغییر، حذف، تخریب یا اخاذی به سیستم‌ها و داده‌های حساس سازمان یا کاربر طراحی شده‌اند. امنیت سایبری همچنین در جلوگیری از حملاتی که هدف آنها ازکارانداختن یا مختل‌کردن عملکرد یک سیستم یا دستگاه است، مفید است (محمدی، ۱۳۹۹).

صنعت امنیت سایبری: با توجه به مفهوم امنیت سایبری و تعریف صنعت، می‌توان به مجموعه‌ای که با نگاه اقتصادی، پژوهشی و به جهت بازدارندگی سایبری، به طراحی، تولید و تأمین محصولات، تجهیزات و خدمات امنیت سایبری که با ساختار، فرایند و قوانین مشخصی می‌پردازد، صنعت امنیت سایبری گفت. این صنعت در حال رونق است، در مورد ارزش‌گذاری سرسام‌آور شرکت‌ها و صنایع امنیتی و حجم عظیم سرمایه (۱۲.۲ میلیارد دلار فقط در سال ۲۰۱۹)، این صنعت در زمره صنایع آینده قرار دارد. البته سرمایه‌گذاران به این صنعت سرازیر شده‌اند، زیرا نسبت به رشد تهدیدهای سایبری، اقبال به این صنعت بیشتر شده است (پیتر سینگر[1]، ۲۰۱۹).

درباره ذی‌نفعان و نقش‌آفرینان صنعت امنیت سایبری، چالش‌های متعددی وجود دارد که در کیفیت استانداردسازی محصولات و خدمات این صنعت مؤثرند. اهم این چالش‌ها عبارت‌اند از: متمرکز بودن تخصص‌ها در حوزه امنیت سایبری، الزامات و مفاد

1. Peter Singer

استانداردهای فنی محصولات و خدمات امنیت سایبری، میزان و رشد دانش کاربردی در این حوزه، سیاست‌ها و قوانین مرتبط و ناقص در این حوزه، انگیزه‌های اقتصادی و مالی در حوزه امنیت سایبری، چرخه عمر محصولات و خدمات امنیت سایبری، اهداف اصلی بازیگران حوزه امنیت سایبری، پیچیدگی‌های مدیریت زنجیره تأمین محصولات و خدمات امنیت سایبری، نبود سکوها در محصولات و خدمات سایبری، نبود زیرساخت‌های لازم و کافی در حوزه امنیت سایبری و صنعتی‌شدن برخی از کشورها در این حوزه به جای صنعتی‌سازی و نبود خطوط تولید هوشمند.

حکمرانی: حکمرانی معادل لفظ Governance تعریف شده است که در پایان قرن بیستم رایج شد. Governance، تبیین شیوه و حالت حکومت‌کردن است و Government ابزار و نتیجه حکومت‌کردن را ترسیم می‌کند. حکمرانی به مجموعه‌ای از فرایندها اشاره دارد که با قدرت، اقتدار و نفوذ، سیاست‌ها و رویه‌هایی را برای حکومت کردن در دست می‌گیرد. کاربرد این مفهوم در زبان فارسی از قدمت زیادی برخوردار نیست و به همین علت با ترجمه‌های متفاوتی در فرهنگنامه‌های جدید مواجه شده است. معادل واژه‌های حکومت، حکمروایی، فرمانروایی، نظارت، حکومت‌گری و حتی مدیریت اجتماعی ترجمه شده است. وادی حکمرانی، وادی هدایت و کنترل است و با خلق و بازتولید قوانین، هنجارهای اجتماعی و اقدامات ساختاریافته در ارتباط است. از طرفی، حکمرانی نیازمند جهت و تنظیم غایت است. یعنی حکمرانی برای هدف و غرض شکل می‌گیرد. ویژگی حکمرانی می‌تواند فرایندمحور، یعنی توجه به اثربخشی فرایند؛ کل‌نگر، یعنی توجه به تمام فعل و انفعالات سیستم و پدیده؛ پیش‌بینی‌پذیر یعنی درک بیرونی درست از واکنش حکمرانی در شرایط متفاوت؛ پاسخگویی یعنی تبیین دلیل تصمیم و مسئولیت‌پذیری در اقدامات؛ مسئله‌محور یعنی انضمامی و ناظر به مکان و زمان مشخص و درنهایت جهت‌دار یعنی هدایت و کنترل برای دستیابی به تعالی و ارتقاء مشخص باشد. درواقع حکمرانی، تعیین زمین بازی، وضع قوانین و نظارت بر اجرای آنهاست. یکی از موضوعات جالب در جغرافیای سیاسی، بررسی و مطالعه رابطه حکمرانی و دولت به نیابت از حکومت است. درواقع برای رهایی از مشکلاتی که دولت در امر اداره کشور با

آن روبه‌رو است، حکمرانی و چگونگی شیوه آن، راه‌حل مناسبی به‌نظر می‌رسد(یوروکاکس[1]، ۲۰۱۸).

حکمرانی، فرایند تصمیم‌گیری و عملیاتی‌کردن تصمیم‌هاست و شامل همه بازیگران رسمی و غیررسمی می‌شود. بنابراین، حکمرانی بسیار گسترده‌تر از حکومت است و این فرایند نه‌تنها حکومت، وزارتخانه‌ها، نهادها و سازمان‌های رسمی را دربرمی‌گیرد، بلکه سازمان‌های غیردولتی، انجمن‌ها، سندیکاها، نهادهای تحقیقاتی، رهبران مذهبی، احزاب سیاسی، بخش‌های نظامی و حتی رسانه‌ها، لابی‌ها، شرکت‌های خصوصی و شرکت‌های چندملیتی را هم شامل می‌شود که هر یک به‌نوعی در تصمیم‌گیری نقش دارند (هفتی[2]، ۲۰۱۱).

حکمرانی چابک: حکمرانی چابک به‌عنوان سیاستگذاری انطباقی، انسان‌محور، جامع و پایدار تعریف می‌شود و تأییدی بر این موضوع است که توسعه سیاست دیگر به دولت‌ها محدود نیست، بلکه هر روز بیشتر از روز قبل، به چالشی با حضور چندین ذی‌نفع تبدیل می‌شود. در این نوع حاکمیت، درحالی‌که ذی‌نفعان در ارزش کاربر نهایی واقعی یا احتمالی سهیم هستند، پیوسته برای تغییرات منفی که به‌سرعت اتفاق می‌افتند، پذیرفتن مستمر و فعالانه تغییرات و یادگیری از این تغییرات آمادگی دارند (احمدی، ۱۴۰۰).

حکمرانی صنعت امنیت سایبری: در حکمرانی سایبری، حکمرانی متعلق به مفهومی به نام سایبر است. مفهوم سایبر در عین سادگی و درک عمومی، دارای ابعاد گسترده و ناشناخته است. عالم نوپدید سایبر در حال بلعیدن عالم کنونی است و زیست‌جهان نوینی را بر پایه فناوری، شتاب و همگرایی در حال شکل دادن است که همه رفتارهای فردی و اجتماعی را در خود جای داده و بزرگ‌تر از عالم عادت‌شده کنونی است، زیرا هر مفهوم و هر پدیده‌ای در این عالم نوپدید، دارای بطن‌های مختلف و متنوعی است. عالم سایبر که ما هم‌اکنون در حال گذار و حرکت به سمت این عالم هستیم، در حال دمیدن روح سایبر است. خودروی سایبری، کارخانه سایبری، شهر سایبری، پتروشیمی سایبری و ... که دارای امتدادی در فضای سایبر هستند و غیر از کنشگری در عالم عادت‌شده با

[1] EUROCACS
[2] Hufty

روح سایبری، کنش سایبری نیز دارند. جنگ شناختی و تغییر هویت دینی و ملی با فضای سایبر انکارناپذیر نیست. این تغییر در لابه‌لای جذابیت فناوری، روزآمد بودن، کسب‌وکارهای دیجیتالی، اعتماد به شبکه‌های اجتماعی و ... نهفته است. وجود صنعتی که امنیت فضای سایبری را تضمین کند، برای یکپارچه‌سازی همه ظرفیت‌های علمی و عملی در سط کشور و بین‌الملل ضروری است. نیازمندی به تعریف زمین بازی در امنیت سایبری، وضع قوانین و نظارت بر اجرای صحیح آنها و همچنین رصد و اصلاح با استفاده از بازخوردها، جز از طریق الگوی حکمرانی صنعت امنیت سایبری ممکن نیست. صنعتی که می‌بایست با یک ساختار مطلوب به طراحی، تولید، تأمین آموزش، خدمات پشتیبانی و صیانت از زیرساخت‌ها با بررسی دوره‌ای بپردازد. بر این اساس می‌توان برای طرح‌ریزی حکمرانی صنعت امنیت سایبری متناسب با اهداف انقلاب اسلامی، گام‌های زیر را برداشت (پژوهشگر):

۱. ترسیم غایت و آرمان حکمرانی صنعت امنیت سایبری: غایت و نتیجه حکمرانی صنعت امنیت سایبری، همان دستیابی به اهداف انقلاب اسلامی است که در آینده‌سازی هنجاری سایبری، مؤثر و عامل بازدارندگی است.

۲. تنظیم حکیمانه سیاست‌های کلان صنعت امنیت سایبر: بایستی سیاست‌های کلان صنعت امنیت سایبری را حکیمانه ترسیم کرد.

۳. نقش‌ها و مسئولیت‌ها: بر اساس سیاست‌های کلان، لازم است تقسیم‌کار ملی در تحقق هر سیاست درراستای اهداف کلان حاکمیت امنیت سایبری کشور انجام شود.

۴. نظامات کنترل و نظارت مستمر: عالم سایبر و فناوری‌های سازنده آن، محیطی پویا را از حیث خدمات و تعاملات پدید آورده است. لازمه حرکت مستمر و مبتنی‌بر اقتضائات سایبر و اهداف پیش‌رو، تنظیم نظامات کنترل سیاست‌ها و راهبردهاست.

الگوی مفهومی پژوهش:

در مدیریت راهبردی، الگو، مسیر دستیابی به اهداف راهبردی را ترسیم می‌کند و می‌تواند شامل چند مدل، چارچوب مفهومی و رهیافت‌ها باشد. الگو، نمادی از واقعیت است و از طریق تشابه، به شناخت واقعیت کمک می‌کند. این کار با برجسته کردن عنصر تشابه، درک روشن‌تری از شباهت میان واقعیت و انگاره‌های ذهنی فراهم می‌کند.

بر این اساس و با توجه به مطالب مطرح‌شده، حکمرانی صنعت امنیت سایبری، مفهوم کلیدی در این پژوهش به‌شُمار می‌رود.

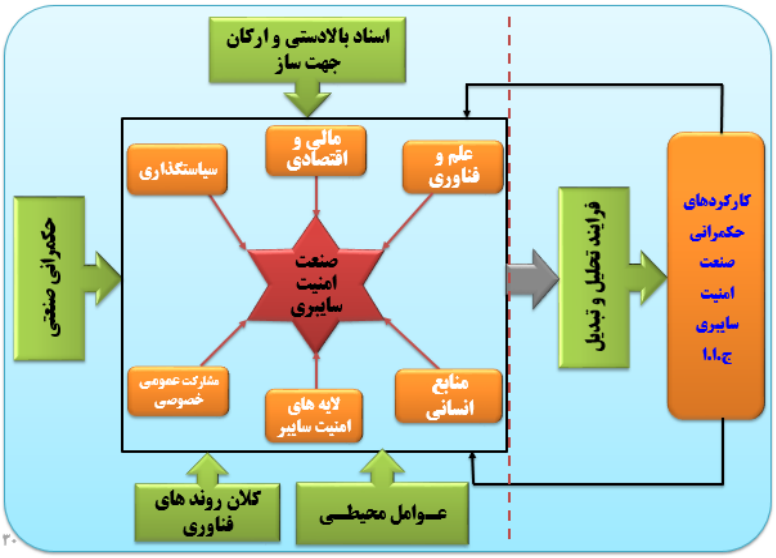
کلان‌روندهای فناوری در حوزه سایبری به‌عنوان عوامل مداخله‌گر در ابعاد و مؤلفه‌ها و نیز ارکان جهت‌ساز و توسعه صنعتی در کشور از عوامل تأثیرگذار بر کیفیت صنعت امنیت سایبری می‌باشد. حکمرانی صنعتی نیز به‌عنوان یکی از نتایج تحقق سیر انقلاب صنعتی، واقعیتی است که جهانی متفاوت را پیش‌روی بشر در آینده خواهد گشود.

از طرف دیگر مطالعات و تحلیل مضمون پژوهشگر در ادبیات موجود منابع داخلی و خارجی که پس از انجام مصاحبه با خبرگان و کارشناسان و نیز جمع‌آوری مصاحبه از صاحب‌نظران انجام شده است، شش پایه شامل علم و فناوری، مشارکت عمومی خصوصی، لایه‌های سایبری، سیاست‌گذاری، منابع انسانی و مالی و اقتصادی را به‌عنوان ابعاد تحقیق نشان می‌دهد. برخی از منابعی که به‌عنوان مرجع مطالعات برای استخراج ابعاد تحقیق از آنها استفاده شده، در جدویل زیر ارائه شده است.

جدول ۲. برخی از منابع ابعاد الگو در مبانی نظری

بُعد	منابع ۱	منابع ۲	منابع ۳	منابع ۴	منابع ۵	منابع ۶	منابع ۷
علم و فناوری	مدل بلوغ ظرفیت امنیت سایبری برای کشورها، ۲۰۲۱	دستورالعمل های حاکمیت امنیت سایبری.، ۲۰۱۷	راهنمای حکمرانی خوب در امنیت سایبری.، ۲۰۲۱	شبیه‌سازی برای امنیت سایبری: وضعیت هنر و جهت گیری های آینده.، ۲۰۲۱	چارچوب جامع امنیت سایبری برای فضای سایبری افغانستان.، ۲۰۲۱	تعاریف پایداری همگرا: ابعاد مستقل صنعت	شاخص های جهانی امنیت سایبری
سیاست‌گذاری	مدل بلوغ ظرفیت امنیت سایبری برای کشورها، ۲۰۲۱	دستورالعمل های حاکمیت امنیت سایبری.، ۲۰۱۷	راهنمای حکمرانی خوب در امنیت سایبری.، ۲۰۲۱	شبیه سازی برای امنیت سایبری: وضعیت هنر و جهت گیری های آینده.، ۲۰۲۱	چارچوب جامع امنیت سایبری برای فضای سایبری افغانستان.، ۲۰۲۱	نوانکوو و اوکائوها، ۲۰۱۹	ستیادی و همکاران، ۲۰۱۲
مالی و اقتصادی	مدل بلوغ ظرفیت	دستورالعمل های حاکمیت	شاخص‌ها ی جهانی		چارچوب جامع امنیت	نقش مشارکت و	صنعت امنیت

بُعد	منابع ۱	منابع ۲	منابع ۳	منابع ۴	منابع ۵	منابع ۶	منابع ۷
	امنیت سایبری برای کشورها، ۲۰۲۱	امنیت سایبری.، ۲۰۱۷	امنیت سایبری		سایبری برای فضای سایبری افغانستان.، ۲۰۲۱	همکاری با صنعت امنیت سایبری در آموزش دفاع سایبری	سایبری
لایه های امنیت سایبری	۱۰ لایه امنیت سایبری	انواع لایه‌های امنیت شبکه. ۲۰۲۱	نوانکوو و اوکائوها، ۲۰۱۹	تجزیه و تحلیل مولفه های استاندارد و چارچوب امنیت سایبری	۱۰ لایه امنیت سایبری، آرون هدمن، ۲۰۲۱	شاخص‌های جهانی امنیت سایبری	
مشـــــــارکت عمـــــــومی خصوصی	عوامل تعیین کننده سیاست های مشارکت عمومی و خصوصی، ۲۰۱۹	راهنمای حکمرانی خوب در امنیت سایبری.، ۲۰۲۱	راهنمای حکمرانی خوب در امنیت سایبری.، ۲۰۲۱	ستیادی و همکاران، ۲۰۱۲	چارچوب جامع امنیت سایبری برای فضای سایبری افغانستان.، ۲۰۲۱	شاخص‌های عملکرد مشارکت عمومی خصوصی در بنگلادش: پیامدی برای کشورهای در حال توسعه محمد حسین.۲۰۱۸	شاخص‌ها ی جهانی امنیت سایبری



شکل ۱. الگوی مفهومی پژوهش

روش تحقیق

مطالعه کنونی از دیدگاه‌های مختلف، تحقیقی راهبردی، توصیفی، ترکیبی کیفی و کمی و کاربردی است.

راهبردی است، زیرا به دنبال توسعه الگوی حکمرانی است.

توصیفی است، زیرا به دنبال توضیح و توصیف روابط بین عناصر الگوست.

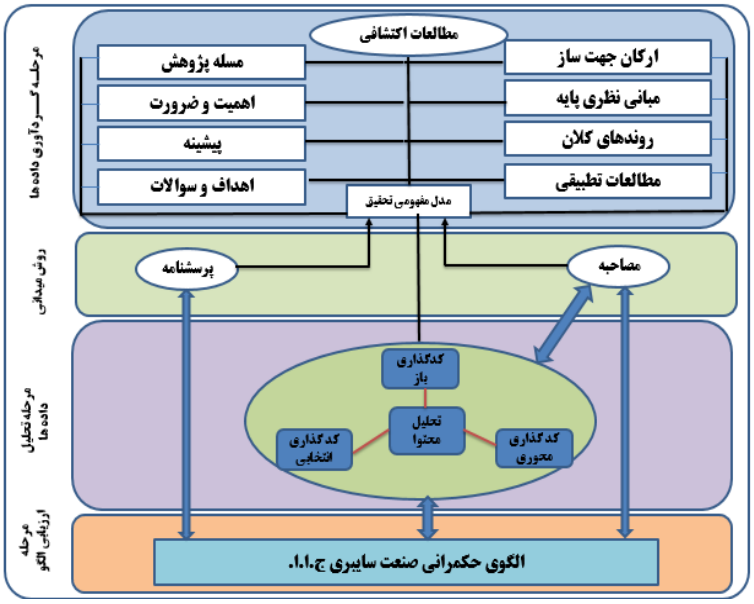
کیفی و کمی است، زیرا در مرحله نخست غیرعینی و ادراکی است و در ادامه مبتنی‌بر تحلیل‌های آماری و روش‌های عددی خواهد بود.

کاربردی است، زیرا هدف آن، استفاده و به‌کارگیری در سطح کشور می‌باشد. برخورد با موقعیت مسئله‌ای، اساس پژوهش کاربردی است.

با توجه به اینکه کل جامعه آماری این تحقیق، شامل افراد آگاه و خبرگان صنعت امنیت سایبری کشور است و تعدادی از آنها برای پژوهشگر شناسایی نشده‌اند، روش نمونه‌گیری در این پژوهش به صورت هدفمند و به صورت گلوله‌برفی است. به بیانی دیگر، در این تحقیق از تکنیک نمونه‌برداری گلوله‌برفی که مبتنی‌بر اشباع نظری است،

استفاده شد. بدین ترتیب که خبرگان اولیه به صورت غیرتصادفی با شرایط زیر انتخاب شدند:

- دارای سوابق تجربی بالای ۲۰ سال در حوزه صنعت، به‌ویژه امنیت سایبری و فناوری اطلاعات در کشور؛
- دارای سوابق مدیریتی بالای ۱۰ سال در حوزه حکمرانی، سیاست‌گذاری و برنامه‌ریزی صنعتی و افتا در کشور؛
- دارای سوابق علمی در حوزه امنیت سایبری در نظام جمهوری اسلامی ایران؛
- دارای سوابق پژوهشی و صاحب تألیفات در زمینه موضوع تحقیق.



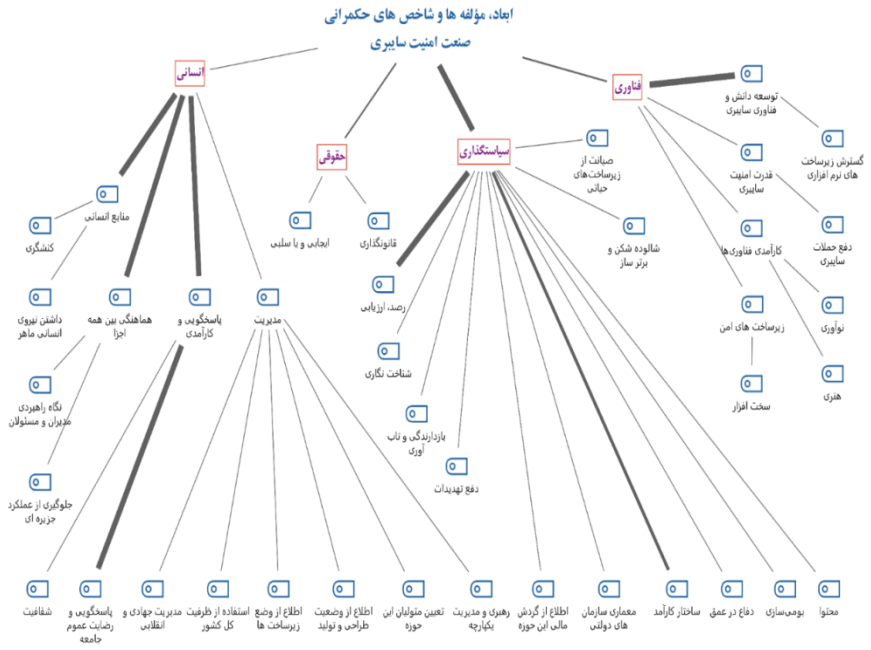
شکل ۲. فرایند اجرای تحقیق

یافته‌های تحقیق

ابتدا محوریت با فرایند و روش نظریه داده‌بنیاد برای شناخت مؤلفه‌های اصلی الگو بوده است که از آن به‌عنوان ابزاری برای روش کیفی یاد می‌کنند. ورودی این بخش از کار، متن مصاحبه با جامعه آماری است که در سه مرحله شناسه‌گذاری باز (به‌منظور استخراج ابعاد، مؤلفه‌ها و شاخص‌هاست)، شناسه‌گذاری محوری (حول محور حکمرانی صنعتی مباحث مرتب شد) و شناسه‌گذاری انتخابی که موضوع اصلی رساله را در میان

مفاهیم مصاحبه بررسی می‌کند. در انتهای این بخش، تعداد شاخص‌ها به ۱۰۷ گویه افزایش یافت و بخش دوم کار یعنی تحلیل کمی با طراحی، توزیع و جمع‌آوری ۹۳ پرسش‌نامه آغاز شد. قسمت دوم توسط نرم‌افزارهای SPSS و LESREL و پس از آن به‌منظور اطلاع از اولویت و تأثیرگذاری ابعاد بر یکدیگر با روش دیمتل فازی ادامه یافت. درنهایت نیز پس از استخراج الگوی نهایی با استفاده از روش تصمیم‌گیری چندمعیاره، اعتبارسنجی الگو انجام شد.

تحلیل کیفی:



شکل ۳. ابعاد، مؤلفه‌ها و شاخص‌های حکمرانی صنعت امنیت سایبری منتج از شناسه‌گذاری باز

تحلیل کمی:

به‌منظور تحلیل داده‌های آماری پژوهش کنونی، ابتدا داده‌های حاصل از اجرای پرسش‌نامه‌ها استخراج و در جدول اطلاعات کلی تنظیم شد؛ سپس همه اطلاعات از

طریق نرم‌افزارهای آماری به‌ویژه نرم‌افزارهای اس پی اس، اکسل و لیزرل با استفاده از روش‌های توصیفی و استنباطی، تحلیل شد.

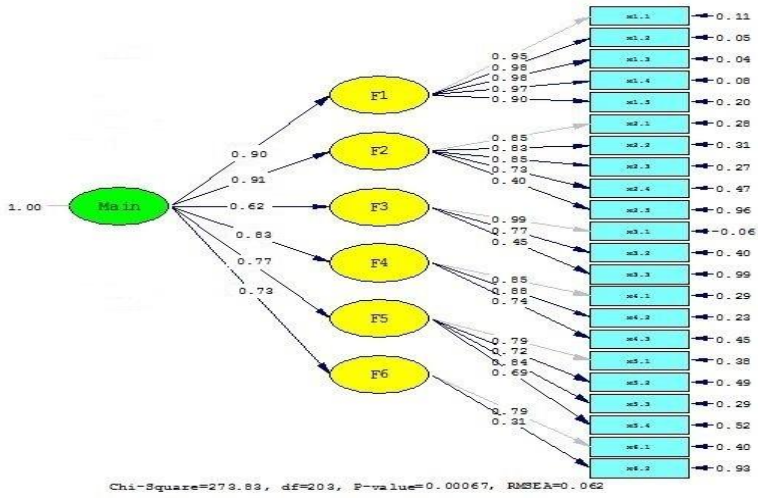
در تحلیل توصیفی اطلاعات، شاخص‌های آمار توصیفی (شامل محاسبه جداول توزیع فراوانی، درصدها، جداول توافقی و محاسبه شاخص‌های گرایش مرکزی و پراکندگی نظیر میانگین و واریانس و ...) محاسبه می‌شوند. در بخش تحلیل استنباطی از آزمون‌های شاپیرو-ویلک، دوجمله‌ای، تی تک‌نمونه‌ای، رتبه‌ای علامت‌دار ویلکاکسون و فریدمن استفاده می‌شود. در جدول زیر، توزیع فراوانی پاسخگویان بر حسب رده مدیریتی پاسخگویان ارائه شده است.

جدول ۳. توزیع فراوانی وضعیت آخرین رده مدیریتی پاسخگویان

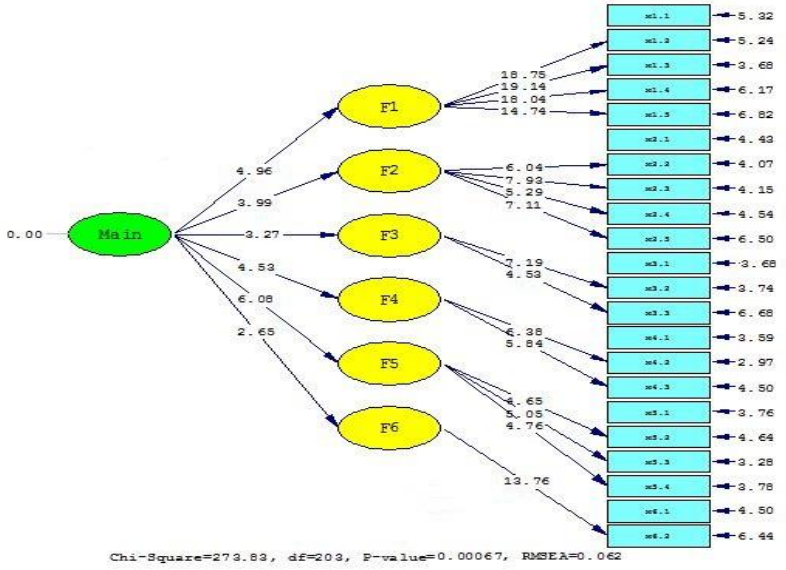
رده مدیریتی	تعداد	درصد
راهبردی	۱۸	۱۹.۴
عملیاتی	۱۸	۱۹.۴
میانی	۲۷	۲۹
کارشناسی	۳۰	۳۲.۳
مجموع	۹۳	۱۰

جدول ۴. ضرایب بتا حاصل از تحلیل عاملی تأییدی مرتبه دوم الگوی حکمرانی صنعت امنیت سایبری

علامت اختصاری	بُعد	ضریب بتا	آماره تی
F2	سیاستگذاری	۰.۹۱	۳.۲۷
F1	علم و فناوری	۰.۹۰	۴.۵۳
F4	لایه‌های امنیت سایبری	۰.۸۳	۴.۹۶
F5	مشارکت عمومی خصوصی	۰.۷۷	۲.۶۵
F6	منابع انسانی	۰.۷۳	۳.۹۹
F3	مالی و اقتصادی	۰.۶۲	۶.۰۸



شکل ۴. بارهای عاملی و ضرایب بتا استاندارد تحلیل عاملی مرتبه دوم الگوی حکمرانی صنعت امنیت سایبری ج.ا.ا



شکل ۵. آماره تی حاصل از تحلیل عاملی مرتبه مرتبه دوم الگوی حکمرانی صنعت امنیت سایبری ج.ا.ا

جدول ۵. شاخص‌های مرکزی و پراکندگی مؤلفه‌های الگوی حکمرانی صنعت امنیت سایبری ج.ا.ا

بُعد	مؤلفه	میانگین	میانه	انحراف معیار	چولگی	کشیدگی	کمینه	بیشینه

علم و فناوری	بومی‌سازی	4.79	5	0.56	-4.4	24.1	1	5
	بازدارندگی	3.57	3.57	0.89	-0.5	-0.2	1	5
	اختراع و نوآوری	4.77	5	0.55	-3.4	13.4	1.63	5
	اثربخشی و کارآمدی	3.54	3.4	1.00	-0.2	-0.7	1	5
	شبکه همکار	3.41	3.33	0.59	0.3	0.5	2	4.83
سیاست‌گذاری	تنظیم‌گری	4.04	۴	0.90	-0.7	0.0	1	5
	ساختار و سازماندهی	4.77	5	0.59	-3.9	18.9	1	5
	ظرفیت‌سازی	3.84	4	0.94	-0.8	0.1	1	5
	مسئله‌یابی	4.80	5	0.51	-3.5	13.5	2	5
	نظارت و ارزیابی و روزآمدسازی	4.80	5	0.48	-2.8	8.2	2.5	5
مالی و اقتصادی	حمایت مالی از توسعه و روزآمدسازی زیرساخت‌ها	3.57	3.5	0.79	-0.1	-0.7	1.5	5
	حمایت‌های مالی از پروژه‌ها و ایده‌ها و تحقیقات	3.28	3.25	0.68	-0.2	-0.2	1.5	4.5
	وضعیت مالی	3.41	3.33	0.59	0.3	0.6	2	4.83
لایه‌های امنیت سایبری	لایه داده‌ها و اطلاعات	3.91	4	0.78	-1.0	1.4	1	5
	لایه زیرساخت‌های شبکه	3.91	4	0.78	-0.7	1.1	1	5
	لایه نرم‌افزارهای کاربردی	3.53	3.5	0.83	0.0	-0.7	1.25	5
مشارکت عمومی خصوصی	پایداری محیط سیاسی و اقتصادی	4.08	4.25	0.76	-0.8	-0.1	2	5

	شبکه‌سازی	4.14	4.25	0.70	-0.7	0.3	2	5
	مجوزها	3.83	4	0.72	-0.1	-0.8	2	5
	مسئولیت‌پذیری	3.44	3.5	0.99	-0.3	-1.1	1.5	5
منابع انسانی	آموزش و رشد و یادگیری	3.63	3.75	0.71	-0.5	-0.1	2	4.75
منابع انسانی	برنامه‌ریزی منابع انسانی	3.85	3.8	0.68	-0.6	0.3	2	5

روش دیمتل فازی:

با توجه به اینکه برای استفاده از روش دیمتل به نظرات کارشناسان نیاز داریم و این نظرات دربردارنده عبارات کلامی مبهم و دوپهلوست، به‌منظور یکپارچه‌سازی و رفع ابهام آنها، بهتر است که این عبارات به اعداد فازی تبدیل شوند. برای حل این مشکل، لین و وو (لین و وو، ۲۰۰۸)، الگویی را ارائه کرده‌اند که از روش دیمتل در محیط فازی بهره می‌گیرد. عناوین گام‌های الگوی دیمتل فازی به شرح زیر می‌باشد:

گام اول. مشخص کردن آرمان تصمیم‌گیری و تشکیل کارگروهی برای جمع‌آوری نظرات به‌منظور حل مسئله؛

گام دوم. تعیین معیارهای ارزیابی و طراحی مقیاس کلامی فازی؛

گام سوم. جمع‌آوری ارزیابی‌های تصمیم‌گیرندگان؛

گام چهارم. به‌دست‌آوردن ماتریس نرمال رابطه مستقیم فازی؛

گام پنجم. پیاده‌سازی و تحلیل الگوی ساختاری.

اجرای روش دیمتل فازی:

در این بخش، ابعاد الگوی حکمرانی صنعت امنیت سایبری کشور به‌عنوان سطر و ستون ماتریس تصمیم در نظر گرفته می‌شود. سپس از گروه ارزیابی (شامل ۵ نفر از خبرگان) خواسته شد تا هر یک از ۶ بُعد شناسایی‌شده را به‌طور جداگانه در نظر بگیرند و تأثیر آنها را بر سایر معیارها ارزیابی کنند. ماتریس روابط مستقیم معیارها برای هر ۵ خبره محاسبه و درنتیجه ماتریس نرمال‌شده روابط مستقیم با استفاده از ماتریس ارزش تجمیعی کل با استفاده از رابطه زیر حاصل شده است.

$$\left(\tilde{x}_{ij}\right)=\left(a_{ij},b_{ij},c_{ij}\right)\ ,\ l_{ij}=\min\left\{a_{jk}\right\},m_{ij}=\frac{1}{k}\sum_{k=1}^{k}b_{ijk},u_{ij}=\max\left\{d_{ijk}\right\}$$

با استفاده از ماتریس ارتباط کل دو معیار دیگر P_i (اهمیت کلی از معیار i ام) و E_i (اثر خالص معیار i ام) تعریف می‌شوند. مقدار بالاتر P_i بیانگر میزان بالاتر اهمیت کلی معیار i ام در مقایسه با دیگر معیارها هستند.

جدول ۶. ماتریس ارتباط کل

معیار	D_j	C_i	P_i	E_i
علم و فناوری	1.283	0.277	1.560	1.006
لایه‌های امنیت سایبری	1.121	0.465	1.586	0.656
مشارکت عمومی خصوصی	0.933	0.656	1.589	0.277
منابع انسانی	0.616	0.922	1.538	-0.307
مالی و اقتصادی	0.478	0.768	1.246	-0.290
سیاست‌گذاری	0.277	1.620	1.897	-1.342

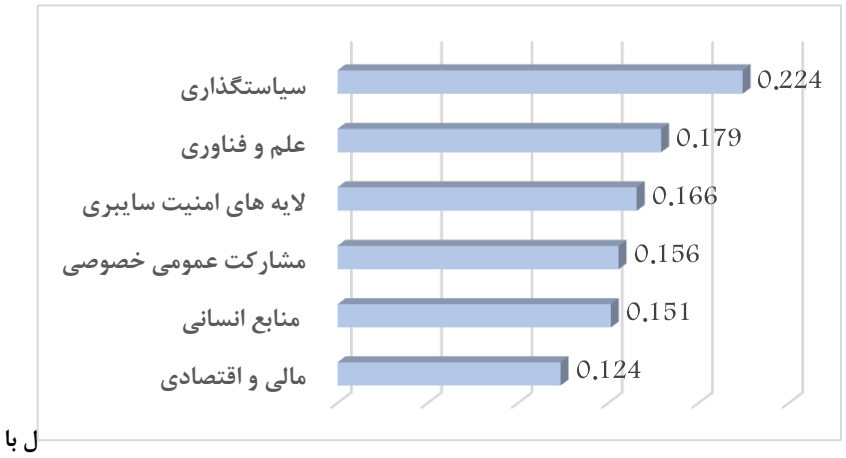
که $P_i = D_j + C_i$ و $E_i = D_j - C_i$.

در ادامه یک دیاگرام تأثیر برای هر معیار می‌توان تعریف کرد که با استفاده از ماتریس روابط کلی اطلاعات آن به‌دست می‌آید. برای تکمیل این مرحله، مقدار ارزش آستانه θ (میانگین ماتریس دفازی‌شده) تبیین می‌شود.

جدول ۷. تعیین درجه اهمیت عوامل با استفاده از روش دالالا

بُعد	P	E	Wi	Wi تعدیلی
سیاست‌گذاری	1.897	-1.342	2.324	0.224
مشارکت عمومی خصوصی	1.589	0.277	1.613	0.156
لایه‌های امنیت سایبری	1.586	0.656	1.716	0.166
علم و فناوری	1.560	1.006	1.856	0.179
منابع انسانی	1.538	-0.307	1.568	0.151
مالی و اقتصادی	1.246	-0.290	1.279	0.124

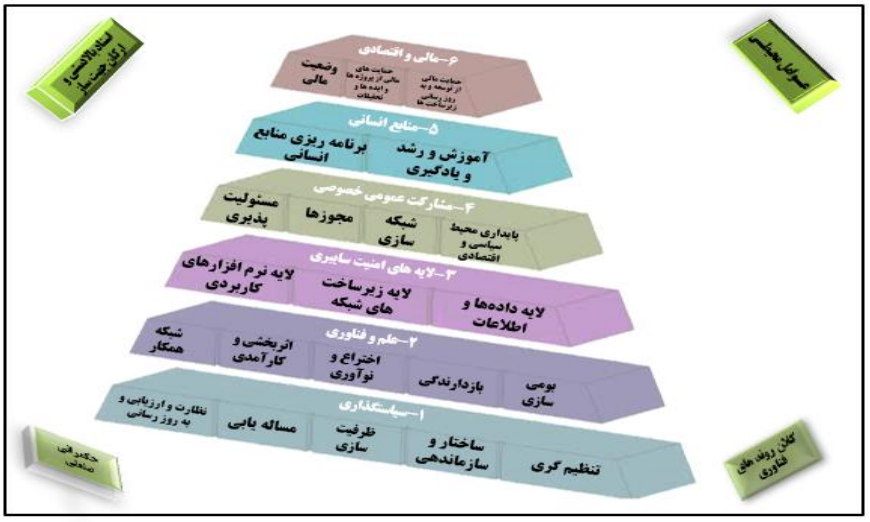
شکل ۶. درجه اهمیت عوام



ل با

استفاده از روش دالالا

الگوی تحقیق:



شکل ۷. الگوی حکمرانی صنعت امنیت سایبری جمهوری اسلامی ایران

اعتبارسنجی الگو:

جدول ۸. پرسش‌های مطرح‌شده و پاسخ‌های دریافتی برای ارزیابی الگو

ردیف	گزاره	میزان اهمیت (بر حسب تعداد)					درصد زیاد و بالاتر
		خیلی زیاد	زیاد	متوسط	کم	خیلی کم	
۱	تا چه اندازه چیدمان لایه‌ها (الگو) را از نظر «ساختاری» صحیح و منطقی ارزیابی می‌کنید؟	۴	۲	۱	۰	۰	85.7٪
۲	تا چه اندازه چیدمان لایه‌ها (الگو) را از نظر «فرایندی» صحیح و منطقی ارزیابی می‌کنید؟	۵	۰	۲	۰	۰	71.4٪
۳	تا چه اندازه چیدمان لایه‌ها (الگو) را از نظر «کارکردی» صحیح و منطقی ارزیابی می‌کنید؟	۳	۲	۲	۰	۰	71.4٪
۴	تا چه اندازه چیدمان لایه‌ها (الگو) را در دستیابی به اهداف کارآمد می‌دانید؟	۶	۰	۱	۰	۰	85.7٪
۵	تا چه اندازه چیدمان لایه‌ها (الگو) را در قدرت تعمیم و پیش‌بینی مناسب ارزیابی می‌کنید؟	۲	۳	۲	۰	۰	71.4٪
۶	تا چه اندازه چیدمان لایه‌ها (الگو) را در تعامل با محیط پیرامونی پویا و منعطف ارزیابی می‌کنید؟	۲	۴	۱	۰	۰	85.7٪

نتیجه‌گیری و بحث

امروزه شرایط فضای رقابتی بیش‌ازپیش پیچیده شده است. بر این اساس لازم است با افزایش قابلیت‌ها و استفاده حداکثری از منابع به تناسب ظرفیت کشور و روند فناوری‌ها و سیر انقلاب صنعتی، حکمرانی صنعتی برای صنایع مادر و حساس تدوین و ریل‌گذاری شود. این پژوهش پس از مطالعه مبانی نظری در بیست کشور، به ترازیابی فناوری و جایگاه صنعت امنیت سایبری در کشور پرداخت و توانست به شش بُعد حکمرانی صنعت امنیت سایبری جمهوری اسلامی ایران، با روش آمیخته که منتج از مصاحبه میدانی و طراحی، توزیع و جمع‌آوری ۹۳ پرسش‌نامه بین کارشناسان، مدیران میانی، فرماندهان و مدیران ارشد است، دست یابد. همچنین الگوی یادشده درمجموع دارای ۶ بُعد، ۲۲ مؤلفه و ۱۰۷ شاخص معنادار می‌باشد.

جدول ۹. ابعاد الگوی حکمرانی صنعت امنیت سایبری جمهوری اسلامی ایران

علامت اختصاری	بُعد	ضریب بتا	آماره تی

۱	سیاست‌گذاری	۰.۹۱	۳.۲۷
۲	علم و فناوری	۰.۹۰	۴.۵۳
۳	لایه‌های امنیت سایبری	۰.۸۳	۴.۹۶
۴	مشارکت عمومی خصوصی	۰.۷۷	۲.۶۵
۵	منابع انسانی	۰.۷۳	۳.۹۹
۶	مالی و اقتصادی	۰.۶۲	۶.۰۸

پیشنهادها

۱. تدوین الگوی راهبردی صنعت امنیت سایبری در وزارت دفاع و نیروهای مسلح، بخش عمومی- دولتی و نیز بخش خصوصی به‌منظور استخراج و شناسایی مأموریت‌ها، چشم‌انداز، اهداف و برنامه‌ها و نقشه‌راه فناوری- محصول؛

۲. تدوین سند نظام مسائل در حوزه فنی صنعت امنیت سایبری و احصاء فاصله ما با دنیا و فناوری‌های نوظهور و بدیع حوزه سایبری و تهدیدات این حوزه؛

۳. تشکیل گروه خبره و فنی به‌منظور ارزیابی صنایع امنیت سایبری بخش دولتی و خصوصی و شناسایی متقن وضع موجود و انحرافات نسبت به برنامه‌ها و مأموریت‌ها؛

۴. بازنگری شرح وظایف سازمان پدافند غیرعامل، افتا و مرکز ملی فضای مجازی؛

۵. تدوین اسناد امنیت سایبری تجهیزات و تسلیحات بومی و غیربومی به‌منظور استخراج استخر فناوری و محصولات با هدف جلوگیری از غافلگیری راهبردی.

منابع

تقی پور، رضا، لشکریان، حمیدرضا، ناصری، علی و یزدانی چهاربرج، رحیم (۱۳۹۸). الگوی راهبردی حفاظت سایبری از زیرساخت های اطلاعاتی حیاتی جمهوری اسلامی ایران. امنیت ملی، ۹(۳۴)، ۷-۴۸. https://ns.sndu.ac.ir/article_862.html

رفسنجانی‌نژاد، سیما(۱۴۰۰). بازطراحی نظام حکمرانی و سیاست‌گذاری در عصر انقلاب چهارم صنعتی. چاپ اول. تهران: مرکز بررسی‌های استراتژیک ریاست جمهوری.

ساختار امنیت سایبری NSA، نسخه ۲۰۱۶.

سند استراتژی امنیت ملی سایبری ایالات متحده آمریکا، نسخه ۲۰۱۸.

سند استراتژی امنیت ملی سایبری رژیم صیهونیستی نسخه ۲۰۱۸.

شرکت صنعت امنیت فضای تبادل اطلاعات صاایران(۱۳۹۷). نظام مدیریت فضای سایبری رژیم صیهونیستی. تهران: انتشارات انستیتو ایز ایران.

شرکت صنعت امنیت فضای تبادل اطلاعات صاایران(۱۳۹۷). نظام مدیریت فضای سایبری انگلیس. تهران: انتشارات انستیتو ایز ایران.

طهماسبی، سیامک، فرتوک‌زاده، حمیدرضا، بوشهری، علیرضا، و رجبی، میثم(۱۳۹۸). تله‌های قابلیت در مسیر توسعه سازمان‌های صنعتی دولتی. اندیشه مدیریت راهبردی. ۱۳(۲)، ۲۳۵-۲۷۵.https://doi.org/10.30497/smt.2019.2740

محمودزاده، ابراهیم، و اسماعیلی، کیوان(۱۳۹۷). الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح. فصلنامه امنیت ملی، دوره ۸، ش ۳۰.

Ahmad Nabi, A.(2021). a comprehensive cybersecurity framework for afghanistan’s cyberspace, International Journal of Engineering Applied Sciences and Technology.

Ahmad Nabi, A.(2021). International Journal of Engineering Applied Sciences and echnology, a comprehensive cybersecurity framework for afghanistan’s cyberspace

Alzoubi, Y.I., Al-Ahmad, A., & Jaradat, A.(2021). Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. Int. J. Electr. Comput. Eng. 11, 5081–5088.

Antonio, C., R.(2021). Marchettib, “ State- industry Relation and Cybersecurity Governance in Europe”, Review of International Political Economy, 2021.

Avery, A., & Oakley, R. L(2019). The Business Case for IT Security as a Core Course in IS Curriculum. Twenty-fifth Americas Conference on Information Systems, Cancun.

Bobir, O.(2020). Tursunov, Aspect of Financial Security of Industrial Enterprises Under Influence of Global Crisis, Asian Journal of Technology & Management Research, Jun-2020.

Girshel, Ch.(2020). Teaching the Cybersecurity Courses at the University in Georgia, All content following this page was uploaded by Girshel Chokhonelidze on 30 April 2020.

Haddad, C. & Binder, C(2019). Governing through cybersecurity: National policy strategies, globalized (in-) security and sociotechnical visions of the digital society. Osterr. Z. Für Soziol.

Hamdi, K.(2021)Simulation for cybersecurity: state of the art and future directions, Journal of Cybersecurity.

Hatcher, W., Meares, W.L., Heslen, J.(2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. J. Cyber Policy. 5, 302–325.

Ihalainen. A.(2022). “The Role of Data Ownership in a strategy Process: Case Study from Cybersecurity Industry”Antti Ihalainen, Alto University, Master’s Programme in Industrial Engineering & Management.

Industry, Science and Technology International Strategy Center, ITRI,2022

J.S. Hollywood(2019). Emerging Technology Trends and Their Impact on Criminal Justice‖ [online]. Rand Corporation, www.rand.org.

Laurene, K.(2019). “New European Data Privacy and Cyber Security Laws: One Year Later“, Communications of the ACM, April 2019, Vol. 62 No. 4, Page 38.

Maija, B. L.(2021). De Nul, “Towards a sustainable, human centric and resilient European industry” 2021.

Melwin Syafrizal, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 12, No. 3, December 2020, Analysis of Cybersecurity Standard and Framework Components.

Mishra, A. Alzoubi, Y.I.,Gill, A.Q.(2022). Anwar, M.J. Cybersecurity Enterprises Policies: A Comparative Study. Sensors.

Paananen, H., Lapke, M., & Siponen, M.(2020). State of the art in information security policy development. Comput. Secur. 88, 101608.

Senol, M. K.(2020). E. Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. J. Eng, 5267564. [CrossRef]

Tissir, N., El Kafhali, S(2021). Aboutabit, N. Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal. J. Reliab. Intell. Environ.

Vitalii, K.(2020). Public-Private Partnership in Cybersecurity, International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30,

Wang, P, & D’Cruze, H(2019). Cybersecurity Certification: Certified Information Systems Security Professional (CISSP). In S. Latifi (Eds.), International Conference on Information

Wang, P, & Kohun, F.(2019). Designing a doctoral program in cybersecurity for working professionals. Issues in Information Systems, 20(1), 88-99.

Weiss, M.; Biermann, F.(2021). Cyberspace and the protection of critical national infrastructure. J. Econ. Policy Reform 2021, 1–18.

Wilson N., Kingsley, C. U.(2019). Socio-Technical Perspectives On Cybersecurity: Nigeria‘s Cybercrime Legislation In Review, international journal of scientific & technology research.

COPYRIGHTS