فصلنامهٔ علمی راهبرد دفاعی، سال هجدهم، شمارهٔ ٦٩، بهار ١٣٩٩

فرمانده معظم کل قوا: «امروز نیروهای مسلح به بهترین نیروی انسانی از لحاظ فکری، عملی، عزم و اراده احتیاج دارند تا بتوانند آسیب‌ناپذیری ملت را در مقابل دشمنی‌ها حفظ کنند.» (١٣٩٦/٠٩/١٢)

مقالهٔ پژوهشی: الگوی توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران[1]

حسن کاویانی[2]، ناصر میرسپاسی[3] و غلامرضا معمارزاده طهران[4]

تاریخ دریافت: ٩٨/٠٩/١٢ تاریخ پذیرش: ٩٨/١٢/٠٧

چکیده

در کنار ابعاد فنی و تجهیزاتی، تحقق امنیت سایبری نیازمند توسعه و پرورش منابع انسانی شایسته و کارآمد است. از این‌رو، در این تحقیق به طراحی الگوی توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران به‌عنوان هدف اصلی تحقیق مبادرت شده است. پژوهش حاضر از لحاظ هدف، کاربردی - توسعه‌ای و از جنبهٔ گردآوری و تحلیل داده‌ها، کمی است. به‌منظور تحقق هدف تحقیق در مرحلهٔ اول با استخراج ١٤٠ شاخص، ٥٠ مؤلفه و ١٥ بُعد از مطالعات اکتشافی، الگوی مفهومی طراحی گردید. در مرحلهٔ دوم بر اساس اجزای الگو، پرسشنامه‌ای تنظیم گردید. روایی (صوری و محتوایی) و پایایی این پرسشنامه با نظرخواهی از تعداد ٨ نفر از خبرگان مورد بررسی قرار گرفت. در مرحلهٔ سوم بر اساس نظریات ٤٣ نفر از خبرگان علمی و اجرایی حوزهٔ امنیت سایبری کشور، مطلوبیت و روابط اجزای الگو با استفاده از نرم‌افزارهای SPSS و PLS مورد ارزیابی قرار گرفت. نتایج این مرحله نشان داد که در سطح $p\leq$ ٠/٠٥ از میان ٢٠ فرضیه تنظیمی به‌جز سه فرضیه، رابطه ابزارهای توسعه کارکنان و فرهنگ جهادی، نقش میانجی بلوغ، مشارکت و همکاری ذی‌نفعان در رابطهٔ بین ابزارهای توسعه ذی‌نفعان و ارتقای حکمرانی امنیت سایبری و نیز نقش میانجی متغیر میانجی گفته‌شده در رابطه بین ابزارهای توسعه ذی‌نفعان و ارتقای شاخص‌های جهانی آمادگی امنیت سایبری، سایر فرضیات معنادار بوده است. در پایان، بر اساس نتایج تحقیق، پیشنهادهایی درخصوص چگونگی تحقق توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ارائه گردیده است.

واژگان کلیدی: توسعهٔ راهبردی منابع انسانی، امنیت سایبری، فضای سایبری، نیروهای مسلح.

---

١. این مقاله برگرفته از رسالهٔ دکترای نویسندهٔ اول می‌باشد.

٢. دانشجوی دکتری مدیریت دولتی، دانشکدهٔ مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران- Hassan.kavyani@gmail.com

٣. استاد مدیریت دولتی، دانشکدهٔ مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (نویسندهٔ مسئول و عهده‌دار مکاتبات)- Mirsepassi@srbiau.ac.ir

٤. دانشیار مدیریت دولتی، دانشکدهٔ مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران- gmemar@gmail.com

مقدمه

ظهور و پیشرفت فناوری‌های ارتباطات و اطلاعات را می‌توان نقطهٔ اهرمی[1] تحولات بنیادین در سیمای جهان و زندگی مردم قلمداد نمود. ابزارهایی که در کنار آثار و مزایای مثبت فراوان بر وجوه مختلف جوامع بشری با متحول نمودن ابزارهای تهدید امنیت ملی، چالش‌های جدیدی را برای دولت‌ها و جامعهٔ بین‌المللی ایجاد نموده‌اند؛ از این‌رو، در دهه‌های اخیر و همزمان با افزایش ضریب نفوذ اینترنت و فضای سایبری[2]، طیف وسیعی از دولت‌ها به‌منظور محافظت از زیرساخت‌ها و شهروندان خود در مقابل تهدیدهای بالقوه و بالفعل سایبری، اقدام به بازطراحی و بازنگری در سیاست‌ها، ساختارها و راهبردهای خود در عرصه‌های امنیتی و نظامی نموده‌اند. در کنار ابعاد فنی و تجهیزاتی، موضوع توسعهٔ توانمندی‌های منابع انسانی و به‌عبارتی نقاط کانونی[3] راهبری و مدیریت فضای سایبری، یکی از محورهای اصلی خط‌مشی‌های این حوزه می‌باشد؛ زیرا درحقیقت توانایی محافظت از زیرساخت‌ها و خنثی نمودن تهدیدهای سایبری به‌میزان آمادگی و صلاحیت آنها بستگی دارد.(Brilingaite, et.al, 2020) با این وجود، شواهد حاکی از آن است که بیشتر کشورهای جهان با چالش کمبود منابع انسانیِ ماهر و توانمند مواجه می‌باشند.(University of Phoenix, 2018)

۱. کلیات

۱-۱. بیان مسئله

فناوری‌های اطلاعات و ارتباطات و فضای سایبری برای ج.ا.ایران نیز همانند سایر کشورها، پیامدهای مثبت و منفی فراوانی به‌همراه داشته است. در حوزهٔ فضای سایبری، کشور با چالش‌های اساسی در حفظ اطلاعات ملی و امنیت سایبری مواجه می‌باشد. برابر برخی آمارها، در سال ۱۳۹٤ روزانه ۱۳ تا ١٤ هزار حملهٔ اینترنتی علیه کشور صورت

1. Leverage Point
2. Cyberspace
3. Focal points

می‌گرفته (فاضلی و افضلی، ١٣٩٤) که تعداد حملات شناسایی و دفع شده آن در سال ١٣٩٨ به‌صورت میانگین به روزانه بیش از ٩٠ هزار حمله افزایش یافته است.(معاون قرارگاه سایبری سازمان پدافند غیرعامل، ١٣٩٨)

نگاهی به سه حمله بزرگ سایبری بدافزارهای «استاکس نت»[1]، «دوکو»[2] و «فلیم»[3] و نیز حملهٔ سایبری به ج.ا.ایران در تاریخ ١٣٩٨/١١/٢٩ نشان می‌دهد که وسعت و ابزارهای به‌کار گرفته شده در این حملات به‌مرور تکمیل‌تر شده و هر بار بر درجهٔ تخریب آنها افزوده شده است. از این‌رو، در دهه‌های اخیر موضوع دفاع و امنیت سایبری در حوزهٔ سیاستگذاری کلان در قالب سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (١٣٨٩) سیاست‌های کلی پدافند غیرعامل (١٣٨٩)، سیاست‌های کلی برنامهٔ ششم توسعه (١٣٩٤) و نیز وظایف و مأموریت‌های شورای عالی فضای مجازی (١٣٩٤) مورد توجه ویژه قرار گرفته است.

در حوزهٔ اجرایی نیز تأسیس و یا بازنگری در مأموریت‌ها، ساختار و وظایف سازمان‌هایی همچون مرکز بررسی‌های راهبردی فضای سایبر، سازمان پدافند غیرعامل، شورای عالی فضای مجازی، پلیس فتا، دادسرای جرایم رایانه‌ای و سازمان امنیت سایبری سپاه پاسداران انقلاب اسلامی نیز حکایت از اهمیت و جایگاه ویژه دفاع و امنیت سایبری در سطح ملی دارد. بر همین اساس و با توجه به اهمیت توسعه منابع انسانی در تقویت توان دفاعی در حوزهٔ امنیت سایبری و نیز وجود سیاست‌ها و ضرورت‌های ایجابی در این خصوص، این سؤال به ذهن متبادر می‌گردد که «آیا در حوزهٔ امنیت سایبری و در سطح نیروهای مسلح، الگو و چارچوب جامعی به‌منظور راهبری و مدیریت فرایندهای توسعهٔ منابع انسانی وجود دارد؟» سؤالی که شواهد مؤید مغفول ماندن آن در حوزهٔ مورد بررسی به‌دلایلی همچون حاکمیت نگرش فنی و نیز نبود یکپارچگی وظایف و مسئولیت‌های نهادهای متولی امنیت سایبری در سطح نیروهای مسلح می‌باشد. بنابراین با توجه به اهمیت

1. Stuxnet
2. Duqu
3. Flame

موضوع توسعهٔ منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران و همچنین خلأ تحقیقاتیِ موجود، این تحقیق به‌دنبال طراحی الگوی توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری و در سطح نیروهای مسلح می‌باشد.

۱-۲. اهمیت و ضرورت تحقیق

عوامل ایجابی اهمیت تحقیق حاضر عبارتند از:

(۱) توسعهٔ الگوهای موجود توسعهٔ راهبردی منابع انسانی متناسب با حوزهٔ امنیت سایبری و نیروهای مسلح ج.ا.ایران.

(۲) ایجاد فهم و بینش مشترک درخصوص موضوع توسعه و آموزش مصرحِ در سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (۱۳۸۹).

(۳) ایجاد فرصت و بستر مناسب جهت تبیین بیشتر و بهتر نقش و جایگاه توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران.

(٤) ایجاد هم‌افزایی در بین سازمان‌های مسئول در حوزهٔ امنیت سایبری در سطح نیروهای مسلح از طریق ایجاد نقشهٔ راه جامع و متناسب با حوزهٔ امنیت سایبری و زیست‌بوم ج.ا.ایران.

(۵) ارائهٔ ابزاری متناسب با شرایط نیروهای مسلح ج.ا.ایران و حوزهٔ امنیت سایبری جهت بررسی اثربخشی و کارایی سازوکارهای کنونی توسعه و آموزش منابع انسانی و طراحی نظام (سیستم)های مناسب و اثربخش.

عوامل سلبی ضرورت تحقیق حاضر عبارتند از:

(۱) کاهش خلأ تحقیقاتی و عملی توسعهٔ منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران.

(۲) جلوگیری از مغفول ماندن نقش توسعهٔ منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران.

(۳) شناسایی ابعاد و اجزای اثرگذار بر توسعهٔ منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران.

۱-۳. پیشینهٔ تحقیق

(۱) «سوری‌زاده و همکاران» (۱۳۹۷) در تحقیقی بر اساس نظرات نمونه‌ای ۷۰ نفره از متخصصان، به ارزیابی و اولویت‌بندی شاخص‌های دفاع سایبری پرداخته‌اند؛ بر اساس نتایج به ترتیب توجه به شاخص‌های نیروی انسانی، امنیت، ساختار تشکیلاتی موقعیتی، اقتصادی، نگرش راهبردی سیاسی، فناوری‌های (مدرن) نوین، نظارت مستمر و ارزیابی تخصصی حائز اهمیت می‌باشند.

(۲) «کالینز و همکاران» (۲۰۱٦) با استفاده از تحلیل حوادث مستند شده و با رویکرد تحلیل شکاف وضعیت آموزشی نیروی کار، امنیت سایبری را در صنعت، دانشگاه‌ها و دفاع مورد تحلیل قرار دادند؛ نتایج نشانگر آن بود که در نیروی کار دولتی ایالات متحده در سه طبقه تجزیه و تحلیل، گردآوری اطلاعات و تحقیق و دو حوزهٔ تخصصی عملیات اطلاعاتی و سایبری شکاف وجود دارد. بررسی‌های صورت گرفته در این حوزه بیانگر آن بود که در سه طبقهٔ یادشده، شرح شغل‌های کمی وجود دارد. در بخش صنعت نیز یافته‌ها حاکی از عدم شناخت و آگاهی مدیران و رهبران عالی در زمینه‌های فنی و عملیاتی است. در دانشگاه‌ها نیز بیشتر بر جنبه‌های فنی در آموزش سایبری تأکید می‌شود و دانشجویان جهت پاسخگویی به بخشی از مشکلات آماده می‌شوند. در این حوزه نیاز است تا بر مهارت‌های نرم انسان‌محور ارتقای نوآوری و حل مسئله تأکید گردد.

(۳) «مرکز ملی آمادگی حوادث و راهبرد امنیت سایبری ژاپن» (۲۰۱۱) پس از بررسی وضعیت و چالش‌های امنیت اطلاعات در سطح ملی، اذعان داشت که بهبود کامل امنیت اطلاعات زمانی حاصل می‌شود که توسعهٔ منابع انسانی پیشرفته برای حوزهٔ فناوری اطلاعات و ارتباطات در تمام سطوح نهادینه گردد. این سازمان به این منظور برنامه‌ای را تدوین و ارائه نموده که هدف از آن، توسعهٔ منابع انسانی امنیت اطلاعات در سازمان‌های دولتی، شرکت‌ها و مؤسسه‌های آموزشی است. در این برنامه پنج مفهوم بنیادین در جهت توسعهٔ منابع انسانی امنیت اطلاعات شامل توسعه و حفظ منابع انسانی پیوندی

(هیبریدی)، ایجاد محیط مناسب جهت توسعهٔ منابع انسانی امنیت اطلاعات، تقویت همکاری دانشگاه و صنعت، توسعهٔ منابع انسانی از طریق تحقیق و توسعهٔ پیشرفته و احیای صنعت امنیت اطلاعات و نیز توسعهٔ منابع انسانی به‌عنوان بازیگران بین‌المللی ارائه گردیده است.

بر اساس نتایج بررسی پیشینهٔ تحقیق می‌توان ادعا نمود که در عرصهٔ بین‌المللی، توسعهٔ کارکنان حوزهٔ امنیت سایبری یکی از مسائلی است که در سالیان اخیر بیش از گذشته مورد توجه کشورهای مختلف قرار گرفته است. موضوعی که در حوزهٔ سیاستگذاری در داخل نیز به آن توجه ویژه‌ای مبذول گردیده است.[1] اما بررسی مطالعات داخلی نشان می‌دهد که این موضوع چندان مورد توجه پژوهشگران قرار نگرفته است. از این‌رو، انجام این پژوهش از لحاظ مناسبت و ضرورت تدوین نقشه راهی جامع به‌منظور توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری و سطح نیروهای مسلح، اقدامی نوآورانه محسوب می‌گردد.

۱-۴. سؤال‌های تحقیق

۱-۴-۱. سؤال اصلی

الگوی توسعهٔ راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح چیست؟

۱-۴-۲. سؤال‌های فرعی

(۱) ابعاد، مؤلفه‌ها و شاخص‌های الگوی توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران کدامند؟

---

۱. سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (۱۳۸۹) و احکام انتصاب اعضای شورای عالی فضای مجازی در سال ۱۳۹۴

(٢) روابط بین ابعاد، مؤلفه‌ها و شاخص‌های الگوی توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران چگونه است؟

پس از تدوین الگوی مفهومی برگرفته از مطالعات اکتشافی به‌منظور بررسی روابط بین اجزای الگوی فرایندی توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ٢٠ فرضیه به‌شرح زیر تنظیم و مورد آزمون قرار می‌گیرد:

(١) محیط دور (بین‌المللی) بر محیط نزدیک تأثیری معنادار و مثبت دارد.

(٢) محیط دور (بین‌المللی) بر عوامل سازمانی نهادهای متولی امنیت سایبری (ساختار، فرهنگ، راهبرد و فناوری) تأثیری معنادار و مثبت دارد.

(٣) محیط نزدیک بر عوامل سازمانی نهادهای متولی امنیت سایبری (ساختار، فرهنگ، راهبرد و فناوری) تأثیری معنادار و مثبت دارد.

(٤) عوامل سازمانی بر توسعهٔ راهبردی منابع انسانی در نهادهای متولی امنیت سایبری تأثیری معنادار و مثبت دارند.

(٥) توسعهٔ راهبردی منابع انسانی بر ابزارهای توسعه کارکنان تأثیری معنادار و مثبت دارد.

(٦) توسعهٔ راهبردی منابع انسانی بر ابزارهای توسعه ذی‌نفعان تأثیری معنادار و مثبت دارد.

(٧) ابزارهای توسعهٔ کارکنان بر منابع انسانی پویا تأثیری معنادار و مثبتی دارد.

(٨) ابزارهای توسعهٔ کارکنان بر رهبران تحول‌آفرین تأثیری معنادار و مثبتی دارد.

(٩) ابزارهای توسعهٔ کارکنان بر فرهنگ جهادی تأثیری معنادار و مثبتی دارد

(١٠) ابزارهای توسعهٔ کارکنان بر سازمان پویا تأثیری معنادار و مثبتی دارد

(١١) ابزارهای توسعهٔ ذی‌نفعان بر ارتقای حکمرانی امنیت سایبری تأثیری معنادار و مثبتی دارد

(١٢) ابزارهای توسعهٔ ذی‌نفعان بر بهبود شاخص‌های توسعهٔ انسانی تأثیری معنادار و مثبت دارد.

(١٣) ابزارهای توسعهٔ ذی‌نفعان بر ارتقای شاخص‌های جهانی پایداری امنیت سایبری تأثیری معنادار و مثبت دارد.

(١٤) بلوغ کارکنان تأثیر ابزارهای توسعهٔ کارکنان بر منابع انسانی پویا را تعدیل می‌کند.

(١٥) بلوغ کارکنان تأثیر ابزارهای توسعهٔ کارکنان بر رهبران تحول‌آفرین را تعدیل می‌کند.

(١٦) بلوغ کارکنان تأثیر ابزارهای توسعهٔ کارکنان بر فرهنگ جهادی را تعدیل می‌کند.

(١٧) بلوغ کارکنان تأثیر ابزارهای توسعهٔ کارکنان بر سازمان پویا را تعدیل می‌کند.

(١٨) مشارکت و همکاری سایر ذی‌نفعان تأثیر ابزارهای توسعهٔ ذی‌نفعان بر ارتقای حکمرانی امنیت سایبری را تعدیل می‌کند.

(١٩) مشارکت و همکاری سایر ذی‌نفعان تأثیر ابزارهای توسعهٔ ذی‌نفعان بر بهبود شاخص‌های توسعهٔ انسانی را تعدیل می‌کند.

(٢٠) مشارکت و همکاری سایر ذی‌نفعان تأثیر ابزارهای توسعهٔ ذی‌نفعان بر ارتقای شاخص‌های جهانی پایداری امنیت سایبری را تعدیل می‌کند.

١-٥. روش تحقیق

مطالعه حاضر از لحاظ هدف، نوعی تحقیق توسعه‌ای محسوب می‌گردد. لیکن با توجه به اینکه نتایج این تحقیق به‌منظور حل مسئله توسعهٔ راهبردی منابع انسانی (قلمرو موضوعی تحقیق) در درون سازمان‌های متولی امنیت سایبری در سطح نیروهای مسلح (قلمرو سازمانی تحقیق) مورد استفاده قرار خواهد گرفت، می‌توان آن‌را گونه‌ای از تحقیقات کاربردی قلمداد نمود. همچنین تحقیق حاضر از لحاظ چگونگی اجرا، تحقیقی پس رویدادی و تک‌نمونه‌ای است که با استفاده از تحقیق میدانی، داده‌های مورد نیاز خود را در سال ١٣٩٨ (بازه زمانی پژوهش) گردآوری و با استفاده از رویکرد کمّی، به تحلیل آنها می‌پردازد. در این پژوهش در گام نخست با بررسی پیشینه، نظریه‌ها و اسناد بالادستی، تعداد ١٥ بُعد، ٥٠ مؤلفه و ١٤٠ شاخص به‌عنوان اجزای اصلی الگوی فرایندی توسعهٔ راهبردی منابع انسانی در ج.ا.ایران و حوزهٔ امنیت سایبری تعیین گردیدند. در مرحلهٔ دوم، پس از تدوین پرسشنامه‌ای بر اساس مفاهیم مستخرج از مطالعات اکتشافی، به‌منظور تعیین روایی منطقی (ظاهری و محتوا) و پایایی پرسشنامه در اختیار تعداد ٨ نفر از خبرگان دانشگاهی شاغل در واحدهای عملیاتی و اجرایی

حوزهٔ امنیت سایبری و امنیت اطلاعات نیروهای مسلح ج.ا.ایران قرار گرفت که نتایج روایی محتوا و پایایی ابعاد اصلی الگو در جدول شمارهٔ (١) ارائه گردیده است.

جدول شمارهٔ (١): روایی محتوا و پایایی ابعاد اصلی تحقیق

ردیف	ابعاد	تعداد شاخص	روایی محتوا (Cvr≥0/59)	آلفای کرونباخ (α≥0/7)
١	محیط دور	٤	٠/٧٥	٠/٨٥
٢	محیط نزدیک	١٠	١	٠/٨٦
٣	عوامل سازمانی	١١	٠/٧٥	٠/٨٢
٤	توسعهٔ راهبردی منابع انسانی	٩	١	٠/٩
٥	ابزارهای توسعهٔ کارکنان	٦	٠/٧٥	٠/٧٣
٦	ابزارهای توسعهٔ سایر ذی‌نفعان	٧	٠/٧٥	٠/٨٦
٧	میزان بلوغ کارکنان	٦	٠/٧٥	٠/٨١
٨	بلوغ، همکاری و مشارکت سایر ذی‌نفعان	٣	٠/٧٥	٠/٨٦
٩	پرورش منابع انسانی پویا	١٢	١	٠/٨٩
١٠	پرورش رهبران تحول‌آفرین	٩	١	٠/٩١
١١	فرهنگ جهادی	٩	٠/٧٥	٠/٧٣
١٢	سازمان پویا	١٤	١	٠/٨٧
١٣	ارتقای حکمرانی امنیت سایبری	٨	١	٠/٨١
١٤	بهبود شاخص‌های جهانی آمادگی امنیت سایبری	٩	١	٠/٧٢
١٥	بهبود شاخص‌های توسعهٔ انسانی	٣	٠/٧٥	٠/٨٨

در مرحلهٔ بررسی روایی شاخص‌ها، با توجه به مقادیر ضریب لاشه، ١١ شاخص از مجموع ١٤٠ شاخص ابتدایی به‌علت کسب نمرهٔ نامطلوب حذف و تعداد شاخص‌های الگوی مفهومی تحقیق به ١٢٩ شاخص تقلیل یافت. جامعهٔ آماری پژوهش شامل دو گروه فرماندهان و مدیران عالی حوزهٔ امنیت سایبری (ستاد کل نیروهای مسلح، ارتش ج.ا.ایران، سپاه پاسداران انقلاب اسلامی، نیروی انتظامی و سازمان پدافند غیرعامل کشور) و استادان دانشگاهی و اعضای هیئت‌علمی دانشگاه‌های نظامی (دانشگاه عالی دفاع ملی، دانشگاه امام حسین(ع)، دانشگاه صنعتی مالک اشتر، دانشگاه پدافند هوایی خاتم‌الانبیاء(ص) و دانشکده فارابی) است که تعداد آنها ٥٩ نفر

برآورد گردید. با توجه به محدود بودن تعداد نفرات، از روش تمام شماری جهت توزیع پرسشنامه‌ها و گردآوری اطلاعات استفاده شد. در مرحلهٔ تجزیه و تحلیل داده‌ها با استفاده از نرم‌افزارهای «اس.پی.اس.اس»[1] و «اسمارت پی.ال.اس»[2] و تعداد ٤٣ پرسشنامه دریافتی از خبرگان بررسی گردید.

۲. ادبیات و مبانی نظری تحقیق

۲-۱. توسعهٔ راهبردی منابع انسانی

مفهوم توسعهٔ منابع انسانی در عصر جدید را می‌توان در قالب سه رویکرد آموزش و توسعه، توسعهٔ منابع انسانی و توسعهٔ راهبردی منابع انسانی مورد بررسی قرار داد. مفاهیم درهم آمیخته‌ای که تعیین حدود و ثغور آنها در دنیای واقعی دشوار است.(Sambrook, 2000) آموزش و توسعه به‌عنوان یکی از ابزارهای انقلاب صنعتی درصدد استانداردسازی و تخصصی نمودن وظایف کارکنان بود.(تافلر، ١٣٦٦: ٦٤) در این دوره به کارکنان سازمان‌ها به‌عنوان نیروهایی غیرماهر نگریسته می‌شد که نیاز به آموزش دارند تا به استانداردهای لازم برای کار برسند.(والتون، ١٣٩٢: ٨٠) از این‌رو، برنامه‌های آموزشی در رویکرد برنامه‌ریزی شده بیشتر بر توسعهٔ نیروی انسانی در راستای مشاغل کنونی و مهارت‌های تکموردی متمرکز بودند.(Siugdinien, 2008)

مفهوم توسعهٔ منابع انسانی به‌عنوان دومین رویکرد مطرح در این حوزه در سال ۱۹۷۰ توسط «نادلر» ارائه گردید. از دیدگاه او توسعهٔ منابع انسانی دارای سه شاخصهٔ مهم یادگیری سازمان‌یافته تجارب، یادگیری در دورهٔ زمانی مشخص و یادگیری به‌منظور بهبود عملکرد و یا رشد شخصی است. «نادلر» سه فعالیت آموزش (یادگیری با تمرکز بر مشاغل کنونی یادگیرنده)، تربیت[3] (یادگیری با تمرکز بر مشاغل آتی یادگیرنده) و توسعه[4] (یادگیری بدون تمرکز بر شغل) را به‌عنوان مراحل توسعهٔ منابع انسانی معرفی می‌نماید. در

1. SPSS
2. Smart PLS
3. Education
4. Development

این رویکرد برنامه‌ها در واکنش و پاسخ به راهبردهای کسب و کار تدوین و سپس اجرا می‌گردند.(McCracken&et.al: 2000) با این وجود، بررسی نظریه‌های مطرح در این حوزه نشانگر آن است که در اواخر دههٔ ۸۰ مفهوم توسعهٔ منابع انسانی به‌علت ارائه دیدگاه‌ها، تعاریف و چارچوب‌های نظری بسیار متفاوت و گاهی متناقض دچار بحران هویت گردید.(Mc Goldrick&et.al, 2001) برای مثال، در حالی که نادلر از یادگیری سازمان یافته، رسمی و مبتنی بر زمان و نیز تمرکز بر کارکنان به‌عنوان ارکان و مفروضه‌های توسعهٔ منابع انسانی یاد نموده (Nadler, 1992) برخی دیگر از محققان یادگیری غیررسمی، مادام‌العمر و تمرکز بر اهداف سازمانی را به‌عنوان ویژگی‌های توسعهٔ منابع انسانی مطرح نموده‌اند. (Sambrook, 2001) این عوامل در کنار ظهور برق‌آسای فناوری‌های نوین و لزوم پیش‌بینی و ایجاد تغییرات در مشاغل، دانش و مهارت‌های کارکنان و نیز ظهور مفهوم مدیریت راهبردی منابع انسانی به‌عنوان رویکردی جدید در مدیریت منابع انسانی، بستر توجیهی و نظری لازم برای گذار از توسعهٔ منابع انسانی به رویکرد توسعهٔ راهبردی منابع انسانی به‌عنوان رویکردی مکمل برای فرایندهای آموزش و توسعهٔ منابع انسانی ایجاد نمود.

بر اساس ویژگی‌های تبیین شده، توسعهٔ راهبردی منابع انسانی عبارت از رویکردی جامع، مستمر، تحول‌آفرین و هم‌راستا با اهداف و راهبردهای سازمانی است که در بلندمدت با خلق و توسعهٔ شایستگی‌ها و قابلیت‌های منحصربه‌فرد می‌تواند بر راهبردها و محیط درون و برون‌سازمانی اثرگذار باشد. در این رویکرد بر تمرکز بر سه سطح فردی، سازمانی و اجتماعی به‌صورت هم‌زمان و متوازن تأکید می‌گردد.

۲-۲. توسعهٔ منابع انسانی در حوزه امنیت سایبری

در دهه‌های اخیر و همگام با ظهور و توسعه فناوری‌های نوین ارتباطی و به‌ویژه اینترنت و با توجه به بروز تهدیدها و چالش‌های جدیدی در عرصهٔ بین‌المللی، منطقه‌ای، ملی و داخلی، رویکرد و مفهوم جدیدی در حوزهٔ امنیتی با عنوان «امنیت سایبری» مطرح شده است. امنیت سایبری را می‌توان به‌عنوان حفاظت از اطلاعات و زیرساخت‌ها از حملات اینترنتی تبیین

نمود.(Koong&et.al, 2013) اهمیت این موضوع به اندازه‌ای است که در کنار اقدام‌های داخلی کشورها، جامعهٔ بین‌المللی نیز به‌منظور تقویت همکاری‌های بین‌المللی برای مواجهه و مقابله با تهدیدهای سایبری، اقدام به تهیه و تصویب کنوانسیون جرایم سایبری[1]، تعیین شاخص‌های جهانی امنیت سایبری[2] و ... نموده است. با این‌وجود، در بیشتر موارد، موضوع امنیت سایبری به‌عنوان پدیده‌ای فنی نگریسته شده، در حالی که تجارب و شواهد مؤید آن است که داشتن نیروی کار سایبریِ متعهد و متخصص در کنار شهروندان آگاه نسبت به فضای سایبری، یکی از کلیدی‌ترین شروطِ موفقیت در تأمین امنیت سایبری است.(گروه اطلاعات و حفاظت اطلاعات، ۱۳۹۵)

در سالیان اخیر کشورهای مختلف در راستای ارتقای قابلیت‌های مواجهه و پاسخگویی مناسب به تهدیدهای سایبری اقدام به تدوین چارچوب‌ها، الگوها و شیوه‌نامه‌هایی در راستای توسعه و آموزش نیروی کار متخصص خود نموده‌اند. برای مثال، وزارت امنیت داخلی آمریکا در سال ۲۰۱۶ اقدام به ارائه الگویی در این حوزه نموده است در این الگو، مراحل برنامه‌ریزی در حوزهٔ آموزش نیروی کار سایبری شامل پنج مرحله «بررسی خطرهای امنیت سایبری»، «بررسی موجودی نیروی کار امنیت سایبری»، «تعیین شکاف‌ها»، «بررسی شکاف‌ها» و «بررسی و به‌روزرسانی» تعیین گردیده است. در این الگو به‌شکل همزمان بر توسعهٔ کارکنان و توسعهٔ سازمان تأکید شده است. پیامدهای مطلوب این الگو در حوزهٔ توسعهٔ کارکنان، توسعه و پرورش کارکنان حرفه‌ای و جامع (جنرالیست) و نیز ایجاد و توسعهٔ گروه‌های امنیت سایبری با عملکرد بالا در سطح سازمانی است. در این الگو ۵ ویژگی چابکی، چندوظیفه‌ای بودن، پویایی، منعطف بودن و غیررسمی بودن برای گروه‌های امنیت سایبری در نظر گرفته شده است. (Department of Homeland, 2016)

طرح آموزش امنیت سایبری به‌عنوان یکی از جامع‌ترین الگوها و چارچوب‌های مطرح در حوزهٔ آموزش و توسعهٔ منابع انسانی در حوزهٔ امنیت سایبری در سال ۲۰۱۲ توسط

1. Convention on Cybercrime
2. Global Cybersecurity Index

مؤسسهٔ ملی استاندارد و فناوری و با همکاری سایر سازمان‌های دولتی، دانشگاه‌ها و بخش خصوصی منتشر شد. هدف نهایی این طرح، پرورش نیروی کار توانمند در حوزهٔ سایبری (در سطح جهانی) عنوان شده است. این چارچوب شامل هفت طبقه تخصصی (ارائهٔ ایمن، عملیات نگهداری، حفاظت و دفاع، تجزیه و تحلیل، گردآوری و عملیات، تحقیق و نظارت و راهبری سازماندهی) است که هر کدام از آنها شامل چند حوزهٔ تخصصی (در مجموع ۳۱ حوزه) و هر حوزه خود شامل چندین نقش کاری است. در این چارچوب برای هر نقش کاری به‌تفصیل مجموعه دانش، مهارت و توانایی‌های مورد نیاز تعیین شده است. در این الگو که در سالیان اخیر به‌عنوان الگویی جامع توسط برخی کشورها مورد استفاده قرار گرفته، به‌منظور آموزش و توسعهٔ نیروی کار مستعد در حوزهٔ امنیت سایبری، سازوکارهایی همچون کار راهه شغلی، آموزش گروهی و گردش شغلی پیشنهاد شده است.(William&et.al, 2017)

۲-۳. الگوی مفهومی تحقیق: پس از مطالعات اکتشافی و کدگذاری مفاهیم مستخرج مطابق جدول شمارهٔ (۲) تعداد ۱۵ بُعد، ۵۰ مؤلفه و ۱٤۰ شاخص به‌عنوان اجزای اصلی الگوی توسعهٔ راهبردی منابع انسانی در ایران و حوزهٔ امنیت سایبری تعیین گردیدند.

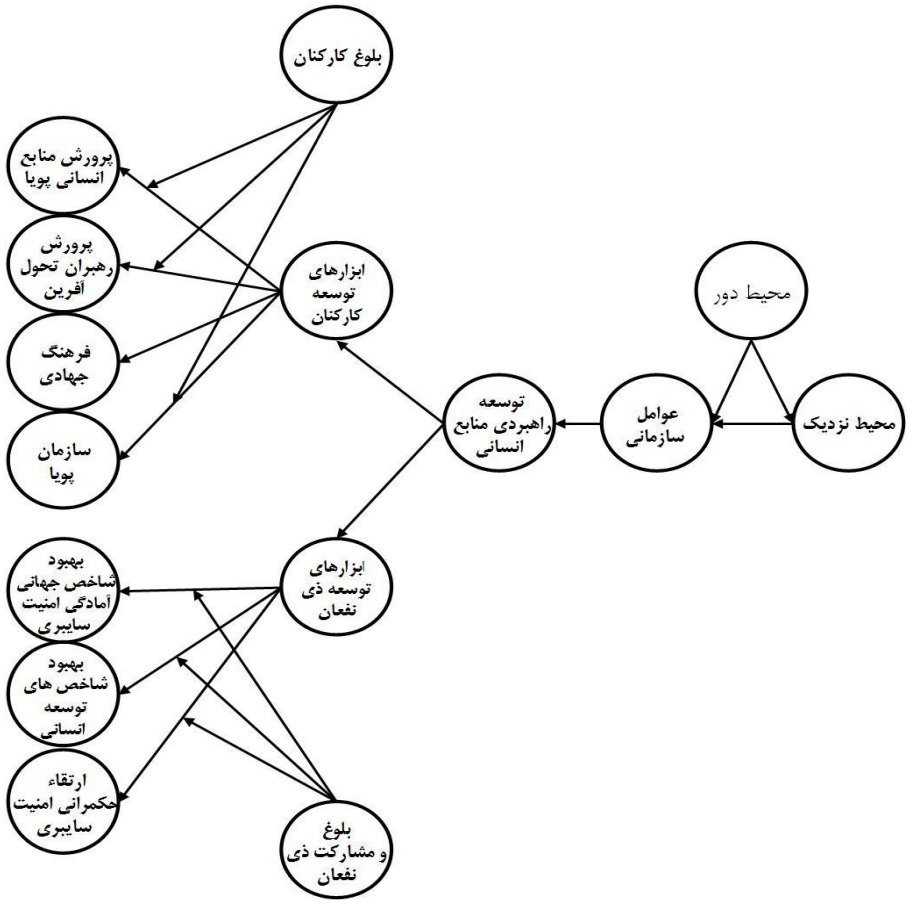
جدول شمارهٔ (۲): ابعاد و مؤلفه‌های توسعهٔ راهبردی منابع انسانی در ایران و حوزهٔ امنیت سایبری

ردیف	ابعاد	مؤلفه	برخی منابع
۱	محیط دور	سیاست‌های بازیگران فراملی تغییرات فناوری و پیچیدگی محیطی	کمیسیون تدوین استراتژی امنیت ملی آمریکا (۱۳۸۳)، قوچانی خراسانی و حسین‌پور (۱۳۹٦)، Department of Homeland (2016) , Kovacich (2016)
۲	محیط نزدیک	الزام‌های حاکمیتی (استقلال و امنیت)، اسناد بالادستی الزام‌های مدیریتی و شرایط بازار کار	سیاست‌های کلی نظام در افتا، پدافند غیرعامل، انتصاب شورای عالی فضای مجازی Commission on enhancing national cybersecurity (2016), National Cyber Resilience Leaders' Board (2018)

ردیف	ابعاد	مؤلفه	برخی منابع
۳	عوامل سازمانی	راهبرد، فرهنگ ساختار، فناوری	سوری‌زاده (۱۳۹۷)، کمیسیون تدوین استراتژی امنیت ملی آمریکا (۱۳۸۳) Bamberger&et.al (2014), Alagaraja (2013), Peterson (2008)
٤	توسعهٔ راهبردی منابع انسانی	رویکرد جامع، دوراندیشانه تحول‌آفرین رویکرد تلفیقی	آرمسترانگ (۱۳۹۳)، میرسپاسی (۱۳۸۸) Hoffman&et.al (2012), Joseph&etal (2016) Department of Homeland (2016)
٥	ابزارهای توسعهٔ کارکنان	رویکردهای رسمی (دورهٔ آموزشی) و رویکردهای غیررسمی (فرایندها)	Department of Homeland (2016), Hu (2007), Allen&etal (2015), Simmonds&et.al (2006), William&et.al (2017)
٦	ابزار توسعهٔ سایر ذی‌نفعان	رویکرد نیازمحور (حل مسئله) و رویکردهای ظرفیت‌ساز	کمیته پدافند غیرعامل (۱۳۹٤) Kovacich (2016), Cornish&et.al (2011) National center of incident readiness and strategy for cybersecurity (2011)
۷	پرورش منابع انسانی پویا	شایستگی سایبری، مهارت‌های انسانی و فرهنگی، اندیشه‌ورزی انعطاف‌پذیری منابع انسانی	کاویانی و همکاران (۱۳۹۷)، قاضی‌زاده و همکاران (۱۳۹٤) Department of Homeland (2016), Zeng (2016)
۸	پرورش رهبران تحول‌آفرین	رهبران فراتخصصی (جنرالیست) مهارت رفتاری، متعهد	سلطانی و همکاران (۱۳۹٤)، جمشیدی (۱۳۹٥) هاشمی و همکاران (۱۳۸۹)، محمدی و همکاران (۱۳۹٤) Khalil&et.al (2017)
۹	فرهنگ جهادی	معنویت محوری نظامی امنیتی پویایی	موسویان (۱۳۹۷)، (پورصادق، ۱۳۹٦)، فرهی و همکاران (۱۳۹٥) Shim&et.al (2015), Tu&et.al (2014)
۱۰	توسعه سازمان پویا	ارتقای تاب‌آوری سایبری بهبود دوسو توانی سازمانی ارتقای سرمایه‌های سازمانی تقویت گروه‌های سایبری	Department of Homeland (2016), National Cyber Resilience Leaders' Board (2018), Hyland&et.al (2005), Mercedes&et.al (2016)
۱۱	ارتقای حکمرانی سایبری	سواد سایبری، خودحفاظتی تمرکززدایی، یکپارچگی مشارکت‌پذیری، پاسخگویی	باقری چوکامی (۱۳۹٥) Alfred&et.al (2018), Ameli&et.al (2018) National center of incident readiness and strategy for cybersecurity (2011)

ردیف	ابعاد	مؤلفه	برخی منابع
١٢	بهبود شاخص‌های جهانی آمادگی امنیت سایبری	حقوقی، فنی سازمانی، ظرفیت‌سازی همکاری	قوچانی خراسانی و حسین‌پور (١٣٩٦) ITU(2018), Alfred&et.al (2018), Department of Homeland (2016)
١٣	بهبود شاخص‌های توسعهٔ انسانی	زندگی سالم و طولانی دستیابی به دانش، دستیابی به استانداردهای زندگی	میرسپاسی (١٣٨٨) Garavan&et.al (2010), Tara&et.al (2008) United Nations Development Programme (2018)
١٤	بلوغ کارکنان	ویژگی‌های شخصیتی افراد دانش و سطح معلومات کارکنان	عباسپور و همکاران (١٣٩٥)، معمارزاده و همکاران (١٣٨٩)، ذوالفقاری و همکاران (١٣٩٣)، زنوزی مشرفی (١٣٨٩)
١٥	بلوغ، همکاری و مشارکت سایر ذی نفعان	آگاهی و مشارکت مردم بخش خصوصی و مراکز تخصصی آگاهی‌رسانی، پشتیبانی و امدادرسانی (آپا) سایبری، همکاران در سطح ملی	National center of incident readiness and strategy for cybersecurity (2011) ,Alfred&et.al (2018), Cornish&et.al (2011), William&et.al (2017)

در ادامه، بر اساس ابعاد مستخرج از مطالعات اکتشافی و با ارتباط دادن ابعاد در حول بُعد اصلی (توسعهٔ راهبردی منابع انسانی) مطابق شکل شمارهٔ (١) «الگوی مفهومی» تدوین گردیده است. توسعه الگوی یادشده تلفیقی از الگوی مدیریت راهبردی منابع انسانی میرسپاسی (تأکید بر سه حوزهٔ فردی، سازمانی و اجتماعی) و الگوی نظام‌مند نظریهٔ داده‌بنیاد (تعیین پیشرانه‌ها، ابزارها، شرایط مداخله‌گر و پیامدها) است که کدهای استخراج شده از مطالعات اکتشافی در این قالب سازماندهی گردیده‌اند.



شکل شمارهٔ (۱): الگوی مفهومی تحقیق

در این الگوی فرایندی در ابتدا چگونگی اثرگذاری محیط بر راهبردها، ساختار، فناوری و فرهنگ سازمان‌های متولی در حوزهٔ امنیت سایبری و سپس توسعهٔ راهبردی منابع انسانی به‌عنوان مقولهٔ محوری تبیین گردیده است. این بخش از الگو را می‌توان نمایی از ضرورت توسعه و آموزش منابع انسانی و انتخاب رویکرد توسعهٔ راهبردی منابع انسانی به‌عنوان مقوله محوری قلمداد نمود. در بخش فرایندها که در حقیقت شامل ویژگی‌های مطلوب توسعهٔ راهبردی منابع انسانی (رویکرد جامع، دوراندیشانه، تحول‌آفرین و تلفیقی از راهبردهای تجویزی و توصیفی) و ابزارهای اجرایی آن می‌باشد، ابزارهای توسعه و آموزش متناسب با شرایط هر یک از ذی‌نفعان (کارکنان و جامعه) تعیین گردیده‌اند. فرایندی جامع که در صورت

اجرایی شدن در سطوح فردی (کارکنان)، سازمان و جامعه می‌تواند به آثار مثبتی ازقبیل پرورش منابع انسانی پویا، پرورش رهبران تحول‌آفرین، سازمان پویا، ایجاد فرهنگ جهادی، ارتقای حکمرانی امنیت سایبری، بهبود شاخص‌های توسعهٔ انسانی و ارتقای شاخص‌های جهانی آمادگی امنیت سایبری منجر شود. پیامدهایی که بخشی از الزام‌های تحقق امنیت سایبری در کشور است؛ بنابراین چگونگی و میزان استفاده از ابزارها تحت تأثیر عواملی همچون میزان بلوغ کارکنان و نیز میزان بلوغ و مشارکت سایر ذی‌نفعان به‌عنوان متغیرهای تعدیل‌گر است.

۳. یافته‌های تحقیق و تجزیه و تحلیل آنها

۳-۱. ویژگی‌های جمعیت‌شناسی پاسخگویان

با توجه به مفروض‌های تعیین‌شده جهت شناسایی خبرگان علمی و اجرایی، تعداد ۵۲ نفر جهت بررسی مقوله‌ها، ابعاد، مؤلفه‌ها و شاخص‌های استخراج شده از مطالعات اکتشافی تعیین گردیدند. پس از هماهنگی‌های صورت گرفته و ارسال پرسشنامه‌ها، تعداد ٤٣ پرسشنامه گردآوری و مبنای تحلیل داده‌ها قرار گرفت. ویژگی‌های جمعیت شناختی پاسخگویان به‌شرح جدول شمارهٔ (۳) می‌باشد.

جدول شمارهٔ (۳): ویژگی‌های جمعیت‌شناسی پاسخگویان

ردیف	ویژگی‌های جمعیت‌شناسی	ابعاد	تعداد
۱	مدرک تحصیلی	دکترا	۲۹
		کارشناسی ارشد	١٤
۲	وابستگی سازمانی	ستاد کل نیروهای مسلح	٥
		ارتش ج.ا.ایران	۱۳
		سپاه پاسداران انقلاب اسلامی	٤
		نیروی انتظامی ج.ا.ایران	۲
		سازمان پدافند غیرعامل کشور	٥
		دانشگاه عالی دفاع ملی	٤
		دانشگاه خاتم‌الانبیاء (ص)	۳
		دانشگاه امام حسین (ع)	۳
		دانشگاه مالک اشتر	۱
		دانشکده فارابی	۳

۳-۲. بررسی برازش الگوی مفهومی

برای اینکه بتوان نتایج حاصل از تخمین روابط الگو را تفسیر نمود، ابتدا باید میزان تناسب الگو یا برازش آن‌را مشخص کرد. به این معنا که آیا الگویی که اساس آن مبانی نظری پیشین بوده، با داده‌های گردآوری شده از نمونهٔ آماری تحقیق متناسب بوده یا خیر؟ در نرم‌افزار «اسمارت پی.ال.اس» این مرحله شامل برازش الگوی اندازه‌گیری (رابطه گویه‌ها با سازه‌ها)، برازش الگوی ساختاری (رابطه میان سازه‌ها) و برازش الگوی کلی است که نتایج آن در جدول شمارهٔ (٤) ارائه گردیده است.

جدول شمارهٔ (٤): نتایج برازش (اندازه‌گیری، ساختاری و برازش کلی) الگوی مفهومی تحقیق

ابعاد اصلی	برازش الگوی اندازه‌گیری				برازش الگوی ساختاری		برازش کلی الگو GOF≥0/3
	ضریب کرونباخ (α≥0/7)	مقادیر اشتراکی (c≥0/6)	پایایی ترکیبی (Cr≥0/7)	روایی همگرا (AVE≥0/5)	R2	Q2	
م دور	۰/۸۳	۰/۸٦	۰/۸۹	۰/٦۸	متغیر برون‌زا		GOF=$\sqrt{0/59 \times 0/86}$ =0/71
م نزدیک	۰/۸۳	۰/۸۳	۰/۸۸	۰/٥٤	۰/۸۰٤	۰/٤	
ع سازمان	۰/۸۲	۰/۸٥	۰/۸۳	۰/٦٦	۰/۷۲۹	۰/٤٦	
توسعهٔ راهبردی	۰/۹	۰/۹۲	۰/۹۳	۰/۷۸	۰/٥۳۷	۰/٤۱	
ابزارهای کارکنان	۰/۷۸	۰/۸۰	۰/۸٥	۰/٥٥	۰/٤۰	۰/۲۱	
ابزارهای ذی‌نفعان	۰/۸٦	۰/۸۷	۰/۹٤	۰/۸۸	۰/۳۲۸	۰/۲۹	
منابع پویا	۰/۹۳	۰/۹٤	۰/۹٤	۰/٥۸	۰/۷۱۳	۰/۳۸	
پرورش رهبر	۰/۹	۰/۹۲	۰/۹٤	۰/۸٤	۰/٥٤	۰/٤٤	
ف جهادی	۰/۷	۰/۷۳	۰/۸۷	۰/۷۷	۰/٥۹۹	۰/۳۹	
س پویا	۰/۸۷	۰/۸۹	۰/۹	۰/٥۱	۰/۷۱۰	۰/۳۳	
حکمرانی سایبری	۰/۷۹	۰/۸۳	۰/۸٦	۰/٥٥	۰/٤۷۷	۰/۲	
آمادگی امنیت سایبری	۰/٥۷	۰/۷٤	۰/۸۱	۰/٦۸	۰/۲۹۰	۰/۲٦	
توسعهٔ انسانی	۰/۸۷	۰/۸۸	۰/۹۲	۰/۸	۰/۷٤۸	۰/٥٤	
بلوغ کارکنان	۰/۷۷	۰/۸٦	۰/۸۹	۰/۸۱	متغیر برون‌زا		
بلوغ سایر ذی‌نفعان	۰/۸۷	۰/۹٤	۰/۹۲	۰/۸	متغیر برون‌زا		

بررسی برازش اندازه‌گیری و ساختاری ابعاد الگوی مفهومی مؤید آن است که در وجوه مورد بررسی، کلیهٔ ابعاد دارای نمره‌های قابل قبول می‌باشند؛ فقط درخصوص ضریب آلفای کرونباخ بُعد بهبود شاخص جهانی آمادگی امنیت سایبری خروجی نرم‌افزار کمتر از میزان قابل قبول است، ولی با توجه به مقدار قابل قبول پایایی ترکیبی و مقادیر اشتراکی این کاستی قابل چشم‌پوشی است. نتایج برازش کلی الگو (۰/۷۱) نیز نشانگر آن است که الگو در پیش‌بینی متغیرهای مکنون درون‌زا دارای قدرت و توانایی بالایی است. از این رو، با توجه به مطلوب بودن نتایج برازش الگوی اندازه‌گیری، ساختاری و الگوی کلی بررسی و آزمون فرضیه‌های تحقیق امکان‌پذیر است.

۳-۳. بررسی فرضیات تحقیق

در این مرحله با توجه به الگوی مفهومی پژوهش، ۲۰ فرضیه تنظیم و سپس با استفاده از داده‌های گردآوری شده مورد ارزیابی قرار گرفته است. نتایج بررسی ضرایب معناداری Z و ضرایب بارهای عاملی در جدول شمارهٔ (۵) ارائه گردیده است.

جدول شمارهٔ (۵): نتایج آزمون فرضیه‌های تحقیق

ردیف	فرضیه‌های پژوهش		ضریب مسیر استاندارد	عدد معناداری	نتیجه آزمون فرضیه صفر
	متغیر پیش‌بین/ تعدیل‌گر	متغیر ملاک			
۱	محیط دور	محیط نزدیک	۰/۸۹۷	٤٦/۸۳	رد
۲	محیط دور	عوامل سازمانی	۰/٤٥۷	۲/٦٤	رد
۳	محیط نزدیک	عوامل سازمانی	۰/۳۹٤	۲/۳	رد
٤	عوامل سازمانی	توسعهٔ راهبردی	۰/۷٤۳	۱۹/۹٤	رد
٥	توسعهٔ راهبردی منابع انسانی	ابزارهای توسعهٔ کارکنان	۰/٦۳۷	۸/٥۲	رد
٦	توسعهٔ راهبردی منابع انسانی	ابزار توسعهٔ ذی‌نفعان	۰/٥۷۳	۸/٤۱	رد
۷	ابزارهای توسعهٔ کارکنان	پرورش منابع انسانی پویا	۰/٤۰۷	٥/۲٥	رد
۸	ابزارهای توسعهٔ کارکنان	پرورش رهبران	۰/۲۲٦	۳/٤٤	رد
۹	ابزارهای توسعهٔ کارکنان	فرهنگ جهادی	۰/۰۸	۰/٦۷٦	تأیید
۱۰	ابزارهای توسعهٔ کارکنان	سازمان پویا	۰/۲۸۰	٤/۱	رد

ردیف	فرضیه‌های پژوهش		ضریب مسیر استاندارد	عدد معناداری	نتیجه آزمون فرضیه صفر
	متغیر پیش‌بین/ تعدیل گر	متغیر ملاک			
١١	ابزارهای توسعهٔ ذی‌نفعان	حکمرانی امنیت سایبری	٠/٣٥٨	٣/٣٢	رد
١٢	ابزارهای توسعهٔ ذی‌نفعان	بهبود توسعهٔ انسانی	٠/٥٠٥	٤/٠٣	رد
١٣	ابزارهای توسعهٔ ذی‌نفعان	آمادگی امنیت سایبری	٠/٦٦٨	٥/٣١	رد
١٤	بلوغ کارکنان	ت کارکنان- منابع پویا	٠/٣٩٢	٢/٢٨	رد
١٥	بلوغ کارکنان	ت کارکنان – پ رهبران	-٠/١٦٣	٢/٠٩	رد
١٦	بلوغ کارکنان	ت کارکنان- ف جهادی	٠/٧٩٧	٣/٥٨	رد
١٧	بلوغ کارکنان	توسعهٔ کارکنان – س پویا	٠/٦٠٥	٦/٩٤	رد
١٨	بلوغ، مشارکت و همکاری سایر ذی‌نفعان	توسعهٔ ذی‌نفعان – حکمرانی امنیت سایبری	-٠/٠٥	٠/٢٩٣	تأیید
١٩	بلوغ، مشارکت و همکاری سایر ذی‌نفعان	ت ذی‌نفعان – توسعهٔ انسانی	٠/٧٣	٢/٨١	رد
٢٠	بلوغ، مشارکت و همکاری سایر ذی‌نفعان	توسعهٔ ذی‌نفعان – آمادگی امنیت سایبری	٠/١٢	٠/٨٥٢	تأیید

بر اساس نتایج تحلیل مسیر در سطح اطمینان ٠/٩٥ از ٢٠ فرضیه تنظیمی، ١٧ فرضیه مورد تأیید قرار گرفت و ٣ فرضیه رد شدند. با این وجود، با توجه به مقادیر R^2 شدت روابط فرضیه‌ها تأیید شده متفاوت است. روابط بین متغیرهای پیش‌بین و ملاک را می‌توان در طیفی از روابط قوی، متوسط و ضعیف تقسیم‌بندی نمود. در این میان، رابطهٔ متغیر محیطِ دور با محیطِ نزدیک با مقدار R^2 معادل ٠/٨٠٤ دارای قوی‌ترین رابطه و رابطهٔ ابزارهای توسعهٔ ذی‌نفعان با ارتقای شاخص‌های جهانی آمادگی امنیت سایبری با مقدار R^2 معادل ٠/٢٩ دارای ضعیف‌ترین رابطه است.

٤. نتیجه‌گیری

٤-١. جمع‌بندی

در این تحقیق با توجه به اهمیت موضوع توسعه و آموزش در حوزهٔ امنیت سایبری به طراحی الگویی فرایندی از توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری

نیروهای مسلح ج.ا.ایران مبادرت نمودیم. در گام اول ابعاد، مؤلفه‌ها و شاخص‌های الگو از طریق مطالعات اکتشافی شناسایی و سپس مورد ارزیابی قرار گرفت. در مرحلهٔ بعد بر اساس نتایج مطالعات اکتشافی چگونگی اثرگذاری و رابطهٔ پیشرانه‌ها، ابزارهای اجرایی و پیامدهای توسعهٔ راهبردی منابع انسانی در حول مقوله محوری توسعهٔ راهبردی منابع انسانی ترسیم و مورد آزمون قرار گرفتند که بر اساس نتایج برازش و آزمون الگوی مفهومی و مطابق نتایج جدول شمارهٔ (٦) با حذف بُعد فرهنگ جهادی ابعاد الگوی نهایی تحقیق به ١٤ بُعد کاهش یافته است. در الگوی نهایی تحقیق مطابق شکل شمارهٔ (٢) توسعهٔ راهبردی منابع انسانی به‌عنوان سازوکاری در جهت بازطراحی و یا اصلاح عوامل سازمانی هم‌راستا با تغییرات و شرایط محیط دور و نزدیک مورد تأیید قرار گرفت.

توسعهٔ راهبردی منابع انسانی به‌عنوان رویکردی جامع با نگاهی دوراندیشانه و تحول‌آفرین ارتقای امنیت سایبری در جامعه را مستلزم توسعهٔ شایستگی‌ها کارکنان و قابلیت‌های نهادهای متولی در این حوزه و نیز افزایش آگاهی و دانش جامعه درخصوص این موضوع قلمداد می‌نماید. با این وجود، با عنایت به تفاوت ذی‌نفعان بدیهی است که ابزارهای متفاوتی در این خصوص باید مورد استفاده قرار گیرد. ابزار و راهبردهایی که با توجه به سطح بلوغ کارکنان و جامعه و نیز اقدام‌ها و فعالیت‌های سایر نهادهای متولی حوزهٔ امنیت سایبری می‌توانند مورد تعدیل قرار گیرند. در صورت تحقق مطلوب سازوکارهای عنوان شده پیامدهایی همچون پرورش منابع انسانی پویا، پرورش رهبران تحول‌آفرین، توسعهٔ سازمان‌های پویا، ارتقای حکمرانی امنیت سایبری، بهبود شاخص‌های جهانی آمادگی امنیت سایبری و به‌دنبال آن بهبود شاخص‌های توسعهٔ انسانی تحقق می‌یابد. پیامدهایی که نتایج آزمون الگو نیز آنها را مورد تأیید قرار می‌دهد.

جدول شمارهٔ (٦): ابعاد و مؤلفه‌های الگوی نهایی توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران

ردیف	ابعاد	مؤلفه‌ها
۱	محیط دور	سیاست‌های بازیگران فراملی، تغییرات فناوری و پیچیدگی محیطی
۲	محیط نزدیک	الزامات حاکمیتی (استقلال و امنیت)، اسناد بالادستی، الزام‌های مدیریتی و شرایط بازار کار
۳	عوامل سازمانی	راهبرد، فرهنگ، ساختار، فناوری
٤	توسعهٔ راهبردی منابع انسانی	رویکرد جامع، دوراندیشانه، تحول‌آفرین، رویکرد تلفیقی
٥	ابزارهای توسعهٔ کارکنان	رویکردهای رسمی (دورهٔ آموزشی)، رویکردهای غیررسمی (فرایندها)
٦	ابزار توسعهٔ سایر ذی‌نفعان	رویکرد نیازمحور (حل مسئله)، رویکردهای ظرفیت‌ساز
۷	پرورش منابع انسانی پویا	شایستگی سایبری، مهارت‌های انسانی و فرهنگی، انعطاف‌پذیری منابع انسانی، مهارت‌های اندیشه‌ورزی
۸	پرورش رهبران تحول‌آفرین	رهبران فراتخصصی (جنرالیست)، مهارت رفتاری، متعهد
۹	توسعهٔ سازمان پویا	ارتقای تاب‌آوری سایبری، بهبود دوسو توانی سازمانی، ارتقای سرمایه‌های سازمانی، تقویت گروه‌های پاسخگوی سایبری
۱۰	ارتقای حکمرانی امنیت سایبری	سواد سایبری، خودحفاظتی، تمرکززدایی، یکپارچگی، مشارکت‌پذیری
۱۱	بهبود شاخص‌های جهانی آمادگی امنیت سایبری	حقوقی، ظرفیت‌سازی و آموزش
۱۲	بهبود شاخص‌های توسعهٔ انسانی	زندگی سالم و طولانی، دستیابی به دانش، دستیابی به استانداردهای زندگی
۱۳	بلوغ کارکنان	ویژگی‌های شخصیتی افراد، دانش و سطح دانستنی‌های کارکنان
۱٤	بلوغ، همکاری و مشارکت سایر ذی‌نفعان	آگاهی و مشارکت مردم، بخش خصوصی و مراکز تخصصی آگاهی‌رسانی، پشتیبانی و امداد سایبری (آپا) همکاران در سطح ملی

٤-٢. پیشنهادها

٤-٢-١. پیشنهادهای اجرایی

بر اساس نتایج و شاخص‌ها و مؤلفه‌های الگوی نهایی تحقیق و به‌منظور اجرایی نمودن الگوی توسعهٔ راهبردی منابع انسانی در حوزهٔ امنیت سایبری نیروهای مسلح ج.ا.ایران پیشنهادهای زیر دارای اهمیت می‌باشند:

(١) نهادینه‌سازی فرایندهای مدیریت دانش یکی از مهم‌ترین ابزارهای توسعه کارکنان است. با این وجود و با توجه به تعدد نهادهای مسئول در حوزهٔ امنیت سایبری نیروهای مسلح در کنار نظام‌های داخلی مدیریت دانش، ایجاد سامانهٔ (سیستم) جامع پردازش مرکزی جهت گردآوری، یکپارچه‌سازی و تسهیم اطلاعات این نهادها ضروری است. سازوکاری که ارتش آمریکا جهت گردآوری و تسهیم اطلاعات رزمی تا سطوح راهکنشی (تاکتیکی) و ردهٔ گردان در قالب سامانهٔ تحلیل منابع آزاد[1] آن‌را اجرایی نموده است.

(٢) در کنار آموزش‌های رسمی، سازوکارهایی همچون گردش شغلی، توسعه و غنی‌سازی ازجمله شیوه‌های توسعهٔ منابع انسانی پویا و به‌ویژه افزایش انعطاف‌پذیری کارکنان است که سازمان‌های مسئول در حوزهٔ امنیت سایبری نیروهای مسلح بایستی در برنامه‌های آموزشی مورد توجه قرار دهند.

(٣) آگاهی از فرهنگ و باورهای کشورهای مختلف و به‌عبارتی هوش فرهنگی ازجمله عوامل اثرگذار بر چگونگی پیش‌بینی و مقابله با تهدیدهای سایبری است؛ بنابراین پس از ارزیابی توانایی‌های کارکنان در ابعاد شناختی، فیزیکی و احساسی و انگیزشی باید برنامه‌های آموزشی مناسب به‌منظور تقویت این شایستگی‌ها طراحی گردد. برای مثال، برای افراد ضعیف در بُعد فیزیکی شرکت در کلاس‌های آموزش رفتاری، افراد دارای ضعف در بُعد شناختی شرکت در دوره‌های استدلال قیاسی و توان تحلیلی باید در نظر گرفته شود.

---

1. All source analysis system

(٤) به‌منظور نهادینه‌سازی تفکر راهبردی نیاز است در سطح نیروهای مسلح و به‌ویژه سازمان‌های مسئول در حوزهٔ امنیت سایبری، دوره‌های آموزشی مناسبی در جهت تقویت مهارت‌های کنکاش و رصد محیطی، تشخیص و شناخت فرصت‌های حال و آینده، چشم‌اندازسازی و نیز خلق راهبردها و تصمیم‌های هوشمندانه طراحی گردد. ازجمله دوره‌های آموزشی متداول در این حوزه (در عرصهٔ امنیتی و نظامی) می‌توان به استفاده از نرم‌افزارهای شبیه‌سازی جنگ‌های آینده و نیز نظریهٔ بازی‌ها اشاره نمود.

(۵) پرورش مدیران تحول‌آفرین نیازمند استفاده از سازوکارهایی متفاوت از سازوکارهای آموزش رسمی و متداول در مؤسسه‌های عالی است؛ زیرا در حقیقت اهداف و مأموریت دانشگاه‌ها متفاوت از سازمان‌ها و نهادهای متولی در حوزه‌های امنیتی و دفاعی است. در دانشگاه‌ها تمام فعالیت‌ها و برنامه‌ها در راستای آموزش افراد در حوزه‌های علمی و کاملا تخصصی است؛ در حالی که در حوزهٔ امنیت سایبری، تربیت افرادی فراتخصصی با توانایی نگرش چندوجهی و تحلیلی قدرتمند (کارکنان جنرالیست) باید مورد توجه قرار گیرد. این اهداف تربیتی و آموزشی بیشتر از طریق شبیه‌سازی تهدیدها و حمله‌های سایبری با استفاده از سازوکارهایی همچون «گروه (تیم) قرمز و آبی»[1]، SDL[2]، بازی‌های مدیریتی، ایفای نقش و ... تحقق می‌یابند. بنابراین در کنار ضرورت بهره‌گیری از ظرفیت مؤسسه‌های آموزش عالی در جهت تقویت وجوه علمی و دانش تخصصی، به‌نظر می‌رسد با توجه به تعدد نهادهای متولی آموزش در حوزهٔ امنیت سایبری در صورت بازطراحی یکپارچه مأموریت و وظایف این سازمان، اهداف یادشده به‌گونه‌ای اثربخش تحقق خواهند یافت.

(٦) ارتقای تاب‌آوری سازمان‌های متولی امنیت سایبری در سطح نیروهای مسلح نیازمند تقویت توانمندی‌های این سازمان‌ها درخصوص توانایی تشخیص و ترسیم

1. Red team & Blue team
2. Sceniro definition language

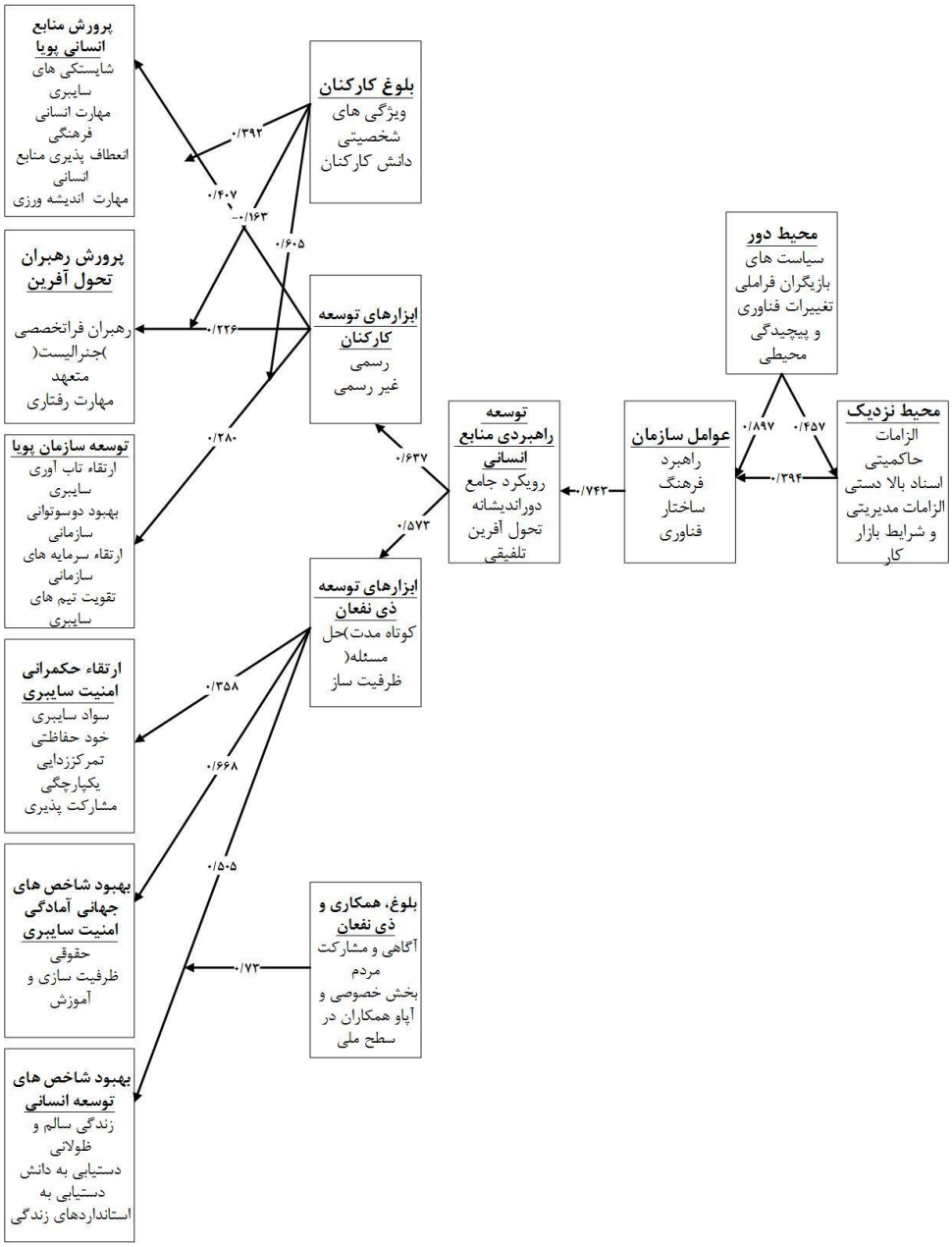
آینده‌های بدیل، توانایی تغییر مسیر پس از دریافت اولین نشانه‌های هشداردهنده با حداقل هزینه، توانایی توسعه و به‌کارگیری راهکارهای مناسب، توانایی بازسازی خود و ایجاد تناسب با محیط و درنهایت انتقال دانش و تغییر رفتار خود بر اساس بینش جدید است. رویکردهایی که در طراحی دوره‌های تربیتی و آموزشی سازمان‌ها باید به آنها توجه ویژه نمود.

(۷) به‌منظور افزایش اثربخشی و کاهش هزینه‌های فرایندهای توسعهٔ راهبردی منابع انسانی، ضروری است که پیش از اجرایی نمودن دوره‌های تربیتی و آموزشی، میزان بلوغ کارکنان از دیدگاه سطح دانش و آگاهی و نیز ویژگی‌های شخصیتی مورد ارزیابی قرار گرفته و بعد از آن بر اساس نتایج به‌دست آمده، سازوکارهای اجرایی و آموزشی مناسب طراحی و اجرا گردد.

٤-٢-٢. پیشنهادهای پژوهشی

(۱) امکان‌سنجی تعمیم الگو در سطح کلیهٔ نهادهای دولتی مسئول در حوزهٔ امنیت سایبری کشور؛

(۲) شناسایی سایر رویکردهای اثرگذار (متغیرهای مکنون) در ارتقای وضعیت حوزهٔ امنیت سایبری در سطح نیروهای مسلح.



شکل شمارهٔ (۲): الگوی نهایی تحقیق

*****

فهرست منابع

الف. منابع فارسی

١. آرمسترانگ ، مایکل، (١٣٩٣)، ***مدیریت استراتژیک منابع انسانی (راهنمای عمل)***، ترجمهٔ محمد صائبی، تهران، چاپ دوم، انتشارات مرکز آموزش مدیریت دولتی.

٢. باقری‌چوکامی، سیامک، (١٣٩٥)، امکان‌سنجی نقش الگوهای خودحفاظتی در پیشگیری پایدار از تهدیدات سازمان‌های امنیتی، ***فصلنامهٔ پژوهش‌های حفاظتی و امنیتی***، سال ٥، شمارهٔ ١٧.

٣. پورصادق، ناصر، (١٣٩٦)، شناسایی و تبیین فرهنگ سازمانی جهادی، ***فصلنامهٔ پژوهش‌های مدیریت انتظامی***، سال دوازدهم، شمارهٔ ٢.

٤. تافلر، آلوین، (١٣٦٦)، ***موج سوم***، ترجمهٔ شهین‌دخت خوارزمی، تهران، چاپ سوم، نشر نو.

٥. جمشیدی، محمدحسین و محسن اسلامی، (١٣٩٦)، تفکر و فرهنگ بسیجی در اندیشهٔ امام خمینی(ره)، ***دوفصلنامهٔ مطالعات قدرت نرم***، سال هفتم، شمارهٔ ١٦.

٦. زنوزی‌مشرفی، عباس، (١٣٨٩)، مدیریت دانش؛ چالش‌ها و موانع استقرار آن در ارتش ج.ا.ایران، ***فصلنامه علوم و فنون نظامی***، سال هفتم، شمارهٔ ١٩.

٧. سلطانی، محمدرضا و مصطفی سلیمان‌تبار، (١٣٩٤)، بررسی عوامل مؤثر بر توسعهٔ منابع انسانی با رویکرد نهادی، ***پژوهش‌های مدیریت منابع انسانی***، سال هفتم، شمارهٔ سوم.

٨. سوری‌زاده، امیر و مهران شیرخانی، (١٣٩٧)، ارزیابی شاخص‌های توسعهٔ دفاع سایبری در سازمان‌های نظامی، ***فصلنامهٔ علمی تحقیقاتی محقق***، شمارهٔ ٨٠.

٩. عباسپور، عباس، منیژه احمدی، حمید رحیمیان و علی دلاور، (١٣٩٥)، تبیین و ارائه مدل شایستگی سربازرسان در سازمان بازرسی کل کشور با رویکرد نظریهٔ داده بنیاد، ***فصلنامهٔ آموزش و توسعهٔ منابع انسانی***، سال سوم، شمارهٔ ١٠.

١٠. فاضلی، حبیبا... و توحید افضلی، (١٣٩٤)، دیپلماسی ایالات‌متحده در قبال ج.ا.ایران در دولت اوباما (با تأکید بر فضای سایبری)، ***دوفصلنامهٔ مطالعات قدرت نرم***، شمارهٔ ١٢.

١١. فرهی، علی، محمدابراهیم سنجقی، محمدرضا سلطانی و یدا... محمدیان، (١٣٩٥)، طراحی الگوی فرهنگ جهادی یکی از نهادهای انقلاب اسلامی، ***پژوهش‌های مدیریت منابع انسانی***، دورهٔ ٨، شمارهٔ ٢.

١٢. قاضی‌زاده فرد، سیدضیاءالدین، علیرضا نادری خورشیدی، علی‌محمد احمدوند و فیض‌اله جلالی کوهستانی، (١٣٩٤)، ارائه الگوی مدیریت راهبردی تربیت و آموزش در دانشگاه‌های نیروهای مسلح، ***فصلنامهٔ راهبرد دفاعی***، سال سیزدهم، شمارهٔ ٤٩.

١٣. قوچانی خراسانی، محمدمهدی و داود حسین‌پور، (١٣٩٦)، حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری، ***فصلنامهٔ فرایند مدیریت و توسعه***، شمارهٔ ٣٠.

١٤. کاویانی؛ حسن، جمشید صالحی صدقیانی و حسین فتح‌آبادی، (١٣٩٧) ،بررسی رابطه بین تفکر راهبردی و دو سو توانی سازمانی (مورد مطالعه یگان های نظامی)، ***پژوهش‌نامهٔ مدیریت تحول***، سال دهم، شماره دوم، ٢١-٤٥

١٥. کمیته دائمی پدافند غیرعامل کشور، (١٣٩٤)، ***سند راهبردی پدافند سایبری کشور***، قابل دسترسی در: www.saramad.ir

١٦. کمیسیون تدوین استراتژی امنیت ملی آمریکا، (١٣٨٣)، ***استراتژی امنیت ملی آمریکا در قرن ٢١***، ترجمهٔ جلال دهمشگی و دیگران، تهران، مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، چاپ چهارم.

١٧. گروه اطلاعات و حفاظت اطلاعات، (١٣٩٥)، راهبرد سایبری ترکیه: اصول و محورها، ***ماهنامه تخصصی مطالعات امنیت ملی***، سال سوم، شماره ٤٧ و ٤٨.

١٨. محمدی، ابوالفضل، علی فرهی، محمدرضا سلطانی و خدایار تارودی‌پور، (١٣٩٤)، طراحی و تبیین الگوی توسعه منابع انسانی یکی از سازمان‌های نیروهای مسلح، ***پژوهش‌های مدیریت منابع انسانی***، سال هفتم، شمارهٔ ١.

١٩. معاون قرارگاه سایبری سازمان پدافند غیرعامل، (١٣٩٨)، ***ایران ٣٣ میلیون حمله سایبری را دفع کرد***، قابل در دسترسی در: www.irinn.ir

٢٠. معدنی، جواد، داوود حسین‌پور و معصومه یاری، (١٣٩٥)، طراحی مدل فرهنگ جهادی مبتنی بر مبانی دینی و ارزش‌های انقلاب اسلامی در دانشگاه اسلامی (مورد مطالعه دانشگاه علامه طباطبایی)، ***مدیریت در دانشگاه اسلامی***، سال پنجم، شمارهٔ ٤٩.

٢١. معمارزاده، غلامرضا و احمد مهرنیا، (١٣٨٩)، بررسی ضرورت تناسب شخصیت شاغل با مشاغل عملیاتی پرخطر «جذب و استخدام صحیح و افزایش کارایی»، ***مدرس علوم انسانی***، دورهٔ ١٤، شمارهٔ ٣.

٢٢. موسویان، سیدعلی، (١٣٩٧)، شاخصه‌های روحیهٔ جهادی، ***فصلنامهٔ اسلام‌پژوهان***، سال پنجم، شمارهٔ هفتم.

٢٣. میرسپاسی، ناصر، (١٣٨٨)، ***مدیریت استراتژیک منابع انسانی و روابط کار***، تهران، انتشارات میر، ویرایش سوم.

٢٤. والتون، جان، (١٣٩٢)، ***پرورش راهبردی منابع انسانی***، جلد اول، ترجمهٔ ناصر میرسپاسی و داریوش غلامزاده، تهران، نشر میر، چاپ سوم.

٢٥. هاشمی، حسین، حسن علی‌اکبری، محمد بازرگانی و علیرضا نادری خورشیدی، (١٣٨٩)، طراحی الگوی آینده‌پژوهی در توسعهٔ منابع انسانی (مورد: سپاه پاسداران انقلاب اسلامی)، ***پژوهش‌های مدیریت منابع انسانی***، سال ٢، شمارهٔ ٢.

ب. منابع انگلیسی

1. Alagaraja, Meera, (2013), Mobilizing organizational alignment through strategic human resource development, ***Human Resource Development International***, No. 16.
2. Alfred, Bauer & Mohseni ,Ahooei, (2018), Rearticulating Internet Literacy, ***Journal of Cyberspace Studies***, No. 2.
3. Allen, Julia, Crabb Gregory, D.Curtis Pamela, Nader Mehravari Brendan, & Tobar David, (2015), ***Structuring the Chief Information Security Officer Organization,*** Carnegie Mellon University.

4. Ameli, Reza & Ahooei Mohseni, (2018), Internet (Information/Skill) Literacy in Iran. ***Journal of Cyberspace Studies***, No. 2.
5. Bamberger, Peter A, Biron Michal & Meshoulam Ilan, (2014), ***Human Resource Strategy Formulation, Implementation, and Impact***, Second Edition published by Routledge.
6. Brilingaite, Agne, Bukauskas Linas & Juozapavicius Aušrius, (2020), A framework for competence development and assessment in hybrid cybersecurity exercises. ***Computers & Security***.
7. Caulkins Bruce, Bockelman Patricia, Badillo-Urquiola Karla & Leis Rebecca, (2016), Cyber Workforce Development Using a Behavioral Cybersecurity Paradigm, ***International Conference on Cyber Conflict (CyCon U.S.).***
8. Commission on enhancing national cybersecurity, (2016), ***Report on securing and growing the digital economy***, available at: www.iapp.org
9. Cornish, Paul, David Livingstone, Dave Clemente, & York Claire, (2011), ***Cyber security and UK s critical national infrastructure, Chatham House***. available at: www.chathamhouse.org
10. Department of Homeland, (2016), *Cybersecurity workforce development toolkit How to Build a Strong Cybersecurity Workforce*, at: www.niccs.uscert.gov
11. Garavan, Thomas N & McGuire David, (2010), Human Resource Development and Society: Human Resource Development's Role in Embedding Corporate Social Responsibility, Sustainability, and Ethics in Organizations, ***Advances in Developing Human Resources***, No.12.
12. Hoffman, Lance, Burley Diana & Toregas Costis, (2012), Holistically Building the Cybersecurity Workforce, ***IEEE Security and Privacy Magazine***, No. 10.
13. Hu, Po, (2007), Theorizing Strategic Human Resource Development: Linking Financial Performance and Sustainable Competitive Advantage, ***Paper presented at the International Research Conference in the Americas of the Academy of Human Resource Development ,Indianapolis.***
14. Hyland, Paul, Lee Di Milia, & Karen Becker, (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***, at available: www.eprints.qut.edu.au
15. International Telecommunication Union, (2018), ***ITU/BDT Cyber Security Programme Global Cybersecurity Index (GCI),*** www.itu.int
16. Joseph, Lakatos & Bethany ,Davidson, (2016), The Dynamic Organizational Model: Its Principles, Implementation Methods and Impact on Corporate Culture, ***The Journal of Global Business Management***, No. 12.
17. Khalil, M & Dirani, Christine, (2017), Human resource education in the Middle East region, ***European Journal of Training and Development***, No. 41.
18. Kovacich, Gerald L, (2016), ***The information systems security officer's guide Establishing and Managing a Cyber Security Program***, Third edition, Published by Elsevier.
19. Koong, Kai, Mohammad Merhi & Jun Sun, (2013), Push and pull effects of homeland information security incentives, ***Information Management & Computer Security,*** No. 21.

20. McCracken Martin & Mary Wallace, (2000), Towards a redefinition of strategic HRD, ***Journal of European Industrial Training***, 24 (5), 281-290
21. Mc Goldrick, J. Stewart & S Watson, (2001), Theorizing human resource development, ***Human resource development international***, No. 4.
22. Mercedes, Úbeda, Enrique García, Claver Bartolome & Z Patrocinio, (2016), Toward organizational ambidexterity in the hotel industry: the role of human resources***, Cornell Hospitality Quarterly***, No. 57.
23. Nadler Leonard, (1992), HRD:Where has it been, where is it going, ***Studies in Continuing Education***, No.14.
24. National center of incident readiness and strategy for cybersecurity, (2011), ***Information Security Human Resource Development*** Program, available at: www.nisc.go.jp
25. National Cyber Resilience Leaders' Board, (2018), ***A cyber resilience strategy for Scotland,*** available at: www.gov.scot
26. Peterson, S (2008), Creating and sustaining a strategic partnership: a model for human resource development, ***Journal of Leadership Studies***, No. 2.
27. Sambrook Sally, (2000),Talking of HRD, ***Human Resource Development International***, No. 3.
28. Sambrook Sally, (2001), HRD as an Emergent and Negotiated Evolution: An Ethnographic Case Study in the British National Health Service, ***Human resource development quarterly***, No. 12.
29. Shim, Woohyun, (2015), Agency Problems in Information Security ***:Theory and Application to Korean Business***.
30. Simmonds, David & Cec, Pedersen (2006), HRD: the shapes and things to come***, Journal of Workplace Learning***, No. 18.
31. Šiugždinien Jurgita, (2008), Enabling characteristics of the strategic human resource development system, ***Filosofija sociologija***, No.19.
32. Tara, Fenwick & Laura, Bierema, (2008), Corporate social responsibility: issues for human resource development professionals, ***International Journal of Training and Development***, No. 12.
33. Tu, Zhiling & Yufei ,Yuan, (2014), Critical Success Factors Analysis on Effective Information Security Management: A Literature Review, ***Twentieth Americas Conference on Information Systems***, Savannah.
34. United Nations Development Programme, (2018), ***Human Development Indices and Indicators 2018 Statistical Update***, available at: www.hdr.undp.org
35. University of Phoenix, (2018), ***Competency Models for Enterprise Security and Cybersecurity***, at available: www.apollo.edu
36. William Newhouse, Keith Stephanie, Scribner Benjamin & Greg Witte, (2017), ***National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework***, publication at: www.doi.org
37. Zeng, Kui, (2016), ***Exploring cybersecurity requirements in the defense acquisition process***, A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Science Capitol technology university