فصلنامه مدیریت و پژوهش‌های دفاعی

شاخصه‌های نیروی انسانی سایبر (متعهد به ارزش‌های انقلاب اسلامی)

هانی رحیم اف[1] | محمدرضا موحدی صفت[2]

۹۹

سال بیست و دوم
بهار ۱۴۰۲

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۱/۱۱/۱۰
تاریخ پذیرش:
۱۴۰۲/۰۴/۱۰
صص: ۱۲۱-۹۹

شاپا چاپی: ۶۱۲۱-۲۰۰۸
الکترونیکی: ۵۲۱۸-۲۶۴۵

چکیده

توانمندی جمهوری اسلامی ایران در انجام اقدامات پیشگیرانه سایبری، مصداقی از فرمایش مقام معظم رهبری در رویکرد تهدید در برابر تهدید است. ارزشمندترین سرمایه سایبری کشور، نیروی انسانی آن بوده که نقش تعیین‌کننده‌ای در موفقیت اقدامات سایبری ایفا می‌نمایند. به‌کارگیری، حفظ و ارتقاء نیروی انسانی مناسب و متعهد به ارزش‌های نهادین انقلاب اسلامی، ضامن پیشرفت در عرصه سایبری است. در پژوهش حاضر، شاخصه های نیروی انسانی سایبر، به‌طور اکتشافی، با رویکرد آمیخته (کمی و کیفی) و استفاده از روش تحقیق تحلیل محتوا و عقلایی، از طریق مصاحبه عمیق با ۹ نفر از فرماندهان و مدیران سطوح راهبردی و عملیاتی حوزه پژوهش و ارائه پرسشنامه به ۶۲ خبره اقدامات سایبری جمهوری اسلامی ایران، به‌دست آمد. بر این اساس، سه مفهوم مهارت، توانایی، عقاید و ارزش‌ها به‌مثابه ابعاد اصلی الگو مورد شناسایی قرار گرفتند و سپس مؤلفه‌های هر یک از این ابعاد استخراج و شاخص‌های هر مؤلفه تعیین گردیدند. پس از تجزیه‌وتحلیل آماری نتایج پرسشنامه، شاخصه های نیروی انسانی سایبر در سه بعد، هفت مؤلفه و سی‌وپنج شاخص ارائه شد.

کلیدواژه‌ها: نیروی انسانی؛ کارشناس سایبری؛ اقدامات سایبری

DOR: 20.1001.1.20086121.1402.22.99.6.6

۱. دانشجوی دکتری، گروه فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران
۲.دانشیار، مدیر گروه فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران

مقدمه

رویکرد تهدید در برابر تهدید، راهبرد جدیدی است که فرمانده معظم کل قوا، در عرصه دفاعی کشور مطرح نموده و نقش مهمی در بازدارندگی در مقابل تهدیدات دشمنان دارد.(کرم روان, ۱۳۹۸, ص. ۶) معظم له طی سخنانی در دانشگاه افسری امام علی علیه‌السلام، می‌فرمایند: «ما اهل تجاوز به هیچ ملتی و هیچ کشوری نیستیم، ما هرگز اقدام به جنگ خونین نمی‌کنیم، ملت ایران این را به اثبات رسانده است، اما ما ملتی هستیم که هرگونه تجاوز را، بلکه هرگونه تهدید را، با استواری و باقدرت کامل پاسخ خواهیم‌داد. ما ملتی نیستیم که بنشینیم تماشا کنیم قدرت‌های پوشالیِ مادی که از درون کرم‌خورده و موریانه خورده‌اند، ملت استوار و پولادین ایران را تهدید کنند. ما در مقابل تهدید، تهدید می‌کنیم.» (مقام معظم رهبری, ۱۳۹۰) توان انجام موفق اقدامات سایبری، یکی از مصادیق این رویکرد در فضای سایبر به شمار آمده و نقش مهمی در بازدارندگی سایبری دارد. نیروی انسانی به‌عنوان یکی از ارکان اصلی قداماتسایبری، در موفقیت آن نقش راهبردی ایفا می‌نماید. درواقع، "نیروی انسانی سهم عمده‌ای در توسعه داشته و مهم‌ترین زیرساخت هر سازمان است. انسان به‌عنوان عنصر اصلی ساختار و مدیریت، می تواند توسعه را به ارمغان آورده یا مانع بزرگ توسعه باشد؛ بنابراین منابع انسانی ارزشمندترین منابع سازمان‌ها محسوب می‌شوند که با تلاش همگانی و ایجاد هماهنگی میان آن‌ها و به‌کارگیری صحیح از آنان و دیگر اجزای سازمان، می توان اهداف سازمانی را تحقق بخشید. این منابع دارای توانایی ها و قابلیت‌های بالقوه‌ای هستند که در محیط سازمانی به فعل تبدیل می‌شوند." (عباس زاده واقفی, ۱۴۰۰, ص. ۲) مجهز بودن یک سازمان به منابع سازمانی توانمند، یک اصل حیاتی است. و هرگاه سازمان‌ها بخواهند در دنیای پیچیده و پویای امروزی به حیات خود ادامه دهند به نیروی انسانی نیازمند بوده و می‌بایست از آن استفاده کنند. (حیدرزاده و همکاران, ۱۳۹۹, ص .۳) بر این اساس شناخت نیروی انسانی مستعد و کارآمد جهت به‌کارگیری در ترفند سایبری، از عوامل مهمی است که موفقیت، توسعه و پیشرفت اقدامات سایبری را در پی دارد. شاخصه های نیروی انسانی سایبر، در پی یافتن ابعاد، مؤلفه‌ها و شاخص‌های بومی‌شده ایست که یک کارشناس سایبری جمهوری اسلامی ایران را تعریف می‌نماید. با به‌کارگیری چنین افرادی ضمن افزایش اثربخشی قدامات سایبری، شاهد ایجاد بازدارندگی و دفاع از زیست‌بوم سایبری جمهوری اسلامی ایران خواهیم بود.

با توجه به اینکه «درس‌آموزی از هر جنگی منجر به کاهش آسیب‌های جنگ بعدی و ارتقای بهره‌وری سازمانی می‌شود؛ سازمان‌های نظامی نیازمند این هستند که با اقدامی خارج از قواعد بروکراسی اداری، دانش فرماندهان و کارکنان خود را حفظ نمایند تا در نبردهای آینده دچار مشکل نگردند. کسب دانش از فرماندهان و سپس انتقال آن به سایر کارکنان و همچنین روزآمد کردن درس آموخته‌ها طی یک مقطع زمانی، امری بسیار حیاتی است.» (جهانفر و همکاران, ۱۳۹۷, ص. ۵) در صورت فقدان شاخصه های نیروی انسانی سایبر، به‌ناچار از الگوهای غیربومی یا نامتناسب با زیست‌بوم سایبری جمهوری اسلامی ایران استفاده خواهد شد که در این صورت، افراد جذب‌شده یا با آرمان‌ها و ارزش های انقلاب اسلامی همخوان نخواهند بود و یا شرایط لازم جهت بکارگیری به‌عنوان کارشناس سایبری را نخواهند داشت. بنابراین ضمن هدر رفت منابع، دست‌یابی به نتیجه مطلوب نیز حاصل نخواهد شد.

با توجه به موارد فوق‌الذکر، در تحقیق حاضر تلاش شده است از طریق اخذ نظرات و مستندسازی دانش و تجربیات فرماندهان، مدیران و خبرگان سایبری با رویکرد اکتشافی، ابعاد، مؤلفه‌ها و شاخص‌های بومی مدیریت و فرماندهی نیروی انسانی در اقدامات سایبری تهیه و الگوی آن ارائه گردد؛ بنابراین، تحقیق حاضر، به دنبال پاسخ به این سؤال اصلی است که: « شاخصه های نیروی انسانی سایبر(متعهد به ارزش‌های انقلاب اسلامی) چیست؟» برای دستیابی به پاسخ این پرسش، این سؤالات فرعی مطرح می‌گردد که «ابعاد، مؤلفه‌ها و شاخص‌های بومی مدیریت و فرماندهی نیروی انسانی سایبرکدام است؟» و «ارتباط این ابعاد، مؤلفه‌ها و شاخص‌ها با یکدیگر چگونه است؟» می‌باشد.

ادبیات نظری پژوهش

بر اساس سند وزارت دفاع آمریکا، اقدامات تهاجمی سایبری عملیاتی است که برای اعمال قدرت با استفاده از زور در فضای سایبر یا از طریق آن، انجام می‌شود. (DoD JP 3-12, 2018, p. GL-5) در تعریف ناتو، عملیات تهاجمی سایبری شامل اقداماتی در/ یا از طریق فضای سایبری است که قدرت ایجاد اثراتی را برای دستیابی به اهداف نظامی طرح‌ریزی می‌کند. (AJP-3.20, 2020, p. 4) در حقیقت هدف حمله سایبری ایجاد مزیت نسبی در عرصه سایبری یا دیگر

عرصه‌های فیزیکی برای نیروهای خودی با به‌کارگیری توان رزم سایبری است. (Williams, 2014, p. 19) عملیات سایبری با درجه بالایی از گمنامی و انکارپذیری همراه بوده و نتایج حاصل از آن عموماً نامشخص است. همچنین ممکن است زمان اجرای آن از دهم ثانیه تا چندین سال متغیر باشد. (Smeets, et. al, 2020, p. 2) بر اساس دستورالعمل سیاست‌های اجرایی رئیس‌جمهور آمریکا، عملیات و برنامه‌ها و فعالیت‌های مرتبط (غیر از دفاع شبکه‌ای ، جمع‌آوری سایبری و اقدامات سایبری تدافعی) چه توسط دولت آمریکا یا با مجوز دولت در فضای سایبری باهدف ایجاد آثار سایبری در خارج از شبکه‌های دولتی آمریکا انجام شود به‌عنوان عملیات تهاجمی سایبری تعریف می‌گردد.(The White House, 2004, p. 3)

کارشناسان سایبری[1] گروهی خبره با دانش فناوری اطلاعات هستند که درک وسیعی از مهارت‌های سایبری داشته و علاوه بر توانایی آغاز اقدامات سایبری، قادر به دفاع از زیرساخت‌های مهم نظامی و راهبردی دولتی نیز می‌باشند. نقش تهاجمی کارشناسان سایبری شامل آغاز فعالانه و واکنشی سایبری با استفاده از تسلیحات سایبری علیه دشمنان است که با مقاصد از بین بردن، سوءاستفاده، اختلال یا جمع‌آوری اطلاعات صورت می‌پذیرد. (Barara, 2019, p. 1) جنگجویان سایبری اغلب در داخل و از طریق فضای سایبری فعالیت می‌کنند تا بر سیستم‌های فیزیکی و ذهن‌های دشمن تأثیر بگذارند. (Allen, 2020, p. 6)

مقاله (وحید سجادی و همکاران, ۱۳۹۹, صص ۱۷.–۲۰) ضمن بررسی راه‌های مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری آمریکا، آموزش نیروی انسانی سایبری متناسب با عملیات سایبری ارتش آمریکا را بالاترین اولویت در ارتقاء توان ارتش جمهوری اسلامی ایران دانسته و تأکید می‌نماید که: "تقویت توان فنی سایبری خودی در هر دو حوزه حمله سایبری و بهره‌گیری سایبری به‌منظور انجام اقدامات تهاجمی علیه شبکه اطلاعاتی وزارت دفاع آمریکا از نظر صاحب‌نظران حائز بالاترین اولویت است."

مقاله (Barara, 2019, pp. 2–4) وجود نیروی انسانی متخصص جهت ایجاد سازمانی با وظیفه انجام عملیات سایبری توسط دولت‌ها را به دلیل وجود تهدیدات متعدد فضای سایبر، قانونی و مشروع به‌حساب آورده و جزء دفاع مشروع قرار می‌دهد؛ همچنین استخدام نیروی انسانی داخلی

1. Cyber Warriors

یا خارجی متخصص در عملیات سایبری و آموزش و ارتقاء سطح مهارت‌های آن‌ها را از ملزومات تشکیل سازمان عملیات سایبری می‌داند. وظیفه اصلی این سازمان، حفاظت از حاکمیت سایبری دولت ملی و زیرساخت‌های نظامی، دولتی و غیرنظامی سایبری بوده و برای دستیابی به این هدف، ایجاد ارتباط مؤثر بین نیروی انسانی فعال در حوزه سایبر ملی و استخدام، آموزش و تقویت ظرفیت آن‌ها همچنین همکاری با متخصصان سایبری خارجی را بسیار حائز اهمیت می‌داند.

(اندرس, ۱۳۹۷, صص ۲۳۱.–۲۴۰) در کتابش بیان می‌دارد که:" در حال حاضر تعداد قابل‌ملاحظه‌ای از نیروی انسانی سایبری آمریکا را نظامیان سابق، افسران ارتش و افراد جذب‌شده از طریق دانشگاه‌های نظامی تشکیل می‌دهند. پیمانکاران دفاعی -که اغلب نیروی کاری اصلی را در این زمینه به کار می‌گیرند- تمایل بیشتری به استفاده از نظامیان سابق دارند؛ زیرا این افراد با مهارت‌های نظامی آشنایی کامل داشته و مسائلی مانند پاک‌سازی ردپا را به‌خوبی می‌شناسند. امروزه اقدامات سایبری، به خط مقدم نبرد تبدیل‌شده است و بازتاب این عمل در محتوای دروسی که در دانشگاه‌های نظامی تدریس می‌شوند نیز تأثیر گذاشته است. وظیفه آژانس امنیت ملی است که این دوره‌های آموزشی را بررسی کرده و کیفیت این مؤسسات آموزشی را تعیین نماید. مهارت‌های عملیات سایبری بیشتر بر توانایی‌های تهاجمی تمرکز دارند. متخصصان آزمون نفوذ و فارغ‌التحصیلان رشته‌هایی مانند مهندسی شبکه، توسعه شبکه و سایر رشته‌های مرتبط می‌توانند بجای حفظ و نگهداری زیرساخت، سیستم‌ها و برنامه‌ها، از مهارت‌هایشان برای از کار انداختن آن‌ها استفاده نمایند. مهارت‌هایی که برای انجام اقدامات سایبری استفاده می‌شوند غیرمعمول نیستند اما کسانی که در این حوزه فعالیت می‌کنند نسبت به همتایان خود در این صنعت بر روی مسائل متفاوت‌تری تمرکز می‌کنند. خصوصیات نیروی انسانی سایبری با نیروی انسانی سنتی تفاوت‌های محسوسی دارد. یکی از این تفاوت‌ها سن افراد است. نیروی انسانی جوان و برخوردار از قدرت جوانی، در جنگ‌های سنتی سختی‌های مبارزه را تحمل کرده و از پس مشکلات برمی‌آید؛ اما معیارهایی نظیر سن، قدرت فیزیکی و آمادگی جسمانی در نیروی انسانی سایبری، از اهمیت کمتری برخوردار بوده و بجای آن معیارهای دیگری مانند هوش، مهارت‌های یادگیری و خلاقیت در حل مسائل، اهمیت فراوانی دارند. نوع نگرش نیروی انسانی اقدامات سایبری نیز با نیروی انسانی جنگ‌های سنتی متفاوت است. افرادی که در اقدامات سایبری شرکت می‌کنند

تمایلی به پیروی از دستورات مقامات بالاتر نداشته و مایل هستند تصمیم گیری ها را خود بر اساس دانش شخصی اتخاذ کنند. این افراد تمایل کمتری برای به اشتراک گذاری دانش و تکنیک‌های مورداستفاده دارند. درواقع توانایی‌های ارزشمند برای نیروی انسانی عملیات سایبری عبارتند از داشتن توانایی‌های ذهنی، خلاقیت، مهارت‌های فنی، توانایی نشستن طولانی‌مدت بر روی یک صندلی، قابلیت ردیابی چندین فعالیت در مجموعه‌ای از نمایشگرها، توانایی یادگیری، توانایی انجام کار گروهی و غیره.

مقاله (کشوری و همکاران ,۱۳۹۷,ص .۴) ویژگی‌های موردنیاز نیروی انسانی در هر مأموریت عملیات سایبری را مطابق جدول ۱ بیان می‌دارد.

جدول.۱. توانایی موردنیاز نیروی انسانی در هر مأموریت عملیات سایبری (کشوری و همکاران ,۱۳۹۷,ص .۴)

ردیف	عنوان مأموریت	اولویت‌های مؤلفه‌های زیست‌آهنگ مأموریت (از راست به چپ اولویت کاهش می‌یابد)
۱	مدیر عملیات	تعامل، تفکر، سناریوپردازی، قوای جسمی
۲	مدیر گروه‌ها	تعامل، تفکر، سناریوپردازی، قوای جسمی
۳	عناصر جمع‌آوری و رصد محیطی	تفکر، تعامل، سناریوپردازی، قوای جسمی
۴	طراح و تحلیل‌گر	تفکر، سناریوپردازی، تعامل، قوای جسمی
۵	برنامه‌نویس و طراح اکسپلویت	تفکر، سناریوپردازی، قوای جسمی، تعامل
۶	سناریونویس و نظریه‌پرداز	سناریوپردازی، تفکر، تعامل، قوای جسمی
۷	عناصر پشتیبانی و فنی	تفکر، قوای جسمی، تعامل، سناریوپردازی
۸	عناصر پشتیبانی واداری	قوای جسمی، تعامل، تفکر، سناریوپردازی
۹	ارزیابی و اثربخشی عملیات	تفکر، تعامل، سناریوپردازی، قوای جسمی
۱۰	تحلیل‌گر محیطی و ارزیابی اثربخشی عملیات	تفکر، سناریوپردازی، تعامل، قوای جسمی
۱۱	مأموریت مهندسی اجتماعی	تعامل، تفکر، سناریوپردازی، قوای جسمی
۱۲	مأموریت‌های خاص آفندی و پدافندی	تفکر، سناریوپردازی، تعامل، قوای جسمی

مقاله (نصرت آبادی و همکاران ,۱۳۹۸ ,ص .۲۰) نیز عامل انسانی را یکی از مؤلفه‌های اصلی عملیات سایبری دانسته و چابکی، فرصت‌طلبی، خلاقیت، دانش، استعداد و تجربه را از شاخص‌های آن برمی‌شمارد.

مقاله (Imamverdiyev, 2015, p. 7) مهارت‌ها و تعداد نیروی انسانی موردنیاز برای ایجاد سازمانی با وظیفه اجرای عملیات سایبری را چنین بیان می‌دارد: تحلیلگر آسیب‌پذیری ۱۰ نفر، برنامه‌نویس بهره‌برداری از آسیب‌پذیری ۷۰ نفر، کارشناس انجام عملیات ۲۰ نفر، کارشناس جمع‌آوری بات ۶۰ نفر، کارشناس شبکه بات ۲۲۰ نفر، کاروَر ۶۰ نفر، برنامه نویسان ۴۰ نفر، متخصص آزمایشگاه سایبری ۱۵ نفر، مشاور فنی ۲۰ نفر، مدیر عالی ۱۰ نفر، مدیر میانی ۵۷ نفر.

همچنین این مقاله یکی از بزرگ‌ترین چالش‌ها در تشکیل چنین سازمان‌هایی را تأمین نیروی انسانی دانسته و بیان می‌دارد که به دلیل کمبود متخصص، دولت‌ها نمی‌توانند مانند نهادهای خصوصی، شرایط مطلوب استخدامی را برای جذب نیروی انسانی عملیات سایبری فراهم کنند لذا بازنده این رقابت هستند. این مطلب، مسئله مشترک بین اکثر کشورهای دنیا است. کمیت و کیفیت دانشجویانی که در رشته‌های فناوری، مهندسی و ریاضی تحصیل می‌کنند، شاخص مهمی برای توسعه منابع انسانی سایبری است. به‌طور مثال، آکادمی نیروی دریایی آمریکا[1] از سال ۲۰۱۶ اقدام به آموزش متخصص عملیات سایبری نموده است. شواهد نشان می‌دهد که مدیران این آکادمی، پنج سال را صرف تدوین برنامه درسی این رشته نموده‌اند. بعلاوه دانشجویان عملیات سایبری، این فرصت را خواهند داشت که در شرکت‌های غیرنظامی مرتبط یا سازمان‌های دولتی مانند آژانس امنیت ملی و اداره تحقیقات فدرال به کارآموزی بپردازند.

در کشور آمریکا، فرماندهی سایبری عهده‌دار به‌کارگیری نیروی انسانی جهت انجام اقدامات سایبری است. این فرماندهی در ۲۳ ژوئن ۲۰۰۹ به‌دستور وزیر دفاع وقت آمریکا در زیرمجموعه فرماندهی راهبردی برای تمرکز بر عملیات سایبری با اهداف نظامی تشکیل و از ۳۱ اکتبر ۲۰۱۰ به‌طور رسمی آغاز به فعالیت نمود. در ۸ اوت ۲۰۱۷ رئیس‌جمهور آمریکا توصیه وزیر دفاع مبنی بر انتزاع فرماندهی سایبری از فرماندهی راهبردی و تأسیس فرماندهی رزمی مستقل متولی عملیات سایبری را پذیرفت و از ۴ می ۲۰۱۸ فرماندهی سایبری آمریکا با وظایفی ازجمله آماده‌سازی، هدایت و اجرای عملیات سایبری با اهداف نظامی به‌منظور ایجاد توانمندی در همه حوزه‌ها و تضمین آزادی عمل آمریکا و متحدانش در فضای سایبر همچنین جلوگیری از اقدام مشابه دشمنان و رقبا تشکیل شد. (وحید سجادی و همکاران, ۱۳۹۹, صص ۱۱۰-۱۱۲) انجام سایبری استاکس‌نت[2] به این فرماندهی با همکاری رژیم صهیونیستی منتسب گردید. این عملیات سایبری، اولین حمله سایبری در دنیا به زیرساخت حیاتی محسوب شده و تأسیسات هسته‌ای جمهوری اسلامی ایران را هدف قرار داد. برای تولید سلاح و اجرای "اقدامات" سایبری استاکس‌نت، منابع قابل‌توجهی از نیروی انسانی، زمان و منابع مالی صرف شده است. متخصصانی که در این حوزه فعالیت می‌کنند؛ بیان

1 Annapolis
2 Stuxnet

داشته‌اند که برای تولید سلاح سایبری استاکس‌نت حداقل به تیمی متشکل از پنج تا ده برنامه‌نویس و کار مداوم و تمام‌وقت به مدت ۶ ماه نیاز است. (Chenands, 2011, p. 93) هر یک از ۴ آسیب‌پذیری روز صفرم مورداستفاده در سلاح سایبری استاکس‌نت، حدود صدها هزار دلار ارزش‌داشته و برای توسعه و ساخت چنین بدافزار پیچیده‌ای حداقل به یک تیم شامل ۵ الی ۱۰ متخصص علوم مختلف رایانه و کار مداوم و تمام‌وقت به مدت ۵ الی ۱۰ ماه با بودجه‌ای میلیون دلاری نیاز است. این موضوع، حمایت و پشتیبانی دولتی را در تولید سلاح و اجرای این عملیات سایبری تأیید می‌کند. (ساکی و همکاران, ۱۳۹۸, ص ۹.)

در کره شمالی نیز نیروی انسانی سایبری بالغبر ۳۰۰۰ نفوذگر نخبه می‌باشد. این افراد در اداره ۹۱ به‌عنوان قرارگاه عملیات سایبری، واحد ۱۲۱ به‌عنوان نفوذ به شبکه‌های خارج از کره شمالی، آزمایشگاه ۱۱۰، واحد ۳۵ به‌عنوان آموزش نیروی انسانی سایبری و عملیات سایبری داخلی، واحد ۲۰۴ به‌عنوان جاسوسی سایبری و جنگ شناختی و درنهایت، اداره ۲۲۵ به‌عنوان مختص در کشور کره جنوبی مستقر هستند. در کشور چین نیز سازمان مجری عملیات سایبری، از سال ۱۹۹۹ تشکیل‌شده و نیروی انسانی آن بالغبر ۶۰۰۰ نفوذگر نظامی است. علاوه بر این تعداد، بیست هزار نیروی انسانی دولتی غیرنظامی نیز با این افراد همکاری می‌نمایند. همچنین بالغبر دو میلیون نفر نیروی انسانی غیردولتی و غیرنظامی نیز مجری سایبری تخریبی هستند.(Imamverdiyev, 2015, pp. 4–5)

روش پژوهش

این تحقیق با روش توصیفی- تحلیلی و موردی- زمینه‌ای به‌صورت آمیخته صورت می‌پذیرد. دلیل توصیفی- تحلیلی بودن، این است که برای گردآوری اطلاعاتی که مدون نشده به کار می‌رود و با این روش، توصیف عینی، واقعی و منظم موضوعات انجام می‌گردد. علت موردی- زمینه‌ای بودن نیز این است که مطالعه عمیق روی نمونه‌هایی از یک پدیده در محیطی واقعی صورت می‌گیرد.

نوع پژوهش درزمینه شناخت شاخصه های نیروی انسانی سایبری، توسعه‌ای خواهد بود؛ زیرا دانش موجود در خصوص موضوع پژوهش را گسترش می‌دهد. از سوی دیگر، کاربرد الگوی ارائه‌شده در حوزه دفاعی و جهت تقویت بازدارندگی جمهوری اسلامی ایران است؛ بنابراین مقاله

حاضر از این منظر کاربردی محسوب گردیده و درمجموع توسعه‌ای- کاربردی خواهد بود. برای جمع‌آوری اطلاعات از روش تحلیل محتوا در کتابخانه علمی- تخصصی و سایت‌های معتبر اینترنتی بهره برده شد. همچنین با روش عقلایی به‌صورت میدانی مصاحبه با خبرگان عملیات سایبری و تنظیم پرسشنامه صورت پذیرفت. برای تحلیل داده‌های بخش کمی (داده‌های حاصل از پرسشنامه) نیز از روش‌های آمار توصیفی و استنباطی ازجمله معادلات ساختاری، تحلیل واریانس، ضریب همبستگی استفاده‌شده است.

به‌منظور اخذ نظر خبرگان جهت ارائه الگوی اولیه پژوهش، مصاحبه عمیق با روش اشباع نظری با جامعه آماری ۹ نفر به‌صورت تمام شمار صورت گرفت؛ بنابراین حجم نمونه با حجم جامعه برابر است. سپس به‌منظور ارزیابی الگوی احصاء شده، پرسشنامه‌ای بر اساس طیف لیکرت تنظیم گردید. با توجه به جامعه آماری ۶۲ نفره -بر اساس جدول مورگان- پرسشنامه به‌صورت تمام شمار به خبرگان ارسال شد؛ بنابراین در این مرحله نیز حجم نمونه با حجم جامعه برابر است. مشخصات خبرگانی که مصاحبه عمیق با آن‌ها صورت پذیرفته یا پرسشنامه به آن‌ها ارسال گردید است؛ در جداول ۲ تا ۴ آمده است. پرسشنامه به لحاظ روایی ظاهری و محتوا به تائید جمعی از اساتید رسانده شد و به لحاظ پایایی با استفاده از نرم‌افزار SPSS آلفای کرونباخ پرسشنامه ۰,۷۷۸ محاسبه شد که پایایی قابل قبولی است.

جدول ۲: وضعیت متغیر سن در جوامع آماری مصاحبه عمیق و پرسشنامه

وضعیت متغیر سن در جامعه آماری مصاحبه عمیق			وضعیت متغیر سن در جامعه آماری پرسشنامه	
سن	فراوانی	درصد فراوانی	فراوانی	درصد فراوانی
کمتر از ۳۵ سال	۰	۰	۱۷	۲۷/۴
35تا ۴۵ سال	۵	۵۵/۶	۴۵	۷۲/۶
بالاتر از ۴۵ سال	۴	۴۴/۴	۰	۰

جدول ۳: وضعیت متغیر سابقه خدمت در جوامع آماری مصاحبه عمیق و پرسشنامه

وضعیت متغیر سابقه خدمت در جامعه آماری مصاحبه عمیق			وضعیت متغیر سابقه خدمت در جامعه آماری پرسشنامه	
سابقه	فراوانی	درصد فراوانی	فراوانی	درصد فراوانی
کمتر از ۱۰ سال	۰	۰	۱۷	۲۷/۴
۱۰ تا ۲۰ سال	۵	۵۵/۶	۴۵	۷۲/۶

بیشتر از ۲۰ سال	۴	۴۴/۴	۰	۰

جدول ۴: وضعیت متغیر تحصیلات در جوامع آماری مصاحبه عمیق و پرسشنامه

وضعیت متغیر تحصیلات در جامعه آماری مصاحبه عمیق			وضعیت متغیر تحصیلات در جامعه آماری پرسشنامه	
تحصیلات	فراوانی	درصد فراوانی	فراوانی	درصد فراوانی
کارشناسی	۰	۰	۱۷	۲۷/۴
کارشناسی ارشد	۵	۵۵/۶	۴۵	۷۲/۶
دکتری	۴	۴۴/۴	۰	۰

جهت بررسی الگو این تحقیق نیز از روش آماری حداقل مربعات جزئی[1] استفاده‌شده است. این روش، در قالب کلی مدل معادلات ساختاری[2] مطرح می‌باشد. الگوسازی معادلات ساختاری از دو بخش الگوی اندازه‌گیری و الگوی ساختاری تشکیل‌شده است. الگوی اندازه‌گیری شامل سؤالات (شاخص‌های) هر بعد به همراه آن بعد است و روابط میان سؤالات و ابعاد در این بخش مورد تجزیه‌وتحلیل قرار می‌گیرد. بخش الگوی ساختاری نیز شامل تمامی سازه‌های مطرح در الگوی اصلی تحقیق است و میزان همبستگی سازه‌ها و روابط علی میان آن‌ها در این قسمت موردسنجش قرار می‌گیرد. شاخص‌ها که معمولاً به سؤال‌های پرسشنامه اطلاق می‌شود، متغیرهای آشکار تحقیق به شمار می‌روند که توسط پاسخگویان به‌طور مستقیم و بی‌واسطه موردسنجش قرار می‌گیرند؛ اما لایه‌های بعدی که مؤلفه‌ها و ابعاد پرسشنامه هستند متغیرهای مکنون[3] می‌باشند که قابلیت سنجش مستقیم نداشته و با استفاده از روابط بین آن‌ها و نشانگرها یا متغیرهای آشکارشان موردسنجش قرار می‌گیرند. (علی نژاد, ۱۳۹۹, ص. ۱۵) اگر مقدار بار عاملی بین سؤالات پرسشنامه و متغیرهای مکنون بیشتر از ۰،۴ باشد نتیجه می‌گیریم که سؤالی که برای آن سازه به‌کاربرده‌ایم به‌خوبی متغیر مکنون موردنظر را سنجیده است. مقدار آماره t درواقع ملاک اصلی تأیید یا رد فرضیات است. اگر این مقدار آماره به ترتیب از ۱،۶۴، ۱،۹۶ و ۲،۵۸ بیشتر باشد نتیجه می‌گیریم که آن فرضیه در سطوح ۹۰، ۹۵ و ۹۹ درصد تأیید می‌شود. همچنین باید گفت که اگر مقدار ضریب مسیر بین متغیر مکنون مستقل و متغیر مکنون وابسته مثبت باشد نتیجه می‌گیریم که با

1 Partial Least Squares
2 Structural Equation Modeling
3 Latent Variables

افزایش متغیر مستقل شاهد افزایش در متغیر وابسته خواهیم بود؛ و بالعکس اگر مقدار ضریب مسیر بین متغیر مکنون مستقل و متغیر مکنون وابسته منفی باشد نتیجه می‌گیریم که با افزایش متغیر مستقل شاهد کاهش در متغیر وابسته خواهیم بود. در این پژوهش برای انجام محاسبات بیان‌شده از نرم‌افزار Smart PLS استفاده‌شده است.

تجزیه و تحلیل داده‌ها

جهت بررسی همبستگی داده‌ها ابتدا باید مشخص شود که داده‌ها پارامتری هستند یا ناپارامتری. برای این منظور از آزمون کلموگوروف- اسمیرنوف استفاده می‌شود. برای بررسی نرمال بودن داده‌ها فرضیه‌ای به شکل زیر مطرح و سپس مورد آزمون قرار گرفت.

H۰: توزیع داده‌های متغیرها نرمال است.

H۱: توزیع داده‌های متغیرها نرمال نیست.

بر اساس اطلاعات به‌دست‌آمده از نتیجه آزمون مذکور، میزان sig متناظر با هر یک از داده‌ها برابر با ۰,۰۰۰ گردید. همان‌طور که مشخص است مقدار مذکور از ۰,۰۵ کمتر است؛ بنابراین داده‌های پرسشنامه از توزیع نرمال برخوردار نیستند و از آمار ناپارامتریک برای تحلیل استنباطی آن‌ها استفاده می‌کنیم. تمامی آزمون‌های آماری بر اساس سطح معناداری قضاوت می‌شود (چه آزمون‌های پارامتریک و چه ناپارامتریک). اگر سطح معناداری کمتر از مقدار خطای ۰,۰۵ به‌دست آمد فرضیه H۱ تائید و اگر بیشتر به‌دست آمد، فرضیه H۰ تائید می‌گردد.

با توجه به ناپارامتری بودن داده‌ها، برای محاسبه ضریب همبستگی از آزمون اسپیرمن بهره می‌بریم.

الف) بررسی ارتباط بین مؤلفه‌ها و ابعاد:

ارتباط بین مؤلفه‌ها و ابعاد با استفاده از ضریب همبستگی اسپیرمن محاسبه‌شده است. فرض H0 بیانگر عدم وجود همبستگی معنی‌دار است و فرض H1 وجود همبستگی معنی‌دار می‌باشد. نتایج این آزمون به شرح جدول ۵ ارائه‌شده است.

(۱) ارتباط بین ابعاد شاخصه های نیروی انسانی عملیات سایبری

جدول ۵: نتایج همبستگی بین ابعاد شاخصه های نیروی انسانی سایبری

بعد	آماره	مهارت	توانایی	عقاید و ارزش‌ها
شاخصه های نیروی انسانی عملیات سایبری	ضریب همبستگی	۰/۸۱۷	۰/۵۸۴	۰/۷۰۹
	سطح معناداری	۰/۰۰۰	۰/۰۰۰	۰/۰۰۰

سطوح معناداری قیدشده در جدول ۵ نشان می‌دهد که در تمامی موارد، ابعاد با همدیگر دارای ارتباط مثبت و معنادار هستند. همچنین همبستگی بین ابعاد ذکرشده با شاخصه های نیروی انسانی سایبری در تمامی موارد معنادار است که نشان‌دهنده وجود همبستگی قوی بین این ابعاد و کل پرسشنامه است.

(۲) ارتباط بین مؤلفه‌های بعد مهارت و بعد مذکور

جدول ۶: نتایج همبستگی بین مؤلفه‌های بُعد مهارت

بعد / مؤلفه		تبحر در دانش عملیات سایبری	یادگیری مستمر	شبکه‌سازی و تیم‌سازی
مهارت	ضریب همبستگی	۰/۶۴۷	۰/۸۹۹	۰/۶۶۲
	سطح معناداری	۰/۰۰۰	۰/۰۰۰	۰/۰۰۰

سطوح معناداری در جدول ۶ نشان می‌دهد که همبستگی بین مؤلفه‌های بعد مهارت با بُعد مربوطه در سطح کمتر یا مساوی ۰/۰۰۱ معنادار است که نشان‌دهنده وجود همبستگی معنادار و غیر تصادفی بین مؤلفه‌های مذکور و بُعد مهارت است.

(۳) ارتباط بین مؤلفه‌های بعد توانایی و بعد مذکور

جدول ۷. نتایج همبستگی بین مؤلفه‌های بُعد توانایی

بعد	مؤلفه	جسمی	روانی
توانایی	ضریب همبستگی	۰/۸۶۲	۰/۸۳۶
	سطح معناداری	۰/۰۰۰	۰/۰۰۰

سطوح معناداری در جدول ۷ نشان می‌دهد که در تمامی موارد، همبستگی بین مؤلفه‌های بُعد توانایی با بعد مربوطه؛ با اطمینان بیش از ۹۹ درصد معنادار است؛ که نشان‌دهنده وجود همبستگی قوی بین این مؤلفه‌ها و بُعد توانایی است.

(۴) ارتباط بین مؤلفه‌های بعد عقاید و ارزش‌ها و بعد مذکور

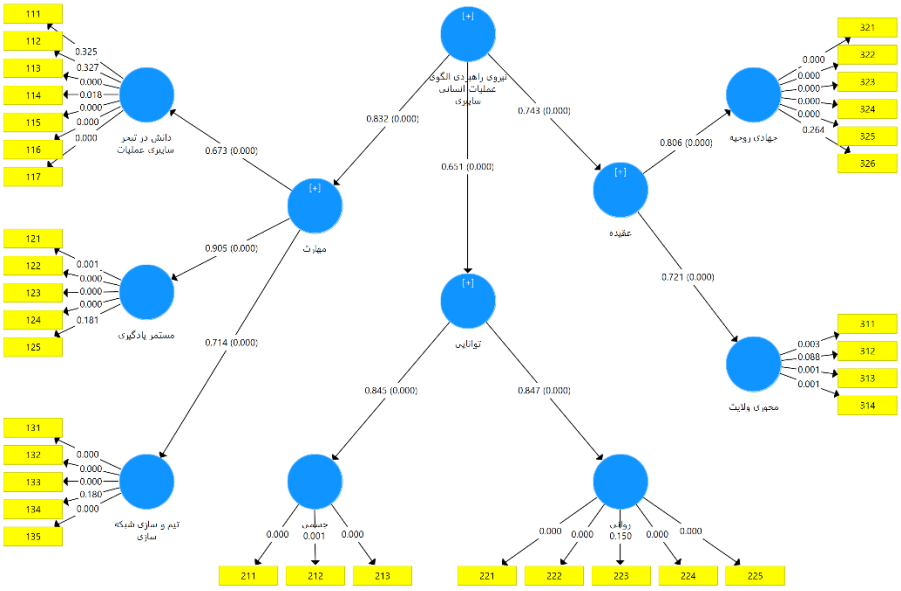
جدول ۸: نتایج همبستگی بین مؤلفه‌های بُعد عقاید و ارزش‌ها

بعد / مؤلفه		ولایت محوری	روحیه جهادی
عقاید و ارزش‌ها	ضریب همبستگی	۰/۷۳۲	۰/۸۲۲
	سطح معناداری	۰/۰۰۰	۰/۰۰۰

سطوح معناداری قیدشده در جدول ۸ نشان می‌دهد که در تمامی موارد، همبستگی بین مؤلفه‌های بُعد عقاید و ارزش‌ها با بعد مربوطه؛ با اطمینان بیش از 99 درصد معنادار است؛ که نشان‌دهنده وجود همبستگی قوی بین این مؤلفه‌ها و بُعد عقاید و ارزش‌ها است.

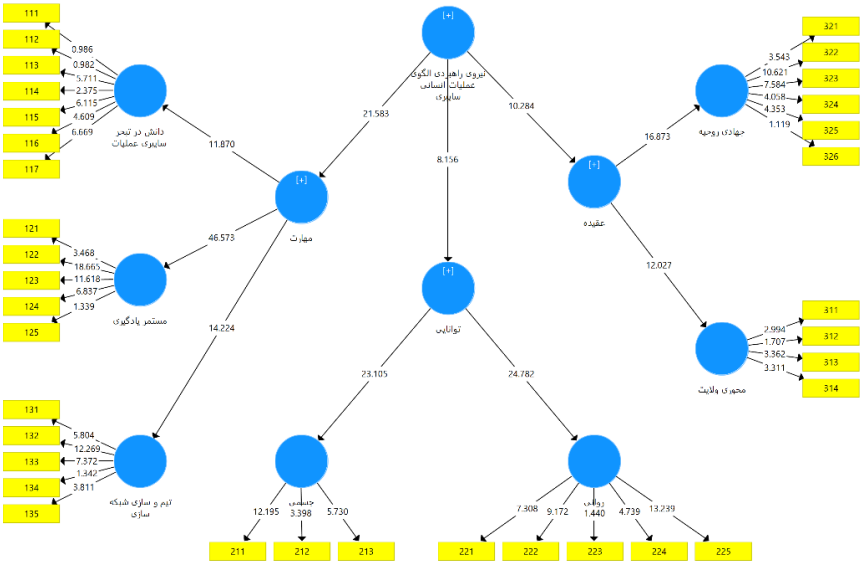
ب) بررسی الگوی تحقیق:

(۱) الگوی ساختاری تحقیق: در شکل‌های ۱ و ۲ الگوی ساختاری تحقیق به همراه ضرایب مسیر الگو، مقادیر t الگوی ساختاری و مقدار P ترسیم‌شده است.



شکل ۱: الگوی ساختاری تحقیق به همراه ضرایب مسیر الگو و مقدار P

در الگوی ساختاری شکل ۱ ابعاد، مؤلفه‌ها و شاخص‌های مورد تأیید نشان داده‌شده‌اند. در این الگو شاخص‌ها همان متغیرهای آشکار هستند که به مؤلفه‌های مربوط به خود متصل شده‌اند. همچنین مقدار بار عاملی، ضرایب مسیر و مقدار P مربوط به ابعاد، مؤلفه‌ها و شاخص‌ها نیز در الگو مشخص‌شده است. در شکل ۲ نیز الگوی ساختاری تحقیق به همراه ضریب معناداری (آماره t) به تصویر درآمده است. با توجه به اینکه مقدار t برای تمام ابعاد و مؤلفه‌های پژوهش بیشتر از ۱/۹۶ هست بنابراین رابطه بین ابعاد و مؤلفه‌ها تائید می‌شود.



شکل ۲: الگوی ساختاری تحقیق به همراه مقادیر t الگوی ساختاری

(۲) نتایج الگوی ساختاری

جدول ۹: نتایج حاصل از یافته‌های الگوی ساختاری تحقیق

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه
مهارت ← شاخصه های نیروی انسانی سایبری	۰/۸۳۲	۰/۰۳۹	۲۱/۵۸۳	۰/۰۰۰	تأیید رابطه
توانایی ← شاخصه های نیروی انسانی سایبری	۰/۶۵۱	۰/۰۸۰	۸/۱۵۶	۰/۰۰۰	تأیید رابطه

عقاید و ارزش‌ها← شاخصه های نیروی انسانی سایبری	۰/۷۴۳	۰/۰۷۲	۱۰/۲۸۴	۰/۰۰۰	تأیید رابطه

جدول ۹ نشان می‌دهد که همه ضرایب الگوی ساختاری با سطح اطمینان ۹۹ درصد یا بیشتر از آن به معناداری آماری رسیده‌اند. معناداری ضرایب آماری نشان می‌دهد که شاخصه های نیروی انسانی سایبری از ابعاد مهارت، توانایی و عقاید و ارزش‌ها تشکیل‌شده است. بعد مهارت با ضریب مسیر ۰٫۸۳۲ بیشترین تبیین را نسبت به شاخصه های نیروی انسانی سایبری دارد؛ به‌عبارت‌دیگر تغییری به‌اندازه یک انحراف معیار در بعد مهارت، موجب ایجاد تغییری به‌اندازه ۰٫۸۳۲ انحراف معیار در الگوی ارائه‌شده خواهد شد. این نتایج نشان می‌دهد که ساختار شاخصه های نیروی انسانی سایبری از استحکام بالایی برخوردار است.

(۳) نتایج الگوهای اندازه‌گیری

جدول ۱۰: نتایج حاصل از یافته‌های شاخصه ها اندازه‌گیری تحقیق

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه
تبحر در دانش عملیات سایبری → مهارت	۰/۶۷۳	۰/۰۵۷	۱۱/۸۷۰	۰/۰۰۰	تأیید رابطه
یادگیری مستمر← مهارت	۰/۹۰۵	۰/۰۷۹	۴۶/۵۷۳	۰/۰۰۰	تأیید رابطه
شبکه‌سازی و تیم-سازی← مهارت	۰/۷۱۴	۰/۰۵۰	۱۴/۲۲۴	۰/۰۰۰	تأیید رابطه
جسمی → توانایی	۰/۸۴۵	۰/۰۳۷	۲۳/۱۰۵	۰/۰۰۰	تأیید رابطه
روانی← توانایی	۰/۸۴۷	۰/۰۳۴	۲۴/۷۸۲	۰/۰۰۰	تأیید رابطه
ولایت محوری← عقاید و ارزش‌ها	۰/۷۲۱	۰/۰۶۰	۱۲/۰۲۷	۰/۰۰۰	تأیید رابطه
روحیه جهادی←	۰/۸۰۶	۰/۰۴۸	۱۶/۸۷۳	۰/۰۰۰	تأیید

عقاید و ارزش‌ها					رابطه

نتایج جدول ۱۰ نشان می‌دهد که:

مؤلفه‌های تبحر در دانش سایبری، یادگیری مستمر و شبکه‌سازی و تیم‌سازی دارای تأثیر مثبت و معنادار بر بعد مهارت هستند. دراین‌بین مؤلفه یادگیری مستمر بیشترین تبیین را نسبت به بعد مهارت دارد. به‌عبارت‌دیگر تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰٫۹۰۵ انحراف معیار در بعد مهارت خواهد شد.

مؤلفه‌های توانایی جسمی و توانایی روانی دارای تأثیر مثبت و معنادار بر بعد توانایی هستند. دراین‌بین مؤلفه توانایی روانی بیشترین تأثیر را نسبت به بعد توانایی دارد. به‌عبارت‌دیگر تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰٫۸۴۷ انحراف معیار در بعد توانایی خواهد شد.

مؤلفه‌های ولایت محوری و روحیه جهادی دارای تأثیر مثبت و معنادار بر بعد عقاید و ارزش‌ها هستند. دراین‌بین مؤلفه روحیه جهادی بیشترین تبیین را نسبت به بعد عقاید و ارزش‌ها دارد. به‌عبارت‌دیگر تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰٫۸۰۶ انحراف معیار در بعد عقاید و ارزش‌ها خواهد شد.

یافته‌ها

بر اساس تجزیه‌وتحلیل‌های بیان‌شده، نیروی انسانی سایبری به سه بعد، هفت مؤلفه و سی‌وپنج شاخص که هر یک در ذیل به‌اختصار بیان می‌شود؛ تقسیم‌بندی می‌گردد.

الف) بعد مهارت

مؤلفه تبحر در دانش عملیات سایبری

بر اساس فرهنگ فارسی عمید، تبحر به معنی بسیار دانا بودن و در امری علم و اطلاع بسیار داشتن است. بدیهی است که یک نیروی عملیات سایبری باید در دانش این‌گونه عملیات تبحر و تسلط داشته باشد. شاخص‌های این مؤلفه عبارتند از: تسلط بر تاکتیک‌ها و تکنیک‌های سایبری، تسلط بر سیستم‌عامل ویندوز و لینوکس، تسلط بر سطوح مقدماتی و متوسط شبکه‌های رایانه‌ای و

امنیت آن، آشنایی با سطح پیشرفته شبکه‌های رایانه‌ای و امنیت آن، تسلط بر مجازی‌سازی، تسلط بر شبکه‌های اجتماعی، تسلط بر یک زبان برنامه‌نویسی.

مؤلفه یادگیری مستمر

دانش رایانه و عملیات سایبری روزبه‌روز در حال پیشرفت و تغییر است. یک کارشناس سایبری برای به‌روز نگه‌داشتن خود باید روحیه یادگیری مستمر را داشته باشد. شاخص‌های این مؤلفه عبارتند از: علاقه و تلاش برای یادگیری،

خلاقیت و نوآوری، مشورت و استفاده از فکر دیگران، داشتن روحیه رشد دهنده، نقادی سازنده و روحیه پرسشگری.

مؤلفه شبکه‌سازی و تیم‌سازی

شاخص‌های این مؤلفه عبارتند از: روحیه و توان انجام کار گروهی و برقراری تعاملات مؤثر، برخورداری از توان ارتباط کلامی با دیگران، نقدپذیری، روحیه انتقال دانش و هم‌افزایی علمی، توانایی تفویض اختیار و تقسیم وظایف.

ب) بعد توانایی

مؤلفه جسمی

ممکن است انجام عملیات سایبری به نظر کار کم‌تحرکی قلمداد شود که توانایی‌های اندکی را نیاز داشته باشد اما به دلیل متفاوت بودن مکان فیزیکی تیم عامل و خطرات احتمالی که در رکن امنیت عملیات به آن‌ها پرداخته شد، نیروی انسانی عملیات سایبری لازم است توانایی جسمی قابل قبولی را دارا باشد. شاخص‌های این مؤلفه عبارتند از: توانایی فیزیکی انجام کار با رایانه، توانایی نشستن طولانی‌مدت برای کار با رایانه، آمادگی جسمانی و تسلط به فنون رزمی برای انجام مأموریت‌های خاص عملیات سایبری زیرا ممکن است گروه مجری سایبری برای رعایت ملاحظات امنیت اقدامات سایبری در مکانی پرخطر مستقر شود. در این صورت لازم است نیروی انسانی سایبری علاوه بر داشتن آمادگی جسمانی بالا، بر فنون رزمی نیز تسلط داشته باشند.

مؤلفه روانی

سلامت روان نیروی انسانی عملیات سایبری اگر از سلامت جسم مهم‌تر نباشد، دارای اهمیت کمتری نیست. شاخص‌های اصلی این مؤلفه عبارتند از: اطمینان به توانمندی‌های شخصی، منطقی بودن و ثبات در رفتار، توانایی اظهارنظر و نقادی، درک شرایط محیطی و تغییرات آن، مثبت نگری واقع‌بینانه.

پ) بعد عقاید و ارزش‌ها

مؤلفه ولایت محوری

ولایت محوری به‌عنوان رکن اصلی جمهوری اسلامی ایران در تمامی امور حاکمیتی نقش پررنگی داشته و نمی‌توان انجام این امور را بدون اصل ولایت محوری در نظر گرفت. شاخص‌های اصلی این مؤلفه عبارتند از: شناخت اصول و مبانی ولایت‌فقیه، فصل‌الخطاب قرار دادن تدابیر و مواضع ولی‌فقیه، عمل به فرامین، توصیه‌ها و رهنمودهای ولی‌فقیه، دفاع همه‌جانبه از ولی‌فقیه و ارزش‌های انقلاب اسلامی.

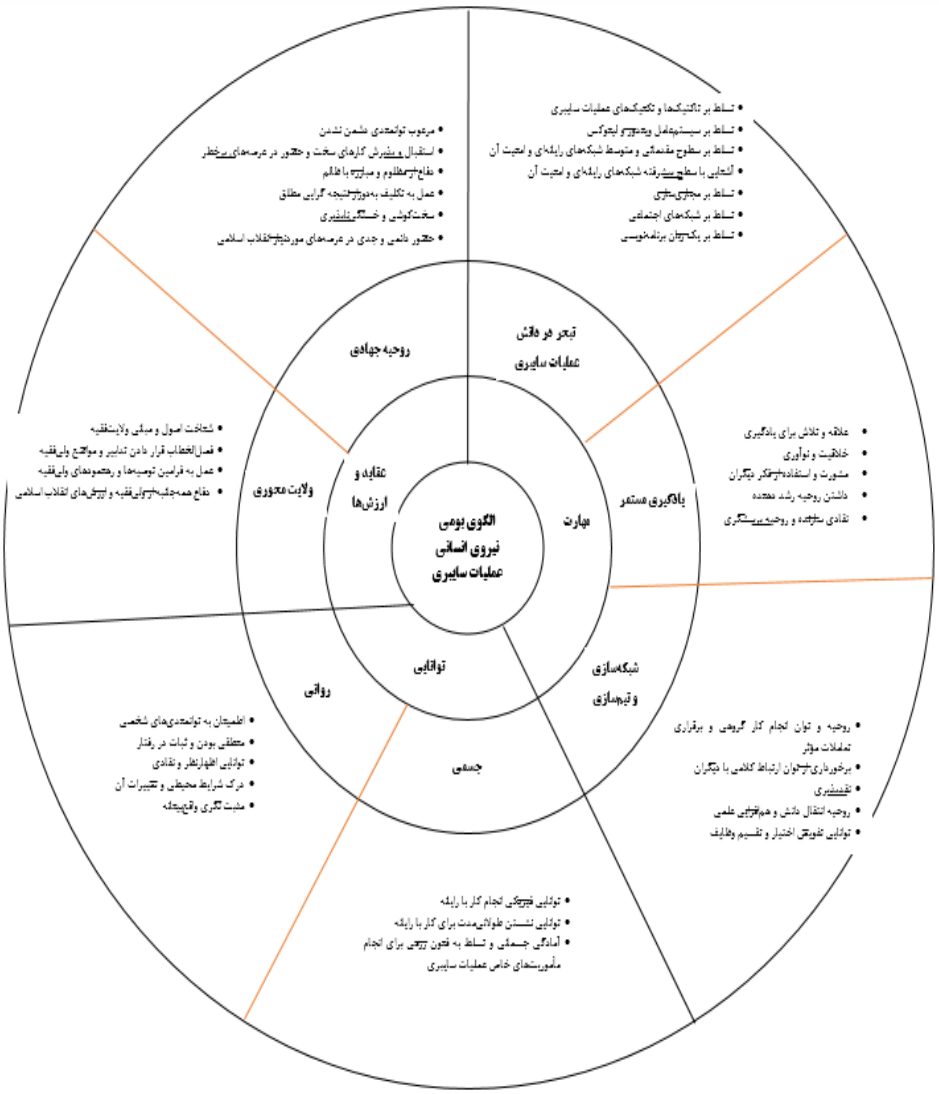
مؤلفه روحیه جهادی

مقام معظم رهبری در ۱۴ دی‌ماه ۸۴ در دیدار با کشاورزان در خصوص روحیه جهادی چنین فرموده‌اند که: «هر بخشی از بخش‌های گوناگون صنعتی و فنی و علمی و تحقیقاتی که ما باروحیه‌ی جهادی وارد شدیم، پیش رفته‌ایم. روحیه‌ی جهادی یعنی چه؟ یعنی اعتقاد به این‌که «ما می‌توانیم»؛ و کارِ بی‌وقفه و خستگی‌ناپذیر و استفاده از همه‌ی ظرفیت وجودی و ذهنی و اعتماد به جوان‌ها. آلان در همین بخش انرژی هسته‌ای که این‌همه دنیای استکبار را سراسیمه کرده، اکثر کسانی که در آنجا مشغول کار هستند، جوان‌های تحصیل‌کرده‌اند؛ صدها جوانِ کم‌سال و تحصیل‌کرده، این چرخ را می‌چرخانند و این عزت را برای کشور پدید آورده‌اند. در همه‌ی بخش‌ها همین‌طور است. به نیروهای بااستعداد، چه از جوان‌ها باشند و چه از انسان‌های باتجربه، اعتماد کنند. اعتماد به این افراد و توکل به خدای متعال و اخلاص نیت برای خدا، اساس کار است.» (مقام معظم رهبری, ۱۳۸۴) شاخص‌های اصلی این مؤلفه عبارتند از: مرعوب توانمندی دشمن نشدن، استقبال و پذیرش کارهای سخت و حضور در عرصه‌های پرخطر، دفاع از مظلوم و مبارزه با

ظالم. در این خصوص مقام معظم رهبری در بیانیه «گام دوم انقلاب» خطاب به ملت ایران چنین می‌فرمایند که: «[انقلاب اسلامی ملّت ایران]، با صراحت و شجاعت در برابر زورگویان و گردنکشان ایستاده و از مظلومان و مستضعفان دفاع کرده است. این جوانمردی و مروّت انقلابی، این صداقت و صراحت و اقتدار، این دامنه‌ی عمل جهانی و منطقه‌ای در کنار مظلومان جهان، مایه‌ی سربلندی ایران و ایرانی است»(مقام معظم رهبری, ۱۳۹۷) یک کارشناس سایبری از فضای سایبر جهت تحقق این مهم استفاده می‌نماید. شاخص دیگر این مؤلفه، عمل به تکلیف به‌دوراز نتیجه گرایی مطلق است. امام خمینی(ره) در سخنرانی خود در ۲۹ بهمن ۵۷ چنین می‌فرمایند که: «من یک تکلیف الهی دارم و مطابق تکلیف الهی عمل می‌کنم. کشته بشوم، عمل کردم به تکلیف الهی؛ پیش ببرم، عمل کردم به تکلیف الهی‌ام. شما تکلیف الهی دارید. متکی به خدا باشید. متکی به امام زمان ـ سلام‌الله‌علیه ـ باشید؛ و شما پیش می‌برید ان‌شاءالله» (امام خمینی(ره), ۱۳۵۷) نیروی انسانی سایبری با این رویکرد تمام تلاش خود را جهت عمل به وظیفه می‌نماید و صرفاً متکی به نتیجه آن نیست. سایر شاخص‌های این مؤلفه عبارتند از: سخت‌کوشی و خستگی‌ناپذیری، حضور دائمی و جدی در عرصه‌های موردنیاز انقلاب اسلامی

نتیجه‌گیری

بر اساس یافته‌های پژوهش، نیروی انسانی سایبری به سه بعد، هفت مؤلفه و سی‌وپنج شاخص تقسیم‌بندی گردید. مهارت به سه مؤلفه تبحر در دانش سایبری، یادگیری مستمر و شبکه‌سازی و تیم‌سازی تقسیم می‌گردد. بعد توانایی نیز به دو مؤلفه جسمی و روانی بخش‌بندی می‌شود؛ و درنهایت بعد عقاید و ارزش‌ها نیز به دو مؤلفه ولایت محوری و روحیه جهادی تقسیم می‌گردد. با توجه به ابعاد، مؤلفه‌ها و شاخص‌های نهایی شده که به تأیید ۶۲ نفر از خبرگان سایبری رسیده است؛ الگوی بومی به شرح شکل ۳ ارائه می‌گردد:



شکل ۳: الگوی تحقیق

پیشنهاد

با توجه به اینکه دانش عمده مرتبط با فضای سایبر در اختیار کشورهای محدودی قرار داشته و عموم کشورها از انتشار دانش عملیات سایبری اجتناب می‌نمایند؛ پیشنهاد می‌شود به‌عنوان

پژوهش‌های آتی برای توانمندسازی نیروی انسانی عملیات سایبری الگوی بومی در سطوح راهبردی و عملیاتی ارائه گردد.

همچنین با توجه به محدودیت نیروی انسانی متخصص سایبری و لزوم استفاده بهینه از توانمندی‌های آن‌ها، پیشنهاد می‌شود به‌عنوان ادامه پژوهش حاضر بر روی شناخت و اولویت‌بندی عوامل مؤثر بر بهره‌وری نیروی انسانی سایبری پژوهشی صورت پذیرفته و الگوی بومی ارتقاء بهره‌وری نیروی انسانی سایبری ارائه گردد.

بعلاوه با توجه به رویکرد بازدارندگی جمهوری اسلامی ایران و راهبردهای ارائه‌شده در این حوزه، پیشنهاد می‌شود طرح‌های راهبردی جهت توانمندسازی یا افزایش بهره‌وری نیروی انسانی اقدامات سایبری جمهوری اسلامی ایران تهیه گردد.

درنهایت، با توجه هجوم تبلیغاتی دشمنان علیه جمهوری اسلامی ایران و صدور کیفرخواست علیه برخی از شهروندان ایرانی به اتهام انجام عملیات سایبری علیه آمریکا پیشنهاد می‌شود ضمن بررسی عوامل مؤثر بر ماندگاری سازمانی نیروی انسانی سایبری، الگوی آن احصاء شده و طرح آن ارائه گردد.

فهرست منابع

امام خمینی(ره). (۱۳۵۷). سخنرانی در جمع نویسندگان (تفرقه بین روحانیون و روشنفکران) ». http://www.imam-khomeini.ir/fa/C207_42096

مقام معظم رهبری. (۱۳۸۴). بیانات مقام معظم رهبری در دانشگاه افسری امام علی «علیه السلام ». https://farsi.khamenei.ir/speech-content?id=3325

مقام معظم رهبری. (۱۳۹۰). بیانات مقام معظم رهبری در دانشگاه افسری امام علی «علیه السلام ». ۱۷۸۶۸https://farsi.khamenei.ir/speech-content?id=

مقام معظم رهبری. (۱۳۹۷). گام دوم انقلاب اسلامی. https://farsi.khamenei.ir/message-content?id=41673

اندرس, ج. (۱۳۹۷). جنگ سایبری: تکنیک‌ها و تاکتیک‌ها و ابزارها برای فعالان حوزه امنیت. موسسه آموزشی و تحقیقاتی صنایع دفاعی.

جهان‌فر, ر., مقدس, م., مسعود, خلعتبری, پور, ط., & کرمی. (۱۳۹۷). مدیریت دانش و بهره‌گیری از تجربیات دفاع مقدس و تأثیرگذاری آن بر عملکرد سازمان (با تأکید بر تجربیات شهید سرلشکر منصور ستاری در نهاجا). فصلنامه علمی آموزش علوم دریایی, ۵(۳), ۱۱۸–۱۳۶.

حیدرزاده, ر., & عبدالهی, د. (۱۳۹۹). نقش مدیریت و رهبری آموزشی در توانمندسازی نیروی انسانی سازمانها. سومین کنفرانس بین المللی روانشناسی، علوم تربیتی، علوم اجتماعی و علوم انسانی

ساکی, ع., & فیلی, ر. (۱۳۹۸). کالبدشکافی و آنالیز رفتار کرم استاکس نت In .دومین همایش بین المللی افق های نوین در علوم پایه و فنی و مهندسی

عباس زاده واقفی, ش. ا. (۱۴۰۰). نقش شایسته سالاری نیروی انسانی در سازمانها. نهمین کنفرانس بین المللی مدیریت امور مالی، تجارت، بانک، اقتصاد و حسابداری .

علی نژاد, میقانی, احمد, بوالحسنی, & رضایت. (۱۳۹۹). مقاله پژوهشی: طراحی الگوی آرایه‌های پدافند زمین به هوا در مقابله با تهدیدات علیه مراکز حیاتی و حساس در افق چشم‌انداز ۱۴۰۴ :dor ۲۰,۱۰۰۱ . ۱,۲۰۰۸۴۸۹۷ .۱۳۹۹,۱۸ .۱ ۸۰,۳. .مطالعات دفاعی استراتژیک, ۱۸(۸۰), ۵۷–۸۲.

کرم روان, ف. (۱۳۹۸). تحلیل حقوقی سند راهبردی پدافند سایبری کشور In .دومین کنفرانس ملی پدافند سایبری .

کشوری, سامان, عباسی, مصطفی, کشوری, عبدالرحمن, نادری, & حسن. (۱۳۹۷). ارائه مدل تصمیم‌یار فرماندهی عملیات سایبری مبتنی بر مدل مارکوفِ زیست‌آهنگ. پدافند الکترونیکی و سایبری, ۶(۱), ۱۰۹–۱۲۱.

نصرت آبادی, ج., لشکریان, ح., مردانی شهربابک, م., & موحدی صفت, م. (۱۳۹۸). ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران. امنیت ملی, ۹(R۳۱# ۰۰۹۱۲ ,(۱۷۳–۱۹۸ .

وحید سجادی*, & داود آذر. (۱۳۹۹). ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری ارتش آمریکا. علوم و فنون نظامی, سال ۱۶, ۵–۲۶.

AJP-3.20. (2020). Allied Joint Doctrine for Cyberspace Operations. Allied Joint Publication - 3.20.

Allen, P. D. (2020). Cyber Maneuver and Schemes of Maneuver. The Cyber Defense Review, 5(3), 79–98.

Barara, I. S. (2019). Capacity Building for Fighting Cyber Wars. CYBERNOMICS, 1(1), 8–12.

ChenandS, T. M. (2011). Abu-Nimeh,"Lessonsfromstuxnet,." Computer, 44(4), 91–93.

DoD JP 3-12. (2018). Cyberspace Operations. In Joint Publication 3-12. Department of Defense United States.

Imamverdiyev, Y. N. (2015). CYBER-TROOPS: FUNCTIONS, WEAPONS AND HUMAN RESOURCES. İTP Jurnalı, 2, 13–21. https://doi.org/10.25045/jpis.v06.i2.02

Smeets, M. & Work, J. D. (2020). Operational Decision-Making for Cyber Operations. The Cyber Defense Review, 5(1). https://doi.org/10.2307/26902658

The White House. (2004). Presidential Policy Directive. 20(c), 1–18.

Williams, B. T. (2014). The Joint Force Commander's Guide to Cyberspace Operations. Joint Forces Quarterly, 73(2), 12–19. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf?ver=2014-04-01-122156-563%5Cnhttp://ndupress.ndu.edu/Media/News/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations/