فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال ششم، شماره چهار، زمستان ۱۴۰۱

طراحی چارچوب آینده‌نگاری رویارویی پیش فعالانه ارتش جمهوری اسلامی ایران با تهدیدهای سایبری[۱]

خلیل کولیوند[۲]، ابراهیم ایجابی[۲]، نیما فرزام نیا[۳]*

تاریخ دریافت: ۱۴۰۱/۰۸/۲۸ **تاریخ پذیرش: ۱۴۰۱/۱۲/۲۵**

چکیده

تهدیدهای سایبری حملاتی در مقابل یک سازمان هستند که ممکن است برای دستیابی به اهداف مختلفی مورد استفاده قرار بگیرند. یک مهاجم سایبری ممکن است سعی کند که اطلاعات حساس یک سازمان را به سرقت ببرد، توانایی آن سازمان را در فراهم کردن خدمات دچار اختلال کند یا اقدامات دیگری انجام دهد که به نوعی به زیرساخت‌های امنیتی و شبکه‌ای سازمان آسیب می‌رساند. از این رو پژوهش حاضر با هدف طراحی چارچوبی به‌منظور رویارویی پیش فعالانه ارتش جمهوری اسلامی ایران با تهدیدهای سایبری به انجام رسیده است. نوع پژوهش کاربردی است که به صورت آمیخته (کمی و کیفی) انجام گردیده است. به منظور شناسایی ساختار اولیه چارچوب با استفاده از منابع مطالعاتی و اسناد و مدارک کتابخانه‌ای، چارچوب اولیه استخراج و با انجام مصاحبه با خبرگان حوزه سایبر و آینده‌پژوهی ابعاد، مؤلفه‌ها و گویه‌های کلیدی چارچوب شناسایی گردید. سپس با تهیه پرسشنامه محقق ساخت و به کمک جامعه نمونه ۱۲۰ نفره، موارد احصاء شده مورد سنجش قرار گرفتند. در مرحله بعد با استفاده از نرم‌افزار **SPSS** تجزیه و تحلیل توصیفی و استنباطی صورت پذیرفت و به‌منظور مدل‌سازی با استفاده از نرم‌افزار مدل‌سازی معادلات ساختاری با حداقل مربعات جزئی **PLS** برازش چارچوب بررسی و مورد تایید قرار گرفت. در نهایت چارچوب پیشنهادی با تلخیص گویه‌های هر زیربخش با استفاده از نرم‌افزار **Edraw Max** ترسیم شد.

واژگان کلیدی: چارچوب آینده‌نگاری، رویارویی پیش فعالانه، ارتش جمهوری اسلامی ایران، تهدیدهای سایبری.

---

۱ - این مقاله مستخرجه از پایان‌نامه کارشناسی ارشد با موضوع فوق می‌باشد که در دانشکده علوم اجتماعی دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران به تصویب رسیده است.

۲- نویسنده مسئول، دانشجوی کارشناسی ارشد آینده‌پژوهی دفاعی، دانشکده علوم اجتماعی، دانشگاه فرماندهی و ستاد آجا، تهران. ایران. رایانامه: K.Koulivand@casu.ac.ir

۲- استادیار آینده‌پژوهی دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران. رایانامه: e.ejabi@casu.ac.ir

۳- استادیار رایانه دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران. رایانامه: nf@casu.ac.ir

۱. مقدمه

پیچیدگی سامانه‌ها و شبکه‌های مبتنی بر فناوری اطلاعات، چالش‌های امنیتی و سایبری فراوانی را برای سازمان‌ها به همراه دارد. برای مثال اقدام‌های تهدیدآفرین بازیگران قوی و ضعیف در فضای سایبر اعم از دولت‌ها، گروه‌های سازمان‌یافته، گروهک‌های تروریستی و حتی افراد عادی در قالب اقداماتی مانند جنگ سایبری[1]، جرائم سایبری[2]، تروریسم سایبری[3]، جاسوسی سایبری[4] و دیگر انواع آن هر روزه تهدیدهای جدیدی را متوجه زیرساخت‌های سازمان‌ها می‌کند که از اهمیت خاصی برخوردار است. تشخیص این تهدیدات بالقوه، پیامدها و چالش‌های امنیتی آن‌ها در محیط پیچیده و سرشار از عدم قطعیت آینده بر حساسیت کار می‌افزاید [1].

بر این اساس، ارتقاء پایداری عملیاتی و مصون‌سازی زیرساخت‌های حیاتی سازمان‌ها در مقابله با تهدیدهای سایبری نمود ویژه‌ای خواهد یافت. ضمن اینکه اصول نوین حاکم بر فضای سایبر، نهادها و ساختارها را ملزم به شناخت این فضا و استفاده بجا از دانش و ابزارهای به‌روز می‌نماید [2].

یکی از مباحث علمی مرتبط با آینده که بر اساس تعریف آژانس امنیت سایبری اروپا[5] در حوزه تهدیدهای سایبری دارای جایگاه ویژه‌ای برخوردار گردیده، مبحث آینده‌نگاری است. در حال حاضر فناوری‌های مدرن امنیت رایانه برای محافظت از کاربران و زیرساخت‌های حیاتی از مجرمان سایبری مفید هستند، اما آینده‌نگاری سایبری موضوعی برای جلوتر بودن از مجرمان و تهدیدآفرینان سایبری در فضای سرشار از شگفتی آینده به‌شمار می‌آید [3].

در حوزه امنیت سایبری برنامه‌های راهبردی متنوعی می‌توان تنظیم نمود. یکی از برنامه‌های کلانی که در سطح سازمان‌ها می‌تواند توان مجموعه را برای پیش‌بینی، مدیریت و مقابله با تهدیدها و حمله‌های سایبری افزایش دهد، پیامدهای مخرب ناشی از بروز تهدیدها را کاهش داده و بازسازی حوزه‌های آسیب دیده را با کمترین هزینه ممکن، میسر سازد، آینده‌نگاری است [4].

پژوهش حاضر با توجه به ماهیت آینده‌نگاری آن، می‌تواند منجر به ارتقاء توان‌مندی بدنه سایبری اجا در راستای شناسایی، تجزیه‌وتحلیل و دفاع در برابر یا مقابله با حمله‌های سایبری احتمالی آینده باشد. در واقع استفاده از آینده‌نگاری در حوزه امنیت سایبری می‌تواند به شناخت دقیق‌تر و واضح‌تر کلان روندها، پیشران‌ها، چالش‌ها و تهدیدهای آینده این حوزه کمک نموده و ماهیت چند رشته‌ای بودن آن نیز به بررسی دقیق‌تر پیامدهای ناشی از تهدیدهای سایبری بیانجامد.

با توجه به آنچه مطرح شد می‌توان عنوان نمود انجام پژوهش‌های از این دست که تلفیقی از آینده‌نگاری و امنیت سایبری را در بر دارد، مستلزم اجرای یک فرایند آینده‌نگارانه است که در حال حاضر در بدنه ارتش جمهوری اسلامی ایران موجود نیست. هر چند 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 قابل قبولی قرار دارد، اما با توسعه و تحولات روزافزون فناوری‌ها در بخش سایبری و کاربردهای متنوع آن و احتمال وقوع کلان روندهای ناشناخته در این بخش که می‌تواند با شگفتی‌سازهای حوزه سایبر نیز همراه شود، احتمال مواجه با چالش‌های اساسی متصور است.

پژوهش حاضر در راستای توسعه فرایندهای آینده‌نگاری و به‌منظور اتخاذ تصمیم‌های راهبردی متناسب با شرایط مملو از پیچیدگی و عدم قطعیت آینده مهم جلوه نموده و اهمیت انجام آن را در موارد زیر می‌توان یافت:

- نیازمندی‌ها و ویژگی‌های مورد نیاز بدنه سایبری اجا را به‌منظور شناسایی تهدیدهای سایبری در افق زمانی میان‌مدت (دو تا پنج ساله) تبیین می‌نماید؛
- بخشی از نگرانی‌های فرماندهان اجا در حوزه امنیت سایبری در قلمرو زمانی مدنظر پژوهش را برطرف می‌کند؛

1 - Cyber War
2 - Cyber Crimes
3 - Cyber Terrorism
4 - Cyber Espionage
5 - The European Union Agency for Cybersecurity

• از علوم نوین و روش‌های نوظهور آینده‌پژوهی در سازمان‌های نظامی به‌منظور ارتقاء امنیت سایبری با توجه به کلان روندهای مؤثر بر این حوزه بهره‌برداری می‌کند؛

• می‌تواند تا حدود زیادی موجب افزایش کارایی و اثربخشی مجموعه‌های کاری و اداری مستقر در بدنه یگان‌های وابسته به اجا گردد؛

• به راه‌کارهای عملی جهت رویارویی پیش‌فعالانه با توجه به تهدیدهای ناشی از وقوع کلان‌روندهای حوزه سایبر که مؤثر بر ساختار فناورانه ارتش جمهوری اسلامی ایران است، دست خواهد یافت.

هدف پژوهشگران از این پژوهش طراحی چارچوبی به‌منظور رویارویی پیش‌فعالانه ارتش جمهوری اسلامی ایران با تهدیدهای سایبری است و با توجه به موضوع پژوهش سؤال اصلی این گونه می‌تواند مطرح شود که طراحی چارچوبی به‌منظور رویارویی پیش‌فعالانه ارتش جمهوری اسلامی ایران با تهدیدهای سایبر چگونه است؟

و در این راستا سؤالات فرعی زیر مطرح است:

• اجزاء چارچوب آینده‌نگاری به‌منظور رویارویی پیش‌فعالانه ارتش جمهوری اسلامی ایران با تهدیدهای سایبری کدام‌اند؟

• رابطه بین اجزاء چارچوب آینده‌نگاری به‌منظور رویارویی پیش‌فعالانه ارتش جمهوری اسلامی ایران با تهدیدهای سایبری چگونه است؟

۲. مبانی نظری

۲-۱. ادبیات تحقیق:

آینده‌نگاری نخستین بار توسط اچ.جی.ولز[1] در سال ۱۹۳۲ به‌کار گرفته شد. منظور وی از آینده‌نگاری، فرایند تصور آینده‌های بدیل از طریق تلفیق گذشته‌نگاری[2]، نَک‌نگاری[3] و پیش‌بینی بود و تلاشی به‌منظور طرح مباحثی درباره آینده‌های محتمل و گزینه‌های اقدام بود [5].

آینده‌نگاری به‌عنوان یک ابزار بسیار مؤثر جهت سیاست‌گذاری (و به‌خصوص سیاست‌گذاری علم و تکنولوژی) به دولت‌ها کمک می‌نماید تا در شرایط دنیای امروز به چالش‌هایی همچون جهانی شدن و رقابت فزاینده پاسخی مناسب ارائه و اقداماتی مؤثر انجام دهند. در سال‌های اخیر، آینده‌نگاری علم و تکنولوژی به‌عنوان یک ابزار تصمیم‌گیری دولتی، در محیط سیاست علم و تکنولوژی ظاهر شده‌است که در بسیاری از حالات منجر به پاسخ سؤالات راهبردی در رابطه با علم و جامعه در یک چشم‌انداز بلند مدت گردیده است [6].

از سوی دیگر، حتی در صورت انجام آینده‌نگاری و تولید اطلاعات درباره آینده، گاهی اوقات ممکن است مدیران به این دلیل که برخی اطلاعات با فرایندهای رسمی تصمیم‌گیری‌شان جفت‌وجور[4] نیست، این‌گونه اطلاعات را نادیده بگیرند [7]. به‌عنوان‌مثال، با آن‌که خودروسازان آمریکایی از بحران انرژی [افزایش شدید قیمت نفت] در دهه هفتاد میلادی مطلع بودند، ولی در پیش‌نگریِ دلالت‌های آن، دچار شکست شدند [8].

فهرست برجسته‌ترین عناصر موجود در تعاریف مختلف آینده‌نگاری در جدول (۱) درج شده است.

جدول (۱). عناصر کلیدی تعاریف مختلف آینده‌نگاری [9]

عناصر کلیدی تعاریف آینده‌نگاری	پژوهشگر
مطالعات یا فرایند سیستماتیک	مارتین (۱۹۹۵)، جورجیو (۱۹۹۶)، باروز (۲۰۰۱)، مایلز و کنان (۲۰۰۲)، پوپر (۲۰۱۱)، کان وی (۲۰۱۵)، یوکسل و چیفچی (۲۰۱۷)، ساریتاس (۲۰۲۲)
نگاهی به آینده (میان مدت و بلند مدت)	مارتین (۱۹۹۵)، جورجیو و همکاران (۲۰۰۸)، مایلز (۲۰۱۰)، پوپر (۲۰۰۸)، یوکسل و چیفچی (۲۰۱۷)
فرآیند مشارکتی، جمعی، شبکه‌ای	جورجیو و همکاران (۲۰۰۸)، باروز (۲۰۰۱)، مایلز و کنان (۲۰۰۲)، هارپر (۲۰۰۳)، اتحادیه اروپا، کنان و پوپر (۲۰۰۷)، یوکسل و چیفچی (۲۰۱۷)
ساخت چشم‌اندازها	باروز (۲۰۰۱)، مایلز و کنان (۲۰۰۲)، هارپر (۲۰۰۳)، اتحادیه اروپا، کنان و پوپر (۲۰۰۷)،

1- H. G. Wells
2- Hindsight
3- Insight
4- Fit

عناصر کلیدی تعاریف آینده‌نگاری	پژوهشگر
	ساریتاس (۲۰۲۲)، فرگنانی و کوپر (۲۰۲۳)
جمع‌آوری اطلاعات	باروز (۲۰۰۱)، مایلز و کنان (۲۰۰۲)
فرآیند یادگیری	اتحادیه اروپا، کنان و پوپر (۲۰۰۷)، پوپر (۲۰۰۸)، ساریتاس (۲۰۲۲)
پیوستن به عوامل کلیدی تغییر و منابع دانش	باروز (۲۰۰۱)، پوپر (۲۰۰۸)، رایدی (۲۰۲۱)

شـــیخ و همکاران (۲۰۲۲) به نقل از مایلز (۲۰۰۲) عنوان می‌کنند که آینده‌نگاری ترکیبی از رویکردهایی اســـت که از خروجی‌های متقابل سه فعالیت بهره می‌برد: این سه فعالیت شـــامل آینده (تفکر آینده، پیش‌بینی، بلندمدت، آینده‌های جایگزین، ســـناریوها، چشـــم‌لندازها)، برنامه‌ریزی (تحلیل اســـتراتژیک، تعیین اولویت‌ها) و شـــبکه‌ســـازی (گســـترش مشارکت، تکنیک‌های شبکه، کارگروهی) است.

چارچوب آینده‌نگاری یک متا روش[1] اســـت که می‌تواند روش‌های آینده‌نگاری دیگری را در خود بگنجاند. این روش اطلاعات را در قلب‌ها، طبقه‌بندی و جمع‌آوری می‌کند و در جریان‌های منطقی مرتب می‌کند.

بر اســاس نظر اندرســون و راســموســن[2] فرایند آینده‌نگاری اغلب شامل ترکیبی از سه گونه سؤال است:

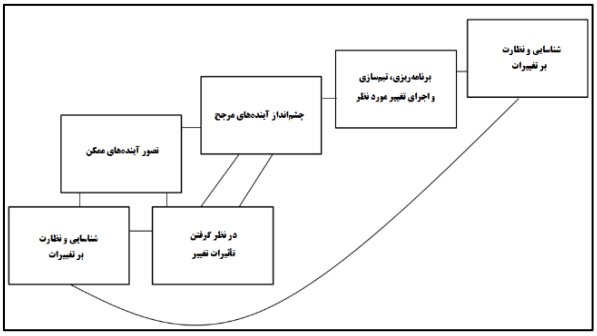
- نقطه عزیمت: اکنون وضعیت چگونه به نظر می‌رسد؟
- آرزوهـا و انتظـارات: چـه توقعـات و انتظـاراتی از پیشرفت‌های آینده در حوزه‌های تمرکز آینده‌نگاری داریم؟

تحقق: چگونـه می‌توان پیشـــرفـت‌هـای موردنظر را محقق ساخت؟ [10].

محققان برای پاسخ به این سه سؤال کلیدی، به پنج عنصر اصـــلی آینده‌نگاری اشـــاره می‌کنند که عبارت‌اند از برآورد ســـاختارمند تحولات و نیازهای آینده، روش‌های تعاملی و مشارکتی؛ ایجاد شبکه اجتماعی همکاری و تعامل؛ سناریوها و توســـعه چشـــم‌لندازهای راهبردی؛ ایجاد تعهد و دیدگاه مشترک. آنچه که موارد مطرح شده را در یک شکل منسجم جمع‌آوری نموده و به صـــورت یکپارچه ارائه می‌نماید، قالب‌هایی اســت که به عنوان چارچوب شـناخته می‌شـوند و در موضـــوع آینده‌نگاری با مطرح شـــدن این چارچوب‌های موضـــوعات مختلف مورد بررســـی و واکاوی قرار گرفته‌اند [11].

چارچوب عبارت اســـت از "ســـیســـتمی از قوانین، ایده‌ها یا باورها که برای برنامه‌ریزی یا تصـــمیم‌گیری درباره چیزی استفاده می‌شود" [12]. چارچوب‌ها بهترین شیوه‌ها و قوانین را برای انجام گروهی از فعالیت‌ها ارائه می‌کنند. از آنجایی که یکی از ویژگی‌های ســتون فقرات آینده‌نگاری یک فرآیند ســیســتماتیک اســت، چارچوب‌های آینده‌نگاری برای شــکل دادن به روش‌شـــناســـی توســـط شـــرکت کنندگان و ذینفعان حیاتی هستند [13].

پنج فعالیت اصـــلی آینده‌نگاری را می‌توان به صـــورت زیر برشـــمرد که اغلب در قالب چارچوب‌های آینده‌نگاری نمود یافته است (شکل (۱)). [14]



شکل (۱). پنج فعالیت حیاتی آینده‌نگاری

(۱)- شـناسـایی و نظارت بر تغییرات: شـرایط گذشـته و حال تجزیه‌وتحلیل و ارزیابی می شـوند تا روندهای جاری و مسائل نوظهور را شناسایی کنند.

(۲)- در نظر گرفتن تأثیرات تغییر: تأثیر تغییرات مداوم برای کشـــف آثار مختلف بر محیط کلان و زندگی روزمره ارزیابی می‌شود.

(۳)- تصور آینده‌های ممکن: بر اساس برون‌یابی روند و تأثیرات بلندمدت مســـائل نوظهور تغییرات، آینده‌های ممکن ارائه می‌شوند.

(٤)- چشـــم‌لنداز آینده‌های مرجح: با توجه به آرمان‌ها، اهداف و ارزش‌های بلندمدت، مدل‌هایی از آینده مطلوب ایجاد می‌شود.

1 - Meta-Method

2- Rasmussen

(۵)- برنامه‌ریزی، تیم‌سازی و اجرای تغییرات موردنظر: منابع برای اجرای طرح تغییر تخصیص داده می‌شود و سازمان برای اعمال چشم‌انداز و تغییرات موردنظر اقدام می‌کند.

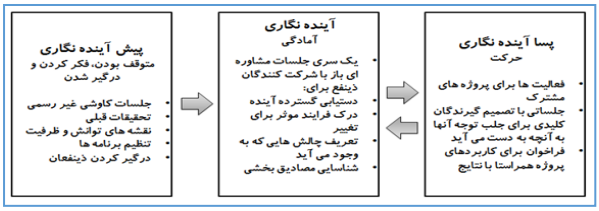
چارچوب آینده‌نگاری را می‌توان نسخه‌ای از چارچوب توصیف‌شده در رابطه با تفکر درباره آینده مشاهده کرد که از شش فعالیت اصلی یک پروژه آینده‌نگاری تشکیل شده است: چارچوب‌بندی، پویش، پیش‌بینی، چشم‌انداز، برنامه‌ریزی، و اقدام. هر مرحله یک مورد را تغذیه می‌کند و مجموعه روش‌های مختلفی را می‌توان در فعالیت‌ها استفاده کرد. چارچوب‌بندی شامل شناسایی جزئیات است. روندها، مسائل در حال ظهور و جزئیات مسائل را یافت می‌کنند. آینده جایگزین در مرحله پیش‌بینی با گرفتن ورودی اطلاعات از مرحله قبل تعیین می‌شوند. چشم‌انداز مرحله‌ای است که یک سازمان اهداف و آینده مطلوب را تعیین می‌کند. تمام خروجی‌های مطالعه به‌منظور دستیابی به اهداف مورد نظر در مرحله راهبردسازی انجام می‌شود (جدول (۲)) [15].

جدول (۲). چارچوب آینده‌نگاری و تفکر در مورد چارچوب آینده

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 در چارچوب مارتین شامل سه مرحله پیش‌آینده‌نگاری (کارهایی که قبل از آینده‌نگاری باید انجام داد)؛ آینده‌نگاری و پساآینده‌نگاری فرایند پیاده‌سازی نتایج آینده‌نگاری می‌باشد (شکل (۲)) [16].

این چارچوب قدیمی‌ترین چارچوب مطرح شده در حوزه آینده‌نگاری بوده و به‌نوعی پایه و اساسی برای چارچوب‌هایی بوده که بعد از مارتین ارائه شده است [16].



شکل (۲). چارچوب آینده‌نگاری مارتین

- **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 نیاز به اولویت‌بندی و اتخاذ سیاست بلندمدت برای علم و فناوری مورد پذیرش قرار گیرد.
- **مرحله آینده‌نگاری**: در مرحله آینده‌نگاری گام‌های طراحی فرآیند آینده‌نگاری، 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 مشتریان تولید می‌کند. تعیین مخاطبین اصلی نتایج آینده‌نگاری و مخاطبین نیازهای آینده‌نگاری، تقویت تعهد، اطمینان از قابلیت سازگاری سیستم تخصیص منابع فعلی برای علم و فناوری، دخالت دادن مردم در پیش‌بینی و سیاست‌گذاری، توجه به سلسله ارتباطات قوانین بین بخش‌ها، یکپارچه‌سازی فشار فناوری و کشش تقاضا در کنار رویکردهای بالا به پایین و پایین به بالا و تعیین رویه انتشار و پیاده‌سازی نتایج از جمله فعالیت‌های این گام است. در گام 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 مشخص شده‌اند انتخاب شوند و بهترین ابزار انتشار نتایج نیز تعیین شود.

- **مرحله پساآینده‌نگاری**: 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 سلسله مراتبی 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 [18].

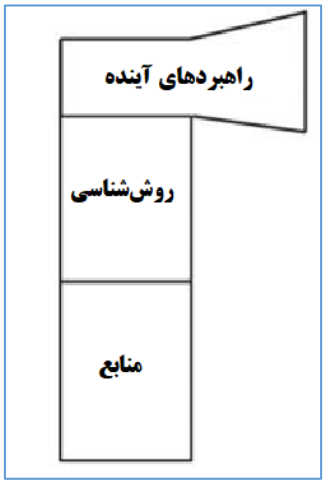
یکی از مطرح‌ترین چارچوب‌ها در حوزه سایبر مربوط به چارچوب آینده‌نگاری امنیت سایبری اروپا است. این چارچوب با بهره‌گیری از حروف کلمه «FORESIGHT» به صورت مراحل عملکردی متوالی در نه بخش به شرح زیر تدوین شده است [19]:

- چارچوب‌بندی[1]: انجام وظایف مربوط به تعیین هدف آینده‌نگاری، محدوده، محتوا و افق زمانی در این بخش انجام می‌شود؛
- به‌دست آوردن[2]: جمع‌آوری داده‌ها و اطلاعات، جمع‌آوری شرکت‌کنندگان، همچنین با استفاده از بخش مشترک به روشی تکراری که با چارچوب آن که در عملکرد قبلی بیان شده، 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 با دانش ایجاد شده، 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 چند رسانه‌ای، اشتراک‌گذاری در رسانه‌های اجتماعی؛
- هدایت[7]: تعریف اقدامات و تغییراتی که انجام خواهد شد، تعیین توالی آنها برای رسیدن به آینده‌های مختلف، تدوین استراتژی و برنامه‌ریزی؛
- مدیریت[8]: انجام اقدامات، ایجاد تغییرات و حل مشکلات برنامه؛
- ردیابی[9]: ارزیابی نتایج و نتایج مدیریت، انجام تجزیه‌وتحلیل تاثیر برای درس گرفتن به‌منظور فرآیند یادگیری.

از دیگر مدل‌های مطرح در حوزه آینده‌نگاری و سایبر می‌توان به مدل پریسکوپ آینده‌نگاری[10] که در واقع یک رویکرد آینده‌نگاری فناوری جدید است و دارای سه ماژول وابسته به هم است، نام برد. این سه ماژول شامل منابع، روش‌شناسی و استراتژی‌های آینده است. مدل از شباهت پریسکوپ استفاده می‌کند، یعنی منابع و روش‌شناسی بخش‌های زیربنایی هستند که سازمان را قادر می‌سازد

1 - Framing
2 - Obtaining
3 - Reviewing
4 - Establishing
5- Synthesizing
6 - Illustrating
7 - Guiding
8 - Handling
9 - Tracking
10 - Foresight Periscope Model

آینده‌های جایگزین را ببیند و استراتژی‌های آتی را برای بقا و رقابت در محیط ارائه دهد. این مدل نیز همانند سایر مدل و چارچوب‌های آینده‌نگاری که مطرح شده از سه جزء اساسی برخوردار است. منابع و ورودی‌ها به عنوان پیش آینده‌نگاری، روش‌شناسی به عنوان آینده‌نگاری و استراتژی‌های آینده در نقش پسا‌آینده‌نگاری به ایفای نقش می‌پردازند [20] (شکل ۳).



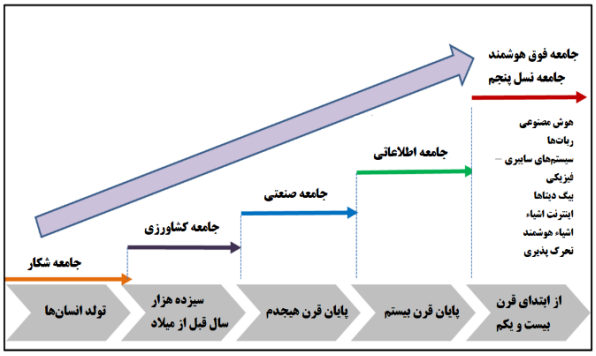
شکل (۳)، مدل پریسکوپ آینده‌نگاری [20]

در یک جمع‌بندی کلی می‌توان چارچوب‌های مختلفی را برای آینده‌نگاری نام برد که توسط صاحب‌نظران مختلف در سنوات گذشته و طی سه دهه گذشته ارائه شده است. این چارچوب‌ها بیان‌کننده فرایند اجرای آینده‌نگاری عمومی است و می‌توان برای انجام مطالعات آینده‌نگاری در حوزه‌های مختلف و با دامنه‌های موضوعی متفاوت از آن‌ها استفاده کرد. با توجه به توضیح‌های ارائه‌شده در مراجع مورد استفاده می‌توان به این نتیجه رسید که صاحب‌نظران و پژوهش‌گران آینده‌نگاری که به ذکر عوامل مهم فرایند اشاره کرده‌اند، 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.

نکته دیگری که در حوزه سایبر و فضای مجازی در ترسیم چارچوب بایستی مدنظر قرار گیرد این است که در این فضا با 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 می‌باشد. یکی از مهمترین کلان روندهای این حوزه را باید سوشتی ۵.۰ ژاپن، واژه‌ای که توسط دولت این کشور ارائه شده است، به حساب آورد. این کلان روند مفهوم جدیدی است که در پنجمین برنامه اصول علم و فناوری معرفی و تدوین شده است. سوشتی ۵.۰ به‌عنوان جامعه‌ای که توانایی ارائه مواد و خدمات مورد نیاز به مردم را در هر زمان که نیاز دارند، تعریف می‌کند. این جامعه می‌تولند نیازهای اجتماعی مختلف را برآورده کند و بر تفاوت‌های علوم انسانی غلبه کند [21].

علاوه بر سوشتی ۵.۰ که تلاشی برای دیجیتالی کردن زیرساخت‌های صنعتی و اجتماعی است ما با کلان روندهایی همچون انقلاب صنعتی ٤.۰ آلمان، اینترنت صنعتی ایالات متحده، پروژه ساخت چین ۲۰۲۵ و شهرهای هوشمند آسیا مواجه هستیم [22].

دوره‌های مختلف جوامع را می‌توان مانند شکل (٤) تعریف کرد، جایی که سوشتی ۱.۰[1] جامعه شکار است که در آن مردم با شکار زنده می‌مانند. سوشتی ۲.۰[2] یک جامعه کشاورزی و مبتنی بر کشاورزی است.



شکل (٤). جوامع انسانی و سوشتی نسل ۵.۰ "جامعه فوق هوشمند"

دوره‌های مختلف جوامع را می‌توان مانند شکل (۱) تعریف کرد، جایی که سوشتی ۱.۰[3] جامعه شکار است که در آن مردم با شکار زنده می‌مانند. سوشتی ۲.۰[4] یک جامعه کشاورزی و مبتنی بر کشاورزی است. سوشتی ۳.۰[5] با

1 - Society 1.0
2 - Society 2.0
3 - Society 1.0
4 - Society 2.0
5 - Society 3.0

انقلاب صـــنعتی و تحولات همراه با تولید انبوه مشـــخص می‌شـود. سـوشـتی ٤.٠،[1] جامعه‌ای اسـت که در آن زندگی می‌کنیم و به اطلاعات و رایانه‌ها نسـبت داده می‌شـود. در نهایت، سوشتی ٥.٠،[2] دوره بعدی خواهد بود [23].

سـوشـتی ٥.٠ بر اسـاس هوش مصـنوعی[3]، فناوری‌های روباتیک، کلان داده، رایانش ابری، سـیسـتم‌های فیزیکی سایبری[4]، اینترنت اشیا، اشیاء هوشمند (ماشین، خانه، لوازم خانگی و غیره) سـاخته شـده اسـت. سـوشـتی ٥.٠ با هدف ادغام فضـای مجازی با فضـای فیزیکی سـاخته شـده اسـت [24].

۲-۲. پیشینه پژوهش:

برابر بررسـی‌های انجام شـده در منابع مطالعاتی و علمی داخلی و خارجی، پژوهشـی که به‌طور مسـتقیم و کامل هم‌راسـتا با موضـوع تحقیق، موجود باشـد، یافت نگردید ولیکن موضوعاتی که به‌نوعی در راستای تحقیق بوده و نتایج حاصله آنها در پیشبرد این پژوهش مؤثر است در بانک‌های اطلاعاتی داخل و خارج کشـور یافت گردید که ادامه موارد مشابه عنوان می‌گردد.

مهدوی‌پور در پایان‌نامه کارشـناسـی ارشـد خود با عنوان عوامل مؤثر بر امنیت سـایبری ارتش جمهوری اسـلامی ایران (مطالعه موردی سـتاد ارتش جمهوری اسـلامی ایران) که در سـال ۱۳۹۹ به انجام رسـیده اسـت مطرح می‌کند که عوامل درون سـازمانی شـامل امن‌سـازی تجهیزات، شـبکه‌ها، نرم‌افزارهای رصـد و پایش رخدادهای سـایبری و واکنش به‌موقع به آن‌ها و ارتقاء دانش سـایبری کارکنان و عوامل برون سازمانی شامل تهدیدهای سایبری انسان‌ساز و طبیعی عوامل مؤثر بر امنیت سـایبری جمهوری اسـلامی ایران را تشکیل می‌دهند.

اسـماعیلی در رسـاله دکتری خود با عنوان که در سـال ۱۳۹۹ و در دانشـگاه عالی دفاع ملی به انجام رسـیده اسـت مهمترین ابعاد الگوی پایش تهدیدات سـایبری ج.ا ایران را پویش، ارزیابی و واکنش در نظر گرفته اسـت و در ادامه وی پیشـنهاد می‌دهد که با توجه به 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.

ایجابی و کولیوند در پژوهشـی در سـال ۱٤۰۱ با عنوان واکاوی تهدیدات امنیتی شـبکه‌های رایانه‌ای سـازمان‌ها با رویکرد آینده‌پژوهی (مطالعه موردی سـتاد فرماندهی نیروی پدافند هوایی آجا) با اسـتفاده از روش چرخ آینده و تلفیق این روش با پنل خبرگی و جلسـات ذهن‌انگیزی در حوزه تهدیدات شبکه ۷۸ تهدید را شناسایی و احصاء نموده‌اند که با بهره‌گیری از روش پنل خبرگان و اسـتفاده از نرم‌افزار آینده‌پژوهی **MicMac** در نهایت تعداد هفت عامل تهدیدزا را در حوزه تهدیدات امنیتی شـبکه‌های رایانه‌ای سـازمان‌ها شناسایی نموده‌اند.

آقایی و همکارانش در پژوهشی در سال ۱۳۹۸ با عنوان ارائه مدل مفهومی منطقی طبقه‌بندی تهـدیدات سـایبری زیرسـاخت‌های حیاتی با اسـتفاده از فراترکیب و اسـتفاده از ضـریب کاپا در قالب مدل مفهومی منطقی، طبقه‌بندی تهدیدات سـایبری زیرسـاخت‌های حیاتی را در ابعاد شـش گانه تهدیدات، عوامل تهدید، مشخصات تهدید، نگاه از دید نفوذگر، توصیف سیستم و منابع شناسایی تهدیدات انجام داده‌اند.

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 جزیی (**PLS**) انجام شده 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 ٤ مؤلفه و برای هر مؤلفه ۳ زیرمؤلفه و ۱۳ شاخص ترسیم می‌نمایند.

1 - Society 4.0
2 - Society 5.0
3 - Artificial Intelligence (AI)
4 - Cyber-physical Systems (CPS)

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

رابان و هوپتمن[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 هک سایبری به سرعت ظهور کرده است. از این رو 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.

آنچه که در پیشینه پژوهش مطرح گردید، نشان می‌دهد که در رابطه با تلفیق آینده‌نگاری و سایبر در سال‌های اخیر فعالیت‌هایی صورت پذیرفته، هر چند که هنوز در ابتدای راه هستند. اما از آنجا که آینده‌نگاری فرایندی سیستماتیک و نظامند است که با بررسی همه جانبه موضوع و درنظر گرفتن صحنه آینده که سرشار از عدم قطعیت و بعضاً شگفتی‌سازهایی است که می‌تواند تحولات اساسی را به‌وجود آورد، زمینه‌های کار پژوهشی و اجرایی در این دو حوزه (آینده‌نگاری و سایبر) وجود دارد.

ضمن اینکه این پژوهش در پی مدلی به منظور رصد و پایش تهدیدهای آینده سایبر با توجه به وقوع کلان روندهای این حوزه در افق زمانی مدنظر پژوهش است و امکان تشخیص تهدیدهای فراروی بستر سایبری اجا را با وقوع پیشران‌هایی از قبیل اینترنت اشیاء[3] در سامانه‌ها و تجهیزات مبتنی بر وب محقق می‌نماید. از سوی دیگر با تشخیص تهدیدهای سایبری آینده سازمان در مواجه با به‌کارگیری فناوری‌هایی از قبیل رایانش ابری، هوش مصنوعی و ... امکان ارائه راهبردهای کاربردی جهت رویارویی پیش فعالانه با تهدیدهای سایبری در محیط سرشار از عدم قطعیت آینده فراهم می‌گردد.

۳. روش‌شناسی پژوهش:

با توجه به تعریف تحقیق‌های کاربردی که مبتنی بر سودمندی عملی است و محقق در پی آن است تا علم به‌کارگیری دانش تولید شده را تبیین نماید، از این رو، پژوهش حاضر نیز از آنجا که می‌تواند در تصمیم‌گیری‌ها و سیاست‌های امنیت سایبری اجا اثرگذار بوده و ملاک عمل و ارجاع قرار بگیرد، از نوع کاربردی است. قاعدتاً باید در نظر داشت که با توجه به ناشناخته‌ها و ابهام‌های آینده‌نگاری و تهدیدهای سایبری، پرداختن به این موضوع‌ها نیازمند کاوش و شناسایی است که نوعاً در پژوهش‌های کیفی بیشتر دنبال می‌شود.

از سوی دیگر هدف این پژوهش ارائه گام‌های کاربردی می‌باشد که به‌نوعی هم شامل نظریه‌پردازی و هم ابزارسازی است. پس انجام چنین امری هم نیازمند پژوهش کیفی و هم پژوهش کمّی است. از این‌رو باید رویکرد پژوهش آمیخته را در دستور کار قرار داد.

با استفاده از مطالعه اسناد و مدارک و مطالعات کتابخانه‌ای چارچوب اولیه پژوهش استخراج گردید و با انجام مصاحبه در قالب پنل‌های خبرگی با خبرگان و کارشناسان حوزه سایبر در یگان‌های متولی سایبر آجا چارچوب اولیه، اجزاء آن، نحوه ارتباط آنها، همچنین اقدامات قابل انجام در هر مرحله تعیین گردید. سپس در مرحله بعد با استفاده از نظرات جامعه نمونه، چارچوب مدنظر به‌صورت پرسشنامه محقق ساخت مورد تأیید قرار گرفت. پس از تأیید جامعه نمونه با استفاده از نرم‌افزار PLS مدل‌سازی ساختاری – تفسیری به روش حداقل مربعات جزئی انجام و چارچوب نهایی (پس از مشخص شدن اجزاء و ارتباط آنها با یکدیگر) با استفاده از نرم‌افزار Edraw Max8.4 ترسیم شد.

1 - Chifchi

2 - Raban & Hauptman

3 - IOT (Internet of Things)

مشخصات جامعه آماری این تحقیق نیز شامل افرادی است مشتمل بر کارشناسان خبره و صاحب‌نظر در موارد از قبیل دانش‌آموختگان رشته سایبر و امنیت رایانه (حداقل مقطع لیسانس) در سطح کل اجا، دانش‌آموختگان تحصیلات تکمیلی رشته آینده‌پژوهی و آینده‌نگاری (دکتری) اجا و وزارت دفاع، کارشناسان سایبری نیروهای چهارگانه اجا و ستاد فرماندهی اجا 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 علم و فناوری و ... در سطح ارتش جمهوری اسلامی ایران. این افراد در حالت حداکثری و با اعمال ضریب حفاظتی، تعداد ۱۴۰ نفر تعیین می‌گردد که با استفاده از فرمول کوکران جامعه نمونه شامل ۱۲۷ نفر انتخاب گردید.از این تعداد هفت نفر به عنوان خبرگان مورد مصاحبه قرار گرفتند و ۱۲۰ نفر در پاسخ‌دهی به پرسشنامه محقق ساخت، پژوهش‌گر را یاری نمودند.

٤. یافته‌های پژوهش

پژوهش حاضر در سه بخش انجام گردید. بخش اول شامل رویکرد کیفی است. در این مرحله با انجام مطالعات کتابخانه‌ای و بررسی اسناد و مدارک علمی که ۲۵ چارچوب آینده‌نگاری را در بر می‌گرفت، چارچوب اولیه شناسایی و معرفی گردید. سپس با انجام مصاحبه با خبرگان و کارشناسان حوزه سایبر و آینده‌پژوهی، بخش‌های مختلف چارچوب اصلاح و بازنویسی شد و با برگزاری پنل‌های خبرگی و انجام توفان فکری زیربخش‌های هرکدام از اجزاء چارچوب شناسایی و استخراج گردید.

٤-١. رویکرد کیفی:

چارچوب اولیه شامل سه بخش اصلی پیش آینده‌نگاری، آینده‌نگاری و پسا آینده‌نگاری است.

بخش پیش آینده‌نگاری شامل چهار زیربخش مطالعه وضعیت سایبری سازمان‌های دشمن، مطالعه وضعیت سایبری سازمان‌های بالادستی و همتراز، مطالعه وضعیت سایبری سازمان و شناسایی کلان روندهای سایبری.

بخش آینده‌نگاری شامل چهار زیربخش تجزیه و تحلیل تهدیدهای سایبری، تفسیر تهدیدهای سایبری، ترسیم وضعیت مطلوب سایبری سازمان و چشم‌انداز سایبری سازمان است.

بخش پسا‌آینده‌نگاری شامل دو زیربخش تصمیم‌سازی و تصمیم‌گیری و راهبردنگاری می‌باشد.

هر کدام از زیربخش‌ها نیز شامل اجزایی است که با بررسی اسناد و مدارک و مطالعات کتابخلنه و انجام مصاحبه با خبرگان بعد از انجام سه فرآیند رویکرد کیفی پژوهش یعنی دسته‌بندی داده‌ها، پردازش داده‌ها و در نهایت قضاوت اطلاعات به شرح جدول (۳) معرفی شدند. برای سهولت کار پژوهش‌گر در انجام رویکرد کمی به هر مؤلفه یک کد اختصاص یافت.

جدول (۳)، اجزاء اولیه چارچوب پیشنهادی پژوهش

اجزاء اصلی چارچوب	زیربخش‌های اجزاء اصلی چارچوب
پیش آینده‌نگاری	**مطالعه وضعیت سایبری سازمان‌های دشمن**
	تعریف دقیق دشمن و تشخیص دوست از دشمن (A1)؛ رصد و پایش تجهیزات، تسهیلات، قابلیت‌ها، ساختارها، روال‌ها و فناوری‌های مورد استفاده (A2)؛ برآورد وضعیت قدرت آفند سایبری دشمن (A3)؛ دیده‌بانی سایبری در جهت شناسایی فناوری‌های برترساز، 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

اجزاء اصلی چارچوب	زیربخش‌های اجزاء اصلی چارچوب
	آگاهی از مأموریت‌ها، وظایف محوله، سیاست‌گذاری‌ها و خط‌مشی‌های صادره (B1)؛ ایجاد تعاملات فی مابین 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
	بررسی آخرین وضعیت موجود از منابع سایبری، مدیریت دارایی‌ها و سرویس‌ها (C1)؛ اطلاع از مأموریت‌ها برابر آخرین ابلاغیه‌ها (C2)؛ شناسایی فرایندها، زیرفرایندها، تجهیزات، ساختارهای سازمانی، اسناد بالادستی (C3)؛ شناخت سرمایه‌های انسانی، نیروهای دانشی و افراد هکر پایه در سازمان (C4).
	شناسایی کلان روندهای سایبری
	رصد و پایش شرکت‌های فناور در زمینه ساخت و تولید محصولات سایبر پایه، فناوری‌های برترساز و پایگاه‌های وب محور (D1)؛ پایش مجامع علمی و کنفرانس‌های بین‌المللی برگزار شده (D2)؛ دیده‌بانی منطقه‌ای در تحولات فناورانه (D3).
آینده‌نگاری	**تجزیه و تحلیل تهدیدهای سایبری**
	تجزیه و تحلیل رفتاری (E1)؛ فرآیند تحلیلی اطلاعات تهدید خارجی (E2)؛ جرم‌شناسی و تعیین چگونگی نفوذ مهاجمان به سیستم‌ها (E3)؛ تجزیه و تحلیل شبکه و قابلیت مشاهده (E4)؛ ارکستراسیون امنیتی، اتوماسیون و پاسخگویی (E5)؛ تجزیه و تحلیل ترافیک شبکه (E6)؛ تحلیل نقاط ضعف سخت‌افزاری و نرم‌افزاری (E7).
	تفسیر تهدیدهای سایبری

اجزاء اصلی چارچوب	زیربخش‌های اجزاء اصلی چارچوب
	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
	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)؛ پیش دستی 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)؛ دست یافته به زیست بوم سایبری (H2)؛ نظام واحد فرماندهی، هدایت، راهبری و کنترل پدافند سایبری (H3)؛ برخوردار از سرمایه‌های انسانی آموزش دیده (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).
	تصمیم‌سازی و تصمیم‌گیری

اجزاء اصلی چارچوب	زیربخش‌های اجزاء اصلی چارچوب
	انجام وظایف در پردازش داده (I1)؛ پشتیبانی، تقویت و ایجاد اتوماسیون 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 تکنیک‌های جنگ سایبری (I6)؛ تشخیص تصمیم‌های مشروط به محیط‌های محتمل آینده و چگونگی عملکرد اجا در آن محیط‌ها (I7).
راهبردنگاری	
	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).

٤-٢. رویکرد کمی

در مرحله بررسی کمی یافته‌های کیفی با تهیه پرسشنامه محقق ساخت بر اساس مؤلفه‌های استخراج شده صحت‌سنجی داده‌ها با استفاده از نظر جامعه نمونه ۱۲۰ نفره مورد سنجش و بررسی قرار گرفت که نتایج حاصل از بازخورد پرسشنامه‌ها در ادامه ارائه می‌گردد.

توزیع فراوانی جامعه آماری برحسب مدرک تحصیلی به شرح جدول (٤) است.

جدول (٤)، فراوانی جامعه آماری برحسب مدرک تحصیلی

تحصیلات		فراوانی	درصد فراوانی
	کارشناسی	۳۷	۳۰.۸۳
داده معتبر	کارشناسی ارشد	٦٥	٥٤.١٧
	دکتری و بالاتر	۱۸	۱٥.۰۰
جمع کل		۱۲۰	۱۰۰

بر اساس نظرات پاسخ‌دهندگان ٦٩.١٧ درصد از جامعه آماری داری مدرک کارشناسی ارشد و بالاتر هستند که این نسبت به دست آمده برای جامعه آماری نشان می‌دهد که جامعه انتخاب شده از نظر سطح تحصیلات و بنیه علمی از صلاحیت لازم برای اظهارنظر درباره متغیرهای احصاء شده برخوردار بودند که در افزایش روایی پاسخ‌ها مؤثر است. لذا نظرات آن‌ها قابل اعتماد است.

توزیع فراوانی جامعه آماری برحسب سوابق خدمتی به شرح جدول (٥) است.

جدول (٥)، فراوانی جامعه آماری برحسب سوابق خدمتی

سوابق خدمتی		فراوانی	درصد فراوانی
داده معتبر	۱۰ تا ۱٥ سال	۲۰	١٦.٦٧
	١٦ تا ۲۰ سال	٦٠	٥٠.۰۰
	بیشتر از ۲۰ سال	٤٠	۳۳.۳۳
جمع کل		۱۲۰	۱۰۰

بر اساس جدول فوق ۸۳.۳۳ درصد از جامعه آماری دارای سنوات خدمتی بالای ۱٥ سال هستند که این امر گویایی این واقعیت است که به دلیل بالا بودن سنوات خدمتی جامعه آماری، مهارت خوبی برای اظهارنظر در خصوص متغیرهای مورد بررسی دارند که در بالا بردن روایی پاسخ‌ها مؤثر است.

٤-٢-١. بررسی پایایی سؤالات پرسشنامه

بهترین روش محاسبه‌ی اندازه ثبات درونی، استفاده از ضریب آلفای کرونباخ 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 ٦).

جدول (٦)، محاسبه پایایی پرسشنامه برای اجزاء چارچوب

بُعد	تعداد سؤالات	آلفای کرونباخ
پیش آینده‌نگاری	۱۸ سؤال	۰.۹۹۸
آینده‌نگاری	۲٤ سؤال	۰.۹٤۹
پساآینده‌نگاری	۲۱ سؤال	۰.۹۹٥

ملاک سنجش پایایی ضریب آلفای کرونباخ بالای ۰.۷ می‌باشد که با توجه به مقدار عددی ضریب آلفای کرونباخ به دست آمده برای ٦٢ سؤال پرسشنامه که به‌طور میانگین بیشتر از ۰.۹٤ درصد است، در نتیجه می‌توان گفت پایایی پرسشنامه عالی است. به منظور سنجش نظرات جامعه نمونه از طیف لیکرت پنج تایی (کاملاً موافقم (٥)، موافقم (٤)، نظری ندارم (٣)، مخالفم (٢) و کاملاً مخالفم (١)) استفاده شد.

٢-٢-٤. تجزیه و تحلیل توصیفی داده‌های بخش پیش‌آینده‌نگاری:

جدول (٧) نتایج میانگین، واریانس و ضریب پراکندگی مربوط به اجزاء بخش پیش آینده‌نگاری را نشان می‌دهد.

جدول (٧)، تجزیه و تحلیل توصیفی بخش پیش‌آینده‌نگاری

ردیف	میانگین	واریانس	ضریب پراکندگی
A1	٤.١٤	١.٠٤	٠.٢٤٦
A2	٤.٣٣	٠.٨٢	٠.٢٠٩
A3	٤.١٦	١.١٥	٠.٢٥٧
A4	٤.١٠	١.٢٦	٠.٢٧٣
A5	٤.٠٩	١.١٢	٠.٢٥٨
A6	٣.٩٨	١.٣٩	٠.٢٩٦
B1	٤.٠٤	١.١٧	٠.٢٦٨
B2	٤.٢٠	١.١٤	٠.٢٥٥
B3	٤.١٣	١.٢٤	٠.٢٧٠
B4	٤.٢٢	١.٠٠	٠.٢٣٨
B5	٤.١٦	١.٠٠	٠.٢٤٠
C1	٤.٣١	٠.٨٠	٠.٢٠٧
C2	٤.٠٧	١.٢٥	٠.٢٧٤
C3	٤.١٢	١.٢٥	٠.٢٧٢
C4	٤.٣٠	٠.٨٨	٠.٢١٨
D1	٤.١٥	١.٠٩	٠.٢٥٢
D2	٤.٠٤	١.٢٩	٠.٢٨١
D3	٤.٠٨	١.٢٥	٠.٢٧٥

بر اساس داده‌های دریافتی مشخص گردید که جامعه نمونه با آرا بالایی تمامی اجزاء را پذیرفته و تایید نمودند. همچنین میانگین به دست آمده برای هر کدام از گویه‌ها حاکی از این است که جامعه آماری اعتقاد دارد که این گویه‌ها از روایی و اعتبار بسیار خوبی برخوردار هستند. به منظور تجزیه و تحلیل استنباطی از آزمون تی – استیودنت و آزمون کای – دو استفاده شد که بر اساس ضرایب توافقی به دست آمده و همچنین نتایج آزمون‌های انجام شده تمامی اجزاء با درصد توافق بالایی مورد تایید جامعه نمونه قرار گرفتند. نتایج حاصل از آزمون تی و آزمون کای دو بخش پیش آینده‌نگاری در جدول (٨) ارائه شده است.

جدول (٨)، تجزیه و تحلیل استنباطی بخش پیش‌آینده‌نگاری

ردیف	آماره آزمون تی	آماره آزمون کای دو	ضریب توافقی
A1	١٢.٢٧	٨٧.٧٥	٠.٦٥
A2	١٦.١١	١٢٤.٠٠	٠.٧١
A3	١١.٨٣	٩٤.٠٠	٠.٦٦
A4	١٠.٧٥	٨٣.٠٠	٠.٦٤
A5	١١.٣٢	٨٤.٦٧	٠.٦٤
A6	٩.٠٦	٦٢.٧٥	٠.٥٩
B1	١٠.٥٣	٧٠.١٧	٠.٦١
B2	١٢.٢٩	١٠١.٧٥	٠.٦٨
B3	١١.٠٥	٨٧.٢٥	٠.٦٥
B4	١٣.٣١	١٠٠.٨٣	٠.٦٨
B5	١٢.٦٩	٩٠.٩٢	٠.٦٦
C1	١٦.٠٦	١١.٥٨	٠.٧١
C2	١٠.٤٧	٧٦.٥٨	٠.٦٢
C3	١٠.٩٣	٨٦.٧٥	٠.٦٥
C4	١٥.٢١	١١٦.٦٧	٠.٧٠
D1	١٢.٠٤	٩١.٦٧	٠.٦٦
D2	١٠.٠٥	٧٤.٥٨	٠.٦٢
D3	١٠.٥٢	٧٧.٩٢	٠.٦٣

نتایج به دست آمده نشان داد که بر اساس ضریب توافقی حاصل از نظرات پاسخ‌دهندگان ارتباط بین آن‌ها و مؤلفه‌های مربوطه مورد تایید است. ضمناً با توجه به آماره آزمون کای –دو مشخص گردید که این ارتباط‌ها معنی‌دار هم هستند. آماره آزمون تی هر کدام از مؤلفه‌ها نیز بیشتر از مقدار بحرانی که ١.٦٤ است شده و آماره آزمون کای – دو همه گام‌ها بیشتر از عدد ٩.٤٨ مقدار بحرانی شده است که این امر اثبات می‌کند

تمام مؤلفه‌ها با الگوی مورد نظر ما ارتباط بسیار خوب و بالایی دارند.

۳-۲-٤. تجزیه و تحلیل توصیفی داده‌های بخش آینده‌نگاری:

جدول (۹) نتایج میانگین، واریانس و ضریب پراکندگی مربوط به اجزاء بخش آینده‌نگاری را نشان می‌دهد.

جدول (۹)، تجزیه و تحلیل توصیفی بخش آینده‌نگاری

ردیف	میانگین	واریانس	ضریب پراکندگی
E1	٤.١٨	٠.٩٨	٠.٢٣٧
E2	٤.٠٣	١.٢٧	٠.٢٨٠
E3	٤.٠٨	١.٣٢	٠.٢٨٢
E4	٤.٢٩	٠.٨٤	٠.٢١٤
E5	٤.١٢	١.٠٩	٠.٢٥٣
E6	٤.١٥	١.١٣	٠.٢٥٦
E7	٤.١٨	١.١٦	٠.٢٥٨
F1	٤.١٠	١.١٤	٠.٢٦٠
F2	٤.١٢	١.٠٩	٠.٢٥٣
F3	٤.١٥	١.١١	٠.٢٥٤
F4	٤.٢٤	٠.٨٥	٠.٢١٧
F5	٤.١١	١.٠٨	٠.٢٥٣
F6	٤.١٤	٠.٩٢	٠.٢٣٢
F7	٤.٠٧	١.١٦	٠.٢٦٥
F8	٤.١٣	١.١٠	٠.٢٥٤
G1	٤.١٩	٠.٨٧	٠.٢٢٣
G2	٤.٢٩	٠.٧٩	٠.٢٠٧
G3	٤.١٣	١.١٨	٠.٢٦٣
G4	٤.١٥	١.١٣	٠.٢٥٦
G5	٤.٠٩	١.١٢	٠.٢٥٨
G6	٤.١٨	٠.٩٦	٠.٢٣٥
G7	٤.٢٣	٠.٧٣	٠.٢٠٢
G8	٤.٢٠	٠.٨٤	٠.٢١٩
G9	٤.٢٤	٠.٩٠	٠.٢٢٤
H1	٤.١٧	٠.٩٢	٠.٢٣٠
H2	٤.٢٨	٠.٧٧	٠.٢٠٥
H3	٤.٢٦	٠.٩٢	٠.٢٢٦
H4	٤.١٩	٠.٩٧	٠.٢٣٥
H5	٤.٢١	٠.٩٠	٠.٢٢٥
H6	٤.١٠	١.٢٤	٠.٢٧٢
H7	٤.١٦	٠.٨٧	٠.٢٢٤
H8	٤.١٨	٠.٩٢	٠.٢٢٩

بر اساس داده‌های دریافتی مشخص گردید که جامعه نمونه با آرا بالایی تمامی اجزاء را پذیرفته و تایید نمودند. همچنین میانگین به دست آمده برای هر کدام از گویه‌ها حاکی از این است که جامعه آماری اعتقاد دارد که این گویه‌ها از روایی و اعتبار بسیار خوبی برخوردار هستند. به منظور تجزیه و تحلیل استنباطی از آزمون تی – استیودنت و آزمون کای – دو استفاده شد که بر اساس ضرایب توافقی به دست آمده و همچنین نتایج آزمون‌های انجام شده تمامی اجزاء با درصد توافق بالایی مورد تایید جامعه نمونه قرار گرفتند. نتایج حاصل از آزمون تی و آزمون کای دو بخش آینده‌نگاری در جدول (۱۰) ارائه شده است.

جدول (۱۰)، تجزیه و تحلیل استنباطی بخش آینده‌نگاری

ردیف	آماره آزمون تی	آماره آزمون کای دو	ضریب توافقی
E1	١٣.٠٢	٩٤.١٧	٠.٦٦
E2	٩.٩٥	٧٢.٧٥	٠.٦١
E3	١٠.٢٥	٨٠.٢٥	٠.٦٣
E4	١٥.٤٤	١١٨.٠٨	٠.٧٠
E5	١١.٧٤	٨٨.٤٢	٠.٦٥
E6	١١.٨٦	٨٩.٦٧	٠.٦٥
E7	١١.٩٥	٩٨.٤٢	٠.٦٧
F1	١١.٢٩	٨٣.١٧	٠.٦٤
F2	١١.٧٤	٨٢.٤٢	٠.٦٤
F3	١١.٩٥	٨٨.٠٨	٠.٦٥
F4	١٤.٧٥	١٠٧.٩٢	٠.٦٩
F5	١١.٦٨	٨١.٤٢	٠.٦٤
F6	١٣.٠٣	٨٧.٣٣	٠.٦٥
F7	١٠.٨٤	٧٥.١٧	٠.٦٢
F8	١١.٨٤	٨٩.٧٥	٠.٦٥
G1	١٣.٩٨	١٠٢.٤٢	٠.٦٨
G2	١٥.٩٢	١١٧.٠٨	٠.٧٠
G3	١١.٤٢	٨٩.٩٢	٠.٦٥
G4	١١.٨٦	٩٤.١٧	٠.٦٦

ردیف	آماره آزمون تی	آماره آزمون کای دو	ضریب توافقی
G5	۱۱.۳۲	۸٤.٦۷	۰.٦٤
G6	۱۳.۱۳	۹٦.۲٥	۰.٦۷
G7	۱٥.۸۲	۱۰۷.٥۸	۰.٦۹
G8	۱٤.۳۱	۱۰۹.٥۰	۰.٦۹
G9	۱٤.۳٤	۱۰٦.٤۲	۰.٦۹
H1	۱۳.۳۱	۱۰۱.۸۳	۰.٦۸
H2	۱٦.۰۲	۱۱۸.٦۷	۰.۷۱
H3	۱٤.۳۳	۱۱۳.٤۲	۰.۷۰
H4	۱۳.۲٤	۱۰۰.۰۸	۰.٦۷
H5	۱۳.۹۷	۱۰٦.۰۸	۰.٦۸
H6	۱۰.۸۲	۸۳.٥۸	۰.٦٤
H7	۱۳.٦۳	۹٥.٥۸	۰.٦۷
H8	۱۳.٥٤	۹۹.۰۸	۰.٦۷

نتایج به دست آمده نشان داد که بر اساس ضریب توافقی حاصل از نظرات پاسخ‌دهندگان ارتباط بین آن‌ها و مؤلفه‌های مربوطه مورد تایید است. ضمناً با توجه به آماره آزمون کای –دو مشخص گردید که این ارتباط‌ها معنی‌دار هم هستند. آماره آزمون تی هر کدام از مؤلفه‌ها نیز بیشتر از مقدار بحرانی که ۱.٦٤ است شده و آماره آزمون کای – دو همه گام‌ها بیشتر از عدد ۹.٤۸ مقدار بحرانی شده است که این امر اثبات می‌کند تمام مؤلفه‌ها با الگوی مورد نظر ما ارتباط بسیار خوب و بالایی دارند.

٤-۲-٤. تجزیه و تحلیل توصیفی داده‌های بخش پساآینده‌نگاری:

جدول (۱۱) نتایج میانگین، واریانس و ضریب پراکندگی مربوط به اجزاء بخش پساآینده‌نگاری را نشان می‌دهد.

جدول (۱۱)، تجزیه و تحلیل توصیفی بخش پساآینده‌نگاری

ردیف	میانگین	واریانس	ضریب پراکندگی
I1	٤.۰۷	۱.۱۰	۰.۲٥۷
I2	٤.۲٥	۰.۸۲	۰.۲۱۳
I3	٤.۱۳	۱.۰۸	۰.۲٥۲
I4	٤.۲۸	۰.۷۷	۰.۲۰٥
I5	٤.۲۲	۰.۸٤	۰.۲۱۷
I6	٤.۲۱	۰.۹۰	۰.۲۲٥
I7	٤.۰٥	۱.۲۳	۰.۲۷٤
J1	٤.۲۸	۰.۸۳	۰.۲۱۳
J2	٤.۲۰	۰.۹۹	۰.۲۳۷
J3	٤.۰۹	۱.۰۸	۰.۲٥٤
J4	٤.۲٥	۰.۷۹	۰.۲۰۹
J5	٤.۱۸	۰.۹۹	۰.۲۳۹
J6	٤.۱۸	۰.۹۲	۰.۲۲۹

بر اساس داده‌های دریافتی مشخص گردید که جامعه نمونه با آرا بالایی تمامی اجزاء را پذیرفته و تایید نمودند. همچنین میانگین به دست آمده برای هر کدام از گویه‌ها حاکی از این است که جامعه آماری اعتقاد دارد که این گویه‌ها از روایی و اعتبار بسیار خوبی برخوردار هستند. به منظور تجزیه و تحلیل استنباطی از آزمون تی – استیودنت و آزمون کای – دو استفاده شد که بر اساس ضرایب توافقی به دست آمده و همچنین نتایج آزمون‌های انجام شده تمامی اجزاء با درصد توافق بالایی مورد تایید جامعه نمونه قرار گرفتند. نتایج حاصل از آزمون تی و آزمون کای دو بخش پساآینده‌نگاری در جدول (۱۲) ارائه شده است.

جدول (۱۲)، تجزیه و تحلیل استنباطی بخش آینده‌نگاری

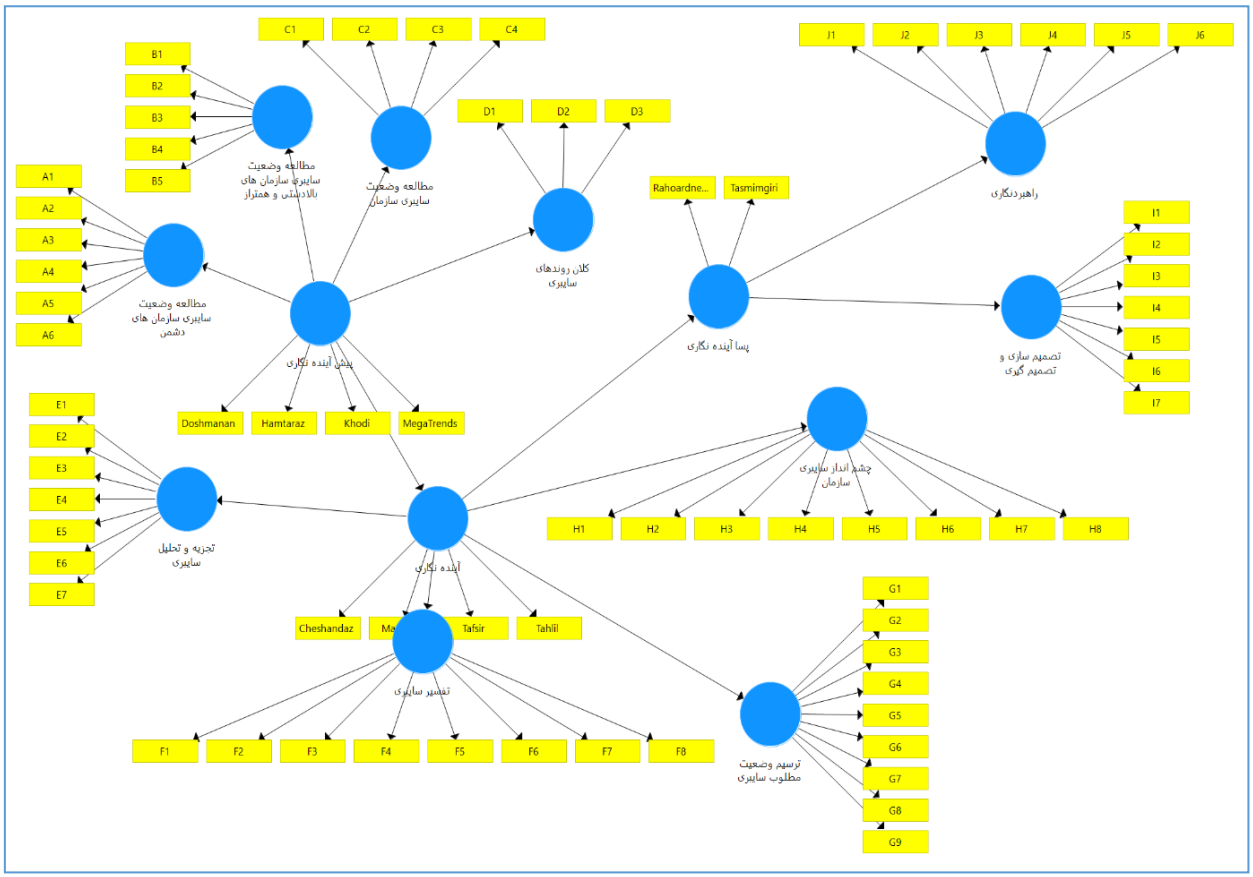
ردیف	آماره آزمون تی	آماره آزمون کای دو	ضریب توافقی
I1	۱۱.۱٦	۸٤.۱۷	۰.٦٤
I2	۱٥.۱۱	۱۱۳.۹۲	۰.۷۰
I3	۱۱.۹۳	۹۱.۹۲	۰.٦٦
I4	۱٥.۹٦	۱۱۲.٤۲	۰.۷۰
I5	۱٤.٥۷	۱۰٦.٤۲	۰.٦۹
I6	۱۳.۹۷	۱۰٦.۰۸	۰.٦۸
I7	۱۰.۳۷	۷۸.۲٥	۰.٦۳
J1	۱٥.۳۱	۱۱٥.۹۲	۰.۷۰
J2	۱۳.۱۹	۱۰۳.٦۷	۰.٦۸
J3	۱۱.٤۹	۹۰.٦۷	۰.٦٦
J4	۱٥.٤۳	۱۱۰.٦۷	۰.٦۹
J5	۱۲.۹۱	۹۹.۰۸	۰.٦۷
J6	۱۳.٥٤	۱۰٥.٥۰	۰.٦۸

نتایج به دست آمده نشان داد که بر اساس ضریب توافقی حاصل از نظرات پاسخ‌دهندگان ارتباط بین آن‌ها و مؤلفه‌های مربوطه مورد تایید است. ضمناً با توجه به آماره آزمون کای –دو مشخص گردید که این ارتباطها معنی‌دار هم هستند. آماره آزمون تی هر کدام از مؤلفه‌ها نیز بیشتر از مقدار بحرانی که ۱.٦٤ است شده و آماره آزمون کای – دو همه گام‌ها بیشتر از عدد ۹.٤٨ مقدار بحرانی شده است که این امر اثبات می‌کند تمام مؤلفه‌ها با الگوی مورد نظر ما ارتباط بسیار خوب و بالایی دارند.

۳-٤- مدل‌سازی ساختاری تفسیری چارچوب با استفاده از نرم‌افزار PLS

در این بخش به مدل‌سازی معادلات ساختاری با استفاده از روش حداقل مربعات جزئی با استفاده از نرم‌افزار PLS پرداخته شده و برازش چارچوب اندازه‌گیری و مورد بررسی قرار می‌گیرد. سپس با بررسی ضرایب معناداری مربوط به هر یک از گویه‌ها و ابعاد تشکیل‌دهنده چارچوب، نسبت به تائید و یا رد صحت روابط اجزاء تشکیل‌دهنده مدل اقدام می‌گردد. روش مدل‌سازی معادلات ساختاری با رویکرد حداقل مربعات جزئی توسط ولد (۱۹۷٤) ابداع گردید و در ادامه نسخه پیشرفتهتر این روش توسط لمولر (۱۹۸۹) ارائه گشت. از جمله دلایل استفاده از رویکرد حداقل مربعات جزئی می‌توان به حجم کم نمونه، داده‌های غیرنرمال، مدل‌های اندازه‌گیری از نوع سازنده، قدرت پیش‌بینی مناسب، پیچیدگی مدل، تعداد زیاد سازهها و یا شاخص‌ها، تحقیق اکتشافی، توسعه تئوری و نظریه، استفاده از متغیرهای طبقه‌بندی شده و برر سی همگرایی اشاره نمود.[25]

شکل (۵) چارچوب اولیه طراحی شده در نرم‌افزار PLS را نشان می‌دهد.



شکل (۵)، چارچوب اولیه طراحی شده در نرم‌افزار PLS

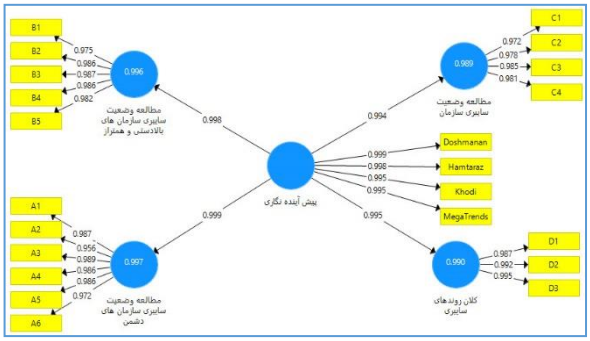
۱-۳-٤- سنجش بارهای عاملی

بارهای عاملی از طریق محاسبه مقدار همبستگی شاخص‌های یک سازه با آن سازه محاسبه می‌شوند که اگر این مقدار برابر و یا بیشتر از ۰.٤ شود، موید 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

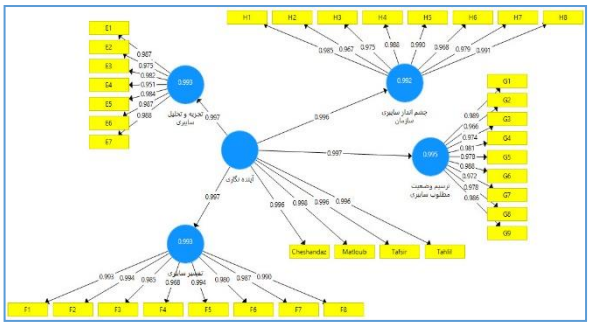
قابل قبول است. البته برخی عدد ۰.۵ را به‌عنوان مقدار ملاک بارهای عاملی ذکر نموده‌اند. نکته مهم در اینجا اینست که اگر محقق پس از محاسبه بارهای عاملی بین سازه و شاخصهای آن با مقادیری کمتر از ۰.٤ مواجه شود، باید آن شاخص‌ها (سؤالات پرسشنامه) را اصلاح نموده و یا از پژوهش خود حذف نماید. [26]

در این تحقیق همانگونه که از شکل‌های (٦) تا (۸) مشخص است، تمامی سؤالات دارای ضرایب بارهای عاملی بیشتر از معیار هستند که نشان از مناسب بودن این معیارها و اجزاء دارد.

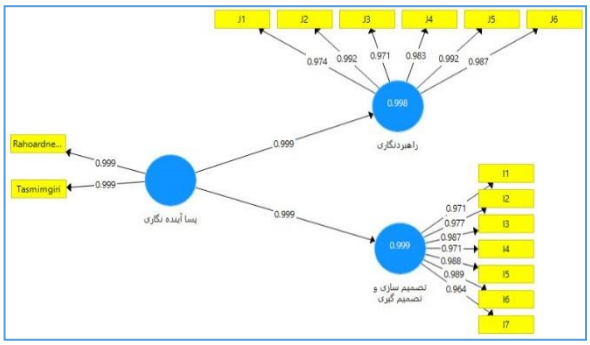
با توجه به آنچه مطرح شده و همچنین بر اساس بارهای عاملی که تماماً بیشتر از ۰.٤ و حتی بیشتر از ۰.۵ هستند، می‌توان گفت که بخش‌های سه گانه چارچوب پیشنهادی از پایایی مطلوبی برخوردار است.



شکل (٦)، ضرایب بار عاملی بخش پیش آینده‌نگاری



شکل (۷)، ضرایب بار عاملی بخش آینده‌نگاری

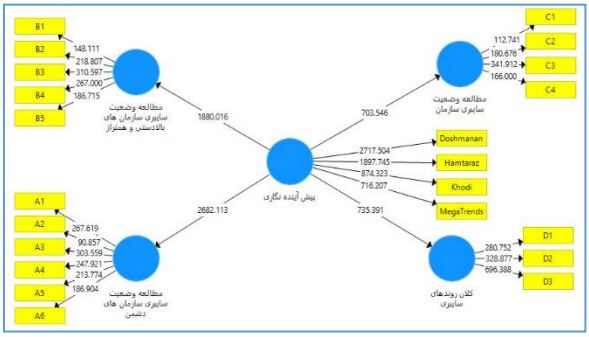


شکل (۸)، ضرایب بار عاملی بخش پسا آینده‌نگاری

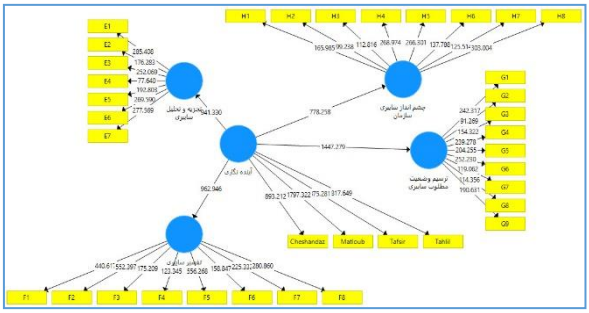
۲-۳-٤- ضریب معناداری

برای اینکه ضرایب معناداری برای چارچوب قابل قبول باشد بایستی اعداد محاسبه شده از ۱.۹٦ حداقل آماره آزمون بیشتر باشد [25]. از این رو با استفاده از محاسبه آماره تی در نرم‌افزار برای بخش‌های مختلف چارچوب این ضریب بررسی شد.

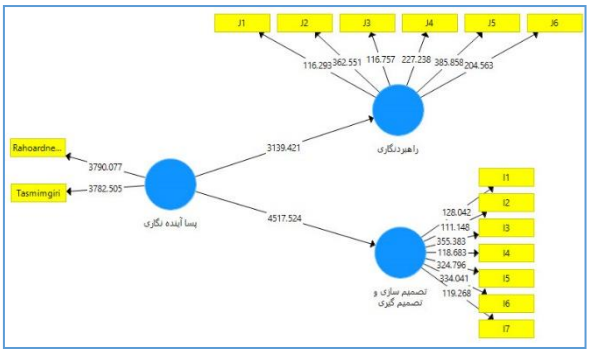
با توجه به به اعداد به دست آمده که تماماً بیشتر از ۱.۹٦ است، مشخص شد که بخش‌های سه گانه چارچوب پیشنهادی از ضریب معناداری بسیار مطلوبی برخوردار است. این مهم را می‌توان در شکل‌های (۹) تا (۱۱) مشاهده نمود.



شکل (۹)، محاسبه ضریب معناداری بخش پیش آینده‌نگاری



شکل (۱۰)، محاسبه ضریب معناداری بخش آینده‌نگاری



شکل (۱۱)، محاسبه ضریب معناداری بخش پساآینده‌نگاری

۳-۳-٤- ضریب R^2

یکی از معیارهایی که برای بررسی برازش مدل ساختاری در یک پژوهش، ضرایب R^2 مربوط به اجزاء چارچوب است. این معیار برای متصـــل کردن بخش اندازه‌گیری و بخش ســـاختاری مدل‌سازی معادلات ساختاری به کار می‌رود. R^2 معیاری است که نشان از تأثیر یک جزء چارچوب بر یک جزء دیگر چارچوب دارد و مقدار آن تنها برای سازه‌های درون‌زا چارچوب محاسبه می‌گردد و در مورد سازه‌های برون‌زا، مقدار این معیار صفر است. سه مقدار ۰.۱۹، ۰.۳۳ و ۰.٦۷ به‌عنوان مقدار ملاک برای مقادیر ضعیف، متوسط و قوی R^2 در نظر گرفته می‌شود. [27]

میزان محاسبه این ضریب برای اجزاء شکل دهنده چارچوب پیشنهادی به صورت جدول (۱۳) است.

جدول (۱۳)، ضریب R^2 اجزاء شکل‌دهنده چارچوب

بخش چارچوب	جزء شکل دهنده چارچوب	ضریب R^2
پیش آینده‌نگاری	مطالعه وضـعیت سـایبری سـازمان‌های دشمن	۰.۹۹۷
	مطالعه وضـعیت سـایبری سـازمان‌های بالادستی	۰.۹۹٦
	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
پساآینده‌نگاری	تصمیم‌سازی و تصمیم‌گیری	۰.۹۹۹
	راهبردنگاری	۰.۹۹۸

با توجه به ضرایب به دست آمده معلوم می‌شود که مقدار ملاک R^2 در حالت بسیار قوی ارتباط اجزاء چارچوب را تائید می‌نماید.

٤-۳-٤- معیار Q^2

این معیار قدرت پیش بینی مدل را مشخص می‌سازد. مدل‌هایی که دارای برازش بخش ســـاختاری قابل قبول هســـتند، باید قابلیت پیش‌بینی شاخص‌های مربوط به سازه‌های درون‌زای مدل را داشته باشند. بدین معنی که اگر در یک مدل، روابط بین سازه‌ها به درستی تعریف شده باشند، سازه‌ها قادر خواهند بود تا تأثیر کافی بر شاخص‌های یکدیگر گذاشته و از این راه، درستی مدل یا چارچوب تائید شود. مقدار این معیار تنها برای سازه‌های درون‌زای چارچوب که شاخص‌های آن‌ها از نوع انعکاسی است، محاسبه می‌گردد. در صورتی که 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 پیش بینی ضعیف، متوسط و قوی سازه یا سازه‌های برون‌زای مربوط به آن را دارد [28].

مقادیر مربوط به مقدار Q^2 سازه‌های درون‌زای چارچوب در جدول (۱٤) درج شده است.

مقدار Q^2 از طریق محاسبه جمع مربع مقادیر خطا در پیش‌بینی شـاخص‌های سـازه‌ی درون‌زا و جمع مقادیر مربع مربوط به شاخص‌های سازه‌ی برون‌زا به دست می‌آید.

جدول (۱٤)، ضریب Q^2 اجزاء شکل‌دهنده چارچوب

بخش چارچوب	جزء شکل دهنده چارچوب	ضریب Q^2
پیش آینده‌نگاری	مطالعه وضـعیت سـایبری سـازمان‌های دشمن	۰.۹۵۱
	مطالعه وضـعیت سـایبری سـازمان‌های بالادستی	۰.۹۵۸
	مطالعه وضعیت سایبری سازمان	۰.۹٤۱
	کلان روندهای سایبری	۰.۹٦۸
آینده‌نگاری	تجزیه‌وتحلیل سایبری	۰.۹٤۷
	تفسیر سایبری	۰.۹٦۰
	ترسیم وضعیت مطلوب سایبری	۰.۹٤۷
	چشم‌انداز سایبری سازمان	۰.۹٤۸
پساآینده‌نگاری	تصمیم‌سازی و تصمیم‌گیری	۰.۹٤۷
	راهبردنگاری	۰.۹٤۵

بر اساس جدول فوق و با توجه به اینکه ضریب به دست آمده بیشتر از ۰.۳۵ است پس می‌توان مطرح نمود که چارچوب مدنظر از قدرت پیش‌بینی بسیار بالا و قوی برخوردار است.

۵-۳-٤- بررسی برازش مدل کلی

شاخص نکویی برازش[1]، به‌عنوان یک معیار کلی از تناسب مدل برای مدل معادلات ساختاری حداقل مربعات جزئی توسعه یافته است. این شاخص، مجذور ضرب دو مقدار متوسط مقادیر اشتراکی و متوسط ضرایب تعیین است. با این حال، از آنجایی که شاخص نکویی برازش نمی‌تواند به‌طور قابل اعتمادی مدل‌های معتبر را از نامعتبر تشخیص دهد و از آنجایی که کاربرد آن به تنظیمات مدل خاصی محدود می‌شود، محققان باید از 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 بدست می آید. سه مقدار برای ارزیابی این شاخص در نظر گرفته‌اند:

- ضعیف: اگر بین ۱/۰ تا ۲۵/۰ باشد.
- متوسط اگر بین ۲۵/۰ تا ۳٦/۰ باشد.
- قوی: اگر از ۳٦/۰ 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 درون زای مدل است.

شاخص نکویی برازش عددی بین صفر و یک بدست می آید [29].

Communality = 0.8068
R2 = 0.9882

GOF = √0.8068*0.9882 = 0.8020

با توجه به عدد به دست آمده برازش کلی چارچوب با دقت بسیار بالایی مورد تائید قرار می‌گیرد.

۵. نتیجه‌گیری و پیشنهادات

۵-۱- نتیجه‌گیری

هدف این پژوهش طراحی چارچوبی به منظور رویارویی پیش فعالانه با تهدیدات سایبری در ارتش جمهوری اسلامی ایران بود.

امروزه رویکرد اقدامات نسبت به تهدیدات در فضای سایبری از حالت فعالانه به رویکرد پیش فعالانه که یک اقدام کنشگرایانه به قصد از میان بردن امکان حمله قریب‌الوقوع طرف دیگر است تغییر یافته و سازمان‌ها، نهادها و حتی افرادی شخصی به جای اینکه منتظر وقوع یک رویداد بنشینند از قبل اقداماتی در جهت کاهش آسیب و حتی برطرف نمودن آن انجام می‌دهند.

با توجه به آنچه گذشت و نظر به اهمیت وجودی تهدیدات روزافزون و سرشار از دگرگونی فضای سایبر، رویکرد پیش فعالانه برای این فضا امری اجتناب‌ناپذیر می‌نماید.

پژوهش حاضر با این رویکرد و به‌منظور بکارگیری قابلیت‌های آینده‌نگاری در مواجه پیش فعالانه با تهدیدهای سایبری در سه بخش پیش آینده‌نگاری، آینده‌نگاری و پسا آینده‌نگاری به انجام رسید. بخش پیش آینده‌نگاری شامل چهار زیربخش و ۱۸ مؤلفه، بخش آینده‌نگاری شامل چهار زیربخش و ۳۲ مؤلفه و در نهایت بخش پساآینده‌نگاری شامل دو زیربخش و ۱۳ مؤلفه است.

بررسی برازش کلی مدل در نرم‌افزار PLS و با کمک داده‌های استخراجی از نرم‌افزار SPSS حاصل گردد. در نهایت با استفاده از نرم‌افزار Edraw Max چارچوب نهایی ترسیم گردید که به صورت شکل (۱۲) است.

برای ترسیم چارچوب نهایی عبارات تلخیص شده‌ای به مؤلفه‌های زیربخش‌ها اختصاص یافت که در شکل به خوبی قابل مشاهده است.

1 - Goodness Of Fit

۲-۵- پیشنهادات

• با در نظر گرفتن چارچوب ارائه شـــده، به‌منظور رویارویی پیش فعالانه ارتش جمهوری اســـلامی ایران با تهدیدهای سایبری، پیشنهادهای اجرایی زیر ارائه می‌گردد:

• در مرحله پیش آینده‌نگاری معاونت فاوا آجا و نیروهای چهارگانه آن با همکاری قرارگاه جنگ‌های نوپدید آجا، پایش و رصـــد فناوری‌های نوین و تهدیدهایی که از جانب آن‌ها متوجه بدنه ســایبری آجا (تجهیزاتی و ســرمایه انسـانی) می‌گردد، شـناسـایی، احصـاء و در دسـت اقدام قرار گیرند.

• در مرحله پیش آینده‌نگاری در راسـتای تعاملات فی مابین و برقراری بسـتری به‌منظور تبادل دانش بین سـازمانی، معاونت فاوا اجا و قرارگاه جنگ‌های نوپدید ارتباط کارآمدی با سـازمان پدافند غیرعامل کشـور و فرماندهی مرکز عملیات سایبری سپاه پاسداران انقلاب اسلامی ایران برقرار نمایند تا از این طریق در زمـان‌هـای مورد نیـاز همکـاری و تعـامـل هم‌افزار صورت پذیرد.

• در مرحله پیش آینده‌نگاری با رویکرد اثربخشـــی ســـازمانی و به‌عنوان یک اقدام راهبردی مدیریت منابع دقیق در کلیـه یگـان‌هـای تـابعـه اجـااز طریق فرمـانـدهی عملیـات سایبری آجا محقق گردد.

• در مرحله پیش آینده‌نگاری و با نگاه بلندمدت با تخصـیص بودجه مازاد زمینه آموزش ســرمایه‌های انســانی حوزه سایبر آجا فراهم گردد.

• در مرحله پیش آینده‌نگاری و با امعان نظر به اینکه در مجامع و کنفرانس‌هـای علمی، آخرین رصـــد تحولات فناورلنه صـــورت می‌پذیرد، با محوریت معاونت فاوا آجا و قرارگاه جنگ‌های نوپدید مقالات و پژوهش‌های ارائه شـــده در این همایش‌ها مورد نقد و بررسی و واکاوی قرار گیرند.

• در مرحلـه آینـدمنگـاری و بـا رویکرد تحلیلی، تجزیه‌وتحلیل دائم ترافیک شـبکه در دسـتور کار معاونت‌ها فاوا و فرماندهی‌های ســایبری آجا قرار گیرد. این موضـــوع امروزه بـه‌عنوان یکی از قوی‌ترین و مؤثرترین راهکـارهـا در جهت شناسایی تهدیدهای سایبری مورد توجه قرار می‌گیرد.

• در مرحلـه آینـده‌نگـاری و بـا رویکرد تحلیـل امنیتی، ارکسـتراسـیون امنیتی تحت مدیریت و کنترل یک رابط واحد به‌طور موثر رویدادهای امنیت ســایبری را مشـــاهده، درک، تصمیم‌گیری و در مورد آن‌ها اقدام کند.

• در مرحله آینده‌نگاری معاونت فاوای آجا با همکاری ســـایر بخش‌های مرتبط از جمله 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

• در مرحله پساآینده‌نگاری و در بخش راهبرد به‌منظور تبدیل دانش به دست آمده به راهبردها و طرح‌های پیشنهادی و تـوســـعـه درک انـتـخـاب‌هـای راهـبـردی در مـیـان تصـــمیمگیرندگان، ارزیابی گزینه‌های راهبردی بعمل آمده و درک وسیعی از گزینه‌های راهبردی ایجاد شود تا این ارزیابی متناوب و پیگیری فرآیند پیاده‌سازی تصـمیم‌گیری و اصـلاح مسیر به‌صورت مستمر در دست اقدام قرار گیرد.

همچنین با توجه به نتایج پژوهش حاضـــر و محدودیت پژوهشـگر در خصـوص پرداختن به همه جوانب موضـوع پژوهش و آشـکارسـازی 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:

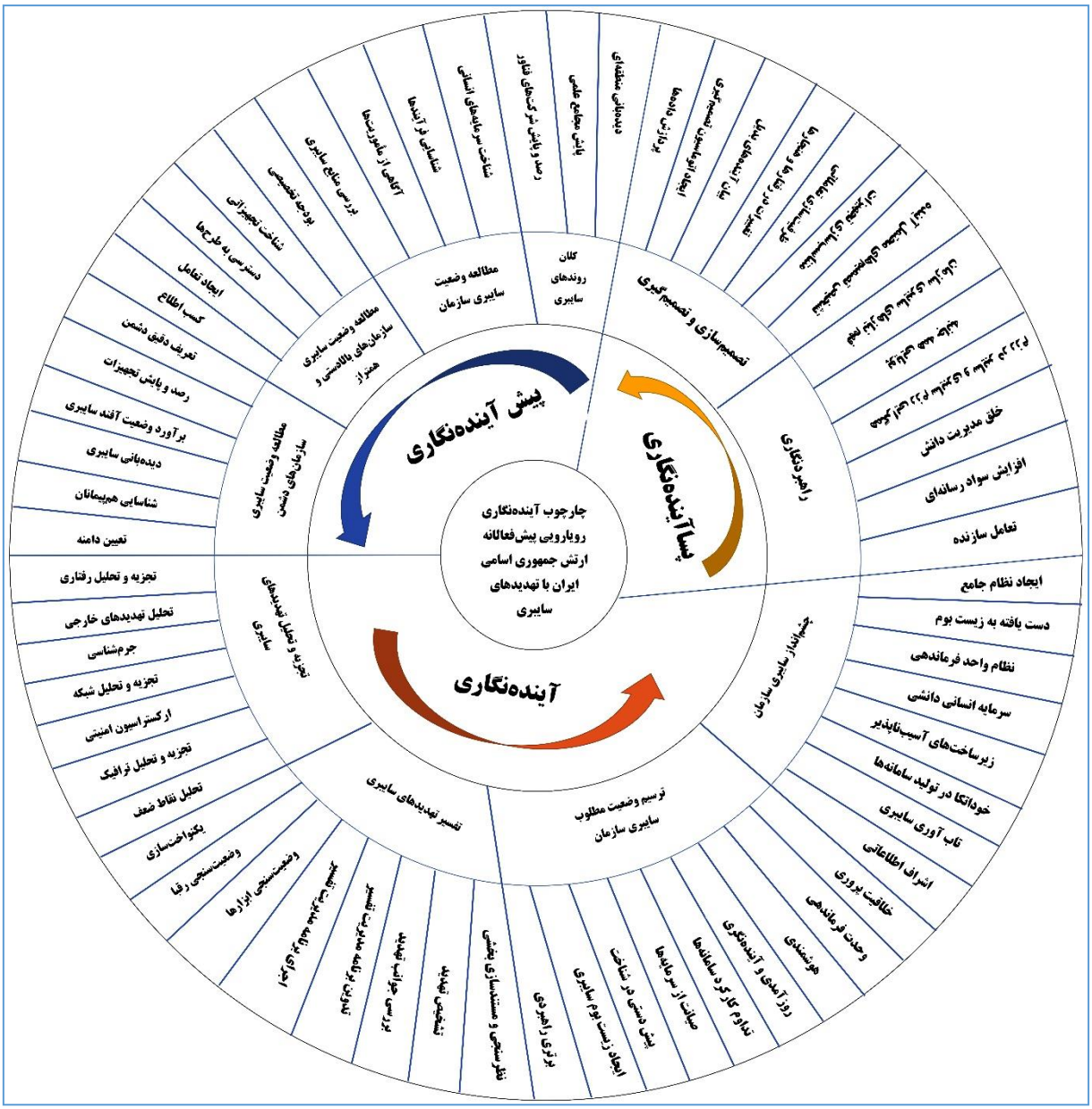
• تدوین سـناریوهای فراروی ارتش جمهوری اسـلامی ایران به منظرو مقابله پیش فعالانه با تهدیدهای ســـایبری در افق میان مدت؛

• تبیین ضـــرورت‌های گذر از پدافند ســایبری به آفند سایبری در مواجه پیش‌فعالانه با تهدیدهای سایبری؛

• تدوین ره‌نگاسـت سـایبری ارتش جمهوری اسـلامی ایران در مقابله پیش فعالانه با تهدیدهای سایبری؛

• طراحی چـارچوب دفـاع پیش فعـالانـه بـا رویکرد امادگی مقابله با کلان روندهای سایبری

- طراحی چارچوب نظام یکپارچه سایبری ارتش جمهوری اسلامی ایران در دفاع پسش دستانه با تهدیدهای سایبری؛
- طراحی مدل ارزیابی قدرت سایبری ارتش جمهوری اسلامی در مواجه با تهدیدهای هوشمند مبتنی بر کلان روندهای سایبری.



شکل (۱۲)، چارچوب نهایی پژوهش

٦. قدردانی

از مشارکت و همراهی اساتید و خبرگان توانمندی که در مراحل مختلف این پژوهش، دانش خویش را سخاوت‌مندانه در اختیار محققان قرار دادند، تشکر و قدردانی می‌نماییم.

۷. منابع و مراجع

[۱]	آقایی، محسن. معینی، علی. عرب سرخی، ابوذر. محمدیان، ایوب. و زارعی، علی اصـــغر. , "ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی،" *امنیت ملی*, جلد ۹(۳۲)، 1398 ,.201-231 .pp.
[۲]	ب. ک. محسن.، "طراحی استراتژی دفاعی در برابر حملات سـایبری و فیزیکی-سـایبری در سـیسـتم قدرت.،" رسـاله دکتری، دانشکده فنی و مهندسی، , دانشگاه اصفهان.، ۱۴۰۰.
[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]	J. Ratcliffe, "Property futures the art and science of strategic foresight," *Journal of Property Investment & Finance*, vol. 38(5), pp. Pp 483-498, 2020.
[6]	L. Zaidi, "Worldbuilding in science fiction, foresight and design," *Journal of Futures Studies*, vol. 23(4), 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), 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. 102916, 2022.
[9]	Fergnani, A. & Cooper, B. , "Metamodern futures: Prescriptions for Metamodern foresight," *Futures*, vol. Volume 149, no. ISSN 0016-3287., p. 103135, 2023.
[10]	S. Saxena, "National open data frames across Japan, The Netherlands and Saudi Arabia: role of culture," *foresight*, vol. 20(1), pp. Pp123-134, 2018.
[11]	Pant, P., Gupta, V. B., Khanna, A., & Saxena, N., "Technology foresight study on assistive technology for locomotor disability," *Technology and Disability*, vol. 29(4), pp. Pp163-171, 2018.
[12]	Cambridge, "Framework. Retrieved October 18, 2018, from https://dictionary.cambridge.org/dictionary/english/framework," Cambridge Dictionary., 2018.
[13]	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), pp. Pp 60-63, 2019.
[14]	Zahraei, S. M., Kurniawan, J. H., & Cheah, L., "A foresight study on urban mobility: Singapore in 2040.," *foresight*, vol. 22(1), pp. 37-52, 2020.
[15]	Hines, A., & Bishop, P. C. , "Framework foresight: Exploring futures the Houston way," *Futures*, vol. 51, p. Pages 31–49, 2013.
[16]	"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.
[17]	Pronina, Y. O., Bogdan, V. V., & Novruzova, O. B., "Foresight: outlook for the legal framework of the national legal system in the future. In Scientific and Technical Revolution: Yesterday, Today and Tomorrow," in *Springer International* , 2020.
[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), pp. 331-344., 2023.
[20]	Yüksel, N., & Çifci, H. , "A new model for technology foresight: Foresight periscope model (FPM).," *In 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, pp. 807-817, 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]	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.
[26]	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), pp. 1-14, 2021.
[27]	J. T. Amora, "Convergent validity assessment in PLS-SEM: A loadings-driven approach.," *Data Analysis Perspectives Journal*, vol. 2(3), pp. 1-6, 2021.
[28]	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.
[29]	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.
[۳۰]	ا. علی.، "طراحی الگوی مفهومی پایش تهدیدات سایبری جمهوری اسلامی ایران،" دانشگاه عالی دفاع ملی.، تهران، ۱۳۹۹.
[۳۱]	م. پ. مهدی، "عوامل مؤثر بر امنیت سایبری ارتش جمهوری اسلامی ایران (مطالعه موردی ستاد ارتش جمهوری اسلامی ایران)،" دانشگاه فرماندهی و ستاد ارتش، تهران، ۱۳۹۹.
[۳۲]	ایجابی، ابراهیم. کولیوند، خلیل.، "واکاوی تهدیدات امنیتی شبکه‌های رایانه‌ای سازمان‌ها با رویکرد آینده‌پژوهی (مطالعه موردی ستاد فرماندهی نیروی پدافند هوایی آجا)،" *آینده‌پژوهی دفاعی*، ۱۴۰۱.
[۳۳]	آقایی، محسن. معینی، علی. عرب سرخی، ابوذر. محمدیان، ایوب. و زارعی، علی اصغر.، "ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت های حیاتی،" *امنیت ملی*، جلد ۹(۳۲)، 1398 ,201-231 .pp.
[۳۴]	قربانی، ولی اله. و ثقفی، کامیار، "ارائه مدل کلان امنیت اطلاعات فضای سایبر در جمهوری اسلامی ایران،" *امنیت ملی*، جلد ۹(۳۳)، pp. ۳۵۳-۳۱۵، ۱۳۹۸.
[35]	H. Çifci, "TECHNOLOGY FORESIGHT AND MODELING: TURKISH CYBERSECURITY FORESIGHT 2040," MIDDLE EAST TECHNICAL UNIVERSITY, 2019.
[36]	Raban, Y., & Hauptman, A., "Foresight of cyber security threat drivers and affecting technologies.," *foresight*, vol. 20(4), pp. 353-363., 2018.