طراحی مدل قابلیت‌های سازمانی در حوزه امنیت سایبری

حسن کاویانی[1]، ناصر میر سپاسی[2]

تاریخ دریافت: ۱۴۰۰/۰۶/۰۱ تاریخ پذیرش: ۱۴۰۰/۰۷/۲۵

فصلنامه مطالعات راهبردی بسیج، سال بیست چهارم، شماره ۹۲، پاییز ۱۴۰۰

20.1001.1.1735501.1400.24.92.5.9

چکیده :

هدف اصلی: در دهه‌های اخیر و هم‌زمان با افزایش ضریب نفوذ اینترنت و فضای سایبری، طیف وسیعی از دولت‌ها به‌منظور محافظت از زیرساخت‌ها و شهروندان خود در مقابل تهدیدات سایبری اقدام به بازطراحی و بازنگری در سیاست‌ها، ساختارها و راهبردهای خود نموده‌اند. یکی از مهم‌ترین این اقدامات، شناسایی قابلیت‌های موردنیاز سازمان‌های متولی امنیت سایبری در جهت تحقق وظایف و مأموریت‌های خود است. ازاین‌رو در این تحقیق به طراحی مدل قابلیت‌های سازمانی در حوزه امنیت سایبری به‌عنوان هدف اصلی تحقیق مبادرت نموده‌ایم

روش پژوهش: پژوهش حاضر از منظر هدف، اکتشافی است که از رویکردی ترکیبی(آمیخته) تبعیت می‌کند. در گام اول پس از بررسی پیشینه، نظریات و اسناد بالادستی و مصاحبه با ۸ نفر از خبرگان حوزه امنیت سایبری مدل قابلیت‌های سازمانی در حوزه امنیت سایبری شامل ۴۵ شاخص، ۲۳ مؤلفه و ۷ بعد استخراج گردید. در مرحله دوم بر اساس اجزاء مدل مستخرج از مطالعات اکتشافی پرسشنامه‌ای شامل ۴۵ سؤال تنظیم و روایی و پایایی آن با استفاده از نظریات ۱۲ نفر از خبرگان مورد تائید قرار گرفت. در مرحله سوم بر اساس نظریات ۴۳ نفر از خبرگان علمی و اجرایی حوزه امنیت سایبری کشور، مطلوبیت اجزاء مدل با استفاده از نرم‌افزارهای spss و pls مورد ارزیابی قرار گرفت.

یافته‌ها: بر اساس یافته‌ها مدل قابلیت‌های سازمانی در حوزه امنیت سایبری شامل هفت بعد منابع انسانی پویا، فرهنگ جهادی، تاب‌آوری سایبری، دوسوتوانی سازمانی، سرمایه‌های سازمانی، تیم‌های

---

[1] - (نویسنده مسئول) دکتری مدیریت دولتی، پژوهشگر دانشگاه پدافند هوایی خاتم الانبیاء (ص) ، تهران، ایران
Hassan.kavyani@gmail.com

[2]- استاد، گروه مدیریت دولتی، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران
hassan.kavyani61@yahoo.com

قدرتمند پاسخگوی سایبری و رهبران تحول‌آفرین است؛ که بر اساس این ابعاد پیشنهادهای کاربردی لازم ارائه‌شده است.

واژگان کلیدی:

امنیت سایبری، قابلیت‌های سازمانی، شایستگی، جمهوری اسلامی ایران

۱- مقدمه و بیان مسئله

۱-۱- مقدمه موضوع:

توسعه فضای سایبری را می‌توان مهم‌ترین عامل تغییر سیمای جوامع بشری قلمداد نمود. فضای سایبری یک محیط الکترونیکی و غیر فیزیکی است که به‌مثابه رشته‌های عصبی در بدن انسان، اطلاعات در آن ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شوند. در این فضا با بهره‌گیری از فناوری‌های نوین تحولات شگرفی در حوزه‌های اقتصادی، سیاسی، اجتماعی و فرهنگی صورت پذیرفته است. بااین‌وجود، اینترنت و فناوری‌های نوین ارتباطی دولت‌ها را در مقابل چالش‌های امنیتی جدیدی قرار داده است. هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری ازاین‌رو در دهه‌های اخیر بسیاری از کشورها ضمن تأمین زیرساخت‌های قانونی و حقوقی موردنیاز در حوزه امنیت سایبری با ایجاد و بازطراحی ساختارها و نهادهای دفاعی و امنیتی خود درصدد مواجهه با تهدیدهای سایبری و کاهش آسیب‌پذیری‌های خود در این حوزه برآمده‌اند.

در حوزه فضای سایبری در حال حاضر کشور با چالش‌های اساسی در حفظ اطلاعات ملی کشور و امنیت سایبری مواجه است برابر برخی آمارها در سال ۱۳۹۴ روزانه ۱۳ تا ۱۴ هزار حمله اینترنتی علیه کشور صورت می‌گرفته است (فاضلی و همکاران، ۱۳۹۴) درحالی‌که تعداد حملات شناسایی و دفع شده آن در سال ۱۳۹۸ به‌صورت میانگین به روزانه بیش از ۹۰ هزار حمله افزایش‌یافته است (معاون قرارگاه سایبری سازمان پدافند غیرعامل،۱۳۹۸) علی‌هذا نگاهی به سه حمله بزرگ سایبری بدافزارهای استاکس نت[1] دوکو[2] و فلیم[3] و نیز حمله سایبری به شبکه توزیع سوخت کشور در آبان ماه سال ۱۴۰۰ نشان می‌دهد که وسعت و ابزارهای بکار گرفته‌شده در این حملات به‌مرور تکمیل‌تر شده‌اند و هر بار بر درجه تخریب آن‌ها افزوده‌شده است. ازاین‌رو در دهه‌های اخیر موضوع دفاع و امنیت سایبری در حوزه سیاست‌گذاری کلان مستقیماً در قالب سیاست‌های کلی امنیت فضای تولید و تبادل

1-Stuxnet
2- Duq
۳،۲u
3- Flame

اطلاعات و ارتباطات (۱۳۸۹) و به‌صورت موردی در سیاست‌های کلی پدافند غیرعامل (۱۳۸۹)، سیاست‌های کلی برنامه ششم توسعه (۱۳۹۴) و نیز وظایف و مأموریت‌های شورای عالی فضای مجازی (۱۳۹۴) موردتوجه قرارگرفته است. در حوزه اجرایی نیز تأسیس و یا بازنگری در مأموریت‌ها، ساختار و وظایف سازمان‌هایی چون مرکز بررسی‌های راهبردی فضای سایبری، سازمان پدافند غیرعامل، شورای عالی فضای مجازی، پلیس فتا، دادسرای جرائم رایانه‌ای و سازمان امنیت سایبری سپاه پاسداران انقلاب اسلامی نیز حاکی از اهمیت و جایگاه ویژه دفاع و امنیت سایبری در سطح ملی دارد.

۱-۲- ضرورت موضوع

در حوزه امنیت سایبری ایجاد، توسعه و حفظ قابلیت‌های سازمانی[۱] و به عبارتی توانایی و ظرفیت‌های منحصربه‌فرد و غیرقابل تقلید به‌عنوان یکی از ارکان اصلی کاهش آسیب‌پذیری‌ها، مواجه مناسب با تهدیدات سایبری و نیز وارد نمودن ضربات سهمگین به دشمنان قلمداد می‌گردد بدین‌جهت طراحی مدل‌ها و الگوهای قابلیت‌های سازمانی در حوزه امنیت سایبری بیش از هرزمان دیگری موردتوجه دولت‌ها و نیز مؤسسات فعال در این حوزه قرارگرفته است. مقوله‌ای که علی‌رغم تصریح در حکم انتصاب شورای عالی فضای مجازی (۱۳۹۴) و نیز سند راهبردی پدافند سایبری کشور (۱۳۹۴) تاکنون چارچوب اجرایی مناسب و جامعی در قالب قانون، تصویب‌نامه و یا آئین‌نامه اجرایی برای آن تدوین نگردیده است. موضوعی که مؤید مغفول ماندن این موضوع راهبردی در بدنه اجرایی کشور است. در حوزه علمی نیز باوجود برخی تلاش‌های انجام‌شده در راستای طراحی و معرفی قابلیت‌های موردنیاز سازمان‌ها در حوزه‌های امنیتی و دفاعی لیکن تلاش منسجم و جامعی در خصوص تبیین قابلیت‌های سازمانی لازم در حوزه امنیت سایبری انجام‌نشده است

۱-۳- اهمیت موضوع

در تحقیقات و اسناد مرتبط با حوزه امنیت سایبری و حوزه‌های امنیتی و دفاعی موضوع ایجاد، ارتقاء و نهادینه‌سازی قابلیت‌ها و ویژگی‌های منحصربه‌فرد در سطوح فردی، سازمانی و گروهی مورد تأکید قرارگرفته است. به عبارتی یکی از مهم‌ترین الزامات تحقق حکمرانی سایبری و نیز توسعه راهبردها و سیاست‌های اثربخش در حوزه امنیت سایبری شناخت و توسعه قابلیت‌های سازمانی می‌باشد(سازمان امنیت سایبری سنگاپور، ۲۰۲۱) (دانشگاه فونیکس، ۲۰۱۸) (اداره فناوری اطلاعات عمان، ۲۰۱۷) (شورای امنیت سایبری، ۲۰۱۴) این قابلیت‌ها به دنبال تبیین چگونگی استفاده از منابع و دارایی‌های سازمان در جهت

۱- Capability

پیش‌بینی، مواجهه و پاسخگویی به تهدیدات سایبری می‌باشند. ازاین‌رو عوامل ایجابی ذیل باعث اهمیت این تحقیق‌شده‌اند:

الف) طراحی مدل‌های قابلیت‌های سازمانی منطبق با بوم ایران و حوزه امنیت سایبری می‌تواند با ایجاد ابزارهای مناسب به‌منظور راهبری و مدیریت حوزه موردمطالعه در سه سطح فردی، گروهی و سازمانی به افزایش اقتدار امنیتی و دفاعی منتهی می‌گردد.

ب) توسعه مدل‌های موجود قابلیت‌های سازمانی متناسب با بوم ایران، رشته مدیریت دولتی و صنعت امنیت سایبری از دیگر وجوه اهمیت تحقیق حاضر است.

ج) باعث ایجاد فهم، بینش و معیارهای مشترک در خصوص چگونگی تحقق سیاست‌های کلی نظام در حوزه‌های امنیت فضای تولید و تبادل اطلاعات و ارتباطات، پدافند غیرعامل و سند راهبردی پدافند سایبری و نیز تحقق اسناد بالادستی می‌گردد.

د) باعث کاهش خلأ تحقیقاتی و پژوهشی در خصوص قابلیت‌های سازمانی موردنیاز سازمان‌های مسئول در حوزه امنیت سایبری کشور می‌شود.

۱-۴- مسئله اصلی

بسیاری از صاحب‌نظران در حوزه مطالعات سازمانی معتقدند که قابلیت‌های سازمانی به‌عنوان عامل اصلی تحقق مزیت رقابتی پایدار بر اساس صنعت و نوع سازمان متفاوت می‌باشند (ریما و همکاران، ۲۰۲۱) ازاین‌رو با توجه به مغفول ماندن طراحی و تدوین مدل جامع قابلیت‌های سازمانی در حوزه امنیت سایبری و مبتنی بر اقتضائات نظام مقدس جمهوری اسلامی ایران به‌عنوان مسئله اصلی پژوهش، این سؤال ذهن نویسندگان را به‌عنوان چالش و دغدغه اصلی به خود معطوف نموده است که مدل قابلیت‌های سازمانی در حوزه امنیت سایبری چگونه است؟

در این راستا دستیابی به هدف اصلی تحقیق، سؤالات فرعی به شرح ذیل تنظیم‌شده است:

۱) ابعاد و مؤلفه‌های مدل قابلیت‌های سازمانی در حوزه امنیت سایبری کدام‌اند؟

۲) میزان مطلوبیت ابعاد و مؤلفه‌های مدل قابلیت‌های سازمانی حوزه امنیت سایبری به چه اندازه می‌باشد؟

نحوه سازمان‌دهی مقاله

در این مقاله به‌تناسب مسئله اصلی و اهداف تبیین شده مطابق شکل (۱)، در مرحله اول بر اساس نتایج مطالعات اکتشافی (مرور ادبیات و پیشینه تحقیق و مصاحبه نیمه ساختاریافته با ۸ نفر از خبرگان) مدل مفهومی اولیه طراحی گردید. در مرحله دوم روایی صوری و پایایی اجزاء مدل با نظرخواهی از تعداد ۱۲ نفر از خبرگان موردبررسی قرار گرفت. در مرحله سوم

بر اساس نظریات ۴۳ نفر از خبرگان علمی و اجرایی حوزه امنیت سایبری کشور، مطلوبیت اجزاء مدل با استفاده از نرم‌افزارهای spss و pls مورد ارزیابی قرار گرفت.

شکل (۱): مراحل اجرایی تحقیق

۲- ادبیات موضوع و پیشینه

قابلیت‌های سازمانی مفهومی نسبتاً مبهم در مطالعات سازمانی می‌باشد. این مفهوم برگرفته از دیدگاه مبتنی بر منابع[1] در مدیریت راهبردی می‌باشد. در حوزه مدیریت راهبردی دو رویکرد عمده دیدگاه سازمان صنعتی[2] و دیدگاه مبتنی بر منابع مطرح می‌باشند. در رویکرد سازمان صنعتی عوامل تعیین‌کننده عملکرد شرکت و کسب مزیت رقابتی پایدار در خارج از بنگاه فرض می‌شوند لذا این عوامل در ساختار صنعت تبیین می‌گردند و تأکید اصلی بر نقش محیط، موقعیت‌یابی و بازار است. (جروین[3] و همکاران، ۲۰۱۰) در دیدگاه مبتنی بر منابع بر ضرورت تمرکز بر منابع سازمانی به‌منظور کسب مزیت رقابتی پایدار تأکید می‌گردد. بر اساس این دیدگاه طیف وسیعی از منابع در سازمان وجود دارد که می‌تواند در ایجاد مزیت رقابتی پایدار نقش اساسی ایفا نمایند. (آرمسترانگ[4] و همکاران، ۲۰۱۹) لکن دراین‌خصوص باید به نکته مهم توجه نمود که بر طبق دیدگاه مبتنی بر منابع همه منابع راهبردی نیستند بلکه منابع بادوام، کمیاب و غیرقابل‌فروش راهبردی و بااهمیت فرض می‌شوند.

1- Resource based view
2- Industrial organisation
3- Jeroen , K
4 Armstrong, M

(پانکج[1]،۲۰۰۹) در این نظریه مقصود از قابلیت‌ها، مجموعه‌ای از رفتارهای الگو بردار و تکراری سطح بالاست که سازمان‌ها آن‌ها را آموخته و قادرند این رفتارها را بهتر از رقبا به انجام برسانند. مفهوم قابلیت‌ها نمایانگر هویت و شخصیت سازمان است. به عبارتی قابلیت سازمانی توانایی منحصربه‌فرد سازمان برای کسب مزیت رقابتی (رضایت‌مندی شهروندان و اجری خط‌مشی عمومی) در جهت بهینه ساختن فرآیند دستیابی به اهداف سازمانی می‌باشند (دانایی‌فرد و همکاران، ۱۳۹۴) بااین‌وجود برخی از محققان مفاهیم قابلیت و شایستگی[2]را معادل یکدیگر فرض می‌نمایند و برخی دیگر این دو مفهوم را متفاوت و با کارکردهای متمایز قلمداد می‌نمایند. به‌طور مثال به اعتقاد اولریش شایستگی‌ها به دانش، مهارت‌ها و رفتاری برمی‌گردد که افراد در خلال انجام کارشان نشان می‌دهند لیکن قابلیت‌ها، توانایی‌های جمعی یک سازمان هستند که می‌توانند ماهیت فنی داشته باشند (مانند شناخته شدن سونی به خبرگی در ریز سازی یا نبوغ اپل در طراحی محصول) یا بیشتر اجتماعی تعریف شوند (مانند تأکید پپسی برای پاسخگویی یا کارایی افسانه‌ای خطوط هوایی ساث وست) (اولریش[3]و همکاران،۱۳۸۸:۵۰)

در دهه‌های اخیر تقسیم‌بندی‌های متنوعی از قابلیت‌های سازمانی ارائه‌شده است. کولیس (۱۹۹۴) قابلیت‌های سازمانی را در قالب چهار دسته تقسیم‌بندی نموده است. گروه اول قابلیت‌های سازمانی عبارت از توانایی‌های موردنیاز سازمان برای انجام فعالیت‌های اصلی و عملیاتی می‌باشند. گروه دوم قابلیت‌ها به فعالیت‌های بهبود مستمر اشاره دارد. در گروه سوم قابلیت‌های سازمانی شامل توانایی شناخت ارزش ذاتی سایر منابع و یا توسعه راهبرهای بدیع قبل از رقبا خواهد بود. دسته چهارم قابلیت‌ها به‌عنوان فرا قابلیت‌ها[4]شناخته می‌شوند این سطح به قابلیت‌های یادگیری برای یادگیری اشاره دارد (گورکان و همکاران، ۲۰۱۵) در تقسیم‌بندی دیگری وینتر (۲۰۰۳) آن بخش از قابلیت‌ها را که برای حفظ بقاء سازمان در مقیاس کنونی آن از طریق فروش محصولات فعلی به مشتریان موجود، ضروری هستند، قابلیت‌های صفر یا گروه صفر نامیده است. او از قابلیت‌هایی که به تغییر برنامه‌ریزی‌شده در محصولات، فرآیند تولید، مقیاس کسب‌وکار و یا بازارهای تحت پوشش سازمان منجر می‌شوند به‌عنوان قابلیت‌های سطح یک و به عبارتی قابلیت‌های پویا یاد می‌نماید. (مایلز، ۹۹:۱۳۹۸)

1- Pankaj
2-competency
3-Ulrich, D
4-Meta Capabilities

در این تحقیق قابلیت‌ها به‌عنوان توانایی و ظرفیت منحصربه‌فرد و غیرقابل تقلید سازمانی سطح یک در نظر گرفته‌شده‌اند که کارکنان شایسته و شایستگی‌ها کارکنان نیز بخشی از این قابلیت‌ها محسوب می‌گردند.

امنیت سایبری:

از اوایل دهه ۷۰ میلادی اکثریت تغییر و تحولات مهم و تأثیرگذار ابتدا در حوزه فناوری اطلاعات و ارتباطات صورت پذیرفته است. تحولاتی که در قالب گسترش ارتباطات بین‌المللی و از طریق شبکه‌های جهانی و فضای سایبری[1] زندگی سیاسی، اجتماعی، اقتصادی و فرهنگی مردم و کشورها را به‌صورت چشمگیری تحت تأثیر خود قرار داده است. ازاین‌رو در دهه‌های اخیر از اینترنت و فضای سایبری به‌عنوان قوی‌ترین محرک تغییرات اجتماعی و رونق اقتصادی یادشده است (کمیسیون ملی ارتقاء امنیت سایبری[2]،۲۰۱۶) لکن محیط فناوری اطلاعات و فضای سایبر همانند تمام انقلاب‌های فنّاورانه در کنار مزایای خود معمولاً یک لبه تاریکی و تنگناهای ویژه‌ای با خود ایجاد نموده است، این فنّاوری‌ها با ایجاد تحول شگرف در منابع، نوع و ابزار تهدید هم ازلحاظ کمی (تعداد و تنوع منابع تهدید) و هم ازلحاظ کیفی (پیچیده‌تر شدن و کارآمد شدن ابزارهای سنتی تهدید) ابزارهای تهدید امنیت ملی را در سطح بین‌المللی متحول کرده‌اند بااین‌وجود با توجه به حجم وسیع آسیب‌پذیری‌های فضای سایبری و نیز با اذعان به اینکه فناوری اطلاعات و ارتباطات و به‌ویژه اینترنت در توسعه اقتصادی، سیاسی، فرهنگی و.. کشورها و سازمان‌ها دارای نقشی حیاتی هستند، ضروری است که ضمن حفظ ویژگی‌ها و کارکردهای مثبت، آن‌ها را در برابر حملات و سوءاستفاده‌های احتمالی مقاوم کنیم مقوله‌ای که تحت عنوان امنیت سایبری[3] درصدد شناسایی تهدیدها و آسیب‌پذیری‌ها، تدوین طرح‌های متناسب و اقدام به‌موقع در مقابل حملات سایبری به‌منظور حفاظت از اطلاعات و زیرساخت‌ها می‌باشد (کونگ وهمکاران[4]،۲۰۱۳)

به‌منظور بهبود کارکردهای امنیت سایبری و کاهش آسیب‌پذیری‌های، طراحی مدل‌ها و الگوهای قابلیت‌ها در حوزه امنیت سایبری به یکی از رویکردهای متداول دولت‌ها و مؤسسات خصوصی مبدل گشته است. این مدل‌ها عموماً به‌منظور تقویت امنیت سایبری سازمان‌ها، توانمندسازی سازمان‌ها جهت ارزیابی معیارهای امنیت سایبری، تسهیم دانش و بهترین

1- Cyberspace
2-Commission on enhancing national cybersecurity
3- Cyber security
4- Koong et al

تجارب این حوزه و اولویت‌بندی فعالیت‌ها و سرمایه‌ها برای بهبود امنیت سایبری ارائه گردیده‌اند. (سازمان امنیت سایبری سنگاپور، ۲۰۲۱) (دانشگاه فونیکس، ۲۰۱۸) (وزارت انرژی ایالات‌متحده،۲۰۱۹) این مدل‌ها در حوزه امنیت سایبری غالباً به‌عنوان مدل بلوغ قابلیت‌ها[۱] برای بهبود ابعاد فنی طراحی و ارائه می‌گردند

بررسی دقیق مدل‌های قابلیت‌های سازمانی در حوزه امنیت سایبری مؤید آن است که این الگوها و چارچوب‌ها را می‌توان به دو گونه مدل‌های بلوغ قابلیت‌ها و مدل‌های قابلیت‌های سازمانی تقسیم‌بندی نمود. مدل‌های بلوغ قابلیت‌ها به‌منظور بهبود ابعاد فنی طراحی و ارائه می‌گردند. . اولین مدل بلوغ قابلیت‌ها در حوزه فناوری‌های اطلاعات و ارتباطات در اواسط دهه ۱۹۸۰ توسط موسسه مهندسی نرم‌افزار[۲] ارائه گردیده است(مارسلو و همکاران، ۲۰۱۷) از منظری دیگر و بر اساس رویکرد حاکم بر مطالعات سازمانی برخی دیگر از مدل‌های قابلیت‌های سازمانی بر عوامل و ویژگی‌های منحصربه‌فرد سازمانی متمرکز می‌باشند در این مدل‌ها با نگاهی مدیریتی عوامل مؤثر و موردنیاز برای تحقق اهداف و مأموریت‌ها و کار ویژه‌های تخصصی و فنی به‌عنوان قابلیت‌های سازمانی موردتوجه قرار می‌گیرد. رویکردی که مبنای عمل در تحقیق حاضر می‌باشد از این در این پژوهش سعی شده است با نگاهی جامع‌نگر بر کلیه ابعاد و مؤلفه‌های موردنیاز در سطوح فردی، گروهی و سازمانی تأکید شده و از تأکید بر مسائل فنی اجتناب گردد.

۲-۲- پیشینه پژوهش

درزمینه طراحی مدل قابلیت‌ها در حوزه امنیت سایبری تحقیق‌های فراوانی صورت گرفته است لیکن اغلب این پژوهش‌ها بر طراحی مدل‌های فنی و به عبارتی مدل بلوغ قابلیت‌ها متمرکز بوده‌اند. بااین‌وجود برخی از مهم‌ترین تحقیقات صورت گرفته در خصوص مدل‌های قابلیت سازمانی در حوزه امنیت سایبری به شرح ذیل است.

۱- Cybersecurity Capability Maturity Models

۲ Software Engineering Institute

جدول (۱): خلاصه‌ای از پیشینه تحقیق

نویسندگان- روش استفاده‌شده	اهداف و یا سؤالات اصلی	مهم‌ترین یافته‌ها
ولوی و نیک‌نفس (۱۴۰۰) – آمیخته	شناسایی ابعاد مدل بلوغ، رصد، پایش و هشدار دهی سایبری	ابعاد این مدل شامل: ساختار سازمانی، رهبری و مدیریت، فرهنگ‌سازمانی، مهارت کارکنان، چابکی فرآیندها، یکپارچگی فرآیندها، تعریف فرآیندها، ارزیابی فرآیندها، صاحبان فرآیندها، الگوبرداری از فرآیندها، طراحی فرایندها
وزارت انرژی ایالات‌متحده (۲۰۱۹)- کیفی	طراحی مدل بلوغ قابلیت‌ها در حوزه امنیت سایبری	این مدل بر ۱۰ حوزه مدیریت ریسک، مدیریت پیکربندی، دارایی و تغییرات، مدیریت هویت و دسترسی، مدیریت آسیب‌پذیری و تهدیدات، آگاهی موقعیتی، اشتراک اطلاعات و ارتباطات، پاسخ رویداد و حادثه و تداوم عملیات، مدیریت زنجیره تأمین و وابستگی‌های خارجی، مدیریت نوآوری کاری و مدیریت برنامه امنیت سایبری تمرکز دارد.
نیروی دریایی ایالات‌متحده (۲۰۱۹)- کیفی	شناسایی الزامات تحقق امنیت سایبری	این الزامات عبارت‌اند از: کارکنان متخصص و ماهر، الزامات ساختاری سرمایه‌های ساختاری و ارتباطی فرهنگ‌سازمانی، تاب‌آوری سایبری، فرآیندهای اجرایی
شورای ملی رهبری تاب‌آوری سایبری اسکاتلند (۲۰۱۸) - کیفی	شناسایی عوامل مؤثر بر مدیریت مناسب تهدیدات در حوزه امنیت سایبری مبتنی بر شواهد و تجارب پیشین	ایجاد و حفظ تاب‌آوری سایبری، تغییر و ایجاد فرهنگ یادگیرنده و نهادینه‌سازی نوآوری (دوسوتوانی) به‌عنوان قابلیت‌های اصلی موردنیاز جهت مدیریت صحیح تهدیدات و آسیب‌پذیری‌های این حوزه یادشده است.
وزارت امنیت میهنی ایالات‌متحده (۲۰۱۶)- کیفی	طراحی جعبه‌ابزاری جهت توسعه نیروی کار شاغل در حوزه امنیت سایبری	در این جعبه‌ابزار ۵ ویژگی (قابلیت) چابکی، چندوظیفه‌ای بودن، پویایی، انعطاف‌پذیری و غیررسمی بودن برای تیم‌های امنیت سایبری در نظر گرفته‌شده است.

امیرلی و تقی پور (۱۳۹۹)- مدل ساختاری تفسیری و مقایسه زوجی	طراحی مدل فرآیندی دفاع سایبری	فرآیندهای فرهنگ‌سازی، آموزش و پایش، رصد، تشخیص و نیز نوآوری و خودکفایی به‌عنوان بخشی از قابلیت‌های سازمانی موردنیاز حوزه امنیت سایبری تبیین گردیده‌اند.
تقی پور و همکاران (۱۳۹۸)- آمیخته	طراحی الگوی راهبردی حفاظت از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران	الگوی راهبردی حفاظت از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران مشتمل بر چهار بعد حکمروایی، حقوقی، مدیریت امنیت و عملیات می‌باشد. ظرفیت‌سازی، توانایی راهبری، اقدامات تشخیصی و مدیریت حوادث برخی از مؤلفه‌های مدل نهایی تحقیق را تشکیل می‌دهند.

وجه نوآوری مقاله حاضر نسبت به مطالعات پیشین: واکاوی تحقیقات صورت گرفته در حوزه امنیت سایبری مؤید آن است که علیرغم ازدیاد طراحی و توسعه مدل‌های قابلیت‌های فنی در حوزه امنیت سایبری، موضوع شناسایی قابلیت‌های سازمانی موردنیاز سازمان‌های متولی امر در حوزه امنیت سایبری به‌گونه‌ای جامع و با مدنظر قرار دادن سطوح فردی، گروهی و سازمانی به‌ویژه در داخل کشور چندان موردتوجه قرار نگرفته است موضوعی که به‌عنوان وجه تمایز تحقیق حاضر با سایر تحقیقات مشابه قلمداد می‌گردد.

۳- روش تحقیق

۳-۱- نوع و استراتژی کلی تحقیق

با توجه به هدف پژوهش حاضر و نیز ضرورت تدوین مدلی متناسب با شرایط و زیست‌بوم جمهوری اسلامی ایران دیدگاه خردگرایانه کمّی نمی‌تواند به‌تنهایی مبنای تحقیق قرار گیرد. به همین منظور از رویکردی ترکیبی (آمیخته) به‌منظور شناسایی مدل قابلیت‌های سازمانی در حوزه امنیت سایبری استفاده‌شده است. با عنایت به اینکه هدف اصلی این تحقیق بررسی مسئله یا پدیده‌ای است که در مورد آن شناخت چندانی وجود ندارد می‌توان این تحقیق را در زمره پژوهش‌های اکتشافی قلمداد نمود. ازاین‌رو، بخش اول این تحقیق بدون طرح فرضیه انجام می‌شود و به‌جای آزمودن فرضیه، محقق در پی یافتن پاسخی برای پرسش زیر می‌باشد مدل قابلیت‌های سازمانی در حوزه امنیت سایبری چگونه است ؟

برای پاسخ به این پرسش اصلی، نیازمند پاسخ به سؤال فرعی ذیل هستیم
ابعاد و مؤلفه‌های مدل قابلیت‌های سازمانی در حوزه امنیت سایبری کدام‌اند؟

۳-۲- روش‌های گردآوری و تحلیل داده‌ها

در این پژوهش داده‌های موردنیاز با استفاده از سه روش مطالعات کتابخانه‌ای، مصاحبه با خبرگان و پرسشنامه جمع‌آوری‌شده است. در بخش مطالعات کتابخانه‌ای واکاوی ادبیات و پیشینه تحقیق و نیز اسناد بالادستی موردبررسی دقیق قرار گرفت در بخش دوم اطلاعات موردنیاز با استفاده از مصاحبه با تعداد ۸ نفر از خبرگان گردآوری گردید. در بخش سوم (کمی) داده‌های موردنیاز جهت ارزیابی مطلوبیت مدل، ابعاد و مؤلفه‌های آن با استفاده از پرسشنامه محقق ساخته گردآوری‌شده است.

۳-۳- روش تحلیل داده‌ها

در این تحقیق اطلاعات جمع‌آوری‌شده از مطالعات کتابخانه‌ای و مصاحبه‌های نیمه ساختاریافته با استفاده از روش تحلیل تم مورد تجزیه و تحلیل قرارگرفته است. در بخش کمی نیز تعداد ۴۳ پرسشنامه دریافتی با استفاده از نرم‌افزارهای Spssو Smart pls مورد تجزیه‌وتحلیل قرارگرفته‌اند.

۳-۴- جامعه و نمونه آماری

جامعه آماری این تحقیق در مرحله اول شامل خبرگان حوزه امنیت سایبری (با حداقل ۵ سال اشتغال در مسئولیت مدیریت ارشد در حوزه امنیت سایبری، داشتن مدرک دکترای تخصصی، داشتن مدرک رشته مدیریت در حداقل یکی از مقاطع تحصیلی) می‌باشند. که با استفاده از روش نمونه‌گیری هدفمند قضاوتی و دنبال کردن روش گلوله برفی با هشت نفر از آن‌ها تا رسیدن به اشباع نظری مصاحبه عمیق نیمه ساختاریافته انجام شد. در این پژوهش پس از مصاحبه با ۶ خبره، اشباع نظری حاصل گردید ؛ اما برای افزایش مطلوبیت داده‌ها، مصاحبه‌ها تا خبرهٔ هشتم نیز ادامه یافت..

در بخش کمی نیز جامعه آماری پژوهش شامل دو گروه فرماندهان و مدیران عالی حوزه امنیت سایبری (ستاد کل نیروهای مسلح، ارتش جمهوری اسلامی ایران، سپاه پاسداران انقلاب اسلامی، نیروی انتظامی و سازمان پدافند غیرعامل کشور) و اساتید دانشگاهی و اعضای هیئت‌علمی دانشگاه‌های نظامی (دانشگاه عالی دفاع ملی، دانشگاه امام حسین (ع) دانشگاه مالک اشتر، دانشگاه پدافند هوایی خاتم‌الانبیاء (ص) و دانشکده فارابی) است؛ که

تعداد آن‌ها ۵۹ نفر برآورد گردید. با توجه به محدود بودن تعداد نفرات از روش سرشماری جهت توزیع پرسشنامه‌ها و جمع‌آوری اطلاعات استفاده شد.

۳-۵- روایی و پایایی ابزار جمع‌آوری اطلاعات

در بخش کیفی از روش روایی تفسیری برای اعتبار سنجی استفاده شده است بدین صورت که با ارائه بازخورد مصاحبه ها به مصاحبه شوندگان، نکات اصلاحی آن ها اعمال گردید. در بخش دوم پس از تدوین پرسشنامه‌ای حاوی ۴۵ سؤال بر اساس مدل مستخرج در بخش کیفی، به‌منظور تعیین روایی و پایایی، پرسشنامه در اختیار تعداد ۱۲ نفر از خبرگان حوزه امنیت سایبری (با حداقل ۲ سال اشتغال در مسئولیت مدیریت ارشد در حوزه امنیت سایبری، داشتن حداقل مدرک دکترای تخصصی) قرار داده شد که نتایج از تائید روایی ظاهری و ضریب آلفای کرون باخ معادل ۰/۸۶ برای کل پرسشنامه حکایت دارد.

۳-۶- مراحل انجام و به‌کارگیری روش

۱) بررسی پیشینه، نظریات و اسناد بالادستی و مصاحبه با ۸ نفر از خبرگان حوزه امنیت سایبری و استخراج ۴۵ شاخص، ۲۳ مؤلفه و ۷ بعد به‌عنوان اجزاء مدل قابلیت‌های سازمانی در حوزه امنیت سایبری

۲) تدوین پرسشنامه‌ای حاوی ۴۵ سؤال بر اساس مفاهیم مستخرجِ از مطالعات اکتشافی و بررسی روایی و پایایی، پرسشنامه بر اساس نظریات ۸ نفر از خبرگان حوزه امنیت سایبری

۳) بررسی مطلوبیت مدل، ابعاد و شاخص‌ها بر اساس ۴۳ پرسشنامه دریافتی از نمونه‌های آماری و با استفاده از نرم‌افزارهای Spss و Smart pls

۴- یافته‌های تحقیق

۴-۱- یافته‌های کیفی

با توجه مرور ادبیات و پیشینه تحقیق و نیز انجام ۸ مصاحبه نیمه ساختاریافته با خبرگان حوزه امنیت سایبری ۱۵۶ کد استخراج شد این کدها با استفاده از روش تحلیل مضمون (تم) و پس از حذف کدهای مشابه و شناسایی ارتباطات مفاهیم مطابق جدول ۲ به ۲۳ مضمون پایه (مؤلفه) و ۷ مضمون سازمان دهنده (ابعاد) تبدیل شد.

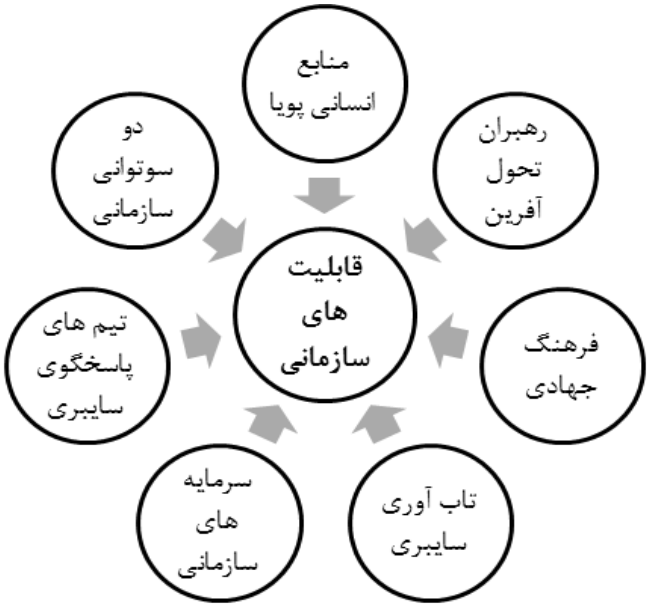
جدول ۲: مضامین پایه و سازمان دهنده و تعریف عملیاتی ابعاد مدل قابلیت‌های سازمانی در حوزه امنیت سایبری

ردیف	مضمون سازمان دهنده (ابعاد)	تعریف عملیاتی مضمون سازمان دهنده (ابعاد)	مضامین پایه	منابع
۱	منابع انسانی پویا	کارکنانی منعطف دارای شایستگی سایبری (دانش و مهارت فنی و تخصصی در چهار رشته مخابرات، الکترونیک، رایانه و مدیریت فناوری اطلاعات)، مهارت انسانی و فرهنگی و مهارت‌های اندیشه ورزی می‌باشند که توانایی ایجاد تحول در محیط پیچیده را دارا می‌باشند	۱-شایستگی سایبری ۲-مهارت انسانی و فرهنگی ۳-انعطاف‌پذیری منابع انسانی ۴-مهارت اندیشه ورزی	سازمان امنیت سایبری سنگاپور(۲۰۲۱)، نیروی دریایی آمریکا (۲۰۱۹)، مرکز ملی آمادگی حوادث و استراتژی امنیت سایبری ژاپن (۲۰۱۱) سند پدافند سایبری کشور (۱۳۹۴)، جعبه‌ابزار وزارت امنیت میهنی ایالات‌متحده (۲۰۱۶)، دانشگاه فونیکس(۲۰۱۸) حکم انتصاب اعضای شورای عالی فضای مجازی (۱۳۹۴) مصاحبه با خبرگان
۲	رهبران تحول‌آفرین	رهبر تحول‌آفرین فردی است دارای ویژگی‌های مثبت شخصیتی، مقید به اصول انقلاب، بصیر نسبت به محیط، سازمان و کارکنان، نوآور با توانایی تأثیرگذاری و انگیزش زیردستان و فرودستان.	۱-جنرالیست (همه‌چیزدان) ۲- مهارت رفتاری ۳- متعهد	سازمان امنیت سایبری سنگاپور(۲۰۲۱)، آلگاراجا (۲۰۱۳)، پارسون (۲۰۱۰) ، ویلیام (۲۰۱۷) تقی پور (۱۳۹۸) و سند راهبردی پدافند سایبری کشور (۱۳۹۴)، شورای امنیت سایبری(۲۰۱۴) مصاحبه با خبرگان
۳	فرهنگ جهادی	فرهنگ جهادی مجموعه‌ای از ارزش‌ها و مفروضات بنیادین برگرفته از آموزه‌های دین مبین اسلام که قابلیت	۱-معنویت محوری ۲- نظامی و امنیتی	دانشگاه فونیکس(۲۰۱۸)، شورای ملی رهبری تاب‌آوری سایبری اسکاتلند (۲۰۱۸)، عتیف و همکاران (۲۰۱۴)، جوزف

		راهبری نگرش و رفتار افراد در جهت تکامل و رشد را دارا است	۳- پویایی (یادگیرندگی)	و همکاران (۲۰۱۶)، مدل قابلیت‌های نیروی دریایی آمریکا (۲۰۱۹)، امیرلی و تقی پور (۱۳۹۹) ، اداره فناوری اطلاعات عمان مصاحبه با خبرگان
۴	تاب‌آوری سایبری	از تاب‌آوری سایبری قابلیتی پویا است که بر توانایی سازمان در پیش‌بینی، تشخیص، مقابله، بازیابی و یادگیری از تهدیدات و اختلالات اشاره دارد.	آینده‌نگری انعطاف‌پذیری چابکی انطباق‌پذیری یادگیرندگی	وزارت نیروی دریایی آمریکا (۲۰۱۹)، دانشگاه فونیکس(۲۰۱۸)، سند راهبردی شورای ملی رهبری تاب‌آوری سایبری اسکاتلند (۲۰۱۸) ، جوزف و دیویدسون (۲۰۱۶)، لن نیک و همکاران (۲۰۱۱)، تقی پور و همکاران (۱۳۹۸)، عسکری و همکاران (۱۳۹۹) مصاحبه با خبرگان
۵	دوسوتوانی سازمانی	دوسوتوانی سازمانی قابلیتی در جهت بهبود مستمر فرآیندها، توانایی‌ها و محصولات (خدمات) کنونی و نیز خلق فرآیندها، توانایی‌ها و محصولات (خدمات) جدید متناسب با تغییرات و تهدیدات آینده است.	اکتشاف بهره‌برداری	سند راهبردی پدافند سایبری(۱۳۹۴) ، شورای ملی رهبری تاب‌آوری سایبری اسکاتلند (۲۰۱۸)، کورت یس و همکاران (۲۰۱۶)هیالندو همکاران (۲۰۰۵) ، عسکری و همکاران (۱۳۹۹) کاویانی و همکاران (۱۳۹۸)، امیرلی و همکاران (۱۳۹۹) مصاحبه با خبرگان
۶	سرمایه سازمانی	سرمایه سازمانی سرمایه‌های فکری (مجموعه‌ای از دارایی‌های ناملموس انسانی، ساختاری و ارتباطی که می‌توانند ایجاد ارزش در	سرمایه فکری سرمایه معنوی سرمایه اجتماعی	نیروی دریایی آمریکا (۲۰۱۹)، نایت (۲۰۱۵)، ظفرو همکاران (۲۰۱۳)، شورای امنیت سایبری (۲۰۱۴) ، کاویانی و همکاران(۱۳۹۹) مصاحبه با خبرگان

		سازمان‌ها را تسهیل نمایند)، معنوی (قابلیتی برگرفته از اعتقادات و ارزش‌های اخلاقی، اعتقادی و انقلابی درونی افراد که بر عملکرد سازمان تأثیرگذار است) و اجتماعی (قابلیتی برگرفته از احساس هویت جمعی، ایجاد شبکه‌ها، اعتماد متقابل و تعامل و ارتباط سازنده میان اعضای سازمان است) می‌باشد.		
۷	تیم‌های قدرتمند پاسخگویی سایبری	مجموعه‌ای از اعضای مختلف سازمان با تخصص‌های متفاوت که به‌منظور پیش‌بینی، شناسایی و مواجهه با رویدادهای سایبری گرد هم آمده‌اند و مسئولیت کامل نتیجه کار را بر عهده‌دارند	مهارت‌های متنوع و مکمل استقلال و اختیار بالا توانمند در امور	وزارت امنیت داخلی ایالات‌متحده (۲۰۱۶)، گزارش کمیسیون ملی ارتقاء امنیت سایبری (۲۰۱۶)، مطالعات کواسیچ (۲۰۱۶)، رضوان و همکاران (۲۰۱۶) مصاحبه با خبرگان

بر اساس نتایج مطالعات اکتشافی، مطابق شکل (۲) مدل قابلیت‌های سازمانی در حوزه امنیت سایبری مشتمل بر هفت بعد منابع انسانی پویا،رهبران تحول‌آفرین، فرهنگ جهادی، دوسوتوانی سازمانی، تاب‌آوری سازمانی، سرمایه‌های سازمانی، تیم‌های قدرتمند پاسخگویی سایبری می‌باشد.



شکل (۲): مدل مفهومی تحقیق

۴-۲- یافته‌های کمی

۴-۲-۱- ویژگی‌های جمعیت شناختی پاسخگویان

با توجه به مفروضات تعیین‌شده جهت شناسایی خبرگان علمی و اجرایی تعداد ۵۹ نفر جهت بررسی ابعاد، مؤلفه‌ها و شاخص‌های استخراج‌شده از مطالعات اکتشافی تعیین گردیده‌اند. پس از هماهنگی‌های صورت گرفته و ارسال پرسشنامه‌های مربوطه تعداد ۴۳ پرسشنامه جمع‌آوری و مبنای تحلیل داده‌ها قرار گرفت. ویژگی‌های جمعیت شناختی پاسخگویان به شرح جدول شماره (۳) است

جدول ۳: ویژگی‌های جمعیت‌شناسی پاسخگویان

ویژگی جمعیت‌شناسی	ابعاد	تعداد
مدرک تحصیلی	دکترا	۲۹
	کارشناسی ارشد	۱۴
وابستگی سازمانی	دانشگاه دفاع ملی	۴
	دانشگاه مالک اشتر	۱
	دانشگاه امام حسین (ع)	۳

	دانشگاه پدافند هوایی خاتم‌الانبیاء (ص)	۳
	ستاد کل نیروهای مسلح	۵
	سازمان پدافند غیرعامل کشور	۵
	ارتش جمهوری اسلامی ایران	۱۳
	سپاه پاسداران انقلاب اسلامی	۴
	نیروی انتظامی	۲

۴-۲-۲ بررسی مطلوبیت ابعاد مدل قابلیت‌های سازمانی در حوزه امنیت سایبری

پس از شناسایی ابعاد، مؤلفه‌ها و شاخص‌های مدل قابلیت‌های سازمانی در حوزه امنیت سایبری در گام اول از تحلیل داده‌ها اجزاء الگو به‌منظور تعیین مطلوبیت در معرض نقد و ارزیابی خبرگان قرار گرفتند که نتایج تعیین مطلوبیت ابعاد بر اساس تعداد شاخص‌ها در جدول (۴) ارائه‌شده است.

جدول ۴: محاسبه میانگین وزنی و مطلوبیت مؤلفه‌ها مدل مفهومی تحقیق

ابعاد	نظرات خبرگان									
	فراوانی نظرات					وزن مؤلفه‌ها		مطلوبیت مؤلفه‌ها		
	خیلی زیاد	زیاد	متوسط	کم	خیلی کم	وزن کلی شاخص‌ها	میانگین وزنی	مطلوب	نسبتاً مطلوب	نامطلوب
فرهنگ جهادی	۲۲۷	۷۸	۵۲	۱۹	۱۲	۱۶۳۵	۴,۲۷	*		
تاب‌آوری سایبری	۱۴۷	۴۰	۲۳	۵	۰	۹۷۴	۴,۵۳	*		
دوسوتوانی سازمانی	۶۴	۱۳	۹	۰	۰	۳۹۹	۴,۶۴	*		
سرمایه سازمانی	۷۶	۲۳	۲۱	۷	۲	۵۵۱	۴,۲۷	*		
تیم‌های سایبری	۸۸	۲۴	۱۲	۵	۰	۴۴۰	۴,۵۱	*		
منابع انسانی پویا	۳۶	۷	۰	۰	۰	۲۰۸	۴,۸۴	*		
رهبران تحول‌آفرین	۳۳	۸	۲	۰	۰	۲۰۳	۴,۷۲	*		

با عنایت به اینکه میانگین وزنی کلیه ابعاد بالاتر از ۴ می‌باشد می‌توان نتیجه گرفت که بر اساس نظریات خبرگان، کلیه ابعاد پیشنهادی مدل قابلیت‌های سازمانی در حوزه امنیت سایبری دارای مطلوبیت لازم می‌باشند.

۲-۴- ۳برازش مدل مفهومی

به‌منظور برازش مدل مفهومی از نرم‌افزار Smart pls استفاده‌شده است. این مرحله شامل برازش مدل اندازه‌گیری (رابطه گویه‌ها با سازه‌ها)، برازش مدل ساختاری (رابطه میان سازه‌ها) و برازش مدل کلی است؛ که نتایج آن‌ها در جدول شماره ۵ ارائه‌شده است.

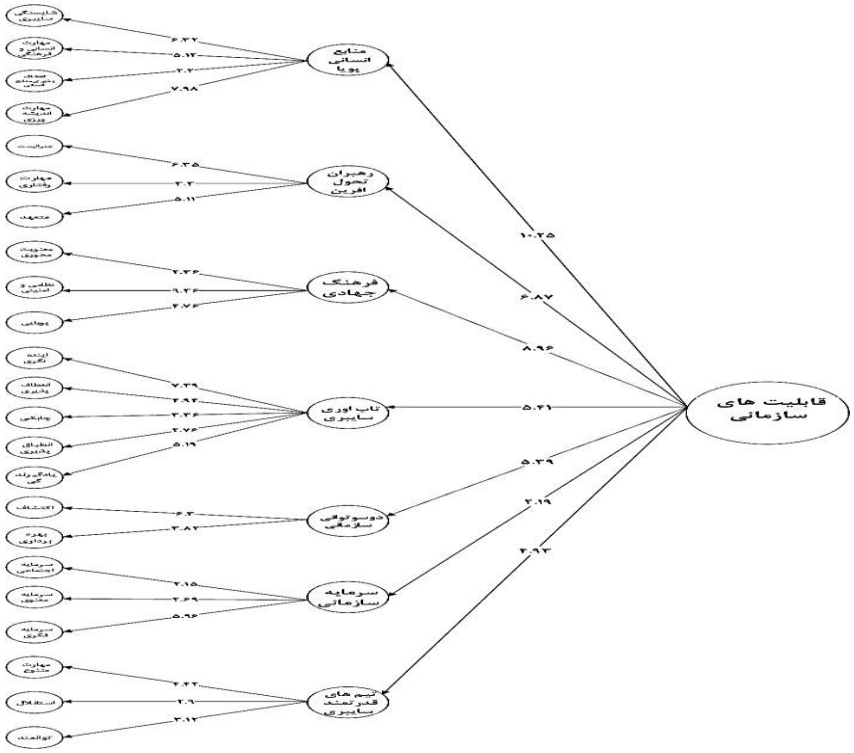
جدول (۵): نتایج برازش (اندازه‌گیری، ساختاری و برازش کلی) مدل مفهومی تحقیق

ابعاد/ مؤلفه	برازش مدل اندازه‌گیری				برازش مدل ساختاری		برازش کلی مدل
	آلفای کرون باخ	مقادیر اشتراکی	پایایی ترکیبی	روایی همگرا	R2	Q2	
قابلیت‌های سازمانی	۰,۹۵	۰,۹۶	۰,۹۶	۰,۵۳	متغیر برون‌زا		$\sqrt{(}$
فرهنگ جهادی	۰,۸۶	۰,۸۷	۰,۹	۰,۵۱	۰,۸۸	۰,۴۲	
تاب‌آوری سایبری	۰,۸۷	۰,۸۸	۰,۹۱	۰,۶۷	۰,۶۷	۰,۴۰	
دوسوتوانی سازمانی	۰,۸۴	۰,۸۴	۰,۹۲	۰,۸۶	۰,۶۶	۰,۵۳	
سرمایه سازمانی	۰,۶۲	۰,۶۳	۰,۷۹	۰,۵۶	۰,۵۰	۰,۳	
تیم پاسخگوی سایبری	۰,۸۲	۰,۸۳	۰,۸۹	۰,۷۴	۰,۴۵	۰,۳۱	
منابع انسانی پویا	۰,۹۳	۰,۹۴	۰,۹۴	۰,۵۸	۰,۹۶	۰,۵۴	
رهبران تحول‌آفرین	۰,۹	۰,۹۱	۰,۹۴	۰,۸۴	۰,۳۹	۰,۳۶	۰,۶۶)=۰,۷×۰,۹۴GOF=√(

بررسی برازش اندازه‌گیری و ساختاری ابعاد مدل مفهومی مؤید آن است که در وجوه موردبررسی، کلیه ابعاد و مؤلفه‌ها حائز نمرات قابل‌قبول می‌باشند. صرفاً در خصوص ضریب آلفای کرون باخ بعد سرمایه سازمانی خروجی نرم‌افزار کمتر از میزان قابل‌قبول است لیکن با توجه به مقدار قابل‌قبول پایایی ترکیبی و مقادیر اشتراکی این کاستی قابل‌اغماض است. نتایج برازش کلی مدل (۰/۶۶) نیز نشان‌گر آن است که مدل در پیش‌بینی متغیرهای مکنون درون‌زا دارای قدرت و توانایی بالایی است.

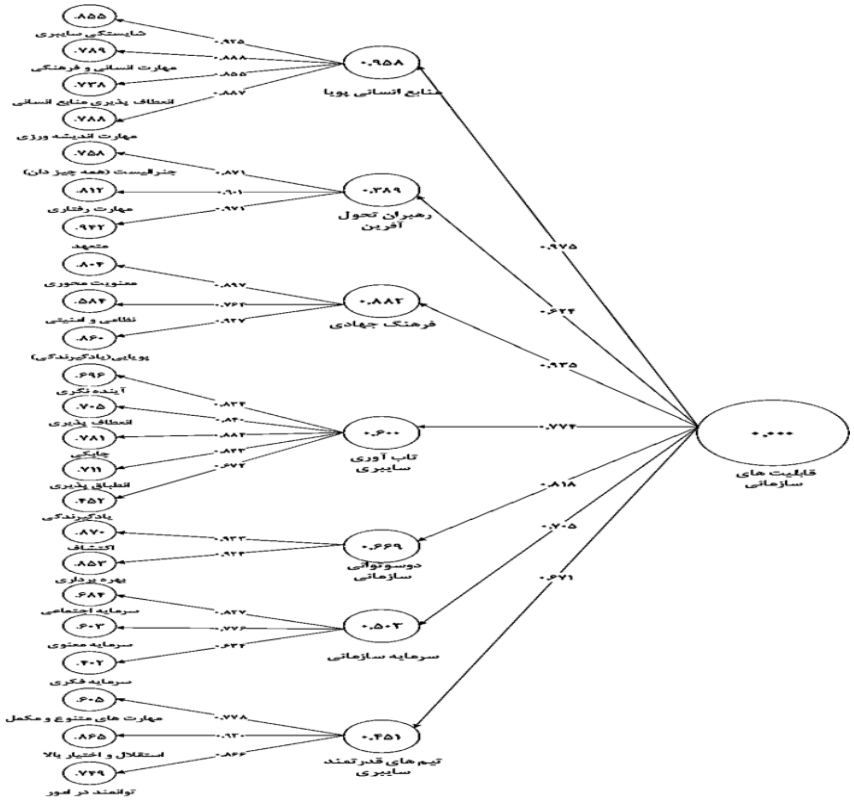
در مرحله بعد با استفاده از داده‌های جمع‌آوری‌شده نحوه ارتباط ابعاد و مؤلفه‌ها مورد ارزیابی قرار گرفت. در گام اول با استفاده از دستور Bootstrapping ضرایب معناداری مسیر میان

متغیرهای مدل مورد ارزیابی قرار می‌گیرد. ضرایب معناداری مسیرهای مدل نشان می‌دهند که آیا فرضیه‌های تحقیق معنادار هستند یا خیر؟ سطح قابل‌قبول برای این مرحله اکتساب عدد ۱/۹۶ است. نتایج مدل ساختاری تحقیق در حالت ضریب معناداری در شکل ۳ ارائه گردیده است.



شکل ۳: مدل ساختاری تحقیق در حالت ضریب معناداری

در گام دوم مطابق شکل ۴ ضرایب استانداردشده بار عاملی با استفاده از دستور Pls Algorithm بررسی گردید که نتایج از قابل‌قبول این ضرایب حکایت دارد.



شکل (۴): حالت استاندارد مدل ساختاری تحقیق

با توجه به اطلاعات حاصل از شکل‌های ۳ و ۴ می‌توان اذعان نمود که مدل نهایی تحقیق از دیدگاه پاسخگویان جامع بوده و قابلیت‌های موردنیاز سازمان‌های فعال در حوزه امنیت سایبری را دربرمی گیرد.

۵- بحث، نتیجه‌گیری و پیشنهادها

۵-۱- بحث و نتیجه گیری

با توجه به خلأ تحقیقاتی و اجرایی موجود در خصوص شناسایی و تبیین ویژگی‌ها و مشخصه‌های منحصربه‌فرد سازمان‌های نظامی متولی امنیت سایبری در کشور در این

پژوهش به طراحی مدل قابلیت‌های سازمانی در حوزه امنیت سایبری در سطح نیروهای مسلح مبادرت نموده‌ایم. بر اساس یافته‌های تحقیق ابعاد این مدل به شرح ذیل می‌باشند.

منابع انسانی پویا: منابع انسانی یکی از ابعاد مدل قابلیت‌های سازمانی در حوزه امنیت سایبری می‌باشد. قابلیتی که در مدل‌ها و الگوهای بین‌المللی چون طرح آموزش امنیت سایبری ایالات‌متحده (نیروی کار توانا و شایسته) و چارچوب مرکز ملی آمادگی حوادث و استراتژی سایبری ژاپن (منابع انسانی هیبریدی) بدان اشاره گردیده است. رویکردی که در حوزه سیاست‌گذاری دربند ۴» حکم انتصاب اعضای شورای عالی فضای مجازی[۱](۱۳۹۴) بر آن توجه ویژه‌ای مبذول شده است. ارجحیت این قابلیت بر سایر ابعاد مدل نیز از منظر آموزه‌های دین مبین اسلام و تأکیدات مقام معظم رهبری (مدظله‌العالی) در این خصوص توجیه‌پذیر است. معظم له در دیدار مورخ ۹۶/۶/۱۲ فرماندهان قرارگاه پدافند هوایی خاتم‌الانبیاء (ص) آجا در این خصوص فرموده‌اند " در هر بخشی از نیروهای مسلح و غیر نیروهای مسلح در کل کشور باید به این توجه کنیم که اولاً اساس کار، نیروی انسانی است. ثانیاً نیروی انسانی ما تواناست. توانایی ذاتی دارد، گیج و بی‌حال و بی‌استعداد و کندذهن نیست، ثالثاً این استعداد درونی اگر بخواهد فعال شود، کار لازم دارد، یعنی باید تلاش کرد، باکار، این استعداد بروز خواهد کرد. "

فرهنگ جهادی: فرهنگ‌سازمانی به‌عنوان یکی از قابلیت‌های اصلی سازمان‌های فعال در حوزه امنیت سایبری در گزارش‌ها و مطالعات نیروی دریایی آمریکا (۲۰۱۹) و شورای ملی رهبری تاب‌آوری سایبری اسکاتلند (۲۰۱۸) در قالب فرهنگ یادگیرنده (پویایی) مورد تأکید قرارگرفته است. بااین‌وجود باتوجه‌به بستر و شرایط ویژه نظام مقدس جمهوری اسلامی ایران بدیهی است که ارزش‌ها و باورهای حاکم بر حوزه موردمطالعه باید باسیاست‌ها، واقعیات و ارزش‌های جامعه همخوانی داشته باشد. فرهنگی که از آن به‌عنوان فرهنگ جهادی یاد می‌شود. مقام معظم رهبری در تاریخ ۱۳۸۲/۱۰/۱۴ ویژگی‌ها و کارکردهای این فرهنگ را به‌خوبی تبیین نموده‌اند " آنچه انقلاب اسلامی به مردم ما داد، فرهنگ جهادی بود. فرهنگ

---

۱ - اهتمام ملی و همه‌جانبه و سرمایه‌گذاری جدی در امر ایجاد و توسعه انواع فناوری‌ها و صنایع کاملاً پیشرفته و رقابتی خصوصاً با استفاده و ایجاد رشته‌های نوین دانشگاهی و تربیت سرمایه‌های انسانی متعهد، متخصص و کارآمد موردنیاز در بخش‌های سخت‌افزاری و نرم‌افزاری، محتوایی و خدماتی در تمامی ابعاد فضای مجازی به‌ویژه در برنامه ششم توسعه و برنامه‌ریزی سالانه کشور

جهادی در همه صحنه‌ها و عرصه‌ها به کار می‌آید و در زمینه کارهای زیربنایی کشاورزی و دامداری و امثال این‌ها هم از اوّل انقلاب، روح و فرهنگ جهادی وارد میدان شد ... خودِ انقلاب دستگاه‌هایی را به وجود آورد که در ذاتشان حرکت و جوشش انقلابی و سریع و جهادی وجود داشت ... این ورود درصحنه کار و ابتکار، این کمک‌رسانی انبوه، مخصوص ملتی است که دل او از حرکت جهادی گرم است و جوشش جهادی در دل او وجود دارد. این همان روحیه بسیجِ دوران دفاع مقدّس است؛ این همان روحیه سنگر سازان بی سنگر جهاد سازندگی است که غسل شهادت می‌کردند، روی بولدوزر می‌نشستند تا خاک‌ریز بزنند. ما این روحیه را باید حفظ کنیم. این روحیه باکار علمی و نظم تشکیلاتی هیچ منافاتی ندارد " در این تحقیق نیز پس از مطالعات اکتشافی صورت پذیرفته فرهنگ جهادی در قالب سه سازه متناسب با مطالعات علمی (پویایی و یادگیرندگی)، نظامی و امنیتی (متناسب با حوزه امنیت سایبری و نیروهای مسلح) و معنویت محوری (متناسب باسیاست‌های جمهوری اسلامی ایران) تبیین و مورد آزمون قرار گرفت که نتایج از تأیید شاخص‌ها و این مؤلفه‌ها حکایت دارد.

دوسوتوانی سازمانی: دوسوتوانی بودن سازمان‌های متولی در حوزه امنیت سایبری دربند ۳ ارزش‌های حاکم بر حوزه پدافند سایبری در سند راهبردی پدافند سایبری مورد تأکید قرارگرفته است. این نتایج با یافته‌های شورای ملی رهبری تاب‌آوری سایبری اسکاتلند (۲۰۱۸)، کورت یس و همکاران (۲۰۱۶) و کاویانی و همکاران (۱۳۹۸) هم‌راستا می‌باشند.

تاب‌آوری سایبری: بر اساس یافته‌های تحقیق تاب‌آوری سایبری یکی از ابعاد اصلی مدل قابلیت‌های سازمانی در حوزه امنیت سایبری می‌باشد. این یافته‌ها با نتایج و توصیه‌های وزارت نیروی دریایی آمریکا (۲۰۱۹)، شورای ملی رهبری تاب‌آوری سایبری اسکاتلند (۲۰۱۸) هم‌راستا است. موضوعی که دربندهای ۵،۶ و ۷ سند راهبردی پدافند سایبری کشور مأموریت‌های پدافند سایبری کشور بر کارکردهای آن تأکید شده است.

سرمایه‌های سازمانی: سرمایه‌های سازمانی، سرمایه‌ها و دارایی‌های غیرملموس یک سازمان است که تحقق مأموریت و اهداف سازمان را امکان‌پذیر می‌نمایند. علی‌هذا در مؤلفه سرمایه فکری در مطالعه نیروی دریایی ایالات‌متحده (۲۰۱۹) بر ضرورت ایجاد و حفظ این قابلیت تأکید شده است.

تیم‌های قدرتمند پاسخگوی سایبری: تیم‌ها پاسخگوی سایبری قلب اجرایی مواجه و پاسخگویی مناسب به تهدیدات سایبری می‌باشند. این یافته‌ها با توصیه‌های وزارت امنیت داخلی ایالات‌متحده (۲۰۱۶) و یافته‌های تحقیق رضوان و همکاران (۲۰۱۶) هم‌راستا می‌باشد.

رهبران تحول‌آفرین: رهبران تحول‌آفرین یکی از ابعاد اصلی مدل قابلیت‌های سازمانی در حوزه امنیت سایبری می‌باشد که در مدل‌های مطرح در حوزه امنیت سایبری همچون وزارت امنیت داخلی ایالات‌متحده (۲۰۱۶) و طرح آموزش امنیت سایبری ایالات‌متحده غالباً در فرایند توسعه بلندمدت کارکنان موردنظر قرارگرفته است. قابلیتی راهگشا که مقام معظم رهبری (مدظله‌العالی) در مورخه ۱۳۹۶/۱/۱ در بیانات خود به‌خوبی نقش و جایگاه آن را تبیین نموده‌اند. " مدیریت فعال، متدین و کارآمد راه‌حل مشکلات کشور است "

۵-۲- پیشنهادها

اگرچه در ادبیات علمی جامعه شناسی، روانشناسی و روانشناسی اجتماعی، ایثار کردن مانند گذشته به منزله بیمار روانی نگریسته نمی شود و نوعی رفتار فرا اجتماعی محسوب می گردد، اما همچنان پژوهش های اندکی در زمینه شناخت این رفتار صورت گرفته است. لزوم شناخت رفتارهای ایثارگرانه در محیط های کاری و سازمانی را می توان با تامل در مشاغل پرخطر و پرفشاری نظیر پرستاری و همچنین مشاغل رسته نظامی و امنیتی دریافت. در این پژوهش با استفاده از روش شناسی پدیدارشناسی به دنبال واکاوی معنی ایثار در سازمان برآمدیم. پژوهش پدیدارشناسی به ما کمک می کند ماهیت یک پدیده را از منظر مشارکت کنندگان پژوهش که به صورت مستقیم پدیده را تجربه کرده اند دریابیم و بفهمیم، از این رو نتایج پژوهش پدیدارشناسی قابل تعمیم نیستند. به عبارت دیگر ما در این پژوهش به واکاوی فهم مدیران جهادی از پدیده ایثار پرداختیم، حال اینکه جوامع آماری متفاوت ممکن است تجارب متفاوتی از ایثار داشته باشند. از سوی دیگر در این پژوهش ایثار را از منظر مدیران جهادی مورد واکاوی قرار دادیم، بررسی این پدیده از زاویه دریافت کنندگان ایثار یعنی کسانی که به طور مستقیم با این مدیران در ارتباط بوده اند نیز می تواند زوایای جدیدی از ایثار در سازمان را برای ما آشکار سازد.

پژوهش های آتی همچنین باید به این پرسش پاسخ دهند که چه عواملی باعث می شود فرد ایثار کند و پیامدها و آثار ایثار برای فرد، دیگران و سازمان چیست و به طور کلی ایثار چه تاثیری بر روابط متقابل افرد در سازمان ها دارد؟ برای مثال، واکاوی تجربه افراد ایثارگر در پژوهش حاضر نشان داد که فرد ایثاگر انگیزه های درونی (لذت و کسب خودپنداره

مثبت) یا انگیزه های بیرونی (خودابرازگری و کسب اعتبار اجتماعی) را به عنوان بخش مهمی از تجربه ایثار خود معرفی می کند، اما سوالی که پدیدارشناسی و پژوهش حاضر پاسخی برای آن نیافت این است که آیا ایثار با انگیزه های درونی (ایثار پنهان) و بیرونی (ایثار آشکار) علل و آثار متفاوتی دارند یا خیر؟

بنابراین به کارگیری سایر روش های پژوهش کیفی نظیر روایت پژوهی و داده بنیاد و روش های کمی نظیر پیمایش و آزمایش در پژوهش های آتی می توانند به درک بهتر پدیده ایثار به ما کمک کنند.

عدم تمایل برخی از مشارکت کنندگان برای به اشتراک گذاری تجارب شخصی ایثارگری خود را می توان به عنوان مهم ترین محدودیت پژوهش حاضر نام برد.

۵-۳- پیشنهادها

باتوجه‌به نتایج تحقیق و به‌منظور تحقق مدل قابلیت‌های سازمانی در حوزه امنیت سایبری موارد ذیل پیشنهاد می‌گردد:

به‌منظور پرورش و توسعه منابع انسانی پویا در کنار آموزش طولی و عرضی متداول، تسهیم اطلاعات و تجارب بین کارکنان و نهادهای متولی امنیت سایبری سازوکاری مؤثر در جهت ارتقاء دانش و مهارت‌های کارکنان قلمداد می‌گردد. این مهم از طریق ایجاد سیستم جامع پردازش مرکزی جهت جمع‌آوری، یکپارچه‌سازی و تسهیم اطلاعات قابلیت اجرایی خواهد داشت. رویکردی که ارتش آمریکا جهت جمع‌آوری و تسهیم اطلاعات رزمی تا سطوح تاکتیکی و رده گردان در قالب سیستم تحلیل منابع آزاد[1] از آن بهره‌برداری نموده است.

توجه به گستره عملیاتی فعالیت‌های کارکنان در حوزه امنیت سایبری ضروری است که کارکنان از فرهنگ‌ها، باورها، مبانی فلسفی حاکم بر سایر کشورها آگاهی داشته باشند؛ لذا پس از ارزیابی توانایی‌های کارکنان در ابعاد شناختی، فیزیکی و احساسی و انگیزشی باید برنامه‌های آموزشی مناسب به‌منظور تقویت این شایستگی‌ها طراحی گردد. به‌طور مثال برای افراد ضعیف در بعد فیزیکی شرکت در کلاس‌های آموزش رفتاری، افراد دارای ضعف در بعد شناختی شرکت در دوره‌های استدلال قیاسی و توان تحلیلی باید در نظر گرفته شود.

نهادینه‌سازی فرهنگ جهادی نیازمند رویکردی توأم با عطوفت، عقلانیت و سعه‌صدر است به عبارتی، جاری و ساری ساختن فرهنگ اسلامی - ایرانی با استفاده از زور و اجبار نه‌تنها

---

[1] All source analysis system

قابلیت اجرا و ماندگاری ندارد بلکه با موازین شرع مقدس و سیره اهل‌البیت نیز همخوانی ندارد. خداوند تبارک‌وتعالی در آیه ۱۲۵ سوره نحل پیامبر اکرم (ص) را به بهره‌گیری از حکمت و موعظه نیکو جهت دعوت خلق به دین و راه خدا امر نموده است.[۱] دعوتی که بنا به‌تصریح آیه ۲۵۶ سوره بقره هیچ اکراه و اجباری در آن نیست[۲] در این رویکرد تبیین آموزه‌های دین اسلام و تأثیرگذاری بر بینش و نگرش افراد از طریق استدلال، تشبیه و تمثیل، تحریک عواطف، تداعی معانی و غیره توصیه‌شده است. در نگاهی جامع‌تر با عنایت به اینکه ایجاد نگرش و اعتقاد به مفاهیم و آموزه‌هایی چون تکلیف گرایی، شهادت‌طلبی، نفی سلطه‌پذیری و امربه‌معروف و نهی‌ازمنکر غالباً در تربیت بلندمدت افراد ریشه دارد. ضروری است که راهبردهای اجرایی مناسب، چند سطحی و قابل‌تبدیل به مفاهیم ملموس با همفکری و مشارکت سازمان‌های متولی تدوین و به اجرا درآید. علی‌هذا به نظرمی رسد باتوجه‌به ماهیت دشوار وتوام با چالش‌های فراوان و مستمر مشاغل نظامی و امنیتی اکثریت افراد متقاضی ورود به خدمت در نیروهای مسلح مزین به ابعاد مذکور می‌باشند لکن حفظ، پرورش و راهبری این ابعاد امری است ضروری که اهمیت توسعه منابع انسانی را بیش‌ازپیش نمایان می‌سازد.

ارتقاء تاب‌آوری سازمان‌های متولی امنیت سایبری در کشور نیازمند تقویت توانمندی‌های این سازمان‌ها در خصوص توانایی تشخیص و ترسیم آینده‌های بدیل، توانایی تغییر مسیر پس از دریافت اولین علائم هشداردهنده با حداقل هزینه، توانایی توسعه و به‌کارگیری راهکارهای مناسب، توانایی بازسازی خود و ایجاد تناسب با محیط و نهایتاً انتقال دانش و تغییر رفتار خود بر اساس بینش جدید است. رویکردهایی که در طراحی فرایندها و دوره‌های تربیتی و آموزشی سازمان‌ها باید بدان‌ها توجه ویژه نمود.

با عنایت به اینکه ایجاد نگرش و اعتقاد به مفاهیم و آموزه‌هایی چون تکلیف گرایی، شهادت‌طلبی، نفی سلطه‌پذیری غالباً در تربیت بلندمدت افراد ریشه دارد. ضروری است که راهبردهای اجرایی مناسب، چند سطحی و قابل‌تبدیل به مفاهیم ملموس با همفکری و

---

[۱] ادْعُ إِلی سَبیلِ رَبِّکَ بِالْحِکْمَهْ وَ الْمَوْعِظَهْ الْحَسَنَهْ وَ جادِلْهُمْ بِالَّتی هِیَ أَحْسَنُ

[۲] لا إِکْراهَ فِی الدِّینِ قَدْ تَبَیَّنَ الرُّشْدُ مِنَ الْغَیِّ فَمَنْ یَکْفُرْ بِالطَّاغُوتِ وَ یُؤْمِنْ بِاللَّهِ فقد استَمْسَکَ بِالْعُرْوَهْ الْوُثْقی لاَ انْفِصامَ لَها وَ اللَّهُ سَمیعٌ عَلیمٌ

مشارکت کلیه دستگاه‌های اجرایی تدوین و به اجرا درآید. علی‌هذا ازجمله راهکارهای کوتاه‌مدت این مهم شناسایی و جذب کارکنان (کارمند یابی) از طریق نهادهای انقلابی من‌جمله بسیج دانشگاه‌ها و مؤسسات عالی و مساجد محلات و پرورش آن‌ها در محیط متناسب است.

دوسوتوانی سازمانی به‌عنوان مفهومی برآمده از ضرورت نوآوری در سازمان‌های امنیتی و دفاعی بر تمرکز توأمان بر بهبود تجهیزات و فناوری‌های کنونی و نیز خلق قابلیت‌های منحصربه‌فرد به‌منظور تغییر سیمای آینده و الزام دشمنان به واکنش در مقابل آن تأکید دارد. براین‌اساس و باتوجه‌به شرایط کنونی کشور و تحریم‌های بین‌المللی توجه به این پدیده مهم بیش از هر زمان دیگری ضرورت یافته است. تجارب موفق کشور در تکیه‌بر توان داخلی و بهره‌گیری از هم‌افزایی صنعت، دانشگاه و دستگاه‌های متولی در استفاده از این ترکیب تأثیرگذار می‌باشد.

تیم‌های پاسخگوی امنیت سایبری به‌عنوان اولین نقطه مواجه با تهدیدات سایبری کشور وظیفه خطیری را بر عهده‌دارند که یقیناً نمی‌توانند از ساختار سنتی و سلسله‌مراتبی حاکم بر سازمان‌های نظامی و امنیتی تبعیت نمایند. در این تیم‌ها غالباً از کارکنان با مهارت‌های متفاوت و مکمل استفاده می‌شود. این تیم‌ها دارای استقلال و اختیارات عملیاتی فراوانی به‌منظور پیش‌بینی، مواجه و بازیابی اختلالات می‌باشند. بااین‌وجود ایجاد تیم‌های قدرتمند در حوزه امنیت سایبری نیازمند بازطراحی فرهنگ، ساختار و کلیه فرایندهای سازمانی بر اساس شرایط مذکور می‌باشد؛ لذا این مهم باید در دستور کار نهادهای متولی این حوزه قرار گیرید.

بر اساس نتایج تحقیق در میان شاخص‌های مهارت‌های اندیشه‌ورزی تفکر راهبردی بیش از سایر مهارت‌ها مورد تأیید قرارگرفته است. به‌منظور نهادینه‌سازی تفکر راهبردی نیاز است که دوره‌های آموزشی مناسبی در جهت تقویت مهارت‌های کنکاش و رصد محیطی، تشخیص و شناخت فرصت‌های حال و آتی، چشم‌انداز سازی و نیز خلق راهبردها و تصمیمات هوشمندانه طراحی گردد. ازجمله دوره‌های آموزشی متداول در این حوزه در عرصه امنیتی و نظامی می‌توان به استفاده از نرم‌افزارهای شبیه‌سازی جنگ‌های آینده و نیز نظریه تئوری بازی‌ها اشاره نمود.

در این تحقیق علیرغم مکاتبات صورت گرفته با برخی دستگاه های اجرایی کشوری مسئول در حوزه امنیت سایبری و نیز هماهنگی های صورت گرفته با برخی مسئولان و اعضای شورای عالی فضای مجازی، نهادها و اشخاص مذکور حاضر به همکاری نگردیدند. این مهم به عنوان مهم ترین محدودیت پژوهش حاضر، در تعمیم نتایج پژوهش به سایر دستگاه های اجرایی تاثیرگذار می باشد. با توجه به تمرکز تحقیق حاضر بر شناسایی قابلیت های سازمانی مرتبط با حوزه مطالعات سازمانی، طراحی مدل بلوغ قابلیت های امنیت سایبری می تواند به عنوان مکمل این موضوع در تحقیات آتی مورد نظر قرار گیرد.

۶- منابع

منابع فارسی

۱) امیرلی، حسین؛ تقی پور، رضا. (۱۳۹۹). **ارائه مدل فرآیندی دفاع سایبری بومی**. فصلنامه امنیت ملی، ۱۰(۳۷)، ۳۸۶-۳۵۳.

۲) تقی پور، رضا؛ لشکریان، حمیدرضا؛ یزدانی، رحیم.(۱۳۹۸). **الگوی راهبردی حفاظت از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران**. فصلنامه امنیت ملی، ۹(۳۴)، ۷-۴۹.

۳) خلیلی پور رکن آبادی، علی ، نور علی وند ، یاسر.(۱۳۹۱). **تهدیدات سایبری و تأثیر آن بر امنیت ملی**. مطالعات راهبردی، ۱۵(۲) ،۱۹۷-۱۶۷.

۴) دانایی فرد، حسن؛ برزگر، فاطمه ؛ احمدی، هانیه.(۱۳۹۴).**سازوکارهای ارتقاء قابلیت های سازمانی در بخش دولتی**. مدیریت سازمان های دولتی، ۳(۳)، ۱۰۶-۹۱.

۵) عسکری, احمد, طاهرپور کلانتری, حبیب‌اله, میری, عبدالرضا. (۱۳۹۹). **معرفی الگوی قابلیت‌های پویا در تبدیل تهدیدها به فرصت‌ها و خلق مزیت رقابتی در ارتش ج.ا.ایران** .فصلنامه علمی راهبرد دفاعی، ۱۸(۱)، ۹۱-۶۷.

۶) علیزاده ثانی، محسن؛ حسینی، ابوالحسن ؛ تبسمی، امیر. (۱۳۹۷). **تاثیر امکانات رفاهی بر سرمایه روانشناختی مثبت**. فصلنامه مطالعات مدیریت، ۲۷(۸۷) ، ۴۴-۲۹.

۷) فاضلی، حبیب الله ؛ افضلی، توحید. (۱۳۹۴). **دیپلماسی ایالات متحده در قبال جمهوری اسلامی ایران در دولت اوباما(با تاکید بر فضای سایبری)**. دو فصلنامه مطالعات قدرت نرم، ۵(۱۲)، ۱۶۰-۱۳۹

۸) کاویانی، حسن؛ میرسپاسی، ناصر؛ معمارزاده طهران، غلامرضا.(۱۳۹۹). **طراحی مدل شایستگی کارکنان در حوزه امنیت سایبری**. فصلنامه مطالعات بین رشته ای دانش راهبردی، ۱۰(۴۱)، ۲۹۸-۲۷۳

۹) کاویانی، حسن؛ علیزاده، حمید؛ فرجی، معرفت.(۱۳۹۸). **بررسی نقش میانجی انعطاف‌پذیری منابع انسانی در رابطه بین دوسوتوانی سازمانی و هوش سازمانی در یگان‌های منتخب اطلاعات نظامی**. مدیریت نظامی، ۱۹(۷۴)، ۸۰-۵۳

۱۰) کاویانی، حسن؛ فتح آبادی، حسین ؛ منوچهری، کمال.(۱۳۹۷). **تأثیر انعطاف‌پذیری منابع انسانی بر دوسوتوانی سازمانی در یگان‌های نظامی**. فصلنامهٔ علمی مطالعات منابع انسانی، ۸(۳)، ۱۱۶-۹۱

۱۱) ولوی, محمدرضا, نیک نفس, علی. (۱۴۰۰). **مدل بلوغ نظام رصد و پایش و هشداردهی سایبری جمهوری اسلامی ایران** .فصلنامه علمی امنیت ملی، ۱۱(۴۰)، ۱۸۲-۱۵۵

۱۲) یزدانیان، حمید ؛جلالی فراهانی، غلامرضا.(۱۳۹۶). **متغییرهای کلیدی منابع انسانی در تقویت دفاع سایبری جمهوری اسلامی ایران**.فصلنامه امنیت ملی، ۷(۲۶)، ۱۴۲-۱۲۷

کتاب‌ها

۱) اولریش، دیو؛ بروک بنک، وین؛جانسون، دنی؛ سندهولتر ،کورت ، یانگر، جان. (۱۳۸۸). **شایستگی های منابع انسانی**، مترجمان: مسعود بینش و افشین دبیری. تهران، انتشارات سرآمد

۲) مایلز، جفری آلن. (۱۳۹۸). **شرح و نقد نظریه های سازمان و مدیریت**، مترجمان: حسین رحمان سرشت، محبوبه حبیبی بدر آبادی، شهرام خلیل نژاد. تهران، انتشارات دانشگاه علامه طباطبایی

اسناد

۱) کمیته دائمی پدافند غیرعامل کشور.(۱۳۹۴). **سند راهبردی پدافند سایبری کشور**.

منابع اینترنتی

۱) پایگاه اطلاع رسانی مقام معظم رهبری به نشانی:www.leader.ir

۲-۶- منابع لاتین

Articles

1. Alagaraja, M. (2013). **Mobilizing organizational alignment through strategic human resource development**. Human Resource Development International, 16(1), 74-93
2. Alan , C .(2008). **The strategic role of Human Resource Development in managing core competencies**. Human Resource Development International, 11(2),183-197
3. Atif ,A ., Sean, M.(2014). **Teaching information security management: reflections and experiences**. Information Management & Computer Security, 22 (5), 513-536
4. Gurkan. Inan ., Umit, Bititci.(2015). **Understanding organizational capabilities and dynamic capabilities in the context of micro enterprises: a research agenda**. Procedia - Social and Behavioral Sciences ,210 , 310 – 319
5. Hyland, P ., Milia, D., Becker , L ., Karen, L. (2005). **The Role of Human Resource Development in Continuous Improvement: Facilitating Learning and Change**. In Proceedings Australia and New Zealand Academy of Management (ANZAM) Operations Management Conference.
6. Jeroen, K., Spender, J., Aard, G.(2010). **The Resource-Based View: A Review and Assessment of Its Critiques**. Journal of Management, 36(1), 349-372
7. Joseph, L ., Davidson ,B.(2016). **The Dynamic Organizational Model: Its Principles, Implementation Methods and Impact on Corporate Culture** .The Journal of Global Business Management, 12(2),129-138
8. Knight, J. (2015). **Investing in Human Resource Development: Strategic Planning for Success in Academic Libraries**. In Advances in Library Administration and Organization.
9. Koong, Kai S., Mohammad , Merhi., Jun, Sun. (2013).**Push and pull effects of homeland information security incentives**. Information Management & Computer Security. 21 (3), 155-176,
10. Lengnick-Hall, C., Tammy , B ., Lengnick-Hall ,M. (2011). **Developing a capacity for organizational resilience through strategic human resource management**. Human resource management review,21(5),243-255
11. Marcelo Angel, R., Tomás, S., Jose A. ., Isaac, D., Sanchez,G.(2017). **Comparative Study of Cybersecurity Capability Maturity Models**.

12. Mercedes, Úbeda., Enrique, G., Claver, B ., Patrocinio, Z .(2016). **Toward organizational ambidexterity in the hotel industry: the role of human resources**. Cornell Hospitality Quarterly, 57(4), 367-378.
13. Pankaj , M.(2009). **Resource based view (RBV) of Competitive Advantages: Importance, Issues and Implications.** Indian Management Research Journal,1(2),1-16
14. Parsons, K., Agata, Mc., Marcus, B ., Ferguson, L.(2010). **Human Factors and Information Security: Individual, Culture and Security Environment**.
15. Razvan, B., Ken-ichi, C., Yasuo, T ., Yoichi, Sh. (2016). **Towards Efective Cybersecurity Education and Training.** Cybersecurity Education and Training
16. Rima, Kabrilyantsa., Bader , Obeidata., Muhammad, Alshuridehc., Ra'ed ,Masa'deh.(2021). **The role of organizational capabilities on e-business successful implementation**. International Journal of Data and Network Science. 5 , 417–432
17. Zafar, H., Jan, G. ., Myung, S. Ko.(2011). **An Exploration of Human Resource Management Information Systems Security**. Journal of Emerging Knowledge on Emerging Markets,3(1),489-510

Books

1) Council on CyberSecurity (2014), **Cybersecurity Workforce Handbook**, Published by Department of Homeland Security
2) Kovacich, G .(2016). **The information systems security officer's guide Establishing and Managing a Cyber Security Program**, Third edition, Published by Elsevier

Reports

1. Armstrong, M ., Duncan, B.(2019). **Strategic Human Resource Management: Back to the future? ,** Institute for Employment Studies (IES)
2. Commission on enhancing national cybersecurity.(2016). **Report on securing and growing the digital economy.**
3. Curtis, B ., Hefley, B ., Sally, M.(2016). People Capability Maturity Model, Carnegie Mellon University
4. Cyber Security Agency of Singapore(2021). **Operational technology (ot) cybersecurity competency framework.**
5. David, M.(1990). **Analysis of: a military leadership assessment development program**, air war collage.
6. Department of Energy.(2019**). Cybersecurity Capability Maturity ModelVersion 2.0**

7. Department of Homeland Security.(2016). **Cybersecurity workforce development toolki .**
8. Department of Navy.(2019). **Cybersecurity readiness review**
9. National center of incident readiness and strategy for cybersecurity.(2011). **Information Security Human Resource Development Program.**
10. National Cyber Resilience Leaders' Board.(2018). **A cyber resilience strategy for Scotland** .
11. Sultanate of Oman Information Technology Authority(2017), **Cyber security governance guidline**.
12. University of Phoenix.(2018**). Competency Models for Enterprise Security and Cybersecurity**
13. William ,N., Keith, S., Benjamin, S ., Witte, G.(2017). **National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework**