*فصلنامه علمی و پژوهشی فرماندهی و کنترل، سال پنجم، شماره چهار، زمستان ۱۴۰۰*

# ارائه چارچوبی برای توانمندسازی سرمایه انسانی در دفاع سایبری

*آرمین یوسفی[۱] ، امیر محترمی*[۲]*

**تاریخ دریافت: ۱۴۰۰/۱۱/۲۰** **تاریخ پذیرش:۱۴۰۱/۰۳/۲۵**

## چکیده

*مفهوم دفاع سایبری، مقوله ای است که علی رغم عمر نه چندان زیاد از ظهورآن، تاکنون به عنوان یک حوزه پژوهشی داغ مدنظر پژوهشگران از حوزه های مختلف مهندسی رایانه، مخابرات، فناوری اطلاعات و ارتباطات و علوم اجتماعی و انسانی قرار گرفته است. با این وجود، به دلیل حاکم بودن رویکرد کلانِ محصول‌گرایِ فناوری-محور، بر پژوهش‌های این حوزه، مقوله سرمایه انسانی کمتر مورد توجه قرار گرفته است. پژوهش پیش‌رو متمرکز بر این مولفه تاثیرگذار در دفاع سایبری است در ابتدا با طرح پرسش‌هایی چون: "چارچوب توانمندسازی سرمایه انسانی در دفاع سایبری کدام است؟؛ ابعاد و مولفه‌های توانمندسازی کدامند؟ ؛ نقش و اثرگذاری منابع انسانی در دفاع سایبری چیست؟ و اینکه چگونه می‌توان با توانمندسازی کارکنان و ایجاد سازمان یادگیرنده، به دفاع مؤثرتر در عرصه سایبری جامه عمل پوشاند؟" از جنبه ای کمتر دیده شده، به مسئله دفاع سایبری می پردازیم. در گام بعدی به مرور مطالعات و مدل‌های توانمندساز پرداخته و ابعاد و مؤلفه‌های اساسی در توانمندسازی را از منظر ارائه چارچوب توانمندساز سایبری مورد مطالعه قرار می‌دهیم. توانمندسازی دارای دو بعد عمومی و تخصصی است. در بعد عمومی توانمندسازی کارهای فراوانی شده است و ما با معرفی موتور توانمندساز سرمایه انسانی سایبری در هسته‌ی این چارچوب آن را تکمیل نموده‌ایم. همچنین این مسئله را یادآور می‌شویم که نگاه ما به نیروی انسانی توانمند می‌بایست راهبردی بوده و تصویرسازی از یک نیروی سایبری و طراحی مفهومی، نخستین گام در استقرار سازمان سایبری محسوب می‌شود.*

**واژگان کلیدی:** دفاع سایبری، موتور توانمندساز سایبری، کارکشتگان سایبری، نیروی پایدار سایبری، سرمایه انسانی سایبری.

[۱] دانشجوی دکترای حرفه ای حکمرانی فاوا، دانشگاه صنعتی مالک اشتر، ar.yousefi@chmail.ir

[۲] نویسنده مسئول، استادیار دانشگاه صنعتی مالک اشتر، Mohtarami@mut.ac.ir

## ۱. مقدمه و بیان مساله

امروزه تحولات روزافزون فضای سایبر و رشد قابل‌توجه وابستگی‌های شخصی تا سازمانی و حتی کشوری به این فضای گسترده کاملاً مشهود است. فضای سایبری به‌عنوان *دامنه مشخص‌شده با استفاده* از الکترونیک و طیف الکترومغناطیسی برای ذخیره، تغییر و تبادل داده‌ها از طریق نظام‌های شبکه و زیرساخت‌های فیزیکی مرتبط تعریف می‌شود[۱]. فضای سایبری دارای تهدیدهای بسیاری است که ریشه آن نه‌تنها از دولت‌های ملی بلکه از سازمان‌های تروریستی، گروه‌های جرم و جنایت سازمان‌یافته و همچنین مجرمان اینترنتی سایبری می‌باشد[۲]. در دنیای فیزیکی، دولت‌ها تقریباً انحصاری در استفاده گسترده از نیروی نظامی دارند، مدافع دارای اطلاعات صحیح زمین است و حملات به علت سستی یا خستگی پایان می‌یابد. تحرک منابع هزینه‌ی زیادی دارند در حالیکه، در دنیای مجازی(فضای سایبر)، بازیگران گوناگون، گاهی ناشناس هستند، فاصله فیزیکی اهمیت نداشته و وقوع جرم اغلب ارزان است. از آنجا که طراحی اینترنت بر پایه سهولت در استفاده بوده است به‌جای امنیت، ارتکاب به جرائم مزیتی ذاتی نسبت به دفاع دارد[۳]. ضمن آنکه موانع نسبتاً کم برای ورود به فضای سایبری در مقایسه با تهدیدات معمولی وجود دارد، یک هکر به‌تنهایی می‌تواند شبکه اطلاعات حیاتی کشوری را ویران کند. با توجه به گسترش دشمنان و تهدیدات در فضای سایبری، کشورها تلاش‌های خود را برای ایجاد سازمان‌های امنیتی سایبری برای حفاظت از شبکه‌های حیاتی خود افزایش داده‌اند. مطابق با سطح قدرت یک کشور، قابلیت‌های جاسوسی سایبری در حال افزایش است. ابزارهای موجود در جنگ سایبری ممکن است به نظر دارای یک ویژگی فناورانه غالب و موازی با پیشرفت‌های قابل‌توجه در فناوری باشد. درعین‌حال تنها با تکیه‌بر جنبه‌های فناورانه در جنگ سایبر، نمی‌توان به موفقیت رسید. فرمانده سابق ارتش ایالات‌متحده آمریکا سرتیپ هرناندز برای توجه به جنبه انسانی امنیت سایبر اعلام کرد: *سایبر تهدید شماره یک امنیت ملی است و فکر می‌کنم مردم، نه فناوری، تهدیدات سایبری را ایجاد می‌کنند*. علاوه بر این، ایوان و ریدر تأکید می‌کنند که یک *عنصر حیاتی از یک استراتژی قوی در زمینه امنیت سایبری، داشتن افراد مناسب در هر سطح برای شناسایی، تربیت کارکنان دفاع و واکنش است*[٤].

برنامه‌ریزی و مدیریت نیروی انسانی در استخدام، آموزش و نگهداری از اهمیت ویژه‌ای برخوردار است. علیرغم تقاضای رو به رشد برای مهارت‌های مربوط به سایبر، کسری قابل‌توجهی از افراد با این مهارت‌ها باقی می‌ماند. علاوه بر این، رقابت برای شناسایی و استخدام استعدادهای سایبری به علت تقاضا از سوی نهادهای دولتی و بخش خصوصی بسیار زیاد است. بر اساس گزارش اخیر رویترز، *گوگل در حال حاضر ۱۲۹ عنوان شغل امنیتی فناوری اطلاعات را تبلیغ می‌کند، درحالی‌که شرکت‌های دفاعی مانند لاکید مارتین پارک*[۲] *و سیستم‌های* ***BAE***[۳] *در این زمینه به دنبال استخدام هستند*. فقدان افراد واجد شرایط همراه با تقاضای در حال افزایش، منجر به نگرانی شده است.

هدف ما در این مقاله معرفی چارچوبی برای توانمندسازی منابع انسانی است؛ نگرش ما به کارکنان حوزه فناوری اطلاعات و سایر علوم مرتبط، به مثابه یک سازمان سایبری خواهد بود؛ در واقع امروز، سازمان، شرکت یا سرمایه‌ای وجود ندارد که بتواند بدون توجه به مسائل سایبری به حیات خود ادامه دهد؛ بنابراین می‌بایست چارچوبی برای تضمین توانمندی‌های منابع انسانی متخصص وجود داشته باشد که امنیت سایبری را در آن عرصه تأمین نموده و آمادگی هرگونه دفاع در مقابله با حملات سایبری را دارا باشند. در واقع می‌خواهیم با ارائه یک چارچوب توانمندساز، امنیت را در لایه توانمندی منابع انسانی موردبررسی و مطالعه قرار دهیم.

## ۲. روش شناسی و نوآوری پژوهش

در این پژوهش از روش‌شناسی ویژه‌ای استفاده شده است و با توصیه‌هایی در مورد اینکه چگونه کشور باید با ایجاد و مدیریت یک نیروی سایبری بسیار ماهر مأموریت حوزه سایبری را پوشش دهد، ختم خواهد شد. بر اساس متدولوژی این تحقیق پس از تجزیه تحلیل مسائل، بر چهار برنامه محوری زیر تمرکز شده است:

- ✓ مدرن‌سازی نیروها و نحوه گزینش

[۲] Lockheed Martin Corp

[۳] BAE systems



فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال پنجم، شمارهٔ چهار، زمستان ۱۴۰۰

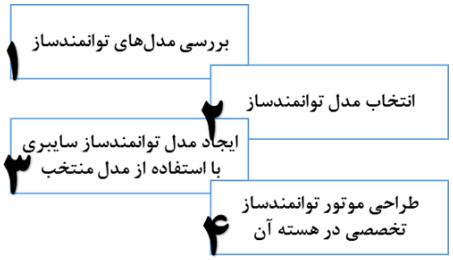
- ✓ نیروی انسانی و آموزش
- ✓ مدیریت منابع
- ✓ راهبرد و اصول

برای این موضوع ایجاد سازمانی رسمی با تمرکز بر قابلیت‌های فضای سایبری امری اجتناب ناپذیر است. هدف از تأسیس این سازمان تأمین نیروهای توانمند سایبری برای انجام آفند و پدافند در فضای سایبری و احیانا به عنوان نبرد مکمل در سایر عرصه‌ها می‌باشد. این پژوهش به سه پرسش مربوط به ایجاد یک نیروی سایبری پایدار می‌پردازد:

۱- قابلیت‌های مورد نیاز برای آماده‌سازی نیروی سایبری و افزایش توان سایبری کدامند؟

۲- نیروی سایبری باید دارای چه مهارت‌هایی باشد و توزیع آن‌ها با تنوعی از پرسنل علمی، کارمند و پیمانکار در حوزه‌های کاربردی چگونه انجام پذیرد؟

۳- چه ساختاری منجر به یک نیروی سایبری پایدار خواهد شد؟




**شکل ۱. مراحل تحقیق**

نوآوری تحقیقاتی این پژوهش در معرفی ابعاد و مولفه‌های توانمندساز نیروی کار دفاع سایبری است، که به جرأت می‌توان گفت در کشور کمتر به این بعد از مولفه توان‌افزا توجه شده است؛ حال آنکه نیازمندی کشور به سرمایه انسانی توانمند سایبری مقدم بر فناوری و محصولات پیشرفته است. چرا که نیروی توانمند، قابلیت تولید فناوری، دانش و محصول را ایجاد می‌نماید.

با پذیرفتن این اصل که در استقرار امنیت یا ایجاد یک ساختار دفاع سایبری می‌بایست در سه بعد فناوری، فرآیند و افراد فعالیت نماییم؛ ما قصد داریم در این تحقیق به بعد افراد یا همان منابع انسانی پرداخته و برای توانمندسازی آن در حیطه‌ی *مهارت، چارچوبی ترسیم نماییم. اهمیت پرداختن به این مؤلفه به عنوان مغزافزار هدف غائی (دفاع سایبری)، بیش از ابعاد دیگر بوده و حتی شکل گیری دو بعد دیگر نیز به قدرت و توانمندی آن بستگی دارد.*

بررسی و ارزیابی آماری چارچوب توانمندسازی ارائه‌شده در این پژوهش، به صورت پرسش‌هایی در قالب پرسشنامه و توزیع و تحلیل آنها با استفاده از نرم‌افزار آماری SPSS انجام شده است. البته ذکر این نکته الزامی است که به فراخور محدودیت‌ها به توزیع ۴۰ پرسشنامه میان کارشناسان ارشد و خبرگان حوزه دفاع سایبری اکتفا نموده‌ایم.

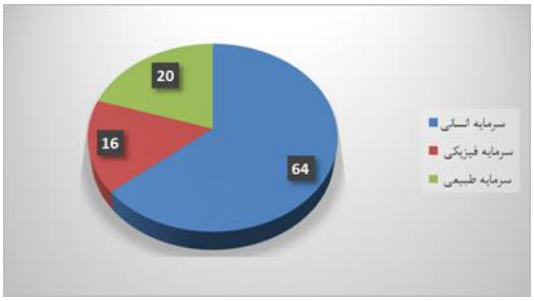
## ۳. مروری بر پیشینه پژوهش

امروزه سازمان‌ها در محیطی کاملاً رقابتی توأم با تحولات شگرف و سریع، باید اداره شوند. تحقیقات نشان داده است که بین فناوریهای سایبری و بطور خاص فناوری اطلاعات و توسعه نواوری در سطوح ملی و سازمانی ارتباط معناداری وجود دارد[۵] و این خود مسبب تحولات مختلف فنی-اجتماعی شده است. این تحولات در عصر حاضر که با تحولات سایبر عجین شده‌اند بیش از پیش ظهور و بروز بیرونی دارد. با چنین شرایطی مدیران فرصت چندانی برای کنترل کارکنان در اختیار نداشته و باید بیشترین وقت و نیروی خود را صرف شناسایی محیط خارجی و داخلی سازمان نمایند و سایر وظایف روزمره را به عهده کارکنان بگذارند. کارکنان زمانی می‌توانند به خوبی از عهده وظایف محوله برآیند که از مهارت، دانش، توانایی و انگیزه لازم برخوردار و با اهداف سازمانی آشنایی کامل داشته باشند. ابزاری که می‌تواند در این زمینه به کمک مدیران بشتابد فرآیند توانمندسازی است؛ در این فرآیند نیروی محرکه از برون انسان به درون او منتقل می‌شود و به او آگاهی می دهد، اهداف کار را روشن می سازد، بطوری که به جای اینکه به افراد بگویند که چه، چگونه و کی انجام بدهند باید به آنها توانایی ببخشند که خود مشکلات خود را حل کرده و برای خود تصمیم بگیرند.

مطالعات صورت گرفته نشان می‌دهد که هر یک دلار سرمایه گذاری در آموزش و پرورش، درآمد ملی را به مراتب بیش از

یک دلار سرمایه گذاری در ایجاد جاده ها، سدسازی، کارخانه ها یا دیگر کالاهای سرمایه‌ای افزایش می‌دهد.

اقتصاددانان از مدتها پیش‌بر آن بوده‌اند که مهم ترین عنصر تشکیل دهنده ثروت مولد یک کشور، سرمایه فیزیکی (دارایی‌های تولید شده) است اما بنابر ارزیابی بانک جهانی در ۱۹۲ کشور سرمایه فیزیکی به طور متوسط تنها ۱۶ درصد ثروت را تشکیل می دهد، سرمایه طبیعی مهم تر است و ۲۰ درصد سرمایه را تشکیل می‌دهد و از همه مهم‌تر سرمایه انسانی است که ٦٤ درصد ثروت را تشکیل می‌دهد.




**شکل ۲. عنصر تشکیل دهنده ثروت مولد یک کشور**

سیطره سرمایه انسانی به خصوص در کشورهایی با درآمد بالا، بارزتر است. در پاره‌ای از کشورها مثل آلمان، ژاپن و سوییس ۸۰ درصد کل ثروت را سرمایه انسانی تشکیل می‌دهد. در آفریقای جنوبی، که منابع انسانی توسعه چندانی نیافته بیش از نیمی از ثروت را منابع طبیعی تشکیل می‌دهد. نتیجه اینکه منابع انسانی، در افزایش توانمندسازی سازمان نقش کلیدی را بازی می‌کند. در واقع منابع انسانی با استفاده از قابلیت‌های خود از جمله قدرت جسمی و معنوی، دانش و مهارتش به آن قدرت آفرینش و خلاقیت می بخشد. مسلماً بدون وجود نیروی کارآمد، ابزارها جز چیزی بی جان نبوده و منابع انسانی نیز تنها با نیروی مشترک مجتمع در گروه‌ها و با استفاده از تجارب و مهارت‌های به جای مانده از گذشته می‌تواند تولید کنند و توانائی‌های بالقوه خود را بروز دهند.

در ارتباط با ضرورت توانمند سازی کارکنان باید بیان نمود، عواملی چون افزایش انتظارات مردم، جهانی شدن و رشد فن آوری‌های برهم‌زن، از جمله آنها بوده و باعث تفاوت چشمگیر سازمان های صده بیست و یکم با سازمان‌های سنتی شده است. در سازمان‌های سنتی صرفاً انرژی کارکنان، مدیریت میشد. در حالی که در سازمان‌های صده بیست و یکم علاوه بر انرژی، نیروی فکری و خلاقیت کارکنان نیز باید مدیریت گردد. تحت این شرایط نه تنها روش های سلسله مراتب دستوری-کنترل مناسب نخواهد بود بلکه کارکنان باید از خودشان ابتکار عمل نشان داده و براساس مشکلات سریعاً تصمیم و اقدام کنند و در واقع قابلیت خودگردانی داشته باشند[٦]. بنابراین، لزوم پرورش کارکنانی که دارای توانایی خود مدیریتی باشند باعث شده که توانمندسازی نیروی انسانی به عنوان یک پارادایم جدید توجه بسیاری از صاحب نظران مدیریت را به سوی خود جلب کند.

### ۳-۱.واژگان و اصطلاحات کاربردی در توانمندسازی

در فرهنگ لغت آکسفورد واژه توانمندسازی، «قدرتمند شدن»، «مجوز دادن»، «ارائه قدرت» و «تواناشدن» معنی شده و در معنای خاص قدرت بخشیدن و دادن آزادی عمل به افرادی برای اداره خود است. و در معنای تخصصی، سپردن اختیار قانونی به فرد و تفویض قدرت قانونی است. تاریخچه اولین تعریف به سال ۱۷۸۸برمی‌گردد. توانمندسازی را به عنوان توزیع روابط به نسبت ثابت بین اجزاء سازمان(به غیر انسان) یا همان ساختار سازمانی و اعطاء اختیار به فرد در نقش سازمانی می‌دانستند. این توانمندسازی یعنی این فرد مشتاق پذیرش مسئولیت بوده و این واژه برای اولین بار بطور رسمی به معنی پاسخگویی تفسیر شد و دومین تعریف، توانایی است[۷].

### ۳-۲.عوامل مؤثر در توانمندسازی

مهم‌ترین عوامل مؤثر در توانمندسازی عبارتند از: سبک رهبری، ساختار، آموزش، انگیزش و رضایت شغلی که به اختصار در خصوص سبک‌های رهبری توضیحاتی ارائه می‌گردد[۷].

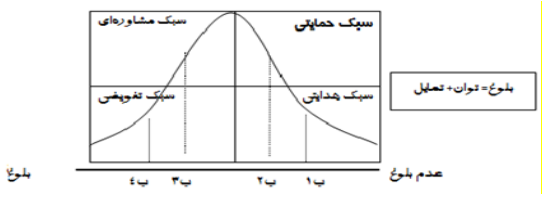
- توانمندسازی[٤] – عبارتست از واگذاری اختیار و مسئولیت بیشتر و قدرت بخشیدن به کارکنان با ایجاد انگیزه، طراحی و ساختار مناسب، آموزش مؤثر و مدیریت کارآمد است. شاخص های توانمندسازی عبارت از آموزش، انگیزش، ساختار سازمانی، رضایت شغلی و سبک رهبری است.

[٤] Empowerment

- آموزش[۵]- فعالیت‌های سازمان یافته که یادگیری را ارتقاء می‌دهد یا درگیر موقعیت‌های یادگیری هستند.
- انگیزش٦- انگیزش را می توان حالتی در افراد دانست که آنان را به انجام رفتار و عمل خاصی متمایل می سازد.

ساختار[۷] - روابط به نسبت ثابت بین اجزاء سازمان (به غیر از انسان) را ساختار گویند.

- ساختار سازمانی[۸]- چنانچه ۳ رکن پیچیدگی، رسمی شدن و تمرکز درهم ترکیب یا ادغام شوند، از مجموع آنها ساختار سازمانی به وجود می آید.
- رضایت شغلی[۲۰]- رضایت شغلی عبارتست از نگرش کلی فرد نسبت به شغلش. عوامل مؤثر بر رضایت شغلی عبارتند از:عوامل سازمانی **مثل دستمزد**، ماهیت کار **که** در ارتباط با محدوده و تنوع شغل است، محیط کار، عوامل فردی **مانند** نگرش، سابقه و صفات شخصیتی است.
- سبک رهبری[۲۱]- الگوی کلی کنش‌های رهبران چنان که از سوی زیردستانشان ادراک می‌شود، به نام سبک رهبری خوانده می شود، سبک رهبری فلسفه، مهارت و نگرش‌های مدیران را در محل نمایان می سازد.




**شکل ۳. ماتریس سبک رهبری با بلوغ**

## ۳-۳.نمونه الگوهای توانمندسازی کارکنان

دیدگاه های مختلفی در توانمندسازی کارکنان وجود دارد. نخستین دیدگاه، دیدگاه عقلانی به توانمندسازی است که برمبنای واگذاری اختیارات و پاسخگویی بنا شده است. در دیدگاه دوم قدرت به معنای نیرو است و بنابراین توانمندسازی می‌تواند به معنای نیروبخشی باشد. با این نگرش توانمندسازی فرآیند تقویت احساس خود اثربخشی در بین اعضا سازمان از طریق شناسایی وضعیت‌هایی که احساس بی قدرتی را در افراد می‌دمند و حذف آنها به همراه ایجاد مجرای انتقال احساس خود اثربخشی است.[۷]

برخی از مهمترین مدل‌های توانمندسازی در جدول(۱) خلاصه شده است.

جدول (۱): برخی از مهمترین الگوها در زمینه توانمندسازی

| عنوان پژوهش | یافته های اصلی |
|---|---|
| **مدل توانمندسازی بیل هارلی[۹]** | ضرورت آگاهی کارکنان از نقش خود در نتایج سازمان جوهره‌ی توانمندسازی تغییر در نحوه توزیع و اعمال قدرت در درون سازمان است. |
| **مدل دنیس کینلا[۱۰]** | توانمندسازی را فرآیند بهبود مستمر در عملکرد سازمان می‌داند که از طریق توسعه و گسترش نفوذ افراد و تیم‌های شایسته و با صلاحیت بوجود می‌آید،عناصر کیفی: اخلاق[۱۱]، تعهد[۱۲]، توانایی[۱۳]. |
| **مدل کارول[۱٤]** | اهمیت و ضرورت کار گروهی |
| **مدل توماس و ولتوس** | چهار بعد از توانمند سازی روانی ۱- تأثیر[۱۵] ۲- عزم شخصی[۱٦] ۳- شایستگی[۱۷] ٤- معنا داشتن. |
| **مدل باون ولاونر** | دسترسی به اطلاعات نقش مهمی در تصمیم گیری ایفا می‌کند که موجب توانمندی می‌شود |
| **مدل یحیی ملهم[۱۸]** | چهار عامل ارتباط مستقیم و تأثیر بسزایی بر توانمندسازی کارکنان در محیط رقابتی دارند (شکل ٤) |
| **مدل کوئین و اسپرتیزر** | ایشان نگرش به توانمندسازی را به دو دیدگاه ایستا و پویا تقسیم بندی می‌کنند (شکل ۵) |
| **مدل ایده آل نولر** | مدلی چهار بعدی برای توانمندسازی که وی آن را مدل ایده آل می‌نامد را ارائه کرده است (شکل ٦) |
| **مدل گلن لاوراک[۱۹]** | این مدل، رویکردی جدید به توانمندسازی است که در آن نقش افراد در تبیین و اجرای مدل بسیار پررنگ است. |

[۵] Education
[۶] Motivation
[۷] Structure
[۸] Organization Structure
[۹] Bill Harley
[۱۰] Dennis Franklin Kinlaw
[۱۱] Morality
[۱۲] Commitment
[۱۳] Ability
[۱٤] Anna Carrol
[۱۵] Impact
[۱٦] Self Determination
[۱۷] Competency
[۱۸] Yahya Melhem
[۱۹] Glenn Lave rack
[۲۰] Job Satisfation
[۲۱] Leadership style

### ۳-٤.نتایج بررسی پژوهش‌های توانمندسازی

بر اساس بررسی پژوهشهای صورتگرفته در زمینه توانمندسازی سازمان، موارد ذیل را می توان در خصوص عوامل موثر بر توانمندسازی کارکنان در سازمان پیشنهاد داد:

۱- سبک رهبری: بین سبک و نوع رهبری بعنوان یک عامل مهم می‌تواند در توانمند سازی کارکنان مؤثر باشد و هرچه این سبک رهبری انعطاف پذیرتر باشد موفقتر است.

۲- ساختار سازمانی: هرچه میزان تمرکز، رسمیت و پیچیدگی در سازمانها بیشتر باشد قدرت تصمیم گیری و خلاقیت از کارکنان سلب می‌گردد درنتیجه روند توانمند سازی کارکنان بسیار کند خواهد بود یک ساختار سازمانی اثربخش و کارآ باید بتواند بین ابعاد (رسمیت، تمرکز و پیچیدگی) و (اندازه، تکنولوژی، استراتژی و محیط) در سازمان تعادل برقرار کند.

۳- انگیزش: مهارتهای انگیزشی برای تقویت خلاقیت و نوآوری، وارد شدن در گروه سازی اجتماعی، توسعه مناسبات همکاری، شناسایی و تشویق رهبران مسئول، ثبات قدم و تعهد مستمر نسبت به وظایف مربوط لازم است.

٤- آموزش: آموزش و توسعه منابع انسانی در نظام مدیریت منابع انسانی نه تنها در ایجاد دانش و مهارت ویژه کارکنان نقش بسزائی دارد بلکه از این طریق باعث ایجاد توانمندی لازم می‌گردد.

۵- رضایت شغلی: افزایش رضایت شغلی و کاهش استرس در کارکنان سبب توانمندی آنان می‌گردد. احساس شایستگی و کفایت نفس از طریق ایجاد علاقه در افراد نسبت به مشاغلشان باعث افزایش رضایت شغلی و درنتیجه توانمندی می‌گردد.

| ویژگی‌های افراد ناتوان | ویژگی‌های افراد توانمند |
|---|---|
| اجتناب از مسئولیت پذیری | مسئولیت پذیر |
| غیرفعال | فعال |
| ترسو | جسور و بی‌باک |
| پیرو سنت قوانین | خلاق |
| بی حال و سست | پرتکاپو و پرانرژی |
| افسرده | خوشحال |
| وابسته | مستقل |
| بی انگیزه | بانگیزه |
| دوری از ریسک | ریسک پذیر |
| غافل | هوشیار |
| شکایت از کار | رضایت از کار |
| بی دقت | حساس و باریک بین |
| از بین بردن پتانسیل‌های درونی | استفاده از پتانسیل‌های درونی |
| کم‌هوش | باهوش |

**شکل ٤. مقایسه ویژگی‌های افراد توانمند و ناتوان**

## ٤. ارائه چارچوب پیشنهادی با رویکرد توانمندسازی سرمایه انسانی سایبری

کشور امریکا از اواخر سال ۲۰۰٦، فضای سایبری را عرصه‌ی مأموریتی جدیدی بعد از زمین، دریا، هوا و فضا معرفی نمود. مهمترین مؤلفه حیاتی در توان سایبری کشور، سرمایه انسانی است که نیروی سایبری را تشکیل می‌دهد[۸]. تحقیقات برای تشکیل یک سازمان سایبری می‌بایست از وزارت فناوری اطلاعات و ارتباطات، وزارت دفاع، سازمان پدافند غیر عامل و بخش‌های عمل کننده‌ی سایبری و مدیریت توسعه در نیروی انسانی و پرسنل انجام پذیرد.

مفهوم فضای سایبری برای عملیات و ساختارهای سازمانی همچنان در حال تحول و تعریف است. درنتیجه، این مطالعه راهبردی جهت کاربرد گسترده در سازمان متولی، طراحی شده است. محل بدست آوردن اطلاعات برای پاسخ به پرسش‌های مطروحه می‌تواند از منابع متعددی از جمله دکترین دفاعی، اسناد برنامه‌ریزی راهبردی و پایگاه داده‌های نیروی انسانی سازمان‌های ذیربط، همچنین مصاحبه با مدیران حوزه کاری و مدیران ارشد و کارکنان مسئول عملیات سایبری و بخش‌های امنیتی انجام پذیرد. یکپارچگی در سازمان متولی در مراحل اولیه توسعه ظرفیت‌های سایبری که شامل آفند، پدافند، و بهره‌کشی سایبری می‌باشد از اهمیت ویژه‌ای برخوردار است. آیا ادغام قابلیت‌های نبرد **فعال و غیر فعال** وجود دارد و اینکه چگونه می‌توان قابلیت‌های سایبری را با عملیات‌های اطلاعاتی و سایر قابلیت‌های عملیاتی با برآورد اثر ناشی از آن، یکپارچه کرد.

سازمان متولی در عرصه سایبری باید با سازماندهی، آموزش و تجهیز نیروی سایبری، خود را مهیای غلبه در سناریوهای نبرد



فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال پنجم، شمارهٔ چهار، زمستان ۱٤۰۰

متصور سازد. از طرف دیگر، نیروها برای آمادگی در نبردهای نامنظم و تقابل با تخاصم دشمنان می‌بایست مهارت استفاده‌ی موثر از ابزارها و تکنیک‌های مبتنی بر سایبر را کسب نمایند.

منابع قابل تحلیل در این پژوهش:

- ✓ دسته‌ی اول مشاغل حائز شرایط لازم با مهارت‌ها و تخصص‌های فعلی هستند؛
- ✓ دسته دوم که نیاز به افزایش مهارت‌های تخصصی فعلی با مهارت‌ها و دانش مرتبط با توانایی‌های خاص دارند، از قبیل: شبکه های کامپیوتری، نرم ازفار، سیستم عامل و..

بیشتر افراد در این سازمان از طریق برنامه‌های آموزشی و کسب مهارت‌های سایبری شایسته احراز مشاغل ترکیبی سایبری[۲۲] خواهند شد. بنابراین نتیجه می‌گیریم که مهم‌ترین اقدام در سیاست‌های اجرایی کشور یا نهاد متولی می‌تواند، ایجاد جایگاه ویژه و کد خاص سایبری(سازمان سایبری)[۲۳]، حضور افسر ناظر[۲۴] در ساختار مشاغل و کلید پست ویژه برای متخصصانی که در ماموریت‌های سایبری نقش دارند. (کد خاص یک کلید پستی است که می تواند نهاد متولی برای شناسایی یک کار خاص استفاده شود. این روش در نیروی هوایی امریکا با عنوان[۲۵]AFCS معرفی می‌گردد. زمانی که فرد مورد نظر برای تصدی پستی خاص می‌بایست شرایط و قابلیت‌های خاصی را داشته باشد، امکان دارد یک پیشوند یا پسوند نیز به همراه AFSC مورد استفاده قرار گیرد. این روش توسط ارتش ایالات متحده و سپاه تفنگداران دریایی ایالات متحده با عنوان [۲۶]MOS نیز استفاده می گردد [۹].

در تبیین مهارت‌های سایبری رویکرد آینده نگرانه الزامی است؛ همچنین تصور اینکه ترکیب قابلیت‌های سایبری با سایر قابلیت‌های موجود منجر به اعمال و استفاده از آن‌ها در نیرو به همراه دیگر ارگان‌های دولتی در اشکال مختلف جنگ و یا در زمان صلح خواهد شد، دور از انتظار نیست. در نتیجه پرسنل سایبری به مهارت‌های فنی، قانونی، سازمانی و عملیاتی نیاز خواهند داشت [۱۰].

مراحل بنیادین پیشنهادی که کشور از آن طریق می‌تواند سرمایه انسانی سایبری خود را مدیریت کند بدین شرح است:

۱- از جمله کارهای اساسی که منجر به یکپارچگی سازمانی و عملیاتی در ایجاد قابلیت‌های لازم می‌شود طراحی مفهومی عملیات[۲۷] است و در آن چگونگی بررسی عملکرد نیرو درون و از طریق فضای سایبری بین طیف گسترده‌ای از فعالیت‌ها مشخص می‌شود.

۲- از طرح مفهومی به عنوان مبنایی برای ذینفعان و مشخص نمودن نیازهای سرمایه انسانی (یعنی کارکنان وظیفه و ذخیره نیرو، غیر نظامیان و پیمانکاران) استفاده می‌شود.

۳- استقرار و وجود افسر ناظر به عنوان روشی برای مدیریت مهارت‌های سایبری و تطبیق آن با سیاست‌ها، دکترین و برنامه‌ریزی‌های انجام شده بخصوص در مورد نیروهای غرق در فضای سایبر بسیار لازم و ضروری می‌باشد.

۴- تخصص‌های مرتبط با فناوری ارتباطات و اطلاعات می‌تواند با تغییراتی به مهارت‌های ویژه عملیات سایبری مبدل گردد. این مجموعه مهارت‌ها در نظام‌های آموزشی موجود، قرابت فراوانی با مجموعه مهارت‌های مورد نیاز در عملیات‌های سایبری داشته و از این همبستگی می‌توان در انتخاب افراد سایبری استفاده نمود. از آنجا که قابلیت‌های سایبری، آسیب‌پذیری‌ها و تهدیدها به سرعت در حال تحول

---

[۲۲] مشاغل ترکیبی سایبری وظایف مهم خارج از حیطه تخصصی، یا تخصص یا مهارتی خاص در یک تخصص

[۲۳] منظور، تعریف کلید پست ویژه به جهت تمایز ایشان از دیگر جایگاه‌های شغلی می باشد.

[۲۴] افسر ناظر فردی است که در کنار نیروهای سایبری وظایف نظارت و انطباق مأموریت با تخصص را دارد.

[۲۵] Air Force Specially Code

[۲۶] Military Occupational Specialty

[۲۷] این موضـوع در ادبیات نظامی امریکا با CONOPS بیان می شـود، به این مفهوم که یک بیانیه شفاهی یا گرافیکی از مفروضات یا قصد فرمانده در رابطه با عملیات یا مجموعه‌ای از عملیات ها ا ست که به و سیله نشریه مشترکی "دفاع از ا صطلاحات نظامی و مرتبط" تعریف شده ا ست. *این طراحی برای ایجاد یک تصویر کلی از یک عملیات طراحی شده‌است.*

هستند، ارزیابی پیوسته *پایداری* نیروهای سایبری از اهمیت ویژه‌ای برخوردار خواهد بود. علاوه بر این، پرسنل سایبری ماهر ممکن است جذب فرصت‌های شغلی در بخش غیر نظامی شوند. برای همگامی با این چالش‌ها، باید نیازهای مهارت‌های سایبری را به طور معمول ارزیابی کند تا مشخص شود که آیا سیاست‌ها و اقدامات فعلی، حفظ نیرو را در پی خواهد داشت یا خیر.

### ٤-١. توانمندسازی چگونه محقق می‌شود

در فرآیند توانمندسازی چالش‌های داخلی و خارجی سازمان نقش زیادی دارند. چالش‌های خارجی افزایش شتاب تغییرات، محیط رقابتی، نیازهای جدید و شرایط خاص فضای سایبری


**شکل ٥. نمودار استخوان ماهی برای نیروی سایبری پایدار**

ایجاد تحول درونی در افراد برای ایجاد نگرشی جدید برای انجام وظایف و نقش سازمانی‌شان است.

در تعریف توانمندی از دیدگاه دانشمندان نیز دودسته وجود دارد:

١. دانشمندانی چون دسلر[٢٩]، شولتز، ایلون[٣٠]، چاپی[٣١]، کارستون[٣٢]، بلاک، پیترز و ... به توانمندسازی به عنوان یک سازه ساختاری توجه دارند و فرآیند توانمندسازی کارکنان را بر عهده مدیریت می‌پندارند. به این نگرش، نگرش ساختاری (توانمندسازی سخت[٣٣] یا بیرونی[٣٤]) نیز گفته می‌شود.

است. چالش‌های داخلی بیشتر بر حفظ و نگهداری نیروی انسانی موجود، افزایش سطح انگیزش، رشد و شکوفایی استعدادها و مهارت‌ها و قابلیت‌های کارکنان تأکید دارد.

توانمندسازی با اعمال فشار مدیران و دستورالعمل محقق نمی‌شود، بلکه فرآیندی است که مستلزم پذیرش فرهنگ توانمندسازی و مشارکت داوطلبانه کارکنان است[١١].

### ٤-٢. رویکردهای توانمندسازی و نگرش تلفیقی به تئوری‌های توانمندسازی

در دنیای رقابتی امروز، سازمان‌هایی پیشتاز هستند که توسعه و منابع انسانی در آنها به عنوان یک اصل مطرح باشد. اصلی که امروز یک مزیت رقابتی[٢٨] برای سازمان‌ها محسوب می‌شود.

در نظریه مک گریگور ایجاد بستر برای نیل به هدف مقدم است بر سرپرستی و هدایت تلاش. درکل به توانمندی با دو دیدگاه متفاوت نگریسته می‌شود:

دیدگاه اول سهیم کردن کارکنان در قدرت و توانایی مشارکت در تصمیم گیری سازمانی داشته و هدف آن قدرتمند شدن کارکنان است. دیدگاه دوم از منظر روانشناختی با هدف ٢. کانگر و کانگو، توماس و ولتهوس، اسپریتزر، زیمر من و ... نیز دانشمندانی هستند که ادراک فرد برای توانمندسازی را مقدم بر هر چیز دیگر می‌دانند. به این نگرش، توانمندسازی انگیزشی و روانشناختی (توانمندسازی نرم[٣٥] یا درونی[٣٦]) نیز گفته می‌شود[٧].

همه کارکنان نیاز دارند که از رسالت، چشم‌انداز، ارزش‌ها، مقررات، اهداف و روش‌های سازمان آگاه باشند و علاوه بر آن جهت گیری کلی سازمان می‌بایست مانند پیامی به منظور تعیین نقش‌های مختلف گروه‌های کاری و افراد منتشر شود. کارکنان همسو نه تنها نقش خود را می‌دانند بلکه خود را وقف حمایت از آن می‌کنند. وقف کردن مترادف «تعهد» است و تعهد نه خریدنی و نه فروختنی است؛ بلکه اکتسابی است[٣٧].

[٢٨] Competitive Advantage
[٢٩] Desler
[٣٠] Ilon
[٣١] Chappy
[٣٢] Carstoon
[٣٣] Hard Empowerment
[٣٤] External
[٣٥] Soft Empowerment
[٣٦] Internal
[٣٧] تر آرتور و دیترو ایروینگ، مدیریت کیفیت فراگیر (TGM)

دومین بعد، پرورش قابلیت‌های کارکنان است. کارکنان باید از توانایی، مهارت و علم مورد نیاز برای انجام وظایفشان برخوردار باشند.

سومین بعد، اعتماد متقابل است. ویلیام شریر، بر این اعتقاد است که اعتمادبه نفس مهم و اعتماد به دیگران، چسبی است که

### ٤-٣. مؤلفه‌های توانمندساز

در این بخش ما با استفاده از ۹ دستور استخراج شده توسط محققین مختلف ]۱۲و۱۱و۷و٦] سعی در بسط این تئوری در فضای سایبری داریم.

۱-۳-٤. شفاف سازی رویکرد و اهداف

پنج ویژگی هدف و رویکرد سازمان (**SMART**) عبارتست از قابل تشخیص و تفکیک (**Specific**)، قابلیت سنجش تحقق اهداف (**Measurable**)، هم سویی اهداف با مقاصد و فکر اصلی سازمان (**Aligned**)، تناسب اهداف با ظرفیت افراد (**Reliable**)، تعیین چارچوب زمانی برای تحقق اهداف ( **Time Bound**). پرورش تجارب و تسلط شخصی، فراهم آوردن حمایت، الگوسازی، برانگیختگی احساس، فراهم آوردن اطلاعات لازم، تأمین منابع مورد نیاز، پیوند دادن نتایج ۳۸، ایجاد اعتماد.

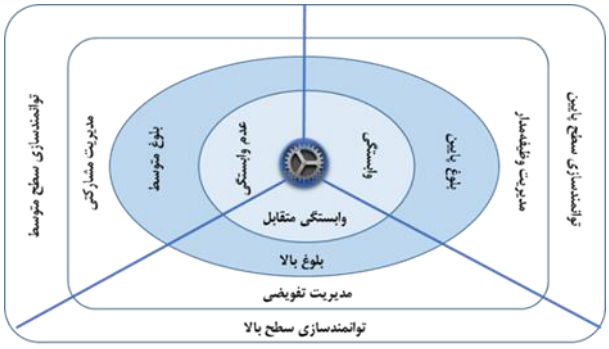
۲-۳-٤. ابعاد توانمندسازی

سازمان‌ها می‌بایست در سه بعد اقدام به توانمندسازی نمایند. اول آنکه همسو کردن نیاز کارکنان با رسالت، ارزش‌ها و چشم‌انداز سازمان است. همه کارکنان نیاز دارند که از رسالت، چشم‌انداز، ارزش‌ها، مقررات، اهداف و روش‌های سازمان آگاه باشند و علاوه بر آن جهت گیری کلی سازمان می‌بایست مانند پیامی به منظور تعیین نقش‌های مختلف گروه‌های کاری و افراد منتشر شود.کارکنان همسو نه تنها نقش خود را می‌دانند بلکه اکتسابی است[۳۹]

دومین بعد، پرورش قابلیت‌های کارکنان است. کارکنان باید از توانایی، مهارت و علم مورد نیاز برای انجام وظایفشان برخوردار باشند.

سومین بعد، اعتماد متقابل است. ویلیام شریر، بر این اعتقاد است که اعتمادبه نفس مهم و اعتماد به دیگران، چسبی است که

اعضای سازمان را به هم پیوند داده و باعث می‌شود که افراد سازمان به یکدیگر احترام گذاشته، همدیگر را به حساب آورده و دارای اهداف مشترک بشوند.




اعضای سازمان را به هم پیوند داده و باعث می‌شود که افراد سازمان به یکدیگر احترام گذاشته، همدیگر را به حساب آورده و دارای اهداف مشترک بشوند.

### ٤-٤. چارچوب پیشنهادی

**شکل ٦. چارچوب پیشنهادی توانمندسازی منابع انسانی**

چهار پرسش در مورد ایجاد یک نیروی سایبری پایدار مطرح می‌باشد، در واقع نگاه مدیریت قرارگاهی در این عرصه مهم و حیاتی، محلی از اعراب ندارد. آنچه امروز در کشور با آن مواجه هستیم برخورد مقطعی با مسئله سایبری است که خود منشأ آسیب برای زیرساخت‌های حیاتی کشور خواهد بود.

۱- استفاده از نیروهای موجود و سایبریزه کردن آن‌ها با توصیفی دقیق از قابلیت‌های سرمایه انسانی تراز.

۲- تبیین پروتکل برای چگونگی توزیع نیروی سایبری برای سازمان‌هایی که به ایشان نیاز دارند.

۳- ضمن توجه به رشد قابلیت‌های سایبری، شناسایی و استفاده حداکثری از مهارت‌های موجود و توجه به نیازهای آینده و متخصصانی که در زمینه های نوین فعالیت داشته‌اند.

٤- ایجاد یک ساختار و سیاست مدون که منجر به ایجاد نیروی سایبری ماهر،عملیاتی و پایدار گردد.

[۳۸] Connecting to Outcome

[۳۹] تر آرتور و دیترو ایروینگ، مدیریت کیفیت فراگیر (TGM)

فرضیاتی نزدیک به واقعیت در این گزارش ارائه میگردد. اولا، چگونگی مفهوم سازی یک نیروی سایبری در طول دوره زمانی مطالعه، عنوان میشود. – ابتدا با تصویرسازی از یک نیروی سایبری آغاز نمودیم. برای این طراحی مفهومی، باید اولین گام‌ها را در جهت ساختن یک مدل از مسئله‌ای که تعریف کرده‌ایم برداریم. ورودی این مرحله، آن چیزی است که در فاز تعریف مسئله تهیه کردیم. خروجی این مرحله، یک مدل مفهومی است که می‌تواند به شکل مدل علت–معلولی یا مدل جریان باشد. – سپس، پاسخ به سوالات تحقیق با تمرکز بر تخصص‌های ویژه‌ی پرسنل نهادهای مربوطه که بیشتر در مأموریت سایبری مورد استفاده قرار می‌گیرند ارائه می گردد. (پرسش‌ها از افراد متخصص و درگیر عرصه و عملیات سایبری اخذ گردیده است) از آنجا که قابلیت‌های فضای سایبری به طور مداوم در حال تحول هستند، همچنین دیدگاهی را در مورد آینده سایبری که کشور ممکن است با آن مقابله کند و پیامدهای بالقوه آن برای این که چگونه کشور نیروی سایبری خود را مدیریت کند، فراهم شده است. با توجه به ماهیت سیال فضای سایبری همچنین تغییرات پیوسته در قابلیت‌های سایبری، بنابراین آینده پژوهی سایبری نیز برای مقابله با پیامد های بالقوه آینده نزدیک نیز اندیشیده و ارائه شده است.

### ٤-٥. چگونگی شکل‌گیری نیروی سایبری

تبیین قابلیت‌ها برای افزایش یا توسعه توان سایبری در کشور می‌تواند از منابع فعال در فضای سایبری آغاز گردد. (هدف ما استخراج قابلیت‌های سایبری است)

پیرو مطلب ارائه شده در خصوص لزوم وجود طرح مفهومی عملیاتی در آغاز کار، مقامات مسئول می‌توانند برای برنامه‌ریزی اولیه و هماهنگی لازم برای عملیاتی کردن اهداف خود، چشم‌اندازی با عنوان مشخص[٤٠] در فضای سایبری تعریف نمایند. (بعد از گردآوری نیروی خبره سایبری تعریف یک مأموریت سایبری در سطح سازمان منجر به استخراج قابلیت‌های موجود سایبری خواهد شد). در جلسات با اعضای کارگروه، در خصوص چیستی و چرایی سازمان سایبری، و صدور فرمان سایبری مسائلی از قبیل زیر میتواند مطرح گردد:

- اهمیت تعیین منطقه ماموریت
- پیش بینی قابلیت‌های سایبری لازم در منطقه مأموریت
- برنامه‌ریزی برای ایجاد قابلیت عملیاتی

برای طراحی یک مانور سایبری که بتواند قابلیت‌های جامعی را از وضع موجود ارائه دهد، لازم است افرادی که برای برنامه‌ریزی منتخب سازمان هستند، چند ویژگی داشته باشند:

۱- فرمان پذیری نیروها

۲- خبرگی در عرصه سایبر

۳- شناخت جامع از وضع موجود و برنامه آینده

وظیفه مأموریت عملیات در فضای سایبر در دکترین کدام یک از سازمان‌های: پدافند غیر عامل، افتا، یا وزارت دفاع و یا... قرار گرفته است؟! به طور خاص، عملیات شبکه کامپیوتری به عنوان یکی از پنج قابلیت اصلی در نظر گرفته می‌شود. بنابراین، اطلاعات–عملیات سازمان یا سازمان‌های عمل کننده و برنامه‌های مشترک آنها می‌تواند منبع دیگری از اطلاعات برای احصاء قابلیت‌های سایبری باشند. دکترین و اسناد پشتیبان، گستره‌ی حوزه ماموریتی سایبری برای بکارگیری قابلیت‌هایش را مشخص می‌سازد. توصیفی از قابلیت‌های سایبری فعلی و مشترک موجود در اسناد پشتیبان و غیره، به ما کمک می‌کند تا تکنیک‌های شامل قابلیت‌های فعلی و بالقوه را درک کنیم. در زمان انجام این تحقیق، اسناد برنامه‌ریزی راهبردی، اسناد برنامه‌ریزی سازمانی و اسناد مربوط به طرح‌ریزی عملیاتی به صورت هماهنگ در حال توسعه بودند (اسناد بالادستی در اختیار به عنوان مرجع اصلی این تحقیق در توسعه نیروی سایبری مورد

[٤٠] عنوان مشخص را از این پس "آمادگی سایبری" می نامیم.

استفاده قرار گرفت). این منابع اطلاعاتی، پنجره‌ای را برای ایجاد قابلیت‌هایی که کشور برای توسعه نیاز دارد را فراهم می‌کند.

یافته‌های این بررسی نشان دهنده‌ی دو بعد راهبردی است.

اول اینکه، هماهنگی درونی سازمانی با ادغام قابلیت‌های کنونی (عملیات نبرد شبکه‌ای و جنگال) و آتی با برگزاری مانورهای سایبری منجر به "آمادگی سایبری" خواهد شد.

عملیات نبرد در فضای سایبر، شامل حمله، دفاع و قابلیت‌های پشتیبانی شبکه است.

- عملیات حمله شبکه متشکل از توانایی‌های هوایی و زمینی است که رقیب را در عرصه‌های زمین، دریا، هوا، فضا و سایبر در معرض خطر نگه می‌دارد.
- قابلیت‌های دفاعی شبکه شامل تجزیه تحلیل‌های تهدید، آماده‌سازی عملیاتی میدان نبرد و دفاع فعال از شبکه‌های رایانه‌ای است.
- پشتیبانی شبکه از قابلیت‌های عملیات شبکه در سطح جهانی و حصول اطمینان از سلامت شبکه‌ها در محیط‌های تهدید مختلف تشکیل شده‌است.

عملیات‌های طیف الکترونیکی، از انرژی الکترومغناطیس استفاده می‌کنند تا بدینوسیله تهاجم به دشمن صورت پذیرد. مثال: جمینگ و فریب الکترومغناطیسی، مدیریت طیف و هاردنینگ الکترومغناطیسی، و هشدار به تهدید امواج الکترومغناطیسی[۴۱]

می‌توان در نظر داشت که قابلیت‌های سایبری تنها در نبردهای سایبری به صورت مستقل بکار گرفته شوند؛ یا قابلیت‌های غیر جنبشی با جنبشی به صورت هماهنگ و از طریق یک مرکز عملیات به بهره‌برداری برسد. دستیابی به هدف ترکیب قابلیت‌های جنبشی (جنگ فیزیکی) و غیرجنبشی (جنگ پشت پرده سایبری) نیز به یکپارچگی عملکردی قابلیت‌های سایبری با قابلیت‌های حاضر اطلاعات-عملیات، هوا و ... بستگی دارد. این یکپارچگی امکان ارزیابی دقیق و استفاده موثر از قابلیت غیر جنبشی یا موثرترین ترکیب و توالی توان سایبری و قابلیت‌های جنبشی را فراهم می‌آورد. با این حال، در زمان انجام این تحقیق، وزارتخانه های متبوع مشخص نکرده اند که چنین یکپارچه‌سازی عملکردی چگونه رخ می‌دهد یا چه تاثیراتی از یکپارچه‌سازی بوجود خواهدآمد.

برای مثال در برگزاری یک مانور سایبری می توان با این موارد اشاره کرد ۱- متولی مانور کیست؟ ۲- چه جنس از قابلیت‌هایی می بایست استخراج گردد؟ ۳- هر کدام از این قابلیت‌ها چه اثری در دفاع یا حمله سایبری دارد؟

دومین یافته ما به یکپارچگی بیرونی می‌پردازد. وزارت فناوری اطلاعات، وزارت دفاع یا سایر وزارتخانه های مرتبط تنها وزارتخانه هایی نیستند که به طور موثر در فضای سایبری عمل می‌کنند. با این حال، در زمان این تحقیق مدرکی دال بر وجود برنامه‌ریزی دقیقی که هدف آن ادغام قابلیت‌های پیش‌بینی‌شده با سایر سازمان‌هایی که دارای قابلیت‌های مشابه یا مکمل هستند، پیدا نشد. به عنوان یک مورد، بررسی شده در کشور ایالات متحده، ارتش، سازماندهی، آموزش و تجهیز را بر عهده داشته و قابلیت‌های دفاعی شبکه خود را در بخش فرماندهی فن‌آوری، و تحت فرمان یک ژنرال، انجام می‌دهند. نیروی دریایی نیز مسئول عملیات‌های شبکه رایانه‌ای است (فرماندهی جنگ شبکه نیروی دریایی) و توسط یک دریاسالار فرماندهی می‌شود. از آنجا که قابلیت‌های نیروی هوایی به ماموریت‌های مشترک کمک می‌کند نتیجه گرفته شد که برنامه‌ریزی برای توسعه و به‌کارگیری قابلیت‌های سایبری نیروی هوایی به یکپارچگی سایر اقدامات منجر خواهد شد.

[۴۱] این دسته از عملیات‌با دستکاری طیف الکترومغناطیسی برای بهبود مقاومت هواپیما یا حمله به اهداف دشمن انجام شود.

### ٤-٦. مدیریت سرمایه‌های سایبری با تمرکز بر نیروی انسانی

مصاحبه در سطح کارکنان، چالش‌هایی را پیرامون مجموعه کاملی از توانایی‌های عملیاتی سایبری در یک محیط با منابع محدود ایجاد کرده و در عین حال تلاش برای شناسایی پرسنلی که بتوانند کادر اولیه سایبر را تشکیل دهند را آشکار ساخت (مطالعات و مصاحبه‌های میدانی در سطح کارکنان، ما را با چالش‌های اجرایی مواجه ساخت که خاص مدیران ارشد به پایین بود). مدیران ارشد درباره مراحل اولیه توسعه طراحی مفهومی بحث و تبادل نظر داشته و اذعان کردند که راهبردهای مدیریت سرمایه انسانی هنوز به طور کامل مورد بررسی قرار نگرفته است. برخی دیگر از کارکنان ستاد شرح دادند که انتخاب هدف برای ایجاد فرماندهی ارشد، وابسته به رویکرد سایبری است؛ ولی به نظر نمی‌رسد دکترین فعلی آن را تایید کرده و موفق به شناسایی مجموعه مهارت‌های سایبری – که بخشی از نیروی سایبری باید آن را داشته باشند – شود.

مصاحبه بعدی با مدیران ارشد و پرسنل سایبری (جدا نمودن کارکنان سایبری از سایر کارشناسان)، در بخش شبکه و آموزشگاه انجام شد. تمرکز این بخش بر مسائل آموزشی و مدیریت جاری مرتبط با سایبر بود. هم اکنون با چالش ایجاد سرمایه انسانی سایبری که مهارت‌های سایبری مهم را هم از لحاظ فنی و هم از لحاظ عملیاتی برای رفع مشکلات موجود در سازمان‌ها دارا باشند مواجه هستیم. اغلب، پرسنل این بخش با دانش سایبری ناکافی و در برخی موارد با عمق ناکافی در حال فعالیت می باشند. بنابراین اولین چالش در ایجاد سرمایه انسانی تأمین پرسنل سایبری می باشد.

می‌توان اسناد برنامه‌ریزی اولیه به سازمان در زمینه‌های مرتبط با کامپیوتر، اطلاعات و سایر حوزه‌های کاری مرتبط به عنوان اسناد پشتیبان اصلی نیروی سایبری پیشنهاد شود. در مصاحبه با مدیران در حوزه کاری مربوطه، بسیاری از مسائل مرتبط با مدیریت سرمایه انسانی مطرح شد، شامل:

۱. کاهش قدرت در عرصه فناوری اطلاعات و ارتباطات در تضاد با رشد قابلیت‌ها و توسعه توانایی سایبری است. در واقع عدم وجود توازن بین مهارت‌های سرمایه‌های انسانی سایبری و رشد نمایی قابلیت‌های سایبری.

۲. چگونگی ادغام بخش‌هایی از کارهای اطلاعاتی، و تضاد بین ابتکار عمل کشور برای تقویت توانایی‌های اطلاعاتی و فراهم نمودن شغلی متفاوت برای پرسنل اطلاعاتی.

۳. چگونگی استخدام و استفاده سایر پرسنل به عنوان نیروی سایبری و عدم وجود نیروی ماهر سایبری تجزیه و تحلیل اطلاعات جمع‌آوری‌شده‌ی ذینفعان، چندین مسأله را روشن ساخت که به احتمال زیاد مدیریت سرمایه انسانی نیروی سایبری را شکل خواهند داد.

← اول اینکه، نیازهای سرمایه انسانی تحت‌تاثیر تعاریف خدمات نظامی از چگونگی عملکرد آن‌ها در فضای سایبری خواهد بود. توانایی‌هایی که مرتبط با امواج طیف الکترومغناطیس، فرکانس هستند در طول مدت نبرد و منازعه افزایش می‌یابد. خصوصیات وزارتخانه های متبوع در زمینه عملیات‌های پدافندی، آفندی و بهره‌برداری از شبکه و نحوه ارائه این توانایی‌های عملی در سراسر منازعات می‌تواند بر میزان و مهارت‌های نیروی سایبری تاثیر گذار باشد. از جمله مصادیقی که وجود پرسنلی مجهز به مجموعه مهارت‌ها و دانش‌های خاص را الزام آور می‌کنند بدین شرح می باشند: برای مثال:

- وجود سطوح مختلف آسیب‌پذیری سایبری در دفاع، حمله.
- بهره‌برداری از طیف وسیعی از اِعمال استراتژی‌ها و فنون برای حفاظت از فرآیندهای سطح‌بالا و روابط، مانند فرماندهی و کنترل، حفاظت از سیستم‌های عملکردی و آسیب‌پذیری‌های فن‌آوری‌های پشتیبان



فصلنامهٔ علمی – پژوهشی فرماندهی و کنترل، سال پنجم ، شمارهٔ چهار، زمستان ۱۴۰۰

- تطبیق عملیات در هر سطح

در نتیجه، تعداد اقدامات پدافند، آفند و یا بهره‌برداری توسط نیروی سایبری در عملیات می‌تواند بر اندازه آن تأثیر بگذارد. با تکامل ماهیت عملیات‌های مشترک و سایبری مربوطه، ممکن است میزان و الزامات مهارتی پرسنل سایبری مشخص گردد.

← ثانیا، تهدیدات سایبری جاری و بالقوه دشمنان، نیاز کشور به ایجاد راهبرد و قابلیت‌های چابک‌ساز در مقابله با این تهدیدات را بیش از پیش روشن خواهد کرد. شواهدی وجود دارد که سازمان‌های دولتی به طور فعال در حال توسعه توانایی‌های سایبری برای بهره‌برداری و حمله به شبکه هستند. کشور باید نیروی سایبری خود را سازماندهی و تجهیز کند تا با موفقیت در هر تعداد از سناریوهای نبرد سنتی پیروز شود. اما قابلیت‌های جنگ سایبری ابزار غیردولتی‌ها نیز می‌باشد. در اقدامات ضد اطلاعاتی و ضد شورش علیه نیروهای ائتلاف (ناتو) در عراق و افغانستان، مشخص شد از فناوری اطلاعات و الکترومغناطیس به عنوان وسیله نفوذ، سازماندهی و حمله استفاده شده است. نیروی سایبریِ کشور به مهارت‌های سایبریی نیاز خواهد داشت که با تکیه بر آنها، استفاده دشمن از ابزارها و تکنیک‌های سایبری را در این نوع جنگ‌ها کاهش داده یا از آن جلوگیری نماید. مفاهیم نوین دفاعی در عرصه سایبر می‌بایست مورد توجه ویژه قرار گیرد که برای نمونه می توان آگاهی وضعیتی و نفوذ آگاهانه سایبری را عنوان کرد.

← سوم، با توجه به رشد سریع فن‌آوری اطلاعات، مدیریت سرمایه انسانیِ سایبری گریز ناپذیر است. به عنوان مثال، پیشرفت در ظرفیت، سرعت و کاربردِ فناوری اطلاعات، احتمالا نتایج ذیل را به دنبال خواهد داشت:

- روش‌های نوین جنگ الکترونیک (EW) برای استفاده و کنترل طیف الکترومغناطیسی
- تحول سریع در تکنیک‌های جنگ، ابزارهای آفند و پدافند از کامپیوترهای شبکه و پشتیبانی از زیرساخت**های** IT با استفاده از طیف الکترومغناطیسی
- ایجاد تکنیک‌ها و ابزارهای اطلاعات-عملیات، به خصوص عملیات نفوذ، که اثرات تولید شده توسط EW و جنگ‌های شبکه را تحت‌تاثیر قرار می‌دهد.

چنین پیشرفت‌هایی می‌تواند حوزه مهارت‌ها و تجربیات عملیاتی را گسترش داده و جنگجویان سایبری را از برتری فنی در برابر دشمنان بالقوه مطمئن سازد.

مقوله نهایی، نحوه مقایسهٔ ویژگی‌های نیروی سایبری فعلی با ویژگی‌های مطلوب نیروی آینده است. در حال حاضر، حوزه‌های شغلی تضمین کننده هدف، دارای کادر کوچکی از افراد هستند که توسط سازمان‌های امنیتی و نظامی در بخش فناوری اطلاعات تایید شده‌اند؛ این افراد می‌بایست دارای مهارت‌های لازم برای تولید قابلیت‌های پیش بینی شده‌ی مورد نیاز سازمان سایبری باشند. اگر در کشور به کمبود پرسنل ماهر سایبری پی ببرند، آنگاه برای افزایش تعداد پرسنل با هدف پدافند، آفند و بهره‌برداری از شبکه‌های کامپیوتری، راهبرد مدیریت سرمایه انسانی را با رویکردی تهاجمی مورد نیاز خواهند دید. مسأله‌ی دیگر نیاز وزارتخانه های متبوع به ترکیبی از متخصصان سایبری در درون و بیرون (سایر

سازمان‌های درگیر با فضای سایبری) وزارت می‌باشد. سرپرستان، تجربه بیشتری را در زمینه استفاده عملی از قابلیت‌های سایبری دارند؛ متخصصان، در فناوری اطلاعات، زیرساخت‌ها، ابزارها و کدهای خاص دارای مهارت هستند. ویژگی‌های سازمان، در نحوه انتخاب، آموزش و توسعه نیروی سایبری تأثیر خواهد گذاشت. اهداف آینده، چگونگی تعریف راهبرد مدیریت سرمایه انسانی را نشان می دهد. همچنین سازمان می‌تواند از افسران و افراد مجرب فعال و آماده بکار (ذخیره) و غیر نظامیان به عنوان سرمایه انسانی استفاده کند. تصمیمات درباره ترکیب کلی نیرو، راهبردهای مدیریت سرمایه انسانی، سازمان مورد نظر را تحت‌تاثیر قرار خواهد داد.

### ٤-٧. رویکردهای راهبردی برای مدیریت سرمایه انسانی سایبری

با توجه به موضوعات متعدد از جمله بروز مسائل مهم[٤٢] سایبری در کشور و وابستگی اجتماعی، اقتصادی و شاید نظامی به این عرصه، می‌توان به این نتیجه رسید که اتخاذ رویکرد راهبردگونه در مدیریت آن هم در بخش سرمایه انسانی که کشور حائز مزیت رقابتی در این حوزه می‌باشد، از نیازهای اساسی کشور است. در زمان این تحقیق، متأسفانه برنامه‌ریزی‌های سرمایه انسانی وزارتخانه های متبوع متوقف در سطح تاکتیکی،کشف راه‌هایی برای تعریف کلیدپست شغل سایبری، ایجاد و هماهنگ کردن قوانین شناسایی نیروی فعلی، متمرکز می‌باشد. اگرچه این فعالیت‌ها و تصمیمات مهم هستند، اما به مؤلفه‌هایی از سرمایه انسانی که در پشتیبانی از اهداف عملیاتی و راهبردی قابلیت‌های سایبری نقش دارند، نمی پردازد.

یک رویکرد راهبردگونه در مدیریت سرمایه انسانی از چند مرحله تشکیل شده است:

اول، تعاملی مؤثر با رویکرد راهبردگونه بین مدیران مرتبط، متخصصان سرمایه انسانی و فرماندهان نیروی سایبری و سازمان‌های سایبری موجود برای توسعه برنامه‌های راهبردی ایجاد گردد.

هدف اصلی هماهنگ سازی راهبردهای سرمایه انسانی با مأموریت و اهداف سازمان سایبری است. این فعالیت بر برنامه‌ریزی سرمایه انسانی برای ایجاد قابلیت‌های اصلی و نیازهای سازمان‌ها متمرکزخواهد بود.

دوم، انتخاب سرمایه انسانی، توسعه، بهره‌برداری و نگهداری باید با برنامه‌ریزی عملیاتی نیروی سایبری هماهنگ شود.

ادغام این ملاحظات در مرحله اولیه، احتمال اینکه سرمایه انسانی با سایر الزامات منابع ارزیابی شود را افزایش می‌دهد.

در نهایت، عوامل کلیدی موفقیت که وسیله ای است برای بدست آوردن ساختار، مهارت و اهداف ترکیبی نیروی سایبری باید شناسایی شوند. بنابراین در بررسی عوامل کلیدی می‌بایست نمونه‌هایی از جمله موارد زیر مورد ارزیابی قرار گیرند:

- دستیابی به تعداد استخدام‌ها و حفظ کارکنان سایبری با مهارت‌های مورد نیاز
- احصاء نسبت نیروهای نظامی به پیمانی و کارکنان غیر نظامی در نیروی سایبری
- شناسایی مراحل حساسی که در تحقق این اهداف می‌بایست مورد ارزیابی قرار گیرند.

### ٤-٨. نیازمندی‌های نیروی انسانی برای تشکیل نیروی سایبری

[٤٢] حملات سایبری مانند Stuxnet، Flame وابستگی بانکی و دولت الکترونیک به فضای سایبر از آن جمله می‌باشد.

برای شروع، سعی شد برآوردی از اندازه و انواع نیروهای قابل در حوزه سایبری انجام پذیرفته و مهارت‌های کنونی این دسته از نیروها استخراج گردد. اطلاعات و داده‌های ما از مدیران فعال در فضای سایبر، بدست آمده است. ایشان درکی جامع از بکارگیری پرسنل و اینکه کجا و چگونه به مثابه دارایی‌های سایبری محسوب می‌شوند، ارائه کردند. همچنین در مورد هرگونه محدودیت موجود (به عنوان مثال، ثبات شغلی، یا مقررات ماموریتی متضاد) در توانایی کارکنان خود برای برآورده کردن نیازهای مورد انتظار -که برای سازمان برنامه ریزی شده- گزارش دادند (این نیازها از جمله نیازهای اولیه منابع انسانی بوده که مقدم بر کسب مهارت های آتی این منابع میباشد). با استفاده از پایگاه داده‌های موجود نیروی انسانی که مشخص کننده‌ی نیاز فعلی پرسنل سایبری از طریق سازمان، تخصص و رتبه بود، برآوردی به صورت تخمینی احصاء شد. برای تکمیل فرآیند اطلاعات تکمیلی را از طریق نیازهای فعلی و پیش بینی شده، مشاهده نمونه ای کوچک از سازمان‌های سایبری، مطالعه سازمان‌های بین المللی همچنین نیروی هوایی ایالات متحده در دو قالب مطالعه میدانی و کتابخانه‌ای جمع آوری نمودیم.

### ٤-٩. تربیت مبارزان سایبری "کارکشته"

پس از بررسی و تحلیل داده‌ها و اطلاعات در اختیار و احصاء شده، به این نتیجه رسیدیم که نیازهای سرمایه انسانی در حوزه سایبر برای سازمان‌های سایبری کشور در سطحی واحد در حال شکل گیری است. سازمان‌های تأثیرگذار در حوزه‌ی سایبری، سعی در ارائه‌ی طراحی مفهومی خود برای قابلیت‌های سایبری می‌باشند. با این حال، می‌توان رویکرد مشابهی را برای توسعه سرمایه انسانی در سازمان‌های مختلف متصور بود. در بسیاری از موارد، این سازمان‌ها تور آموزشی را به عنوان تکلیف در نظر می‌گیرند که تحولی در بهره‌وری و افزایش کارائی در پی خواهد داشت. در میان افسران، می‌توان از واحد اطلاعات،حفاظت از اطلاعات، کامپیوتر و ارتباطات، مهندسین برنامه‌نویس و توسعه دهندگان، مهندسین شبکه به عنوان مبارزان پیش-سایبر بهره برد.[٤٣] برخی از آنها (مبارزان پیش-سایبری) هم‌اکنون در واحدهای اطلاعات جاسوسی، امنیت شبکه و واحدهای ارتباطات رایانه‌ای فعال هستند. بیشتر سازمان‌ها مدعی هستند که اینگونه کارکنان با مهارت و تخصص اصلی که دارا می باشند، با یک آموزش و کسب تجربه شش تا هشت ماهه به مبارزان سایبری "کارکشته" مبدل خواهند شد. بعد از تکمیل این دوره آموزشی (OJT[٤٤])، پرسنل خواهند توانست شرایط لازم برای احراز انواع موقعیت‌ها شغلی در سازمان را کسب نمایند.

با این توصیف مقدماتی سه سوال در مورد مدیریت سرمایه انسانی در حوزه تربیت مبارزان سایبری کارکشته مطرح است:

- چه مهارت‌ها (training)، آموزش‌ها (education) و آزمون‌هایی برای تبدیل وضعیت نیروها به مبارزان سایبری کارکشته ضروری هستند؟
- مؤلفه‌های لازم برای استفاده مؤثر از "کارکشتگان" سایبری چیست؟
- چگونه مبارزان سایبری پس از کسب تجربه و پایان تورهای آموزشی می‌توانند به طور موثر بکار گرفته شوند؟

برای پاسخ به این سؤالها لازم است بررسی وضعیت چند سازمان منتخب که در ایجاد اثرات و قابلیت‌های سایبری مسئولیت دارند؛ انجام گردد. در این بازبینی جایگاه پرسنل هر سازمان کنار گذاشته میشود و جزییات مربوط به پرسنل را از

[٤٣] تمرکز ما بر سازمان‌هایی ا ست که ماموریت آن‌ها ارتباط نزدیکی با آفند، پدافند، و بهره‌کشی سایبری دارد.

[٤٤] On-the-Job Training

طریق تخصص و رتبه پرسنلی آنها در نیرو مورد ارزیابی قرار می‌دهیم. این سوالات مطرح می‌گردد که

- آیا برای حضور در موقعیت‌هایی فعلی، نیازمند مهارت‌های خاص سایبری می‌باشید؟
- آیا بین جایگاه وظیفه‌ای و تخصص تناسبی وجود دارد؟
- آیا مهارت‌های بدست‌آمده در موقعیت‌های مختلف می‌تواند درسازمان‌های مرتبط با سایبر و یا در سازمان‌های غیر سایبری مورد استفاده قرار گیرد یا خیر؟

انتظار می‌رود با ارائه پاسخ به سؤالات دیدگاه‌هایی در قالب پرسش‌های زیر به دست آید:

(۱) چندین موقعیت در این سازمان‌ها نیاز به مهارت‌های ترکیبی سایبری[۴۵] دارند؟ (ترکیب مهارت‌های تخصص-پایه و مهارت‌های خاص سایبری که از طریق آموزش حین خدمت به دست می آید)

(۲) چه نیازهای آموزشی در موقعیت‌های ترکیبی سایبری متداول است؟

(۳) آیا می‌توان از مهارت‌های ترکیبی در تورهای آموزشی بهره برد؟

(٤) آیا تخصص سایبری جدید، موثرترین راه برای مدیریت این سرمایه انسانی خواهد بود؟

### ٤-۱۰. مورد مطالعاتی (مشاغل ترکیبی سایبری نیروی هوایی ایالات متحده به عنوان)

در این بخش نیروی هوایی ایالات متحده به عنوان یک مورد مطالعاتی مناسب که شرایطی مشابه وضعیت فعلی کشور را از سر گذرانده است مورد بررسی قرار گرفته است. همچنین کدهای و عنوان‌های شغلی بیان شده برای کشور ایالات متحده موضوعیت دارد.

بررسی تحلیلی با تمرکز بر نیازمندی‌های ترکیبی سایبری سازمان نیروی هوایی انجام پذیرفت. اولین یافته از این بررسی نشان داد که مشاغل ترکیبی سایبری در رسته جنگ شبکه[٤٦]، مرکز عملیات هوایی[٤٧] و مرکز اطلاعات-عملیات نیروی هوایی[٤٨] توزیع شده‌اند. رسته شصت وهفتم جنگ شبکه، سازمانی اثر گذار در سایبر بوده که در ساختار آن افسران داوطلب و پرسنل غیر نظامی مشاهده می‌شود و بیشتر آن‌ها نیازمند کسب مهارت‌های ترکیبی سایبری شناخته شدند. مرکز ششصد و هشتم عملیات هوایی یک سازمان پرتوان سایبری است که از مرکز عملیات شبکه نیروی هوایی، اسکادران ششصد و هشتم اطلاعات هوایی و اسکادران شسصد و هشتم ارتباط هوایی[٤٩] تشکیل شده است. این سازمان عمدتاً توسط پرسنل نظامی اداره می شود. بیشتر جایگاه‌های ترکیبی سایبری در رسته ششصد و هشتم ارتباطات هوایی یافت می‌شد؛ که در آن ۳۳ جایگاه از ۵۸ جایگاه، نیازمند به کسب مهارت‌های ترکیبی سایبری شناسایی شدند. جایگاهی که نیازمند مهارت‌های ترکیبی سایبری باشد در مرکز اطلاعات-عملیات نیروی هوایی گزارش نشده است و تنها چهار مورد از ٤٥ مورد، در اسکادران ششصد و هشتم اطلاعات هوایی[۵۰] نیازمند کسب مهارت‌های ترکیبی سایبری بودند. مرکز اطلاعات-عملیات نیروی هوایی شامل سازمان‌های اثراگذار و توانمند سایبری است که در زمینه سایبر

[۴۵] وظیفه‌ای مهم و خارج از محدوده‌ی تخصصی که پرسنل دارا می باشند؛ یا تخصصی ویژه

[۴۶] Network Warfare Wing (NWW)

[۴۷] Air Operation Center (AOC)

[۴۸] Air Force Information Operation Center (AFIOC)

[۴۹] Air Comunication Squadron (ACOMS)

[۵۰] Air Information Squadran (AIS)

فعال بوده و در ساختار خود از افسران، سربازان و غیر نظامیان بهره می‌برد. در هر مأموریت نیاز این سازمان به جایگاه شغلی ترکیبی سایبری تعیین می شود. برای مثال در اسکادران سیصد و چهل ششم تست (۳۲ از ۵۹)، اسکادران نود و دوم اطلاعات عملیات (۱۸ از ۲۰)، و بخش فناوری (۲۹ از ۴۲) مقادیر بالاتری از موقعیت‌های ترکیبی سایبری وجود دارد.

تجزیه و تحلیل دقیق‌تری از این مهارت های ترکیبی سایبری در اینجا ارائه شده است. رسته شصت و هفتم جنگ شبکه، مرکز ششصد و هشتم اطلاعات هوایی و مرکز اطلاعات-عملیات نیروی هوایی، دارای ۱۴۵ جایگاه شغلی است که در ۷ تخصص توزیع گردیده است. در میان جایگاه‌هایی که نیازمند مهارت‌های سایبری هستند، ما توجه خاصی به حوزه‌های مهارت سایبری ویژه که برای هر متخصص مورد نیاز بودند، داشتیم. بیشتر پست‌های درجه داری افسری (۱۳ از۱۵) شناسایی‌شده که به مهارت‌های بیشتری نیاز داشتند در جنگ‌های الکترونیک و عملیات‌های اطلاعاتی بودند. سه پست نیازمند تخصص فضایی و موشک بودند که هر کدام نیازمند افزایش مهارت‌های اطلاعاتی و اطلاعات-عملیات بودند. در میان ۴۰ مقام افسر اطلاعاتی در این سازمان‌ها، ده نفر نیازمند تقویت مهارت های شبکه از جمله تجزیه و تحلیل شبکه، تهدیدات سایبری، روش هک کردن و/ یا کارکردن با ابزارها یا سلاح های بهره برداری از کامپیوتر شبکه بودند. نسبت‌های بیشتری از پست‌های افسری ارتباطات-کامپیوتر (۱۶تا۲۹) نیازمند مهارت‌هایی در حوزه‌های دانش امواج الکترومغناطیسی، عملیات‌های جنگ شبکه، دانش تهدیدات سایبری، و/یا اطلاعات-عملیات بودند. نیاز به کسب دانش در حوزه الکترومغناطیس و/ یا مهارت های اطلاعات-عملیات نیز در جایگاه دانشمندان و مهندسین توسعه، که عمدتا در مرکز اطلاعات-عملیات نیروی هوایی یافت می شود، مشاهده گردید. حتی اکتساب مقام افسری برای یک روان شناس بالینی مستلزم کسب مهارت‌های سایبری بیشتری شد. لزوم کسب دانش عملیات جنگ شبکه برای افسران و دانش بیشتر در عملیات نفوذ برای روانشناس بالینی، احصاء گردید.

در مجموع، ۸۸ مورد از ۱۴۵ پست افسری (۶۱ درصد) به عنوان جایگاه‌هایی که برای احراز آن نیاز به کسب مهارت و دانش سایبری می‌باشند، شناسایی شدند. مهارت‌های سایبری بیشتر به طور خاص جهت تکمیل مهارت‌های اصلی تخصص برگزیده و مشخص کردن جنگجویانی که به طور کامل واجد شرایط ماموریت در هر سازمان باشند، بیان گردیده است.


**شکل ۷. افراز دانش سایبری**

بیشترین پست‌های ارزیابی شده در دو حوزه کاری ارتباطات-کامپیوتر (AFSCs، A3،E3 و C3) و اطلاعات (AFSC، N1) بودند. از میان تعداد ۲۰۳ جایگاه بررسی شده که مورد ارزیابی قرار گرفتند، کامپوتر و ارتباطات،۸۱ درصد به کسب مهارت‌های ترکیبی سایبری شناخته شدند. این پست‌های شغلی با مشخصه کسب مهارت‌های بسیار خاص از جمله دانش شبکه‌های کامپیوتری، راه‌های بهره‌برداری و حمله به شبکه‌های کامپیوتری متمایز شدند. حوزه‌های تخصص عبارتند از: عملیات نبرد شبکه، شبکه‌های مرکز عملیات هوایی، حمله به شبکه کامپیوتری و طراحی عملیات، نقشه‌برداری و بهره‌برداری از

شبکه، آشنایی با مجموعه‌های ابزار NSA[۵۱]، و چگونگی مدیریت سیستم‌های حمله شبکه. از میان ۱۴۸ پست اطلاعاتی که مورد بررسی قرار گرفتند، سهم کمتری (۳۶ از ۱۴۸) نیاز به مجموعه مهارت‌های ترکیبی سایبری از جمله: دانش شبکه و زیرساخت‌های مخابراتی؛ کنترل فرمان، ارتباطات و کامپیوترها، هوش شبکه، ابزارهای آنالیز ترافیک شبکه، فرایندهای برنامه‌ریزی (عملیات روانی) و دانش اطلاعات و عملیات. در مجموع، یک سوم (۱۱۸ از ۳۶۱) موقعیت‌های مورد بررسی قرار گرفته به عنوان پست‌های نیازمند به مهارت‌های مرتبط با سایبر شناخته شدند.

همچنین اطلاعاتی در خصوص یک مجموعه کوچک و فوق تخصصی، متشکل از جایگاه‌های غیر نظامی را جمع‌آوری کردیم. پست‌های شغلی مورد اشاره بیشتر در AFIOC[۵۲] یافت می‌شود. آن‌ها مسئول ایجاد قابلیت‌های توانمندسازی-سایبری در گروه ۳۱۸ام اطلاعات-عملیات می باشند و بسیاری از آن‌ها نیازمند کسب مهارت‌های ترکیبی سایبری شناخته شدند. از ۱۲۵ جایگاه غیر نظامی، بخش‌های مهندسی برق و کامپیوتر، علوم رایانه و فن‌آوری اطلاعات، پژوهش عملیاتی، اطلاعات، یا متخصص تحلیلگر برنامه، ۵۶ درصد (۷۰ تا ۱۲۵) به عنوان نیازمند به کسب مهارت‌های سایبری بیشتر شناسایی شدند. نیازمندی در جایگاه مهندسی برق و کامپیوتر به مهارت‌ها و دانش‌های شبکه، مهندسی کد معکوس، تست و ارزیابی (T&E)، اقدامات ضد آسیب پذیری و EW خلاصه می‌شود. بسیاری از علوم کامپیوتر،IT و موقعیت‌های تحقیقاتی عملیاتی نیز نیازمند کسب این مهارت‌ها هستند. تنها بیش از نیمی از پست‌های اطلاعاتی غیرنظامی، نیازمند مهارت‌های بیشتری مربوط به تهدیدات سایبری و روش‌های نفوذ و همچنین دانش شبکه‌ها و بهره‌برداری و بهره‌کشی از شبکه می‌باشند.

### ۴-۱۱. بررسی سازمان‌های مشابه

ر در این بخش با ارائه طرحی مفهومی، چگونگی تشکیل ساختار را در سطح یک کشور مدل می نماییم. ابتدا باید تعداد کل موقعیت‌های ترکیبی سایبری که احتمالا در سراسر کشور وجود دارند را برآورد می‌کنیم. سپس می‌بایست نسبت تخصص به مهارت‌های ترکیبی سایبری را با نمره هر سازمان در نمونه مشخص کرد. میتوان استقراء سایر سازمان‌های سایبری که احیاناً در نمونه نیستند، به عنوان مشابه یا نزدیک به سازمان‌های نمونه انتخاب کرد. سپس نسبت‌های مناسب را به تخصص‌های اصلی در هر سازمان اعمال می کنیم. این رویکرد، با توجه به مأموریت‌های فعلی، مفاهیم عملیات و سازمان‌ها، تقریبا ۲۶۰۰ شغل ترکیبی سایبری برآورد می‌شود. تغییرات اجتناب‌ناپذیر در ماموریت‌ها، مفاهیم عملیات و سازمان‌ها، برآوردی بازنگری شده را دیکته خواهند کرد. همانطور که قبلا ذکر شد، مدیریت سرمایه انسانی نیروهای سایبری به شدت تحت‌تاثیر شرایط آینده سایبری، اندازه و ترکیب نیروی سایبری خواهد بود. سازمان‌های مورد بررسی می توانند دارای شرایط گوناگونی باشند:

- ✓ آن‌هایی که دارای شرایط لازم بوده و تا حد زیادی به مهارت‌های تخصصی سنتی محدود می‌شوند.
- ✓ آن‌هایی که نیاز به افزایش مهارت‌های تخصصی سنتی خود با مهارت‌ها و دانش مرتبط با قابلیت‌های سایبری ویژه دارند.

به طور معمول، این توانمندسازی می‌تواند توسط خود سازمان‌ها ارائه شود، به گونه‌ای که آموزش در سطح واحد خود را برای کسب مهارت‌های لازم سایبری، طراحی کنند. با این حال، بعضی از مقامات و جایگاه‌های بسیار فنی در این سازمان‌ها نیازمند پرسنل با دانش و مهارت‌های سایبری عمیق و ویژه هستند که با توجه به تکالیف محول شده به ایشان ضرورتی

[۵۱] National Security Agency

[۵۲] Air Force's Information Operations Center

اجتناب ناپذیر محسوب می‌شود. رویه طبقه‌بندی و فرآیند تکالیف جاری، تضمینی برای عدم تکرار تکالیف در مشاغل مختلف مربوط به سایبری را فراهم نخواهد کرد. درحالیکه رویکرد غیرمتمرکز برای توسعه، بیشتر الزامات یک سازمان را برآورده می‌کند، اما نمی‌تواند در مورد نیازهای سازمانی عمیق‌تر پاسخ مناسب ارائه دهد. همچنین فقدان تجربه عمیق سایبری در سطوح بالاتر در کشور، به ویژه برای مشاغل سیاستگذار، ارئه دهنده راهبرد و برنامه‌ریز وجود دارد. چنین موقعیت‌هایی نیازمند مهارت‌ها و دانش مرتبط با سایبری می باشند که با تجربه واقعی بدست آمده باشد. با این حال، در زمان این تحقیق، اغلب این پست ها توسط افرادی تکمیل شده است که فاقد تجربه سایبری قبلی بوده اند. برای پرداختن به این کمبودها، ممکن است کشور نیاز به اتخاذ رویکردی نوین برای طبقه‌بندی الزامات مهارت‌های سایبری و پرسنل سایبری داشته باشد که توسعه جامع نیروهای سایبری را تأمین نماید.

### ٤-١٢. ارائه مکانیزم مؤثر در بکارگیری مؤثر

یکی از معضلات و مسائلی که پس از کسب مهارت در خصوص سرمایه انسانی مطرح است، ثبت آن برای کارکنان در راستای توانایی سازمانی است. بهبود عملکرد مدیریت سرمایه انسانی می‌تواند با رویکرد تخصص-محور محقق گردد؛ در مکانیزم پیش رو سعی شده است با افزودن کدها و شناسه‌هایی خاص امکان ثبت و ارزیابی مهارتی متخصصین بخش سایبری را امکان‌پذیر نماییم.

- ✓ شناسه‌ی تجربیات خاص
- ✓ شناسه مهارتی مرتبط
- ✓ شناسه مهارت‌های خاص
- ✓ نحوه گزینش و پیوستن نیرو

نیروی کمکی و ورود متخصص بنا به نیاز؛ پیشنهاد می‌شود جایگزین‌ها در مقابل سه معیار ارزیابی شوند: (۱) قابلیت شناسایی مجموعه‌های مهارتی خاص، (۲) تناسب مدیریت نیروی کار و بهره برداری، و (۳) توانایی ایجاد تجربه مشارکتی.

شناسه تجربیات خاص؛ گاهی اوقات متخصصین سایبری علاوه بر تخصص خود به اقتضاء قرار گرفتن در موقعیت‌های خاص (زمان صلح یا نبرد)، تجارب ویژه‌ای کسب می نمایند. کسب این تجارب میتواند منحصر بفرد و محدود به تعداد اندکی از کارکنان سایبری باشد؛ نکته اینجاست که این دانش در سامانه جامع منابع انسانی برای اشخاص ثبت نمی‌شود، بنابراین امکان استفاده و ارزیابی آن در آینده میسر نمی‌شود. این معرف، اجازه شناسایی سریع متخصصین مورد اشاره را مهیا کرده و به نوعی مدیریت دانش ضمنی را تحقق می بخشد. البته، این شناسه‌ها امکان احصاء طیف گسترده‌ای از مهارت‌های مربوط به یک پست شغلی را فراهم نمی‌کنند. اگر برای مدیریت سرمایه انسانی سایبری به روش فعلی عمل گردد، این روش تجربه سایبری فزاینده را منجر نخواهند شد.

*شناسه مهارتی* نیروی ویژه سایبری، که از آن برای شناسایی توانایی و شرایط خاص استفاده می‌شود. به عنوان مثال، پرسنلی که دوره‌های آموزشی رسمی را طی کرده باشند یک پیشوند به کد شغلی آن‌ها اضافه می‌شود. برای مثال می‌توان از پیشوندی خاص، برای وظیفه پشتیبانی در جنگ الکترونیکی و پیشوندی دیگر برای اطلاعات-عملیات، در شناسایی مهارت‌های سایبری استفاده نمود. اگر این پیشوندها به همراه پیشوندهای جدید برای مدیریت نیروی سایبری استفاده شوند، می‌تواند مهارت‌های فعلی سایبری پرسنل را به دقت طبقه‌بندی کند. با این حال، از آنجا که پیشوند برای هدایت تکالیف آتی خود استفاده نخواهد شد، استفاده از آن نمی‌تواند تجربه سایبری تجمعی ایجاد کند.

*شناسه مهارت‌های خاص* نیروی ویژه سایبری می‌تواند یک کد الفبایی یا عددی باشد که از آن برای مشخص کردن زیرمجموعه‌های مهارتی درون نیروی ویژه سایبری استفاده می‌شود، باشد. هر پسوند یک عنوان است و استفاده از آن

بکارگیری پرسنل در موقعیت شغلی مورد نظر را قابل ارزیابی می‌سازد. بسیاری از نیروهای ویژه سایبری نیازمند استفاده از یک پسوند هستند، اما در برخی موارد پسوند اختیاری است.

مثال(مورد مطالعاتی): نمونه‌ای از این امر در سیستم طبقه‌بندی افسران در بخش تعمیر مهمات و موشک استفاده می‌شود. ممکن است پسوندی استفاده نشود، یا می‌تواند پسوند C برای نشان دادن مهارتهای مربوط به هسته اضافه شود. به طور مشابه، یک پسوند سایبری استفاده شده در ارتباط با AFSCs که معمولا با ماموریت سایبری مرتبط است، می‌تواند برای ایجاد تجربه سایبری تجمعی در این AFSCs ها استفاده شود.

ورود و گزینش به نیروی ویژه سایبری کشور می‌بایست پس از اتمام آموزش‌های لازم و صدور گواهینامه انجام شود. این روش مدیریت سرمایه انسانی بیشتر مناسب شرایطی است که پست‌ها به قدر کافی با شرایط و مهارتی خاص از سایر تخصص‌ها متمایز گردند؛ همچنین آموزش یا تحصیلات برای ورود به رشته تخصصی، کافی باشد. به عنوان یک روش مدیریت سرمایه انسانی، برای اطمینان از تخصیص مناسب پرسنل به پست مورد نیاز نیروی ویژه سایبری، از سطح بندی در گزینش استفاده می شود. در نتیجه، وجود برنامه راهبردی سایبری کشور برای گزینش، تجربیات سایبری هم افزا را برای ایشان ایجاد خواهد کرد.

عنوان نیروی ویژه سایبری کمکی، به پرسنلی که قبلا در نیروهای سایبری دیگر در سایر ارگان‌ها بوده‌اند، اعطا می‌شود. استفاده از نیروی ویژه سایبری کمکی در مدیریت نیروی سایبری و در میان کارکنان مجرب در تخصص‌های مرتبط، می‌تواند به طور سیستماتیک مهارت‌های ترکیبی سایبر را شناسایی کند.

تجزیه و تحلیل این مکانیزم مدیریتی، استفاده از پسوندهای نیروی ویژه سایبری و نیروی ویژه سایبری کمکی، معمولا روش‌های ترجیحی برای حداقل در چند سال آینده خواهند بود.

هر تخصصی که مرتبط با ماموریت‌های سایبری است، می‌تواند از طریق ترکیبی از شناسه تجربیات خاص، پیشوندها، پسوندها و فرآیندهای اعطا گواهینامه، مدیریت شود. سوالی که برای مدیریت نیروی سایبری باید پاسخ داده شود این است که:

کدامیک از این روش‌ها در بهترین حالت با روش‌های خاص مدیریت و توسعه مهارت‌ها هماهنگ بوده و به اهداف ساخت نیروی قوی و پایدار سایبری کمک می‌کند؟

همچنین پرداختن به توسعه گزینش نیروی ویژه سایبری موجود، به خصوص مهارت‌های مربوط به سایبر نیز غیر عملی است، مگر اینکه تخصص به طور کامل *با ماموریت‌های سایبری* هماهنگ شده باشد.

برنامه‌ریزی برای چنین اصلاحاتی در زمینه ارتباطات کامپیوتری که در حال اجرا هستند، می‌تواند انجام پذیرد، اما این تغییرات برای دیگر زمینه‌های کاری مربوط به ماموریت‌های سایبری امکان‌پذیر نمی‌باشد.

پسوندها می‌توانند به طور مؤثری مورد استفاده قرار گیرند. اطلاعات، ارتباطات-کامپیوتر، و تخصص مهندسی توسعه و نیروی ویژه سایبری کمکی می‌توانند به اهداف توسعه‌ی نیروی سایبری برای همه‌ی تخصص‌های مرتبط کمک کنند.

در طول این تحقیق، وزارتخانه های متبوع در حال سازماندهی گزینش در تخصص سایبری بودند. ما ضمن زیر سؤال بردن رویکرد مدیریت افسران سایبری، الزام نیاز به تمایز بیشتر در برخی مشاغل اداری را نیز تشخیص داده‌ایم. استدلال اصلی در مقابل ورود به نیروی ویژه سایبری، از تجزیه و تحلیل در مورد نیازهای مهارتی در پست‌های سایبری است. *به طور کلی مشاغل سایبری افسران در هنگام جذب، نیازمند سطحی خاص از مهارت‌های ویژه در ارتباطات-کامپیوتر، اطلاعات، مهندسی فناوری اطلاعات یا نیروی خبره سایبری می‌باشد.* در مجموع، این مهارت‌ها برای تشکیل یک نیرو ویژه سایبری جداگانه، بسیار نامتجانس و متعدد هستند. در عوض، پسوندها

در نیروی ویژه سایبری یا شناسه تجربیات خاص (به عنوان آخرین چاره) برای تمایز مهارت‌های سایبری مورد نیاز در این پست‌ها بیشتر مفید خواهد بود.

مشاغل ماموریتی سایبری نیز با سایر پست‌های سایبری متفاوت هستند. به عنوان مثال، دانش عملیات و چگونگی اجرای ماموریت‌های مرتبط با این مشاغل، آن‌ها را از عملیات شبکه و مشاغل مربوط به جنگ شبکه که نیازمند دانش تهدیدات سایبری، روش‌های هک و ابزارهای بهره‌برداری شبکه کامپیوتری هستند، جدا می‌کند.

با این حال، تخصص‌های ارزیابی شده در حال حاضر با یک پسوند متمایز *نیرو ویژه سایبری* مدیریت می‌شوند، و به نظر می‌رسد که استفاده از پسوند ارزیابی شده مناسب در تعریف پیشینه ارزیابی، می‌تواند مفید واقع شده و در پست های مرتبط با سایبر نیز استفاده شوند. در نتیجه، در صورت نیاز، استفاده از *شناسه تجربیات خاص* سایبری، سطح بیشتری از تمایز مهارت مورد نیاز برای مدیریت پرسنل ارزیابی شده را با مهارت‌های سایبری فراهم می‌آورد. برای کارکنان نظامی باید به این نکته توجه گردد که به جای مجموعه خاصی از مهارت‌های فنی، دید گسترده سایبری اهمیت ویژه‌ای خواهد داشت. نمونه‌هایی از چنین مشاغلی هم عبارتند از: کارکنان به عنوان مسئول توسعه مفهوم سازی سایبری، کارمندان فاوا در یک سازمان فضای سایبری.

سرمایه انسانی برای چنین شغل‌هایی می‌تواند از طریق ایجاد تخصص سایبری کمکی، توسعه یافته و مدیریت شود. برای جذب افسران در سطح ارشد یا سطوح عالی از یک تخصص سایبری کمکی، می‌بایست براساس تجربه سایبری قبلی که با اعطاء یک پسوند خاص یا پسوند ویژه متمایز گشته‌اند اقدام گردد.

ممکن است ساختار گزینش نیروی ویژه سایبری و روش‌های مدیریت فعلی نسبت به جذب متخصین ICT متمایل‌تر باشد. در یک برنامه مرحله ای، پرسنلی که در حوزه کاری جدید وارد می شوند، ابتدا آموزش بنیادین فن‌آوری اطلاعات و سایبری رادریافت نموده، سپس مهارت‌های اولیه آموزشی برای کسب تخصص در حوزه ارتباطات-کامپوتر سایبری به ایشان ارائه خواهد شد. این برنامه همچنین مدیریت *نیروی ویژه ناظر* را توسط کسب مهارت‌های عملیات سایبری و ارائه مجوز به برخی از کارکنان سیستم ارتباطات سیار، برای انتقال به اپراتور جنگ سایبری و نیروی ویژه جنگ الکترونیک در میدان اداره می کند. کارکنان از تخصص‌های دیگر مانند اطلاعات و یا هواپیمای جاسوسی می‌توانند به صورت افقی به تخصص‌های سایبری جدید انتقال یابند.

در تعیین کار به عنوان عملیات (کد۰۲)، سیگنال ها (۰۳)، شبکه (۰٤)، و بهره‌کشی (۰۵) میتوان از پسوندهای سایبری استفاده کرد تا بتوان تخصص و تجربه سایبری فزاینده را در زمینه کار اطلاعاتی ایجاد نمود.[۵۳] روش فعلی ممیزی مهارت‌ها برای کارکنان هواپیما و معرفی پسوندهای سایبر برای کارهای اطلاعاتی، شناسایی دقیق‌تر پرسنل را برای تغذیه در بخش جنگ ویژه سایبری فراهم می‌سازد.

## ۵. نتیجه گیری

همانطور که می‌دانیم به مؤلفه‌های قدرت نظامی و حیاتی یک کشور پس از ابعاد زمین، دریا، هوا و فضا، فضای سایبری نیز افزوده شده است.

با توجه به وضعیت کنونی فضای سایبری و توجه کمتر به اهمیت مسائل مدیریت سرمایه انسانی و ساختار سازی برای فضای‌سایبری، بر آن شدیم که با شناسایی و تحلیلی مناسب،

[۵۳] در ابتدا، ما یک پسوند رایج در میان این تخصص ها را توصیه می کنیم. به عنوان مفهوم بلوغ، تمایز بیشتر ممکن است لازم باشد. تعداد نهایی پسوندها باید توسط مفاهیم گروه‌بندی کاربردی و تخصص عملی ایجاد گردند.

اهمیت ایجاد یک سازمان در وزارتخانه های متبوع برای سازماندهی فضای سایبری را آشکار سازیم.

نظریه: ما باید در راهبرد ملی خود برای ایمن کردن فضای سایبری، سه هدف را دنبال کنیم؛ – این راهبرد می‌بایست توسط شخص اول هر کشوری ابلاغ و تا حصول نتیجه پیگیری گردد (با توجه به مشخص بودن علت آن از توضیح بیشتر پرهیز می کنیم).

- جلوگیری از حملات سایبری به زیرساخت‌های حیاتی جمهوری اسلامی ایران
- کاهش آسیب‌پذیری ملی در برابر حملات سایبری
- به حداقل رساندن آسیب و کاهش زمان بازیابی پس از وقوع حملات سایبری

با ظهور سازمانی که اصلاً برای عملیات فضای سایبری ایجاد گردیده، وزارت متبوع برای همسو کردن قوای لشکری و کشوری می‌بایست با ارائه‌ای منسجم، قابلیت‌های نیروهای سایبری را ابتدا برای فرماندهان راهبردی کشوری و لشکری داشته باشد. بنابراین، اهداف مورد نظر را اینگونه می توان عنوان کرد:

- جلوگیری یا ایجاد وقفه در حملات فضای سایبری علیه منافع حیاتی
- جلوگیری از شکست ازطریق واکنش سریع به حملات و بازسازی شبکه‌ها
- افزایش قدرت (توان افزایی) دفاع سایبری با یکپارچه سازی ظرفیت‌های موجود فضای سایبری
- دفاع فعال سایبری (اختلال در عملکرد سایبری دشمنان)
- در معرض خطر قرار دادن دشمنان
- تضمین در دسترس پذیری شبکه‌های نظامی و حیاتی ج.ا.ا[۵۴]
- آگاهی وضعیتی سایبری مستمر
- برای دستیابی به این اهداف، باید یکپارچگی عناصر لازم برای یک نبرد سایبری، مد نظر قرار گرفته و در صدد احصاء روش‌هایی برای طراحی مجدد جایگاه‌های شغلی موجود یا ایجاد زمینه‌های شغلی جدید از نیروی انسانی موجود باشیم.

مسئولیت‌های مدیریت عملکردی در حوزه ارتباطی و علوم کامپیوتر می‌تواند بر عهده‌ی دبیر کل معاونت راهبردی وزارت متبوع باشد، یا با ایجاد اداره‌کل تحول فضای سایبری[۵۵]، به عنوان وظایف اصلی ایشان تعریف گردد. این اداره برای **تأمین** نیروی لازم در راستای بکارگیری در حوزه سایبری، در درجه اول نسبت به شناسایی نیازهای آینده افسران و برطرف سازی این نیازها اقدام می‌نماید.

همچنین تأثیر ایجاد این قابلیت‌ها بر سایر مشاغل و سازمان‌های ذینفع و همکار از جمله وزارت فناوری اطلاعات، واحدهای اطلاعات عملیات ن.م، پلیس فتا، سازمان پدافند غیرعامل، افتا ریاست جمهوری، می‌بایست بررسی و مورد توجه قرار گیرد و تعریف پروژه‌ها برای ایجاد قابلیت‌های سایبری نوین با ملاحظه تأثیرات احصاء شده، تبیین گردد.

مدیرکل عملیات سایبری، مسئولیت مدیریت عملکردی بر حوزه کاری اطلاعات–عملیات را داشته و وظیفه‌ی چگونگی یکپارچگی الزامات مهارتی نیروی انتخاب شده و مدیریت افسران حائز شرایط اطلاعات–عملیات را برای بخش نیروی سایبری در حال ظهور بر عهده خواهد داشت. در واقع می توان انتخاب نیروهای آن بخش را به سازمان‌هایی که

[۵۴] سرمایه گذاری در بخش‌های نظامی، حتی چندین برابر ارزش واقعی سرمایه گذاری، می‌تواند تضمینی برای دردسترس پذیری باشد.

[۵۵] پیشنهاد اعضاء اداره کل تحول فضای سایبری: زمینه‌های کاری شامل تعدادی افسر متخصص ارتباطات: رادار زمینی؛ ارتباطات ماهواره‌ای/ وسیع/ تله متری/ هواشناسی/ تصویربرداری رادیویی و آفند؛ ارتباطات/شبکه/ سوئیچینگ و سیستم رمزنگاری؛ کابلی/ آنتن/ تلفن؛ مدیریت اطلاعات و ارتباطات – اپراتورها و برنامه نویسان کامپیوتر؛ اپراتور رادیو ؛ کنترل کننده‌های سیستم‌های کامپیوتری؛ و برنامه‌های کامپیوتری/ پیاده سازی.

به نوعی از ایجاد این قابلیت‌ها و تحولات تأثیر می‌پذیرند و یا تحت فشار قرار می‌گیرند(همان ذینفعان)، سپرد.

نباید سیاست مدیریت اداری – جذب، ارتقاء و تقویت درجه داران – تنها نباید بر افزایش مهارت و آگاهی نیروهای دولت برای ایجاد یک نیروی سایبری متمرکز باشد. بلکه می‌بایست نگاهی گسترده و راهبردی به عنوان متولی فضای سایبری در کشور داشته باشد. این مطالعه تحت‌تاثیر ارزیابی‌ها از نیازهای مختلف مطرح در این بخش می‌باشد. ما به این نتیجه رسیدیم که تجزیه و تحلیل باید:

۱- راهبردی باشد، شناسایی الزاماتی سرمایه انسانی که کشور در مواجهه با فضای سایبری با آن روبرو خواهد شد؛ (برای مثال حفظ و ارتقاء سرمایه انسانی فرا سازمانی)

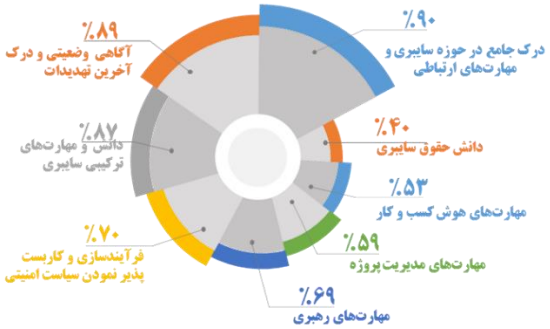
۲- جامع باشد، با در نظر گرفتن الزامات نیازهای سرمایه انسانی در مواجهه با قابلیت‌های سایبری نیروها و احتمالا سایر شرکت‌ها و سازمان ها؛ (مثال: ارائه حقوق بیشتر به کارکنان سازمان مطبوع و مهاجرت کارکنان به یک کشور دیگر)

ارائه چشم اندازی برای تبیین مؤثر سیاست‌های توسعه و مدیریت سرمایه انسانی (با مطالعه میدانی به تولید اسناد پشتیبان پرداخته شود تا سیاست‌هایی که می تواند ایجاد تحول نماید را به درستی تبیین شود)

### ۵-۱. موتور توانمندساز منابع انسانی سایبری

در موتور توانمندساز معرفی شده که در هسته چارچوب پیشنهادی قرار گرفته است، منابع انسانی بالقوه که دارای مشاغل ترکیبی سایبری در حوزه‌های کاری هستند شناسایی و با ورود به موتور، کسب مهارت‌های اشاره شده در شکل زیر برای آن‌ها محرز شده، همچنین به ایشان آموزش لازم در خصوص خود توانمندسازی ارائه می‌گردد.

پس از طی شدن مرحله گذار کارکشتگان سایبری در جایگاه خود بکارگیری خواهند شد.




**شکل ۸. مهارت‌های پراهمیت در حوزه سایبری**

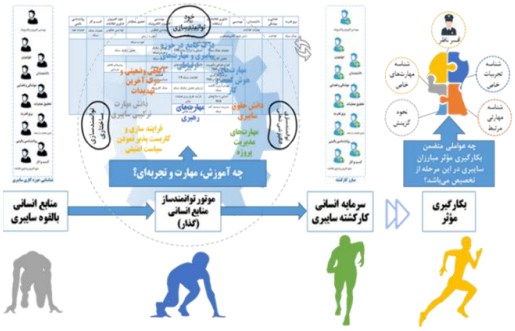
این موتور همچون هر سیستم پویای دیگر نیازمند چرخه‌ی بهبود مستمر بوده و نتیجه‌ی بهبود مستمر، ارتقاء و بهینه‌سازی آن خواهد بود. بنابراین در نسخه‌های ارتقاء یافته بعدی می‌توان فرآیند بازخورد را از سطح افسر ناظر به داخل موتور بسط داد.

### ۵-۲. پاسخ ما به پرسش‌های تحقیق بدین شرح است:

سوال اصلی:

**چارچوب توانمندسازی سرمایه انسانی در دفاع سایبری کدام است؟**

چارچوبی که ضمن توجه به مسائل عمومی توانمندسازی به مسائل عالی و سطوح دانشی و مهارتی نیروی سایبری توجه داشته باشد (مطابق شکل ۹).




**شکل ۹ مدل مفهومی توانمندسازی سرمایه انسانی سایبری**

سوالات فرعی:

**ابعاد و مولفه های توانمندسازی کدامند؟**

توجه به بستر و هسته‌ی تخصصی توانمندساز

**نقش و اثرگذاری منابع انسانی در دفاع سایبری چیست؟**

شالوده اصلی در ایجاد، استقرار و پشتیبانی دفاعی-امنیتی فضای سایبر، سرمایه کارکشته سایبری است.

**چگونه می‌توان با توانمندسازی کارکنان و ایجاد سازمان یادگیرنده، به دفاع موثرتر در عرصه سایبری جامه عمل پوشاند؟**

ایجاد سازمان سایبری و ساختار هدایت و کنترل متمرکز سایبری در کشور – راهبرد متمرکز با نگاشت توزیع شده –

## ٦. مراجع


[1] Fang, B. (2018). Cyberspace Sovereignty Reflections on building a community of common future in cyberspace. Science Press and Springer Nature Singapore Pte Ltd.

[2]Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime science, 7(1), 1-15.

[3] Aggarwal, P., Gutierrez, M., Kiekintveld, C. D., Bošanský, B., & Gonzalez, C. (2021). Evaluating Adaptive Deception Strategies for Cyber Defense with Human Adversaries. Game Theory and Machine Learning for Cyber Security, 77-96.

[4]Erickson, J. M. (2020). The Cyber Defense Review. The Cyber Defense Review, 5(3), 9-12.

[5]Mohtarami, A. (2017). Investigating the relationship between information technology and innovation capability of economies: towards a virtual national innovation system. International Journal of Technological Learning, Innovation and Development, 9(3), 230-249.

[6]Empowerment, W. E. (2018). A review of literature on the associations among employee empowerment, work engagement and employee performance. Modern Applied Science, 12(11), 313-329.

[7] Judge, T. A., & Robbins, S. P. (2017). Organizational behavior. Pearson.

[8] Healey, J., & Korn, E. B. (2019). Defense Support to the Private Sector: New Concepts for the DoD's National Cyber Defense Mission. Cyber Defense Review, 227.

[9]Furnell, S., & Bishop, M. (2020). Addressing cyber security skills: the spectrum, not the silo. Computer fraud & security, 2020(2), 6-11.

[10] Bastian, N. D., Lunday, B. J., Fisher, C. B., & Hall, A. O. (2020). Models and methods for workforce planning under uncertainty: Optimizing US Army cyber branch readiness and manning. Omega, 92, 102171.

[11] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.

[12] Vu, H. M. (2020). Employee empowerment and empowering leadership: A literature review.