Scientific Journal of Electronic & Cyber Defense
Vol. 12, No. 4, Winter 2025, Serial No. 48, PP.65-79
ISSN: 2322-4347, E-ISSN: 2980-8979

Futuristic analysis of the components of the model for cyber threats in the Islamic Republic of Iran Army

K. Koulivand, M. Sepehri*

*Assistant professor،Khatam al-Anbia University of Defense،University, Tehran, Iran

(Received: 2024/08/15, Revised: 2024/12/07, Accepted: 2025/01/02, Published: 2025/02/01)

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.7.1

ABSTRACT

Cyber threats are attacks against an organization in order to achieve different goals, and a cyber attacker tries to steal the organization's sensitive information, disrupt the organization's ability to provide services, or take other actions that somehow affect the security infrastructure and to damage the organization's network. Today, the number of cyber incidents and their types are increasing, especially in our country, and if an organization does not have a process or a plan to respond to cyber incidents, it will take a long time to respond to incidents and restore the organization's systems. Apart from this, the costs of the organization and the amount of damage that may be done to the infrastructure will be much higher than an organization that has already prepared a specific plan to respond to a cyber incident. Therefore, responding to cyber incidents is a very important issue that every organization should pay attention to. Therefore, the present study was conducted with the aim of prospective analysis of the components that make up the pattern of facing cyber threats in Aja, which type is applied in a mixed (quantitative and qualitative) way. In order to identify the components and constituents of the desired model, at first, using study resources and library documents, the primary components were identified, and then through conducting interviews with experts in the field of cyber and future studies, the dimensions, components, and items of the model were identified and counted. Then, by preparing a researcher's questionnaire and with the help of a statistical sample of 120 people, the counted items were measured, and this process was carried out using SPSS software in the form of descriptive and inferential analysis. Then, by using PLS structural equation modeling software and taking into account the partial least squares, the necessary indicators regarding the variables were examined. The final model considered for research in three main sections of forecasting with four subsections and 18 components; The foresight section was explained with four sub-sections and 32 components, and the post-forecasting section was explained with two sub-sections and 13 components.

Keywords: Futures Studies, Pattern of Confrontation, Cyber Threats, Army of the Islamic Republic of Iran.

Cite this article: K. Koulivand, M. Sepehri "Futuristic analysis of the components of the model for cyber threats in the Islamic Republic of Iran Army," Electronic and Cyber Defense, vol.12 , no.4 , pp.65-79 , . DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.7.1

 Publisher: Imam Hossein University

*Corresponding Author Email: sepehri377@chmail.ir

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۴، زمستان ۱۴۰۳، ص ۷۹-۶۵
شاپا الکترونیکی: 2980-8979 شاپا چاپی: 2322-4347

علمی-پژوهشی

واکاوی آینده‌پژوهانه مؤلفه‌های تشکیل‌دهنده الگوی مواجه با تهدیدهای سایبری در آجا

خلیل کولیوند[۱]، محمد سپهری*[۲]

۱- دکتری ، ۲- استادیار، دانشگاه بین‌المللی امام خمینی (ره)، قزوین، ایران.

(دریافت: ۱۴۰۳/۰۵/۲۵، بازنگری: ۱۴۰۳/۰۹/۱۷، پذیرش: ۱۴۰۳/۱۰/۱۳، انتشار: ۱۴۰۳/۱۱/۱۳)

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.7.1

چکیده

تهدیدهای سایبری حمله‌هایی فراروی یک سازمان در جهت دستیابی به اهداف مختلف هستند و یک مهاجم سایبری سعی می‌کند اطلاعات حساس سازمان را به سرقت برده، توانایی آن سازمان را در فراهم کردن خدمات دچار اختلال نموده یا اقدامات دیگری انجام دهد که به‌نوعی به زیرساخت‌های امنیتی و شبکه‌ای سازمان آسیب برساند. امروزه تعداد حوادث سایبری و انواع آن به‌ویژه در کشور ما در حال افزایش است و چنانچه سازمانی فاقد فرآیند یا طرحی برای پاسخ به حوادث سایبری باشد، پاسخ به حوادث و بازگشت سامانه‌های سازمان زمان زیادی می‌گیرد. گذشته از این، هزینه‌های سازمان و میزان آسیبی که ممکن است به زیرساخت‌ها وارد شود، بسیار بیشتر از سازمانی خواهد بود که از قبل طرح مشخصی برای پاسخ به حادثه سایبری آماده کرده باشد؛ بنابراین پاسخ به حوادث سایبری موضوع بسیار مهمی است که هر سازمانی باید با آن توجه کند. ازاین‌رو پژوهش حاضر باهدف واکاوی آینده‌پژوهانه مؤلفه‌های تشکیل‌دهنده الگوی مواجه با تهدیدهای سایبری در آجا به انجام رسیده که نوع آن کاربردی به‌صورت آمیخته (کمی و کیفی) است. برای شناسایی مؤلفه‌ها و اجزاء تشکیل‌دهنده الگو موردنظر، در ابتدا با استفاده از منابع مطالعاتی و اسناد و مدارک کتابخانه‌ای، مؤلفه‌های اولیه شناسایی و سپس از طریق انجام مصاحبه با خبرگان حوزه سایبر و آینده‌پژوهی، ابعاد، مؤلفه‌ها و گویه‌های مدل شناسایی و احصاء گردید. سپس با تهیه پرسش‌نامه محقق ساخت و به کمک نمونه آماری ۱۲۰ نفر، موارد احصاء شده سنجش شدند که این فرآیند با استفاده از نرم‌افزار SPSS در قالب تحلیل‌های توصیفی و استنباطی صورت پذیرفت. سپس با استفاده از نرم‌افزار مدل‌سازی معادلات ساختاری PLS و لحاظ نمودن حداقل مربعات جزئی شاخص‌های لازم در خصوص متغیرهای مکنون موردبررسی قرار گرفت. الگوی نهایی مدنظر پژوهش در سه بخش اصلی پیش‌آینده‌نگاری با چهار زیر بخش و ۱۸ مؤلفه؛ بخش آینده‌نگاری با چهار زیر بخش و ۳۲ مؤلفه و در بخش پسا آینده‌نگاری با دو زیر بخش و ۱۳ مؤلفه تبیین شد.

کلیدواژه‌ها: آینده‌پژوهی، الگوی مواجه، تهدیدهای سایبری، ارتش جمهوری اسلامی ایران.

۱. مقدمه

امنیت سایبری در سازمان‌ها به‌ویژه سازمان‌های نظامی یکی از مسائل مهم و حیاتی است که شامل تعدادی از فن‌ها و رویکردها برای ایمن‌سازی شبکه، زیرساخت‌های دیجیتالی و همچنین دستگاه‌های وابسته به آن‌ها قلمداد می‌شود [۱] و این مهم هنگامی‌که در سازمانی تجهیزات محور به‌مثابه ارتش جمهوری اسلامی ایران مدنظر قرار می‌گیرد، از جایگاه مهم‌تری برخوردار می‌گردد. اقدام‌های تهدید آفرین بازیگران قوی و ضعیف در فضای سایبر اعم از دولت‌ها، گروه‌های سازمان‌یافته، گروهک‌های تروریستی و حتی افراد عادی در قالب فعالیت‌هایی مانند جنگ سایبری[۱]، جرائم سایبری[۲]، تروریسم سایبری[۳]، جاسوسی سایبری[۴] و دیگر انواع آن هرروزه تهدیدهای جدیدی را متوجه زیرساخت‌های سازمان‌ها می‌کند و تشخیص این تهدیدهای بالقوه، پیامدها و چالش‌های امنیتی آن‌ها در محیط پیچیده و سرشار از عدم قطعیت آینده بر حساسیت کار می‌افزاید [۲].

[1] Cyber War.
[2] Cyber Crimes.
[3] Cyber Terrorism.
[4] Cyber Espionage

استناد: کولیوند، خلیل، سپهری، محمد "واکاوی آینده‌پژوهانه مؤلفه‌های تشکیل‌دهنده الگوی مواجه با تهدیدهای سایبری در آجا"، پدافند الکترونیکی و سایبری، ۱۲(۴)، ۷۹-۶۵، ۱۴۰۳. https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.7.1

ناشر: دانشگاه جام امام حسین(ع).

* رایانامه نویسنده مسئول: sepehri377@chmail.ir

یکی از مباحث علمی مهم و مرتبط با آینده، بر اساس تعریف آژانس امنیت سایبری اروپا[1] در رابطه با تهدیدهای سایبری که از جایگاه ویژه‌ای برخوردار است، آینده‌پژوهی[2] است. در حال حاضر فناوری‌های مدرن امنیت رایانه به‌منظور محافظت از کاربران و زیرساخت‌های حیاتی در برابر مجرمان سایبری مفید هستند، اما باتوجه‌به تحولات فزاینده در فناوری‌ها، مبحث آینده‌پژوهی در حوزه سایبر موضوعی در جهت جلوتر بودن از مجرمان و تهدیدآفرینان سایبری در فضای سرشار از شگفتی آینده به شمار می‌آید [۳]. آینده‌پژوهی سایبری در سطح سازمان‌ها می‌تواند توان مجموعه را برای پیش‌بینی، مدیریت و مقابله با تهدیدها و حمله‌های سایبری افزایش داده، پیامدهای مخرب ناشی از بروز تهدیدها را کاهش و بازسازی حوزه‌های آسیب‌دیده را با کمترین هزینه ممکن، میسر سازد [۴].

ازاین‌رو پژوهش حاضر باتوجه‌به ماهیت آن، می‌تواند منجر به ارتقاء توانمندی آجا در راستای شناسایی، تجزیه‌وتحلیل و دفاع در برابر یا مقابله با حمله‌های سایبری احتمالی آینده شود. درواقع استفاده از آینده‌پژوهی در حوزه امنیت سایبری می‌تواند به شناخت دقیق‌تر و واضح‌تر کلان‌روندها، پیشران‌ها، چالش‌ها و تهدیدهای آینده کمک نموده و ماهیت چند رشته‌ای آن نیز به بررسی دقیق‌تر پیامدهای ناشی از تهدیدهای سایبری بی انجامد.

تلفیق آینده‌پژوهی و امنیت سایبری مستلزم اجرای یک فرایند آینده‌پژوهانه است که در حال حاضر در بدنه آجا موجود نیست، هرچند که در حال حاضر توان سایبری ارتش جمهوری اسلامی ایران با بهره‌گیری از پروتکل‌ها، رویه‌ها و دستورالعمل‌های موجود در مواجه با تهدیدهای سایبری در شرایط نسبتاً قابل‌قبولی قرار دارد، اما با توسعه و تحولات روزافزون فناوری‌ها در بخش سایبری و کاربردهای متنوع آن و احتمال وقوع کلان‌روندهای ناشناخته در این بخش که می‌تواند با شگفتی‌سازی‌های حوزه سایبر نیز همراه شود، احتمال مواجه با چالش‌های اساسی متصور است. بر اساس آنچه مطرح شد، انجام این پژوهش ازآنجا اهمیت می‌یابد که:

- در افق زمانی میان‌مدت (دو تا پنج‌ساله) ضرورت‌های بدنه سایبری آجا را به‌منظور شناسایی تهدیدهای این حوزه تبیین می‌نماید؛
- بخشی از نگرانی‌های فرماندهان آجا در حوزه امنیت سایبری در قلمرو زمانی مدنظر پژوهش را برطرف می‌کند؛
- برای نخستین بار از علوم و شیوه‌های نوین همچون آینده‌پژوهی در سازمان‌های نظامی در جهت ارتقاء امنیت سایبری سامانه‌ها و تجهیزات آن‌ها بهره‌برداری می‌کند؛
- تا حد زیادی موجب افزایش کارایی و اثربخشی مجموعه‌های کاری واداری مستقر در بدنه یگان‌های نظامی و به‌ویژه ارتش جمهوری اسلامی ایران گردد؛

هدف اصلی این پژوهش تبیین مؤلفه‌های الگوی مواجه با تهدیدهای سایبری در آجا با رویکرد آینده‌پژوهی است و باتوجه‌به موضوع پژوهش سؤال اصلی این است که مؤلفه‌های تشکیل‌دهنده الگوی مواجه با تهدیدهای سایبری در آجا با رویکرد آینده‌پژوهی کدام‌اند؟

و در این راستا سؤالات فرعی زیر مطرح است:

- زیر مؤلفه‌های الگوی تشکیل‌دهنده مواجه با تهدیدهای سایبری در آجا با رویکرد آینده‌پژوهی کدام‌اند؟
- ارتباط بین زیر مؤلفه‌های مختلف تشکیل‌دهنده الگوی مواجه با تهدیدهای سایبری در آجا با رویکرد آینده‌پژوهی چگونه است؟

۲. ادبیات موضوع و پیشینه تحقیق

۲-۱. ماهیت آینده‌پژوهی و آینده‌نگاری:

آینده‌پژوهی دانش تحلیل، طراحی و برپایی هوشمندانه آینده است. این دانش در پی آن است که به شیوه‌ای آگاهانه، عاملانه و پیش‌دستانه، انسان را از غافل‌گیری در برابر توفان سهمگین تغییرات و پیشرفت‌های سرسام‌آور محافظت کند. روند شتابان علوم و فناوری‌ها و پیامدهای شگرف آن‌ها بر تمامی عرصه‌های حیات بشری، سازمان‌ها و افراد را بر آن داشته که به این حوزه‌ها نگاهی عمیق‌تر داشته باشند. این مقوله به‌ویژه در حوزه‌های راهبردی و فناوری اطلاعات از اهمیت دوچندانی برخوردار است. در جهان امروز که سرشار از سونامی‌های هولناک تغییر و تحول است، فضای آینده، سرشار از غافلگیری راهبردی به همراه ناپایداری، ابهام و عدم قطعیت شده است [۵].

آینده‌پژوهی به‌عنوان یک ابزار بسیار مؤثر در سیاست‌گذاری و به‌خصوص سیاست‌گذاری علم و فناوری به دولت‌ها کمک می‌نماید تا در شرایط دنیای امروز به چالش‌هایی همچون جهانی‌شدن و رقابت فزاینده پاسخی مناسب ارائه و اقداماتی مؤثر انجام دهند. این موضوع به‌عنوان یک ابزار تصمیم گیر دولتی، در محیط سیاست علم و فناوری ظاهرشده که در بسیاری از حالات منجر به پاسخ راهبردی به سؤالات در یک چشم‌انداز بلندمدت شده است [۶].

از سوی دیگر، حتی در صورت انجام این فرآیند و تولید اطلاعات درباره آینده، گاهی اوقات ممکن است مدیران به این دلیل که برخی اطلاعات با فرایندهای رسمی تصمیم‌گیری‌شان هماهنگ[3] نیست، این‌گونه اطلاعات را نادیده بگیرند [۷]. به‌عنوان‌مثال، با

[1] The European Union Agency for Cybersecurity.
[2] Futures Studies.
[3] Coordinated.

آن‌که خودروسازان آمریکایی از بحران انرژی [افزایش شدید قیمت نفت] در دهه هفتاد میلادی مطلع بودند، ولی در پیش‌نگریِ دلالت‌های آن، دچار شکست شدند [۸].

از سوی دیگر واژه‌ای که اغلب آن را بعد عملی آینده‌پژوهی قلمداد می‌کنند، آینده‌نگاری[1] است [۹]. آینده‌نگاری ترکیبی از رویکردهایی است که از خروجی‌های متقابل سه فعالیت بهره می‌برد: این سه فعالیت شامل آینده (تفکر آینده، پیش‌بینی، بلندمدت، آینده‌های جایگزین، سناریوها و چشم‌اندازها)، برنامه‌ریزی (تحلیل راهبردی، تعیین اولویت‌ها) و شبکه‌سازی (گسترش مشارکت، فن‌های شبکه و کارگروهی) است [۱۰].

۲-۲. مدل‌ها و الگوهای آینده‌پژوهی و آینده‌نگاری

مدل‌ها و الگوهای آینده‌پژوهی و آینده‌نگاری فرا روش‌هایی هستند که می‌توانند روش‌های مرتبط با مطالعات آینده دیگر را در خود بگنجانند. این روش‌ها اطلاعات را در قالب‌ها، طبقه‌بندی و جمع‌آوری می‌کند و در جریان‌های منطقی مرتب می‌کند [۱۱].

بر اساس نظر اندرسون و راسموسن[2] فرایند آینده‌نگاری اغلب ترکیبی از سه گونه سؤال است که شامل نقطه عزیمت (اکنون وضعیت چگونه به نظر می‌رسد؟)، آرزوها و انتظارات (چه توقعات و انتظاراتی از پیشرفت‌های آینده در حوزه‌های تمرکز آینده‌نگاری داریم؟) و تحقق (چگونه می‌توان پیشرفت‌های موردنظر را محقق ساخت؟) است [۱۲].

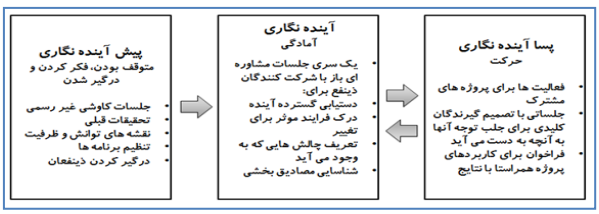
محققان برای پاسخ به این سه سؤال، به پنج عنصر اصلی آینده‌نگاری اشاره می‌کنند که عبارت‌اند از برآورد ساختارمند تحولات و نیازهای آینده، روش‌های تعاملی و مشارکتی؛ ایجاد شبکه اجتماعی همکاری و تعامل؛ سناریوها و توسعه چشم‌اندازهای راهبردی؛ ایجاد تعهد و دیدگاه مشترک. آنچه موارد مطرح‌شده را در یک‌شکل منسجم جمع‌آوری نموده و به‌صورت یکپارچه ارائه می‌نماید، قالب‌هایی است که به‌عنوان الگو، مدل و یا چارچوب شناخته می‌شوند و در موضوع آینده‌نگاری با مطرح‌شدن این قالب‌ها موضوعات مختلف موردبررسی و واکاوی قرارگرفته‌اند [۱۳]. این قالب‌ها عبارت‌اند از "سیستمی از قوانین، ایده‌ها یا باورها که برای برنامه‌ریزی یا تصمیم‌گیری درباره چیزی استفاده می‌شود" [۱۴]. چارچوب‌ها بهترین شیوه‌ها و قوانین را برای انجام گروهی از فعالیت‌ها ارائه می‌کنند. ازآنجایی‌که یکی از ویژگی‌های ستون فقرات آینده‌نگاری یک فرآیند سیستماتیک است، چارچوب‌های آینده‌نگاری برای شکل دادن به روش‌شناسی توسط شرکت‌کنندگان و ذینفعان حیاتی هستند [۱۵].

چارچوب آینده‌نگاری را می‌توان نسخه‌ای از چارچوب توصیف‌شده دررابطه‌با تفکر درباره آینده مشاهده کرد که از شش فعالیت اصلی یک پروژه آینده‌نگاری تشکیل‌شده که شامل چارچوب‌بندی، پویش، پیش‌بینی، چشم‌انداز، برنامه‌ریزی و اقدام است. چارچوب‌بندی شامل شناسایی جزئیات، پویش مبتنی بر بررسی روندها و مسائل در حال ظهور و پیش‌بینی به تبیین جزئیات مسائل می‌پردازد که آینده جایگزین در مرحله پیش‌بینی با گرفتن ورودی اطلاعات از مرحله قبل تعیین می‌شود، چشم‌انداز مرحله‌ای است که یک سازمان اهداف و آینده مطلوب را تعیین می‌کند، و تمام خروجی‌های مطالعه به‌منظور دستیابی به اهداف موردنظر در مرحله راهبرد سازی انجام می‌شود (جدول (۱)) [۱۶].

جدول (۱). چارچوب آینده‌نگاری و تفکر در مورد چارچوب آینده [۱۶]

تفکر در مورد چارچوب آینده	چارچوب آینده‌نگاری
کادربندی	توصیف دامنه
اسکن کردن	ارزیابی فعلی
پیش‌بینی	آینده پایه
	آینده‌های جایگزین
چشم‌انداز	آینده مرجع
	تحلیل مفاهیم
برنامه‌ریزی	برنامه‌ریزی برای آینده
اقدام	شاخص‌های پیشرو
	خلاصه

از قدیمی‌ترین و معتبرترین چارچوب‌های عام آینده‌نگاری می‌توان به فرآیند آینده‌نگاری چارچوب مارتین[3] نام برد که شامل سه مرحله پیش‌آینده‌نگاری (کارهایی که قبل از آینده‌نگاری باید انجام داد)؛ آینده‌نگاری و پسا آینده‌نگاری فرایند پیاده‌سازی نتایج آینده‌نگاری است (شکل (۱)) [۱۷].



شکل (۱). مدل آینده‌نگاری مارتین

[1] Foresight.
[2] Rasmussen.
[3] Martin.

مرحله پیش‌آینده‌نگاری: این مرحله شامل دو گام مهم و اساسی تصمیم برای شروع آینده‌نگاری و فعالیت‌های آماده‌سازی است. انجام آینده‌نگاری به منابع قابل‌توجهی نیازمند دارد که باید در آغاز، تصمیم‌گیری سطح بالا نسبت به آینده‌نگاری انجام شود سپس در گام فعالیت‌های آماده‌سازی اولویت‌بندی و اتخاذ سیاست بلندمدت برای علم‌وفناوری موردپذیرش قرار گیرد.

مرحله آینده‌نگاری: در این مرحله گام‌های طراحی فرآیند آینده‌نگاری شامل تحلیل راهبردی، توافق بر گزینه‌های محتمل و انتشار نتایج حاصل از فرآیند آینده‌نگاری انجام می‌شود. گام طراحی فرایند آینده‌نگاری بسیار حیاتی است؛ زیرا این فرایند باعث تحقق اهداف می‌شود و گزینه‌ها و راه‌حل‌های مناسبی برای کاربران تولید می‌کند. تعیین مخاطبین اصلی نتایج آینده‌نگاری و مخاطبین نیازهای آینده‌نگاری، تقویت تعهد، اطمینان از قابلیت سازگاری سیستم تخصیص منابع فعلی برای علم‌وفناوری، دخالت دادن مردم در پیش‌بینی و سیاست‌گذاری، توجه به سلسله ارتباطات قوانین بین بخش‌ها، یکپارچه‌سازی فشار فناوری و کشش تقاضا در کنار رویکردهای بالابه‌پایین و پایین به بالا و تعیین رویه انتشار و پیاده‌سازی نتایج ازجمله فعالیت‌های این گام است. در تحلیل راهبردی هدف ارزیابی گزینه‌های مختلف در پژوهش‌ها اعم از فعالان، تخصیص منابع و هزینه فرصت‌ها (مانند اثرات اجتماعی اقتصادی و اثرات هم‌افزایی) است. در ادامه باید بر روی گزینه‌های محتمل توافق شود و یک چشم‌انداز از آینده تعریف شود که بیشترین گزینه‌های علمی و فناوری مطلوب را که در فاز تحلیل راهبردی تعریف‌شده، در برداشته باشد. به‌علاوه باید یک راهبرد نیز برای پیگیری گزینه‌های انتخابی اتخاذ شود. در گام انتشار نتایج حاصل از فرایند آینده‌نگاری لازم است که مخاطبان هدف که قبلاً مشخص‌شده‌اند، انتخاب شوند و بهترین ابزار انتشار نتایج نیز تعیین شود.

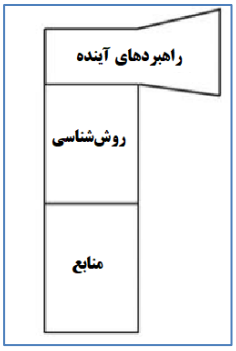
مرحله پسا آینده‌نگاری: در این مرحله گام‌های مختلفی انجام می‌شود. اولین قدم؛ تصمیم‌گیری در زمینه برنامه‌ریزی برای انجام پژوهش یا ایجاد فناوری است. این امر ممکن است نتیجه مستقیم آینده‌نگاری باشد یا به‌طور غیرمستقیم از عوامل سیاسی و مدیریتی منتج شده باشد. همچنین تعریف برنامه و تعیین جهت یکی از کارهایی است که در این بخش باید انجام شود تا سلسله‌مراتبی از اهداف برای برنامه‌ریزی و سپس اتخاذ راهبرد برای دست‌یابی به اهداف و ایجاد سیستم مدیریتی مؤثر به وجود آید. عنصر کلیدی در تعیین سیستم مدیریتی کارا، ارزیابی متناوب و در صورت نیاز تغییر مجدد راهبرد کلی است. در گام تعریف و اجرای پروژه‌ها، بر اساس جهت‌گیری‌های صورت گرفته، پروژه‌ها تعریف و اجرا می‌شوند. در این گام پروژه به‌طور مشروح بیان‌شده و برنامه‌ریزی و اجرا تا سطح جزئیات ارائه می‌شود. درنهایت کاربران بالقوه تعیین‌شده و بهترین رویکرد برای انتشار نتایج و تعیین متولی آن و پیگیری فرآیند پیاده‌سازی تصمیم‌گیری می‌شود [۱۸].

از سوی دیگر یکی از مطرح‌ترین چارچوب‌ها در حوزه سایبر مربوط به چارچوب آینده‌نگاری امنیت سایبری اروپا است. این چارچوب با بهره‌گیری از حروف کلمه «FORESIGHT» به‌صورت مراحل عملکردی متوالی در نه بخش به شرح زیر تدوین‌شده است [۱۹]:

- چارچوب‌بندی[1]: انجام وظایف مربوط به تعیین هدف آینده‌نگاری، محدوده، محتوا و افق زمانی در این بخش انجام می‌شود؛
- به دست آوردن[2]: جمع‌آوری داده‌ها و اطلاعات، جمع‌آوری شرکت‌کنندگان، همچنین با استفاده از بخش مشترک به روشی تکراری که با چارچوب آن‌که در عملکرد قبلی بیان‌شده، سازگار است؛
- بررسی[3]: به اشتراک گذاشتن ایده‌ها و نظرات در مورد داده‌ها و اطلاعات دسترسی یافته مربوط به گذشته و حال، جمع‌بندی و تجزیه‌وتحلیل آن‌ها برای پردازش؛
- استقرار[4]: اندیشیدن به آینده بادانش ایجادشده، تصور کردن احتمالات در ذهن و تصور گزینه‌های جایگزین برای ایجاد آینده؛
- ترکیب کردن[5]: ترکیب همه افکار جایگزین آینده با شرایط و منابع حال حاضر به روش تفسیری. بحث، مذاکره، تسهیل و حل تعارض در این عملکرد صورت می‌گیرد؛
- تصویرسازی[6]: اشاره به آینده‌های احتمالی، چشم‌انداز و تولید گزارش، پخش با چندرسانه‌ای، اشتراک‌گذاری در رسانه‌های اجتماعی؛
- هدایت[7]: تعریف اقدامات و تغییراتی که انجام خواهد شد، تعیین توالی آن‌ها برای رسیدن به آینده‌های مختلف، تدوین راهبرد و برنامه‌ریزی؛
- مدیریت[8]: انجام اقدامات، ایجاد تغییرات و حل مشکلات برنامه؛
- ردیابی[9]: ارزیابی نتایج مدیریت، انجام تجزیه‌وتحلیل تأثیر برای درس گرفتن به‌منظور فرآیند یادگیری.

[1] Framing.
[2] Obtaining.
[3] Reviewing.
[4] Establishing.
[5] Synthesizing.
[6] Illustrating.
[7] Guiding.
[8] Handling.
[9] Tracking.

از دیگر مدل‌های مطرح در حوزه آینده‌نگاری و سایبر می‌توان به مدل پریسکوپ آینده‌نگاری[1] اشاره نمود که درواقع یک رویکرد آینده‌نگاری فناوری نوین است و دارای سه ماژول وابسته به هم است. این سه ماژول شامل منابع، روش‌شناسی و راهبردهای آینده است. مدل از شباهت پریسکوپ استفاده می‌کند، یعنی منابع و روش‌شناسی بخش‌های زیربنایی هستند که سازمان را قادر می‌سازد آینده‌های جایگزین را ببینند و راهبردهای آتی را برای بقا و رقابت در محیط ارائه دهد. این مدل نیز همانند سایر مدل و چارچوب‌های آینده‌نگاری که مطرح‌شده از سه جزء اساسی برخوردار است. منابع و ورودی‌ها به‌عنوان پیش‌آینده‌نگاری، روش‌شناسی به‌عنوان آینده‌نگاری و راهبردهای آینده در نقش پسا آینده‌نگاری به ایفای نقش می‌پردازند (شکل (۲)) [۲۰].



شکل (۲)، مدل پریسکوپ آینده‌نگاری [۲۰]

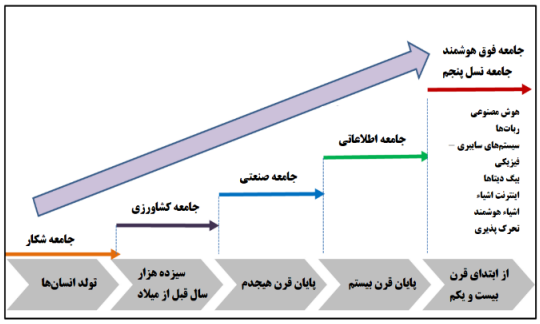
در یک جمع‌بندی کلی می‌توان مدل‌های مختلفی را برای آینده‌نگاری نام برد که توسط صاحب‌نظران مختلف طی سه دهه گذشته ارائه‌شده است. این مدل‌ها بیان‌کننده فرایند اجرای آینده‌نگاری عمومی هستند و می‌توان برای انجام مطالعات آینده‌نگاری در حوزه‌های مختلف و با دامنه‌های موضوعی متفاوت از آن‌ها استفاده کرد. باتوجه‌به توضیح‌های ارائه‌شده در مراجع مورداستفاده می‌توان به این نتیجه رسید که صاحب‌نظران و پژوهشگران آینده‌نگاری که به ذکر عوامل مهم فرایند اشاره‌کرده‌اند، در برخی از مؤلفه‌ها دارای اتفاق‌نظر بوده و در بعضی از این مفاهیم نیز باوجود نام‌گذاری متفاوت، تعاریف یکسانی ارائه داده و برداشت مشابهی داشته‌اند.

۲-۳. دوره‌های مختلف جوامع

نکته دیگری که در حوزه سایبر و فضای مجازی در ترسیم چارچوب بایستی مدنظر قرار گیرد این است که در این فضا با کلان‌روندهایی مواجه هستیم که تأثیرات شگرفی را بر بخش‌های مختلف زندگی بشر نهاده است. فناوری‌های اطلاعات و ارتباطات در هر جنبه‌ای از زندگی روزمره در حال تکامل، پیشرفت و استفاده از آن است. یکی از مهم‌ترین کلان‌روندهای این حوزه را باید جامعه[2] ۵,۰ ژاپن، واژه‌ای که توسط دولت این کشور ارائه‌شده است، به‌حساب آورد. این کلان‌روند مفهوم جدیدی است که در پنجمین برنامه اصول علم‌وفناوری معرفی و تدوین‌شده است. جامعه ۵,۰ به‌عنوان جامعه‌ای که توانایی ارائه مواد و خدمات موردنیاز به مردم را در هر زمان که نیاز دارند، تعریف می‌کند. این جامعه می‌تواند نیازهای اجتماعی مختلف را برآورده کند و بر تفاوت‌های علوم انسانی غلبه کند [۲۱].

علاوه بر جامعه ۵,۰ که تلاشی برای دیجیتالی کردن زیرساخت‌های صنعتی و اجتماعی است ما باکلان روندهایی همچون انقلاب صنعتی ۴,۰ آلمان، اینترنت صنعتی ایالات‌متحده، پروژه ساخت چین ۲۰۲۵ و شهرهای هوشمند آسیا مواجه هستیم [۲۲].

دوره‌های مختلف جوامع را می‌توان؛ مانند شکل (۳) تعریف کرد.



شکل (۴). جوامع انسانی و جامعه نسل ۵,۰ "جامعه فوق هوشمند"

دوره‌های مختلف جوامع را می‌توان؛ مانند شکل (۴) تعریف کرد، جایی که جامعه ۱,۰[3] جامعه شکار است که در آن مردم با شکار زنده می‌مانند. جامعه ۲,۰[4] یک جامعه کشاورزی و مبتنی بر کشاورزی است. جامعه ۳,۰[5] با انقلاب صنعتی و تحولات همراه با تولید انبوه مشخص می‌شود. جامعه ۴,۰[6] جامعه‌ای است که در آن زندگی می‌کنیم و به اطلاعات و رایانه‌ها نسبت داده می‌شود. درنهایت، جامعه ۵,۰[7] دوره بعدی خواهد بود [۲۳].

جامعه ۵,۰ بر اساس هوش مصنوعی[8]، فناوری‌های روباتیک، کلان داده، رایانش ابری، سیستم‌های فیزیکی سایبری[9]، اینترنت اشیا، اشیاء هوشمند (ماشین، خانه، لوازم‌خانگی و غیره) ساخته‌شده است. جامعه ۵,۰ باهدف ادغام فضای مجازی با فضای فیزیکی

[1] Foresight Periscope Model.

[2] Society 5.0.
[3] Society 1.0.
[4] Society 2.0.
[5] Society 3.0.
[6] Society 4.0.
[7] Society 5.0.
[8] Artificial Intelligence (AI).
[9] Cyber-physical Systems (CPS).

ساخته‌شده است [۲۴]. ازاین‌رو آینده‌پژوهی و آینده‌نگاری با نگاه بلندمدت به مسیر تحولات فزاینده در حوزه علم‌وفناوری می‌کوشد تا به تدوین راهبردهای اثربخش در این حوزه بپردازد.

۲-۴. پیشینه پژوهش

برابر بررسی‌های انجام‌شده در منابع مطالعاتی و علمی داخلی و خارجی، پژوهشی که به‌طور مستقیم و کامل هم‌راستا با موضوع تحقیق، موجود باشد، یافت نگردید؛ اما موضوعاتی که به‌نوعی در راستای تحقیق بوده و نتایج حاصل از آن‌ها در پیشبرد این پژوهش مؤثر بود در بانک‌های اطلاعاتی داخل و خارج کشور یافت شد که در ادامه نمونه‌هایی ازاین‌دست پژوهش‌ها ارائه می‌گردد:

مهدوی پور در پایان‌نامه کارشناسی ارشد خود با عنوان عوامل مؤثر بر امنیت سایبری ارتش جمهوری اسلامی ایران (مطالعه موردی ستاد ارتش جمهوری اسلامی ایران) که در سال ۱۳۹۹ به انجام رسیده است مطرح می‌کند که عوامل درون‌سازمانی شامل امن سازی تجهیزات، شبکه‌ها، نرم‌افزارهای رصد و پایش رخدادهای سایبری و واکنش به‌موقع به آن‌ها و ارتقاء دانش سایبری کارکنان و عوامل برون‌سازمانی شامل تهدیدهای سایبری انسان‌ساز و طبیعی عوامل مؤثر بر امنیت سایبری در ارتش جمهوری اسلامی ایران را تشکیل می‌دهند [۲۵].

اسماعیلی در رساله دکتری خود که در سال ۱۳۹۹ و در دانشگاه عالی دفاع ملی به انجام رسیده مهم‌ترین ابعاد الگوی پایش تهدیدات سایبری جمهوری اسلامی ایران را پویش، ارزیابی و واکنش در نظر گرفته و پیشنهاد می‌دهد باتوجه‌به تقابل دائمی ج.ا ایران با استکبار جهانی و نظام سلطه، بایستی در ایجاد و ارتقاء شبکه ملی اطلاعات که می‌تواند منجر به افزایش ظرفیت تاب‌آوری و ظرفیت انطباق شود، کوشید [۲۶].

ایجابی و کولیوند در پژوهشی در سال ۱۴۰۱ با عنوان واکاوی تهدیدات امنیتی شبکه‌های رایانه‌ای سازمان‌ها با رویکرد آینده‌پژوهی (مطالعه موردی ستاد فرماندهی نیروی پدافند هوایی آجا) با استفاده از روش چرخ آینده و تلفیق این روش با پنل خبرگی و جلسات ذهن انگیزی در حوزه تهدیدات شبکه ۷۸ تهدید را شناسایی و احصاء نموده‌اند که با بهره‌گیری از روش پنل خبرگان و استفاده از نرم‌افزار آینده‌پژوهی MicMac درنهایت تعداد هفت عامل تهدید زا را در حوزه تهدیدات امنیتی شبکه‌های رایانه‌ای سازمان‌ها شناسایی نموده‌اند [۲۷].

آقایی و همکارانش در پژوهشی در سال ۱۳۹۸ با عنوان ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی با استفاده از فراترکیب و استفاده از ضریب کاپا در قالب مدل مفهومی منطقی، طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی را در ابعاد شش‌گانه تهدیدات، عوامل تهدید، مشخصات تهدید، نگاه از دید نفوذ گر، توصیف سیستم و منابع شناسایی تهدیدات انجام داده‌اند [۲۸].

قربانی و ثقفی در پژوهشی در سال ۱۳۹۸ با عنوان ارائه مدل کلان امنیت اطلاعات فضای سایبر در جمهوری اسلامی ایران که به روش مدل‌سازی معادلات ساختاری حداقل مربعات جزء (PLS) انجام‌شده است مطرح می‌نمایند که به‌منظور صیانت از اطلاعات کشور در فضای سایبر، باید شناخت کاملی از این فضا و تهدیدات آن وجود داشته باشد، پژوهشگران در این پژوهش با استفاده از روش آمیخته مدل نهایی را در ۸ بعد و برای هر بعد ۴ مؤلفه و برای هر مؤلفه ۳ زیر مؤلفه و ۱۳ شاخص ترسیم می‌نمایند [۲۹].

چیفچی[1] در رساله دکتری خود در سال ۲۰۱۷ با عنوان آینده‌نگاری و مدل‌سازی فناوری: آینده‌نگاری امنیت سایبری ترکیه ۲۰۴۰ با استفاده از به‌کارگیری روش‌های آینده‌پژوهی ازجمله دلفی، پنل خبرگی، توفان فکری و سناریو به آینده‌نگاری امنیت سایبری ترکیه تا سال ۲۰۴۰ پرداخته است [۳۰].

رایان و هویتمن[2] در پژوهشی در سال ۲۰۱۸ با عنوان آینده‌نگاری پیشران‌های تهدیدات امنیت سایبری و فناوری‌های تأثیرگذار مطرح می‌نمایند که صنعت امنیت سایبری در سال‌های اخیر به دلیل افزایش تهدیدات سایبری و افزایش فعالیت‌های نفوذ سایبری به‌سرعت ظهور کرده است. ازاین‌رو پژوهش مذکور در پی انجام یک مطالعه آینده‌نگاری نسبتاً متعادل برای استخراج پیشران‌های تهدید مهم و شناسایی فناوری‌های نوظهور است که احتمالاً تأثیر قابل‌توجهی بر قابلیت‌های دفاعی و حمله در امنیت سایبری دارند [۳۱].

پیشینه فعالیت‌های پژوهشی انجام‌شده نشان می‌دهد در سال‌های اخیر فعالیت‌های پژوهشی محدودی دررابطه‌با آینده‌پژوهی، آینده‌نگاری و تهدیدات سایبری به انجام رسیده؛ اما ازآنجاکه آینده‌نگاری فرایندی سیستماتیک و نظام‌مند به شمار می‌آید، می‌تواند با بررسی همه‌جانبه موضوع و درنظرگرفتن صحنه آینده در پرتو عدم قطعیت‌ها و بعضاً شگفتی‌سازی‌ها، تحولات اساسی را به وجود آورد. این امر زمینه‌های کار پژوهشی و اجرایی در این دو حوزه (آینده‌نگاری و سایبر) را نوید می‌دهد.

۳. روش تحقیق

[1] Chifchi.
[2] Raban & Hauptman.

باتوجه‌به اینکه پژوهش حاضر می‌تواند در تصمیم‌گیری‌ها و سیاست‌های امنیت سایبری آجا اثرگذار بوده و ملاک عمل و ارجاع قرار بگیرد، از نوع کاربردی است و باتوجه‌به اینکه هم شامل نظریه‌پردازی و هم ابزارسازی است و این امر هم نیازمند رویکرد کیفی و هم رویکرد کمّی است، لذا رویکرد آمیخته برای این پژوهش مدنظر قرار گرفت.

الگوی اولیه پژوهش با استفاده از مطالعه اسناد و مدارک کتابخانه‌ای استخراج و با انجام مصاحبه در قالب پنل‌های خبرگی با خبرگان و کارشناسان حوزه سایبر که مسلط به مباحث آینده‌پژوهی و آینده‌نگاری بودند، چارچوب اولیه، اجزاء آن، نحوه ارتباط آن‌ها، همچنین اقدامات قابل انجام در هر مرحله تعیین شد. سپس در مرحله بعد با استفاده از نظرات نمونه آماری، اجزاء الگوی مدنظر به‌صورت پرسش‌نامه محقق ساخت مورد تأیید قرار گرفت.

نمونه آماری انتخاب‌شده شامل افرادی مشتمل بر کارشناسان خبره و صاحب‌نظر در موارد از قبیل دانش‌آموختگان رشته سایبر و امنیت رایانه (حداقل مقطع لیسانس) در سطح کل آجا، دانش‌آموختگان تحصیلات تکمیلی رشته آینده‌پژوهی و آینده‌نگاری (دکتری) آجا و وزارت دفاع، کارشناسان سایبری نیروهای چهارگانه آجا و ستاد فرماندهی آجا شامل اداره امنیت سایبری و قرارگاه جنگ‌های نوپدید و اساتید و محققان مرتبط با موضوع پژوهش همانند فارغ‌التحصیلان مقاطع تحصیلات تکمیلی (حداقل فوق‌لیسانس) در رشته‌های مهندسی فناوری اطلاعات، مدیریت فناوری اطلاعات، مدیریت راهبردی و سیاست‌گذاری علم‌وفناوری در سطح ارتش جمهوری اسلامی ایران بوده است. این افراد در حالت حداکثری و با اعمال ضریب حفاظتی، تعداد ۱۴۰ نفر تعیین شد که با استفاده از فرمول کوکران حجم نمونه انتخابی ۱۲۷ نفر انتخاب گردید. از این تعداد هفت نفر خبره مورد مصاحبه قرار گرفت و ۱۲۰ نفر در پاسخ‌دهی به پرسش‌نامه محقق ساخت، پژوهشگر را یاری نمودند.

۴. نتایج و بحث

فرآیند انجام این پژوهش شامل سه بخش رویکرد کیفی، کمی و آمیخته است. در گام کیفی با انجام مطالعات کتابخانه‌ای و بررسی اسناد و مدارک علمی، ۲۵ چارچوب آینده‌نگاری بررسی و اجزاء کلی الگو و مدل آینده‌پژوهانه شناسایی گردید. سپس از طریق انجام مصاحبه با خبرگان و کارشناسان حوزه سایبر که مسلط به مباحث آینده‌پژوهی و آینده‌نگاری نیز بودند، بخش‌های مختلف الگو اصلاح شد و زیر بخش‌های هرکدام از اجزاء مدل شناسایی و استخراج گردید.

۴-۱. رویکرد کیفی:

الگوی اولیه شامل سه بخش اصلی پیش‌آینده‌نگاری، آینده‌نگاری و پسا آینده‌نگاری است. بخش پیش‌آینده‌نگاری شامل چهار زیر بخش مطالعه وضعیت سایبری سازمان‌های دشمن، مطالعه وضعیت سایبری سازمان‌های بالادستی و هم‌تراز، مطالعه وضعیت سایبری سازمان و شناسایی کلان‌روندهای سایبری است. بخش آینده‌نگاری شامل چهار زیر بخش تجزیه‌وتحلیل تهدیدهای سایبری، تفسیر تهدیدهای سایبری، ترسیم وضعیت مطلوب سایبری سازمان و چشم‌انداز سایبری سازمان است و بخش پسا آینده‌نگاری شامل دو زیر بخش تصمیم‌سازی و تصمیم‌گیری و راهبرد نگاری است. هرکدام از زیر بخش‌ها نیز شامل اجزایی است که بامطالعه اسناد و مدارک و مصاحبه نیمه ساختاریافته با خبرگان بعد از انجام سه مرحله فرآیند تحلیل محتوای کیفی بر پایه دسته‌بندی داده‌ها، پردازش داده‌ها و قضاوت داده‌ها به شرح جدول (۲) تعیین شدند.

جدول (۲)، اجزاء اولیه مدل پیشنهادی پژوهش

اجزاء اصلی	زیر بخش‌های اجزاء اصلی
پیش‌آینده‌نگاری	**مطالعه وضعیت سایبری سازمان‌های دشمن**
	تعریف دقیق دشمن و تشخیص دوست از دشمن (A1)؛
	رصد و پایش تجهیزات، تسهیلات، قابلیت‌ها، ساختارها، روال‌ها و فناوری‌های مورداستفاده (A2)؛
	برآورد وضعیت قدرت آفند سایبری دشمن (A3)؛
	دیده‌بانی سایبری در جهت شناسایی فناوری‌های برتر ساز، شرکت‌های پشتیبانی‌کننده و بهره‌برداران تجهیزات (A4)؛
	شناسایی هم‌پیمانان رقبا و دشمنان (A5)؛
	تعیین دامنه دقیق هدف و شناخت منابع سایبری (A6).
	مطالعه وضعیت سایبری سازمان‌های بالادستی و هم‌تراز
	آگاهی از مأموریت‌ها، وظایف محوله، سیاست‌گذاری‌ها و خط‌مشی‌های صادره (B1)؛
	ایجاد تعاملات فی‌مابین و تبادل دانش بین سازمانی (B2)؛
	دسترسی به طرح‌ها و پروژه‌های در دست اقدام (B3)؛
	شناخت تجهیزات، فرایندها، روال‌ها، امکانات زیرساختی (B4)؛
	میزان سرمایه‌گذاری‌ها در حوزه سایبر (B5).
	مطالعه وضعیت سایبری سازمان

اجزاء اصلی	زیر بخش‌های اجزاء اصلی
	بررسی آخرین وضعیت موجود از منابع سایبری، مدیریت دارایی‌ها و سرویس‌ها (C1)؛
	اطلاع از مأموریت‌ها برابر آخرین ابلاغیه‌ها (C2)؛
	شناسایی فرایندها، زیر فرایندها، تجهیزات، ساختارهای سازمانی، اسناد بالادستی (C3)؛
	شناخت سرمایه‌های انسانی، نیروهای دانشی و افراد رخنه‌گر پایه در سازمان (C4).
	شناسایی کلان‌روندهای سایبری
	رصد و پایش شرکت‌های فناوری در زمینه ساخت و تولید محصولات سایبر پایه، فناوری‌های برتر ساز و پایگاه‌های وب محور (D1)؛
	پایش مجامع علمی و اجلاس‌های بین‌المللی برگزارشده (D2)؛
	دیده‌بانی منطقه‌ای در تحولات فناورانه (D3).
آینده‌نگاری	**تجزیه‌وتحلیل تهدیدهای سایبری**
	تجزیه‌وتحلیل رفتاری (E1)؛
	فرآیند تحلیلی اطلاعات تهدید خارجی (E2)؛
	جرم‌شناسی و تعیین چگونگی نفوذ مهاجمان به سیستم‌ها (E3)؛
	تجزیه‌وتحلیل شبکه و قابلیت مشاهده (E4)؛
	ارکستراسیون امنیتی، خودکارسازی و پاسخگویی (E5)؛
	تجزیه‌وتحلیل ترافیک شبکه (E6)؛
	تحلیل نقاط ضعف سخت‌افزاری و نرم‌افزاری (E7).
	تفسیر تهدیدهای سایبری
	انجام نظرسنجی و شروع به مستندسازی خطرات یا تهدیدهای خاص در هر بخش (F1)؛
	شناسایی و تشخیص تهدید (F2)؛
	بررسی جوانب تهدید (F3)؛
	تهیه برنامه مدیریت تفسیر تهدید (F4)؛
	اجرای برنامه مدیریت تفسیر تهدید (F5)؛
	یکنواخت نمودن روال‌ها و دستورالعمل‌ها (F6)؛
	تفسیر وضعیت رقبا (F7)؛
	تفسیر وضعیت ابزارها و وضعیت پلتفرم‌ها (F8)؛
	ترسیم وضعیت مطلوب سایبری سازمان

اجزاء اصلی	زیر بخش‌های اجزاء اصلی
	ایجاد بروز زمینه‌های نوآوری و خلاقیت (G1)؛
	وحدت فرماندهی پدافند سایبری آجا (G2)؛
	هوشمندی در دفاع سایبری (G3)؛
	روزآمدی و آینده‌نگری (G4)؛
	حفظ تداوم کارکرد سامانه‌های سایبری (G5)؛
	حفظ و صیانت از سرمایه‌های سایبری (G6)؛
	پیش‌دستی در شناخت تهدیدها (G7)؛
	ایجاد زیست‌بوم سایبری بومی، امن و پایدار (G8)؛
	برتری راهبردی و عملیاتی در فضای سایبری (G9).
	چشم‌انداز سایبری سازمان
	برخوردار از نظام جامع پدافند سایبری (H1)؛
	دست‌یافته به زیست‌بوم سایبری (H2)؛
	نظام واحد فرماندهی، هدایت، راهبری و کنترل پدافند سایبری (H3)؛
	برخوردار از سرمایه‌های انسانی آموزش‌دیده (H4)؛
	بهره‌مند از زیرساخت‌های حیاتی آسیب‌ناپذیر راهبردی سایبری (H5)؛
	خوداتکا در تولید سامانه‌های پایه پدافند سایبری (H6)؛
	افزایش توان سازمان در تاب‌آوری سایبری (H7)؛
	کسب و حفظ برتری در حوزه فضای سایبری از طریق اشراف اطلاعاتی (H8).
پسا آینده‌نگاری	**تصمیم‌سازی و تصمیم‌گیری**
	انجام وظایف در پردازش داده (I1)؛
	پشتیبانی، تقویت و ایجاد خودکارسازی تصمیم‌گیری (I2)؛
	مطرح نمودن آینده‌های بدیل در جهت دستیابی سازمان به آن (I3)؛
	انجام تغییرات ساختاری و بنیادین در رفتارها و هنجارهای سازمانی (I4)؛
	ظرفیت‌سازی برای بهره‌گیری از تعامل و مشارکت سازمان‌های فعال کشوری (I5)؛
	متناسب‌سازی تجهیزات و فناوری‌ها و فن‌های جنگ سایبری (I6)؛
	تشخیص تصمیم‌های مشروط به محیط‌های محتمل آینده و چگونگی عملکرد آجا در آن محیط‌ها (I7).
	راهبرد نگاری

اجزاء اصلی	زیر بخش‌های اجزاء اصلی
	فهم نیازهای سایبری سازمان در قلمروهای مختلف متناسب با حیطه‌های کاری حال و آینده (J1)؛ ایجاد پویایی در ساختار، تشکیلات و سازمان‌های شغلی در سطوح مختلف متناسب با گسترش تهدیدهای سایبری (J2)؛ همگرایی و هماهنگی دو حوزه سایبر در رزم و رزم سایبری جهت افزایش تاب‌آوری و بازدارندگی سایبری (J3)؛ خلق مدیریت دانش و انتقال تجارب فنی سایبری به نسل‌های آینده (J4)؛ افزایش سواد رسانه‌ای نسبت به فضای سایبری و تهدیدهای آن (J5)؛ تعامل سازنده با بخش‌های مختلف سایبری نیروهای مسلح و بخش‌های خصوصی صاحب‌نام (J6).

۴-۲. رویکرد کمی

در این مرحله با تهیه پرسش‌نامه محقق ساخت بر اساس مؤلفه‌های استخراج‌شده صحت‌سنجی داده‌ها با استفاده ازنظر نمونه آماری ۱۲۰ نفرِ موردسنجش شد. توزیع فراوانی نمونه آماری برحسب مدرک تحصیلی به شرح جدول (۳) است.

جدول (۳)، فراوانی نمونه آماری برحسب مدرک تحصیلی

تحصیلات		فراوانی	درصد فراوانی
داده معتبر	کارشناسی	۳۷	۳۰,۸۳
	کارشناسی ارشد	۶۵	۵۴,۱۷
	دکتری و بالاتر	۱۸	۱۵,۰۰
جمع کل		۱۲۰	۱۰۰

بر اساس نظرات پاسخ‌دهندگان ۶۹,۱۷ درصد از نمونه آماری داری مدرک کارشناسی ارشد و بالاتر هستند که این نسبت نشان می‌دهد که نمونه انتخاب‌شده ازنظر سطح تحصیلات و بنیه علمی برای اظهارنظر درباره متغیرهای احصاء شده دارای صلاحیت لازم بوده که این امر در افزایش روایی پاسخ‌ها مؤثر است. توزیع فراوانی نمونه آماری برحسب سوابق خدمتی به شرح جدول (۴) است.

جدول (۴)، فراوانی جامعه آماری برحسب سوابق خدمتی

سوابق خدمتی		فراوانی	درصد فراوانی
داده معتبر	۱۰ تا ۱۵ سال	۲۰	۱۶,۶۷
	۱۶ تا ۲۰ سال	۶۰	۵۰,۰۰
	بیشتر از ۲۰ سال	۴۰	۳۳,۳۳
جمع کل		۱۲۰	۱۰۰

بر اساس جدول فوق ۸۳,۳۳ درصد از نمونه آماری دارای سنوات خدمتی بالای ۱۵ سال هستند که این امر بالا بودن سنوات خدمتی آن‌ها را نشان داده و معلوم می‌کند که مهارت خوبی برای اظهارنظر در خصوص متغیرهای موردبررسی دارند.

۴-۲-۱. بررسی پایایی سؤالات پرسشنامه

بهترین روش محاسبه اندازه ثبات درونی، استفاده از ضریب آلفای کرون باخ در اندازه‌گیری پایایی یک پرسش‌نامه است. این روش که بر مبنای هماهنگی و سازگاری سؤالات پرسش‌نامه استوار است، از طریق یافتن واریانس هر سؤال و واریانس مجموع سؤالات به دست می‌آید (جدول (۵)).

جدول (۵)، محاسبه پایایی پرسشنامه اجزاء شناسایی‌شده

بُعد	تعداد سؤالات	آلفای کرون باخ
پیش‌آینده‌نگاری	۱۸ سؤال	۰,۹۹۸
آینده‌نگاری	۲۴ سؤال	۰,۹۴۹
پسا آینده‌نگاری	۲۱ سؤال	۰,۹۹۵

ملاک سنجش پایایی ضریب آلفای کرون باخ بالای ۰,۷ یا همان هفتاد درصد است که باتوجه‌به مقدار عددی به‌دست‌آمده برای ۶۲ سؤال پرسشنامه که به‌طور میانگین بالای ۰,۹۴ درصد است، می‌توان اذعان نمود پایایی پرسشنامه بسیار مطلوب است. به‌منظور سنجش نظرات نمونه آماری از طیف لیکرت پنج گزینه‌ای (کاملاً موافقم (۵)، موافقم (۴)، نظری ندارم (۳)، مخالفم (۲) و کاملاً مخالفم (۱)) استفاده شد.

۴-۲-۲. مدل‌سازی ساختاری تفسیری مدل با استفاده از نرم‌افزار PLS

در این بخش به مدل‌سازی معادلات ساختاری با استفاده از روش حداقل مربعات جزئی با استفاده از نرم‌افزار PLS پرداخته‌شده و برازش مدل، اندازه‌گیری و موردبررسی قرار گرفت. سپس با بررسی ضرایب معناداری مربوط به هر یک از گویه‌ها، نسبت به تأیید و یا رد صحت روابط اجزاء تشکیل‌دهنده مدل اقدام شد. روش مدل‌سازی معادلات ساختاری با رویکرد حداقل مربعات جزئی توسط ولد[1] در سال ۱۹۷۴ ابداع و در ادامه نسخه پیشرفته‌تر این روش توسط لمولر[2] در سال ۱۹۸۹ ارائه شد. ازجمله دلایل استفاده از رویکرد حداقل مربعات جزئی می‌توان به حجم نمونه کم، داده‌های غیر نرمال، مدل‌های اندازه‌گیری از نوع سازنده، قدرت پیش‌بینی مناسب، پیچیدگی مدل، تعداد زیاد

[1] Weld.
[2] Lemoler.

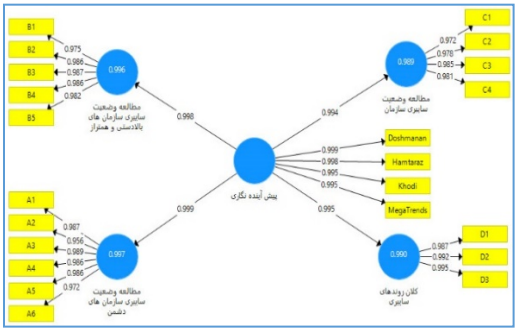
سازه‌ها و یا شاخص‌ها، تحقیق اکتشافی، توسعه نظریه، استفاده از متغیرهای طبقه‌بندی‌شده و بررسی همگرایی اشاره نمود. این روش یک ساختار علی ویژه بین مجموعه‌ای از متغیرهای پنهان و متغیرهای مشاهده‌پذیر است. با استفاده از روش مدل یابی معادلات ساختاری روابط بین متغیرهای پنهان با یکدیگر و نیز گویه‌های سنجش هر متغیر پنهان با متغیر مربوط قابل‌بررسی است [۳۲].

در این نرم‌افزار برای استفاده از مدل و کسب تأییدیه‌های لازم از آن بایستی مواردی از قبیل سنجش بارهای عاملی، ضریب معناداری، ضریب R^2، معیار Q^2 و برازش کلی مدل را بررسی نمود.

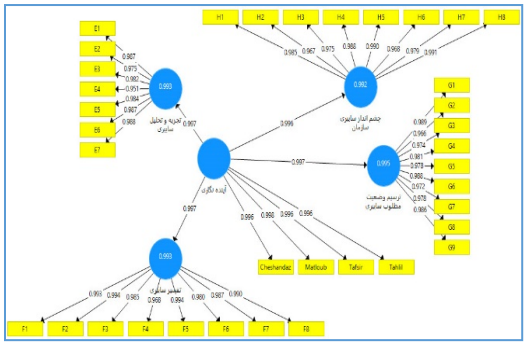
۴-۲-۲-۱. سنجش بارهای عاملی

بارهای عاملی از طریق محاسبه مقدار همبستگی شاخص‌های یک سازه با آن سازه محاسبه می‌شوند که اگر این مقدار برابر و یا بیشتر از ۰/۴ شود، مؤید این مطلب است که واریانس بین سازه و شاخص‌های آن از مقدار واریانس خطای اندازه‌گیری آن سازه بیشتر بوده و پایایی در مورد آن مدل قابل‌قبول است. البته برخی عدد ۰/۵ را به‌عنوان مقدار ملاک بارهای عاملی ذکر نموده‌اند. نکته مهم در اینجا این است که اگر محقق پس از محاسبه بارهای عاملی بین سازه و شاخص‌های آن با مقادیری کمتر از ۰/۴ مواجه شود، باید آن شاخص‌ها (سؤالات پرسش‌نامه) را اصلاح نموده و یا از پژوهش خود حذف نماید. آنچه با اجرای این روش می‌توان انجام داد، بررسی الگوی روابط بین چندین متغیر است، درحالی‌که رابطه احتمالی علی میان آن‌ها تأیید و رد نمی‌شود. روشن است که اگر دو یا چند فرضیه علی از پیش تعیین‌شده را بتوان در یک نمودار مسیر درونداد نمایش داد، اندازه‌های نسبی ضرایب مسیر در نمودار برون داد ممکن است بیان کند که کدام‌یک از آن‌ها از طریق داده‌ها بهتر پشتیبانی می‌شود. روش تحلیل مسیر به این دلیل محبوبیت یافته است که برآورد نقش نسبی متغیرها را در یک شبکه علی امکان‌پذیر و پژوهشگر را ناگزیر می‌سازد ساختار علی زیربنای متغیرها را آشکار نماید. اما دارای این محدودیت است که نمی‌تواند ساختار علی زیربنایی را تأیید کند؛ یعنی بیان می‌کند که نقش نسبی متغیرها بر یکدیگر چیست، اما ساختار علی موردنظر را محقق نمی‌سازد. چون علت باید قبل از معلول باشد، ترتیب زمانی وقوع متغیرها در تهیه نمودار مسیر باید محقق باشد [۳۳].

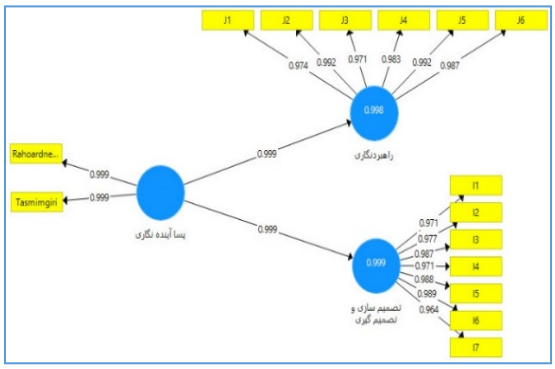
در این تحقیق همان‌گونه که از شکل‌های (۶) تا (۸) مشخص است، تمامی سؤالات دارای ضرایب بارهای عاملی بیشتر از معیار هستند که نشان از مناسب بودن این معیارها و اجزاء دارد. تحلیل مسیر می‌تواند فرضیه‌های علی را ارزشیابی کند و در برخی از موقعیت‌ها نیز دو یا چند فرضیه علی را بیازماید. اما هرگز نمی‌تواند جهت علیت را محقق سازد. تحلیل مسیر زمانی مفید است که فرضیه‌های روشنی برای آزمون، یا تعداد کمی فرضیه که همه آن‌ها را بتوان در یک نمودار واحد نشان داد، در باشد. تحلیل مسیر در مرحله اکتشافی کاربرد اندکی دارد. این روش را نمی‌توانیم در موقعیت‌هایی که حلقه بازخورد در فرضیه‌ها گنجانده‌شده است، به کار ببریم. باتوجه‌به آنچه مطرح شد و همچنین بر اساس بارهای عاملی که تماماً بیشتر از ۰/۴ و حتی بیشتر از ۰/۵ هستند، می‌توان گفت که بخش‌های سه‌گانه الگوی پیشنهادی از پایایی مطلوبی برخوردار است.



شکل (۶)، ضرایب بار عاملی بخش پیش‌آینده‌نگاری



شکل (۷)، ضرایب بار عاملی بخش آینده‌نگاری



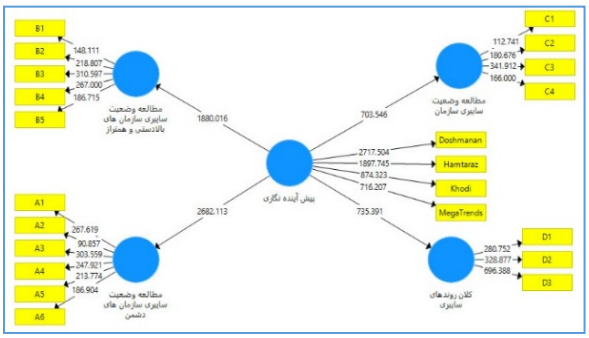
شکل (۸)، ضرایب بار عاملی بخش پسا آینده‌نگاری

۴-۲-۵-۲. ضریب معناداری

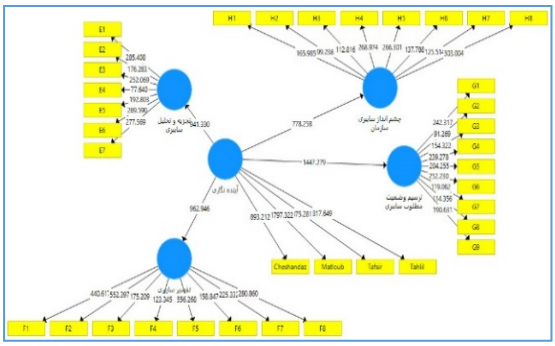
برای اینکه ضرایب معناداری برای یک مدل قابل‌قبول باشد بایستی اعداد محاسبه‌شده از ۱,۹۶ حداقل آماره آزمون بیشتر

باشد [۳۴]. ازاین‌رو با استفاده از محاسبه آماره تـی در نـرم‌افـزار برای بخش‌های مختلف چارچوب این ضرایب بررسی می‌شود.

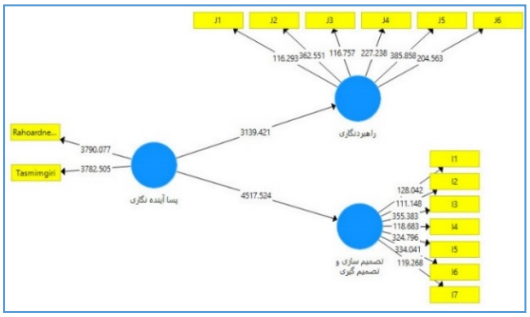
باتوجه‌به به اعداد به‌دست‌آمده که تماماً بیشتر از ۱,۹۶ است، مشخص شد که بخش‌های سه‌گانه مدل پیشنهادی از ضریب معناداری بسیار مطلوبی برخوردار است که این موضوع در شکل‌های (۹) تا (۱۱) قابل‌مشاهده است.



شکل (۹)، محاسبه ضریب معناداری بخش پیش‌آینده‌نگاری



شکل (۱۰)، محاسبه ضریب معناداری بخش آینده‌نگاری



شکل (۱۱)، محاسبه ضریب معناداری بخش پسا آینده‌نگاری

۴-۲-۵-۳. ضریب R^2

ضریب R^2 یکی دیگر از معیارهایی است که برای بررسی برازش مدل ساختاری در یک پژوهش موردبررسی قرار می‌گیرد. این معیار برای متصل کردن بخش اندازه‌گیری و بخش سـاختاری مدل‌سازی معادلات ساختاری به کار می‌رود. R^2 معیاری است که نشان از تأثیر یک جزء مدل بر یک جزء دیگر مدل دارد و مقدار آن تنها برای سازه‌های درون‌زا مدل محاسبه می‌گردد و در مورد سازه‌های برون‌زا، مقدار این معیار صفر است. سه مقدار ۰,۱۹، ۰,۳۳ و ۰,۶۷ به‌عنوان مقدار ملاک برای مقادیر ضعیف، متوسط و قوی R^2 در نظر گرفته می‌شود [۳۵]. میزان محاسبه این ضریب برای اجزاء مدل مدنظر پژوهش به‌صورت جدول (۶) است.

جدول (۶)، ضریب R^2 اجزاء شکل‌دهنده الگو

بخش	جزء شکل‌دهنده الگو	ضریب R^2
پیش‌آینده‌نگاری	مطالعه وضعیت سایبری سـازمان‌هـای دشمن	۰,۹۹۷
	مطالعه وضعیت سایبری سـازمان‌هـای بالادستی	۰,۹۹۶
	مطالعه وضعیت سایبری سازمان	۰,۹۸۹
	کلاون روندهای سایبری	۰,۹۹۰
آینده‌نگاری	تجزیه‌وتحلیل سایبری	۰,۹۹۳
	تفسیر سایبری	۰,۹۳۳
	ترسیم وضعیت مطلوب سایبری	۰,۹۹۵
	چشم‌انداز سایبری سازمان	۰,۹۹۲
پسا آینده‌نگاری	تصمیم‌سازی و تصمیم‌گیری	۰,۹۹۹
	راهبرد نگاری	۰,۹۹۸

باتوجه‌به ضرایب به‌دست‌آمده معلوم می‌شود که مقدار ملاک R^2 در حالت بسیار قوی ارتباط اجزاء را تأیید می‌نماید.

۴-۲-۵-۴. معیار Q^2

معیار Q^2 قدرت پیش‌بینی یک مدل را مشخص می‌سازد. مدل‌هایی که دارای برازش بخش سـاختاری قابل‌قبول هسـتند، باید قابلیت پیش‌بینی شاخص‌های مربوط به سازه‌های درون‌زای مدل را داشته باشند. بدین معنی که اگر در یک مدل، روابط بین سازه‌ها به‌درستی تعریف‌شده باشند، سازه‌ها قادر خواهند بود تا تأثیر کافی بر شاخص‌های یکدیگر گذاشته و از این راه، درستی مدل تأیید شود. مقدار این معیار تنها برای سازه‌های درون‌زای مدل که شاخص‌های آن‌ها از نوع انعکاسی است، محاسبه می‌گردد. درصورتی‌که مقدار Q^2 در مورد یک سازه درون‌زا سه مقدار ۰,۰۲، ۰,۱۵ و ۰,۳۵ را کسب نماید، به ترتیب نشان از قدرت پیش‌بینی

ضعیف، متوسط و قوی سازه یا سازه‌های برون‌زای مربوط به آن را دارد [۳۶]. مقادیر مربوط به معیار Q^2 سازه‌های درون‌زای در مدل پیشنهادی در جدول (۷) درج‌شده است.

جدول (۷)، ضریب Q^2 اجزاء شکل‌دهنده مدل

بخش	جزء شکل‌دهنده الگو	ضریب Q^2
پیش‌آینده‌نگاری	مطالعه وضعیت سایبری سازمان‌های دشمن	۰,۹۵۱
	مطالعه وضعیت سایبری سازمان‌های بالادستی	۰,۹۵۸
	مطالعه وضعیت سایبری سازمان	۰,۹۴۱
	کلان‌روندهای سایبری	۰,۹۶۸
آینده‌نگاری	تجزیه‌وتحلیل سایبری	۰,۹۴۷
	تفسیر سایبری	۰,۹۶۰
	ترسیم وضعیت مطلوب سایبری	۰,۹۴۷
	چشم‌انداز سایبری سازمان	۰,۹۴۸
پسا آینده‌نگاری	تصمیم‌سازی و تصمیم‌گیری	۰,۹۴۷
	راهبرد نگاری	۰,۹۴۵

باتوجه‌به داده‌های جدول فوق قدرت پیش‌بینی مدل مطلوب برآورد می‌گردد.

۴-۲-۵-۵. بررسی برازش مدل کلی

شاخص نکویی برازش[1]، به‌عنوان یک معیار کلی از تناسب مدل برای مدل معادلات ساختاری حداقل مربعات جزئی توسعه‌یافته است. این شاخص، مجذور ضرب دو مقدار متوسط مقادیر اشتراکی و متوسط ضرایب تعیین است. بااین‌حال، ازآنجایی‌که شاخص نکویی برازش نمی‌تواند به‌طور قابل‌اعتمادی مدل‌های معتبر را از نامعتبر تشخیص دهد و ازآنجایی‌که کاربرد آن به تنظیمات مدل خاصی محدود می‌شود، محققان باید در استفاده از آن به‌عنوان معیار مناسب خودداری کنند. این شاخص مربوط به برازش بخش کلی مدل‌های معادلات ساختاری است. بدین معنی که توسط این معیار محقق می‌تواند پس از بررسی برازش بخش اندازه‌گیری و بخش ساختاری مدل کلی پژوهش خود، برازش بخش کلی را نیز کنترل نماید. شاخص نکویی برازش عددی بین صفر و یک به دست می‌آید. سه مقدار برای ارزیابی این شاخص در نظر گرفته‌اند:

- ضعیف: اگر بین ۰/۱ تا ۰/۲۵ باشد.
- متوسط اگر بین ۰/۲۵ تا ۰/۳۶ باشد.
- قوی: اگر از ۰/۳۶ بیشتر باشد.

هر چه مقدار شاخص به عدد یک نزدیک باشد، بیانگر مناسب‌تر بودن مدل است. برازش بخش کلی را نیز کنترل نماید. فرمول شاخص نکویی برازش در زیر آمده است.

$$GOF = \sqrt{\overline{R^2} * \overline{Communality}}$$

Communality (مقادیر اشتراکی) = این مقدار از میانگین مجذور بارهای عاملی هر متغیر به دست می‌آید.

√ Communality = از میانگین مقادیر اشتراکی هر متغیر درون‌زای مدل به دست می‌آید.

R^2 = میانگین مقادیر متغیرهای درون‌زای مدل است. شاخص نکویی برازش عددی بین صفر و یک به دست می‌آید [۳۷].

Communality = 0.8068

R^2 = 0.9882

GOF = √0.8068*0.9882 = 0.8020

باتوجه‌به عدد به‌دست‌آمده برازش کلی مدل با دقت بالایی مورد تأیید قرار می‌گیرد.

۵. نتیجه‌گیری

هدف این پژوهش شناسایی مؤلفه‌های تشکیل‌دهنده الگوی مواجه با تهدیدهای سایبری در ارتش جمهوری اسلامی ایران بود. امروزه رویکرد اقدامات نسبت به تهدیدها در فضای سایبری از حالت فعالانه به رویکرد کنش‌گرایانه به‌منظور ازبین‌بردن امکان حمله قریب‌الوقوع طرف دیگر، تغییریافته و سازمان‌ها، نهادها و حتی افراد شخصی به‌جای اینکه منتظر وقوع یک رویداد بنشینند از قبل اقداماتی در جهت کاهش آسیب و حتی برطرف نمودن آن انجام می‌دهند. باتوجه‌به آنچه گذشت و نظر به اهمیت وجودی تهدیدات روزافزون و سرشار از تحولات فزاینده فضای سایبر، الگوی موردنظر تدوین با رویکرد آینده‌پژوهانه گردید.

پژوهش حاضر با این رویکرد در سه بخش پیش‌آینده‌نگاری، آینده‌نگاری و پسا آینده‌نگاری انجام شد که بخش پیش‌آینده‌نگاری شامل چهار زیر بخش و ۱۸ مؤلفه، بخش آینده‌نگاری شامل چهار زیر بخش و ۳۲ مؤلفه و درنهایت بخش

[1] Goodness of Fit.

پسا آینده‌نگاری شامل دو زیر بخش و ۱۳ مؤلفه شد. بررسی برازش کلی مدل در نرم‌افزار PLS و با کمک داده‌های استخراجی از نرم‌افزار SPSS حاصل گردد.. باتوجه‌به سؤالات فرعی پژوهش، به دو سؤال زیر در این بخش پاسخ داده می‌شود که به‌نوعی اهداف فرعی پژوهش نیز هستند. زیر مؤلفه‌های الگوی تشکیل‌دهنده مواجه با تهدیدهای سایبری در آجا با رویکرد آینده‌پژوهی کدام‌اند؟

ارتباط بین زیر مؤلفه‌های مختلف تشکیل‌دهنده الگوی مواجه با تهدیدهای سایبری در آجا با رویکرد آینده‌پژوهی چگونه است؟ نتایج حاصل از برازش کلی مدل نشان داد که اجزاء احصاء شده ارتباط بسیار خوبی با مدل و الگوی استخراجی دارد.

پیشنهادها

- باتوجه‌به مؤلفه‌های شناسایی‌شده برای مدل پیشنهادی پژوهش حاضر پیشنهاد می‌گردد:
- معاونت فاوا آجا و نیروهای چهارگانه آن با همکاری قرارگاه جنگ‌های نوپدید آجا، پایش و رصد فناوری‌های نوین و تهدیدهایی که از جانب آن‌ها متوجه بدنه سایبری آجا (تجهیزاتی و سرمایه انسانی) می‌گردد، شناسایی و احصاء نموده و جهت برنامه‌ریزی‌های آینده در دست اقدام قرار گیرند.
- در راستای تعاملات فی‌مابین و برقراری بستری به‌منظور تبادل دانش بین سازمانی، معاونت فاوا آجا و قرارگاه جنگ‌های نوپدید ارتباط کارآمدی با سازمان پدافند غیرعامل کشور و فرماندهی مرکز عملیات سایبری سپاه پاسداران انقلاب اسلامی ایران برقرار تا از این طریق در زمان‌های موردنیاز همکاری و تعامل هم‌افزا صورت پذیرد.
- با رویکرد اثربخشی سازمانی و به‌عنوان یک اقدام راهبردی مدیریت منابع دقیق در کلیه یگان‌های تابعه آجا از طریق فرماندهی عملیات سایبری آجا محقق گردد.
- با نگاه بلندمدت با تخصیص بودجه مازاد، زمینه آموزش سرمایه‌های انسانی حوزه سایبر آجا فراهم گردد.
- ازآنجاکه در مجامع و اجلاس‌های علمی، آخرین رصد تحولات فناورانه صورت می‌پذیرد، با محوریت معاونت فاوا آجا و قرارگاه جنگ‌های نوپدید مقالات و پژوهش‌های ارائه‌شده در این همایش‌ها موردنقد و بررسی و واکاوی قرار گیرند.
- با رویکرد تحلیلی به ابعاد تشکیل‌دهنده موضوع، تجزیه‌وتحلیل دائم ترافیک شبکه در دستور کار معاونت‌ها فاوا و فرماندهی‌های سایبری آجا قرار گیرد. باتوجه‌به اینکه این موضوع امروزه به‌عنوان یکی از قوی‌ترین و مؤثرترین راهکارها در جهت شناسایی تهدیدهای سایبری موردتوجه قرار می‌گیرد.
- با رویکرد تحلیلی، هماهنگ‌سازی امنیتی با مدیریت و کنترل یک رابط واحد به‌طور مؤثر به مشاهده، درک و تصمیم‌گیری رویدادهای امنیت سایبری بپردازد.
- معاونت فاوای آجا با همکاری سایر بخش‌های مرتبط ازجمله معاونت اطلاعات آجا، قرارگاه جنگ‌های نوپدید، مرکز مطالعات راهبردی آجا و دافوس آجا، نسبت به رصد مستمر فناوری‌های نوین سایبری و تجزیه‌وتحلیل آن اقدام نماید تا به آگاهی وضعیتی مطلوب و به‌موقع برای مقابله با رخدادهای امنیت سایبری دست یابد.

همچنین باتوجه‌به نتایج پژوهش حاضر و محدودیت پژوهشگر در خصوص پرداختن به همه جوانب موضوع پژوهش و آشکارسازی آینده تهدیدها و تبیین فناوری‌های مورد لزوم در جهت مقابله با این تهدیدهای نوظهور پژوهش در خصوص موضوعات زیر که تقریباً در راستای اهداف این پژوهش می‌باشند، توصیه می‌شود:

- تدوین سناریوهای فراروی ارتش جمهوری اسلامی ایران به‌منظور مقابله با تهدیدهای سایبری در افق میان‌مدت؛
- ضرورت سنجی گذر از پدافند سایبری به آفند سایبری در مواجه با تهدیدهای سایبری؛
- تدوین ره نگاشت سایبری ارتش جمهوری اسلامی ایران در مقابله با تهدیدهای سایبری؛
- طراحی چارچوب دفاع سایبری با رویکرد آمادگی مقابله باکلان روندهای سایبری.
- طراحی مدل ارزیابی قدرت سایبری ارتش جمهوری اسلامی در مواجه با تهدیدهای هوشمند.

۶. قدردانی

پژوهشگران در پایان‌بر خود واجب می‌دانند از کلیه اساتید، خبرگان و صاحب‌نظرانی که با صرف وقت ارزشمند خویش در جهت غنای این اثر گام برداشتند تقدیر و تشکر به عمل‌آورند.

۷. مراجع

[۱] Dadashtabar Ahmadi, K., & mahmoudbabouei, M., "The Presentation of an Active Cyber Defense Model for Application in Cyber Deception Technology," *Electronic and Cyber Defense,* vol. 9(4), no. Dor: 20.1001.1.23224347.1400.9.4.10.3, pp. 125-140, [In Persian], 2022.

[2] Aghaee, M., Moeini, A., Arabsorkhi, A., Mohammadian, A., & Zareei, A. A., "Providing a rational conceptual model for classifying critical infrastructure cyber threats," National Security, vol. 9(32)، no. Dor: 20.1001.1.33292538.1398.9.32.9.5, pp. 201-231, [In Persian], 2019.

[3] Enisa, "Foresight Challenges (A Study to enable foresight on emerging and future cybersecurity challenges), The European Union Agency for Cybersecurity, https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary.," Enisa, Londen, 2021.

[4] M. o. T. a. Infrastructure, "National Cyber Security Strategy171 2016-2019. Ankara. Retrieved from http://www.ubak.gov.tr/.," Retrieved from http://www.ubak.gov.tr/., Ankara, 2019.

[5] Jalali Farahani, G. R., & Beikpoori, M. S. , "Development of the Concept of Deterrence Theory in the Country's Cyberspace Based on Upstream Documents and Available Approaches," Electronic and Cyber Defense, vol. 8(4), no. DOR:20.1001.1.23224347.1399.8.4.14.0, pp. 161-173, [In Persian], 2020.

[6] L. Zaidi, "Worldbuilding in science fiction, foresight and design," Journal of Futures Studies, vol. 23(4), no. DOI:10.6531/JFS.201906_23(4).0003, pp. Pp 15-26, 2019.

[7] G. V. &. P. N. D. Gorelova, "Scientific foresight and cognitive modeling of socio-economic systems," IFAC-PapersOnLine, vol. 51(30), no. doi.org/10.1016/j.ifacol.2018.11.264, pp. Pp145-149, 2018.

[8] Saritas, O., Burmaoglu, S., & Ozdemir, D., "The evolution of Foresight: What evidence is there in scientific publications? ",Futures, vol. 137, no. doi.org/10.1016/j.futures.2022.102916, 2022.

[9] Koulivand, K., & Ghorbanzadeh Savar, G. , " Futuristic analysis of the decline of American power in the geometry of the new world order by the method of casual layered analysis," Futures Studies Of The Islamic Revolution, vol. 4(3), pp. 50-78, [In Persian], 2023.

[10] Barazideh, M., taghvaeeyazdi, M., & Niazazari, K., "Designing a foresight model of electronic governance with organizational transparency of Bank Saderat managers of Tehran province.," Journal of value creating in Business Management, vol. 3(4), no. doi: 10.22034/jvcbm.2023.417577.1197, pp. 131-154, [In Persian], 1402.

[11] Shirvani Naghani, M., Uosefi, A., Ijabi, E., & Bayat, R., "Identifying and Prioritizing Key Success Factors in the Science and Technology Foresight in Iran.," Futures Studies Of The Islamic Revolution, vol. 4(2), pp. 11-40, [In Persian], 2023.

[12] S. Saxena, "National open data frames across Japan, The Netherlands and Saudi Arabia: role of culture," foresight, vol. 20(1), no. doi.org/10.1108/FS-07-2017-0038, pp. Pp123-134, 2018.

[13] Pant, P., Gupta, V. B., Khanna, A., & Saxena, N., "Technology foresight study on assistive technology for locomotor disability," Technology and Disability, vol. 29(4), no. DOI: 10.3233/TAD-170180, pp. Pp163-171, 2018.

[14] Cambridge, "Framework. Retrieved October 18, 2018, from https://dictionary.cambridge.org/dictionary/english/framework," Cambridge Dictionary., 2018.

[15] Oliveira, A., Calili, R., Almeida, M. F., & Sousa, M., "A systemic and contextual framework to define a country's 2030 agenda from a foresight perspective ", Sustainability, vol. 11(22), no. doi.org/10.3390/su11226360, pp. Pp 60-63, 2019.

[16] Hines, A., & Bishop, P. C. , "Framework foresight: Exploring futures the Houston way," Futures, vol. 51, p. Pages 31–49, 2013.

[17] "Minghui, Z., Lingling, Z., Libin, Z., & Feng, W. (2018). Research on technology foresight method based on intelligent convergence in open network environment. In Computational Science–ICCS 2018: 18th International Conference, Wuxi, China, June 11-13, 2018," in 18th International Conference, Wuxi, China, June 11-13, , Proceedings, Part II 18 (Pp. 737-747). , Wuxi, China,, 2018.

[18] Nagimov, A. R., Akhmetshin, E. M., Slanov, V. P., Shpakova, R. N., Solomonov, M. P., & Ilyaschenko, D. P., "Foresight technologies in the formation of a sustainable regional development strategy.," 2018.

[19] Çifci, H., & ÇAKIR, S., "Cybersecurity Technology Foresight: 2040 Scenarios for Turkey. ", Journal of Advanced Research in Natural and Applied Sciences, vol. 9(2), no. doi.org/10.28979/jarnas.1194845, pp. 331-344., 2023.

[20] Yüksel, N., & Çifci, H., "A new model for technology foresight: Foresight periscope model (FPM).," in In 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), 2017.

[21] Vargas-Lama, F., & Osorio-Vera, F. J., "The Territorial Foresight for the construction of shared visions and mechanisms to minimize social conflicts: The case of Latin America," Futures, vol. 123, no. 102625, 2020.

[22] Nastiti, F. E., & Ni'mal'Abdu, A. R. , "Kesiapan pendidikan Indonesia menghadapi era society 5.0. ",Jurnal Kajian Teknologi Pendidikan, vol. 5(1), pp. 61-66, 2020.

[23] Keidanren, "Toward realization of the new economy and society. Policy & Action. Retrieved from http://www.keidanren.or.jp/en/policy/2016/029_outline.pdf ," 2016.

[24] S. Akaike, "Foresight and evidence based policy making in Japan," The 2nd Asian Innovation Forum (AIF), p. Pages 1–35, 2016.

[25] M. Mahdavipour, "Factors affecting the cyber security of the Islamic Republic of Iran Army (a case study of the Islamic Republic of Iran Army Headquarters)," Command University and Army Headquarters, Tehran, 1399.

[26] A. Esmaeili, "Designing a conceptual model for monitoring cyber threats in the Islamic Republic of Iran, Ph.D. Thesis," Supreme National Defense Univ, Tehran, 2021.

[27] Ejabi, E., & Koulivand, K., "Analysis of security threats on the computer networks of organizations with regard to futures studies (Case Study the Air Defense Headquarter of I.R.I.A).," Defensive Future Studies, vol. 8(28), no. doi: 10.22034/dfsr.2022.55, pp. 7-31, [In Persian], 2023.

[28] Aghaei, M. Moini, A. Arab Sorkhi, A. Mohammadian, A., and Zarei, A.A., "Providing a logical

conceptual model for the classification of critical infrastructure cyber threats," National Security,, vol. 9(32), no. DOR: 20.1001.1.33292538.1398.9.32.9.5, pp. 201-231, 2018.

[29] Ghorbani, V., & Saghafi, K., "Designing a Conceptual Model for the Information Security of the Islamic Republic of Iran's Cyberspace," National Security, vol. 9(33), no. DOR: 20.1001.1.33292538.1398.9.33.12.0, pp. 315-353, [In Persian], 2019.

[30] H. Çifci, "Technology Foresight and Modeling: CyberSecurity Forecasting Türkiye 2040," Ph.D. Thesis," Turkey National university, Turkey, 2023.

[31] Raban, Y., & Hauptman, A., , "Foresight of cyber security threat drivers and affecting technologies," foresight,, vol. 20(4), no. doi.org/10.1108/FS-02-2018-0020, pp. 353-363, 2018.

[32] Becker, J. M., Cheah, J. H., Gholamzade, R., Ringle, C. M., & Sarstedt, M., "PLS-SEM's most wanted guidance ",International Journal of Contemporary Hospitality Management, vol. 35(1), no. doi.org/10.1108/IJCHM-04-2022-0474, pp. 321-346, 2023.

[33] Memon, M. A., Ramayah, T., Cheah, J. H., Ting, H., Chuah, F., & Cham, T. H., "PLS-SEM statistical programs: a review. ",Journal of Applied Structural Equation Modeling, vol. 5(1), no. DOI: 10.47263/JASEM.5(1)06, pp. 1-14, 2021.

[34] Becker, J. M., Cheah, J. H., Gholamzade, R., Ringle, C. M., & Sarstedt, M. , "PLS-SEM's most wanted guidance. , ",International Journal of Contemporary Hospitality Management, vol. 35(1), pp. 321-346, 2023.

[35] J. T. Amora, "Convergent validity assessment in PLS-SEM: A loadings-driven approach. ",Data Analysis Perspectives Journal, vol. 2(3), pp. 1-6, 2021.

[36] Hubona, G., & Belkhamza, Z., "Testing a moderated mediation in PLS-SEM: A full latent growth approach. ",Data Analysis Perspectives Journal, vol. 2(4), pp. 1-5, 2021.

[37] Legate, A. E., Hair Jr, J. F., Chretien, J. L., & Risher, J. J., "PLS-SEM: Prediction-oriented solutions for HRD researchers.," Human Resource Development Quarterly, vol. 34(1), pp. 91-109, 2023.