

متغیرهای کلیدی منابع انسانی در تقویت دفاع سایبری جمهوری اسلامی ایران

حمید یزدانیان^۱

غلامرضا جلالی فراهانی^۲

تاریخ دریافت: ۱۳۹۵/۱۲/۱۶

تاریخ پذیرش: ۱۳۹۶/۰۳/۱۶

چکیده:

این پژوهش با هدف تبیین متغیرهای کلیدی منابع انسانی در تقویت دفاع سایبری کشور انجام گرفته است. نمونه تحقیق شامل ۴۰ نفر از نخبگان و دانشجویان کارشناسی، ارشد و دکتری مرتبط با سایبراست که از طریق نمونه‌گیری هدفمند انتخاب گردیده‌اند. نتایج یافته‌های این پژوهش نشان می‌دهد که متغیرهای کلیدی عوامل خارجی تهدیدات منابع انسانی با پارامترهای: «عدم هماهنگی و انسجام نیروهای انسانی واحدهای مختلف دفاع سایبری، نفوذ عوامل سرویس اطلاعاتی در سیستم نیروهای انسانی خودی» و فرصت‌های منابع انسانی با پارامترهای: «طراحی نظام جامع آموزش، توانمندسازی و تربیت منابع انسانی، امکان فعال‌سازی منابع انسانی جوان و با انگیزه برای حضور در دفاع سایبری» بیشترین تأثیرات را دارند.

کلیدواژه‌ها: دفاع سایبر، راهبردها، فرصت‌ها و تهدیدات سایبری، منابع انسانی.

۱- دانش‌آموخته دوره دکتری امنیت ملی دانشگاه عالی دفاع ملی و نویسنده مسئول

۲- استادیار دانشگاه عالی دفاع ملی

مقدمه:

امروزه استفاده از سازوکارهای علمی و بهره‌مندی از فناوری‌های روز به‌عنوان ابزار قدرت برتر، یکی از ارکان اصلی مأموریت‌ها در حوزه‌ی مسائل دفاعی و امنیتی می‌باشد. فناوری سایبری نیز که به عقیده‌ی بسیاری پس از زمین، دریا، هوا و جو خارجی زمین پنجمین حوزه‌ی فعالیت‌های بشری محسوب می‌شود؛ با ویژگی‌های در دسترس‌پذیری، هوشمندی و نوآوری، فراگیرندگی و تأثیرگذاری و نیز انعطاف‌پذیری همزمان با پیچیدگی، تنوع و تحولات سریع پدیده‌ها، در بسیاری از موضوعات بشر مانند پزشکی و سلامت و مراقبت، محافظت و خودکنترلی، ارتباطات، جلوه‌های هنری، محاسبه و پردازش، پیش‌بینی و شبیه‌سازی، آینده‌نگری و رفتارسازی ظهور نموده و با تغییر الگوهای اثرگذار فرهنگی، اجتماعی، سیاسی، اخلاقی، اقتصادی، علمی، ورزشی و بازی پاسخگوی بسیاری از نیازمندی‌های او در این عصر با درنوردیدن ابعاد زمان و مکان گردیده و واقعیت‌های مجازی و تخیلات را با افزایش سرعت، دقت و کاهش هزینه، عینیت بخشیده است. این قدرت گسترده‌ی دستاوردهای فناوری سایبر با چنین عمقی از رسوخ و درنوردیدن حاکمیت حکومت‌های منطقه‌ای و واحدهای سیاسی، می‌تواند حتی در مرزهایی که این فناوری فراگیر نشده باشد، باعث ایجاد فرصت‌ها و تهدیداتی باشد. در این راستا یکی از مؤثرترین عوامل برنامه‌ریزی راهبردی در مدیریت فرصت‌ها و تهدیدات این فناوری، مدیریت منابع انسانی است که به‌عنوان سرمایه‌ای با دستاورد فناوری شبیه‌ساز خود، کسب بالاترین درجه‌ی انطباق‌پذیری را مدنظر قرار داده و با رویکرد یکپارچه‌سازی در تجهیز و تأمین نیرو در شرایط ناپایدار و متغیر ساختار فضای سایبر، سعی در افزایش ضریب استحکام بخشی عوامل خارجی در این هم‌آوردسازی را دارد. بنابراین، فضای سایبر، امکانات و ظرفیت‌هایی را در اختیار مخاطبان قرار می‌دهد که به قدرتمند شدن مخاطب در کنترل افراد، تأثیرگذاری، نقش‌آفرینی، ایجاد تشویش و بی‌نظمی، ایجاد اغتشاش و ناامنی در سطح جامعه کمک می‌کند. از آنجائیکه موضوعات دفاعی و تهدیدات مترصد بر آن، محدود به مراکز ثقل نظامی نیست و عرصه‌های مختلف ملی را با سلطه‌ی اطلاعاتی در حوزه‌های تصمیم‌گیری و شناختی فرماندهی در برمی‌گیرد و نیازمند راهبردهای دفاعی و تقابلی متناسب، هم‌راستا، هم‌زمان و هماهنگ با آهنگی تعریف‌شده در یک دکترین و نظام جامع دفاعی با راهبرد توسعه‌ی همگرا در مرکز فرماندهی فناوری در حوزه‌های تصمیم‌گیری و شناختی را می‌باشد تا با پایش و محاسبه‌ی برخط برآیند نقاط اثر؛ نشانگر جهت و مقدار تهدید و فرصت را در چرخش‌های بهنگام مطلوب هم‌سوی حوزه‌های متأثر توازن قدرت، نمودار و رهنمون سازد.

عناصر و مؤلفه‌های گوناگون این نظام جامع دفاعی، نیز مشخصه‌هایی با همان ماهیت فناوری را می‌طلبد. در رأس هر فناوری؛ نیروی انسانی خلاق و مولد، موجب ظهور عرصه‌ی فناوری است. در این راستا، مدیریت منابع انسانی فناور از جایگاه و اهمیت خاصی برخوردار است که فناوری فضای سایبر نیز با پتانسیل توسعه‌ی ابعاد ناشناخته‌ی آن، از این قاعده مستثنی نیست. طبیعت و ماهیت این مدیریت مستلزم همکاری بسیار نزدیک آن با سایر مدیران و سرپرستان و کلیه‌ی کسانی است که مسئولیت نظارت و کنترل و ایجاد هماهنگی تعدادی از نیروهای انسانی را به عهده دارند (یعقوبی، ۱۳۸۰: ۲۱) و بخش دفاع سایبر نقش ویژه‌ای در تربیت نیروی انسانی متخصص و حرفه‌ای دفاع سایبری و نیز هدایت سیستم عظیمی به نام شبکه‌های دفاع سایبری در حوزه‌های گوناگون را برعهده دارد. بدین ترتیب کمیت و کیفیت نیروی انسانی این سیستم بر سرعت ارائه‌ی خدمات، هزینه و دقت صرف شده و به‌طورکلی کیفیت انجام وظایف دفاع سایبری تأثیر شگرفی دارد؛ پس هدایت این منابع انسانی متناسب با تغییر و تحولات محیط درون و برون در بخش دفاع سایبری، امری ضروری است و در حوزه‌ی دفاع سایبری نیز تا حدودی متفاوت از سایر حوزه‌ها خواهد بود و راهبردهای نشان، جذب، بکارگیری، ارزیابی، ارتقاء، نظارت و کنترل این منابع انسانی نیز به‌طور طبیعی تفاوت‌هایی با سایر حوزه‌ها خواهد داشت. بنابراین پژوهش حاضر با ادعان به موارد فوق با هدف شناسایی متغیرهای کلیدی و تاثیرگذار خارجی (تهدیدات و فرصت‌ها) منابع انسانی در تقویت دفاع سایبر کشور به رشته تحریر درآمده است.

مبانی نظری و پیشینه‌شناسی تحقیق

منابع انسانی در دفاع سایبری

با توجه به پیچیدگی‌ها و تنوع فعالیت‌ها در بخش دفاع سایبری، استفاده از کارکنانی با ویژگی‌های کارکنان قرن ۲۱ ضروری است. ورزشکار در وب‌سایت مدیریتی ایران تفاوت‌هایی بین کارکنان در قرن ۲۰ و ۲۱ قائل است و می‌نویسد کارکنان در قرن بیستم مهم‌ترین و در واقع بی‌نظیرترین کمک و حسن تأثیر مدیریت، پنجاه برابر شدن بهره‌وری کارگران و کارمندان یدی در تولید صنعتی یا خدماتی بوده است. در حالی که در قرن ۲۱ مهم‌ترین سهم و نقش مدیریت، افزایش بهره‌وری کارکنان علمی و کارهای علمی است. در گذشته ارزشمندترین دارایی‌ها، تجهیزات تولید بوده‌اند ولی اکنون ارزشمندترین دارایی، کارکنان علمی آن نهاد و بهره‌وری کارکنان علمی است. در قرن ۲۰ کارکنان مدیریت‌شونده، بوده‌اند ولی امروزه کارکنان یک نیروی دانشگر، مالک دانش خود و

۱۳۰ فصلنامه امنیت ملی، سال هفتم، شماره بیست و ششم، زمستان ۱۳۹۶

مدیریت‌کننده می‌باشند؛ در گذشته فرض بر این بوده که عمر سازمان‌ها از عمر کارکنان طولانی‌تر است ولی اکنون فرض بر این است که عمر انسان از عمر سازمان بیشتر است. در قرن ۲۰ کارکنان در یک جا ثابت می‌مانند ولی اکنون تحرک و جابجایی کارکنان زیاد است.

بنا به گفته پیتتر دراکر^۱، تبدیل کارکنان سنتی و یدی به کارکنان علمی در قرن بیست‌ویکم، ضرورت پایایی و پویا نمودن جوامع محسوب می‌شود که این مهم بایستی در منابع انسانی دفاع سایبری نیز مدنظر قرار گیرد. انعطاف‌پذیری و سازوکاری ساختار و کارکنان با محیط و جامع‌نگری و تصمیم‌سازی از ویژگی‌های کارکنان مدیریت‌کننده در دفاع سایبر می‌توان ذکر کرد (کارگاه گروه مطالعاتی شهید صیاد شیرازی، ۹۳/۱/۲۱).

برخی معتقدند که خود کارکنان قادرند وظایف مدیریت را نیز انجام دهند و به واحد مدیریت جدا و مستقل نیاز ندارند، ولی هنوز مورخین و جامعه‌شناسان، نهادی را نیافته‌اند که بدون داشتن سلسله‌مراتب اداری پایدار مانده باشد (گلوئیک، ۱۹۷۷: ۷). به‌علاوه بسیاری از صاحب‌نظران، موفقیت و شکست نهادها را ناشی از تفاوت در نحوه مدیریت آن‌ها می‌دانند. به اعتقاد پیتتر دراکر، عضو اصلی و حیات بخش هر سازمان، مدیریت آن است (دراکر، ۱۹۷۴: ۳۵۴-۳۵۱). هرولد کونتز، مدیریت را مهم‌ترین زمینه‌فعالیتی انسان می‌داند و معتقد است که وظیفه اصلی مدیران در همه سطوح و همه نهادهای اجتماعی این است که محیطی را طراحی، ایجاد و نگهداری کنند که اعضای سازمان بتوانند با فعالیت و همکاری گروهی در آن، به اهداف معین خود دست یابند (کونتز و همکاران، ۱۹۸۸: ۴).

در آژانس تحقیقات پیشرفته‌ی دفاعی آمریکا، ستاد فنی در آژانس برای یک دوره‌ی ۴ تا ۶ ساله بکارگرفته می‌شود. ^۲DARP مانند هر سازمان قدرتمندی سعی می‌کند تجربه و تغییر را در هم آمیزد. این ستاد دائماً بین افراد در چرخش است. این چرخش تضمین می‌کند که اولاً چشم‌اندازها و ایده‌های نو همیشه وجود داشته باشد و ثانیاً جای خالی برای به خدمت گرفتن افراد فنی از فضاهاى نو در سازمان ایجاد شود. همچنین برای مدیران برنامه‌ها محیطی فراهم می‌شود که در آن از شکست نهراسند و دست به اقدامات مهم و جسورانه بزنند (فروغی و همکاران، ۱۳۹۰).

همچنان‌که سازماندهی نیروهای متخصص برای فعالیت در سطوح بالای تکنولوژی حوزه‌ی سایبر یک فرصت محسوب می‌شود، با این حال بکارگیری نیروی متخصص این حوزه در طرح‌ریزی

^۱ - pitter draker

^۲ - Defence Advance Research Project Agency

حملات جدیدتر و غیرقابل کنترل تر یک تهدید بالقوه به شمار می‌رود.

در حوزه‌ی برنامه‌ریزی منابع انسانی، انجام اقدامات زیر ضروری است:

- ۱- برآورد نیروی انسانی موجود (تجزیه و تحلیل وضعیت موجود نیروی انسانی)؛
 - ۲- پیش‌بینی نیاز به نیروی انسانی؛
 - ۳- مقایسه بین نیروهای انسانی موجود و مورد نیاز که به تعیین کمبود یا مازاد نیروی انسانی و یا تعادل عرضه و تقاضای نیروی انسانی می‌انجامد؛
 - ۴- تعیین هدف‌ها و خط‌مشی‌ها در مورد کمیت و کیفیت نیروی انسانی؛
 - ۵- تنظیم برنامه‌های اجرایی (برنامه‌های گزینش، استخدام، بکارگماری، جابجائی، آموزش و بهسازی)؛
 - ۶- کنترل و ارزیابی به‌منظور تعیین میزان تحقق هدف‌های برنامه‌های نیروی انسانی و مشخص کردن نقاط قوت و ضعف برنامه‌ها؛
- در موضوع آموزش کارکنان بخش‌های دفاع سایبر نیز به ۵ نوع آموزش اشاره می‌گردد که عبارتند از:
- ۱- آموزش مستمر ضمنی؛ ۲- آموزش رسمی؛ ۳- آموزش غیررسمی؛ ۴- آموزش مداوم؛ ۵- آموزش ضمن خدمت
- که به نظر می‌رسد همه این ۵ نوع برای کارکنان بخش‌های دفاع سایبری ضروری است؛ ولی این‌که هر طیفی از کارکنان دفاع سایبری به چه نوع آموزشی بیشتر نیاز دارند در قالب سوالات پرسشنامه قابل دریافت است.
- انعطاف ساختاری منابع انسانی در دفاع سایبر برای تامین، حفظ و نگهداشت سرمایه‌های انسانی ضروری است. شناور کردن ساعات کار و روزهای کار هفته (شیفت‌کاری قابل انعطاف)، شناور کردن مسیر شغلی، چندمهارته کردن افراد، گردش شغلی، غنای شغلی، توسعه شغلی، حقوق و مزایای قابل انعطاف، مشارکت دو یا چند نفر در یک شغل، اشتغال از راه دور (دورکاری)، رهبری اقتضایی (برحسب شرایط) در بکارگیری منابع انسانی دفاع سایبری مورد تأکید است. سیستم جریان خدمت قابل انعطاف به‌وسیله پرداخت براساس تعداد مهارت، پرداخت برحسب پاداش گروهی، پرداخت برحسب سطح دانش، پرداخت برحسب مزایای کیفیت فراگیر، پرداخت برحسب مبنای ارزش مقایسه‌ای، ایجاد محیط کار بهداشتی و حفاظت صنعتی برای کیفیت زندگی کاری در نظام نگهداری منابع انسانی مورد تأکید است (میرسپاسی، ۱۳۸۹: ۷). برهمین اساس، سازمان تشکیل شده در حوزه‌ی دفاع سایبری نیز، باید سازمان دانش‌محور باشد که در چنین

سازمانی تجربه‌های افراد سازمان، گزارش‌ها، بانک‌های اطلاعاتی و پرونده‌ها مورد استفاده قرار می‌گیرد. نیروهای تربیت‌شده و دارای انگیزه‌ی خوب را با یک مجموعه درست از مهارت‌ها، تجربه و دانش ارتقاء می‌دهند. اطلاعات و دانش در اختیار نیروی کار بوده و به‌طور خلاصه می‌توان گفت که تفکر "دانش به منزله قدرت است" بر چنین سازمان‌هایی حکم فرماست. همچنین سازمان‌ها در حوزه دفاع سایبری باید یادگیرنده به‌منزله سازمانی که در آن خلق، اکتساب و انتقال دانش و در تعدیل رفتارش در جهت انعکاس دانش و بینش جدید مهارت دارد، باشند (Garvin, 1993:80). در تعریف سیستماتیک، یک سازمان یادگیرنده سازمانی است که با قدرت و به‌صورت جمعی یاد می‌گیرد و دائماً خودش را به نحوی تغییر می‌دهد که بتواند با هدف موفقیت مجموعه سازمانی به نحو بهتری اطلاعات را جمع‌آوری، مدیریت و استفاده کند (Marquardt, 1995:19). همچنین واژه سازمان‌های یادگیرنده، به ظرفیت یادگیری سازمان از تجربیات گذشته اشاره دارد که دارای ویژگی‌های زیر می‌باشد:

- ۱- دانش و تخصص کارکنان خود را به‌روز می‌کند؛
- ۲- دوره‌های آموزشی برگزار کند؛
- ۳- با مراکز آموزش عالی و دانشگاه‌ها ارتباط دارد. در نتیجه سبب ارتقاء دانش کارکنان خود برای بررسی و حل مسائل پیش‌آمده در روند کاری می‌شود؛
- ۴- سازمان‌هایی که در آن افراد به‌صورت مستمر، ظرفیت‌های خود را برای خلق نتایج مطلوب به‌کار می‌گیرند؛
- ۵- سازمان‌هایی که الگوهای جدید تفکر را پرورش می‌دهند؛
- ۶- سازمان‌هایی که بیان آرزوها و آرمان‌های جمعی برای افراد آزاد است؛
- ۷- سازمان‌هایی که یاد گرفتن با یکدیگر را به‌صورت جمعی، مستمر و بلندمدت تشویق می‌کند (نانسی دیکسون، ۱۹۹۴).

عوامل انسانی موثر در تقویت دفاع سایبری کشور

به‌طور مشخص در زمینه‌ی فرصت‌ها و تهدیدات منابع انسانی در حوزه دفاع سایبری، تحقیق خاصی صورت نگرفته است، لذا برای تکمیل این بحث با برخی متخصصین این حوزه مصاحبه شده و برخی از نکات مطرح شده به شرح ذیل می‌باشد:

وجود بسترهای جلب همکاری منابع انسانی با سرویس‌های اطلاعاتی بیگانه، تغییر تدریجی هنجارها و ارزش‌های اساسی منابع انسانی، رشد ناهماهنگ دانش دفاعی منابع انسانی با تهدیدات

توسعه‌ی سایبری در سطوح مختلف، چالش‌های ناشی از آموزش و پژوهش مبتنی بر متون غربی، کمبود نیروی انسانی کیفی و نبود انگیزش کافی در میان نخبگان برای اشتغال اثربخش در این حوزه، تأخیر فاز دستیابی منابع انسانی به ابزار و نرم‌افزارهای دفاعی در برابر تهاجمات سایبری، نبود فرهنگ حفاظتی مناسب در اقشار مختلف، عدم هماهنگی و انسجام واحدهای مختلف دفاع سایبری، ناشناخته ماندن ارزش منابع انسانی ماهر در حوزه سایبری به علت پیچیدگی بالای فناوری‌های این حوزه، وجود دیدگاه منفی نسبت به متخصصین حرفه‌ای نفوذ و ارزیابی امنیتی در بین طیفی از مدیران، کمبود محتوای علمی و فناورانه در برنامه‌های آموزش کشور در حوزه سایبری و عدم تکافوی آموزش‌های کشور در ایجاد مهارت در جامعه از مهم‌ترین چالش‌های این بخش می‌باشد.

از سوی دیگر، امکان عضوگیری و به خدمت گرفتن منابع انسانی در سفرهای خارجی (دیپلماسی علمی، نمایندگانه‌ها و...)، عامل‌گیری منابع انسانی خودی توسط سرویس حریف، نفوذ به منظور دستیابی و افشای اطلاعات منابع انسانی توسط حریف، آثار تهاجم فرهنگی و جنگ نرم دشمن بر منابع انسانی، کانالیزه نمودن متخصصان دفاع سایبری به ارائه‌ی آخرین دستاوردهای علمی کشور در قالب مقالات آی.اس.آی، راهبرد دشمن مبنی بر تشویق و تسهیل مهاجرت نخبگان، فروش تجهیزات و سامانه‌های آلوده و ضدحفاظتی به سازمان دفاع سایبر خودی، آموزش‌ها و مرجع‌سازی‌های علمی غیربومی، ترویج قابلیت‌های شبکه‌های اجتماعی برای عضویت، نفوذ عوامل سرویس‌های اطلاعاتی در سیستم خودی از مهم‌ترین تهدیدات این حوزه می‌باشد (کارگاه گروه مطالعاتی شهید صیاد شیرازی، ۹۳/۱/۲۱).^۱

در تهدید نرم که هرگونه اقدام روانی و تبلیغات رسانه‌ای را دربرمی‌گیرد، نیروهای هدف نشانه گرفته می‌شوند و بدون درگیری به شکست وادار می‌شوند. برای دست‌یافتن به قدرت نرم و ایجاد فرصت سه سطح موردنظر قرار می‌گیرد. در سطح راهبردی، هدف افزایش قدرت هنجارسازی خود و تضعیف قدرت حریف در سطح بین‌المللی است. هدف حریف هم از تهدید نرم، شناسایی رهبران فکری و تأثیرگذاری در آنان است. در سطح میانی قدرت نرم که به مردم و قدرت ملی

۱ - با توجه به ضعف منابع مطالعاتی و پژوهشی بومی در حوزه دفاع سایبری، کارگروه موصوف با حضور جمعی از نخبگان این حوزه تشکیل و به روش طوفان مغزی، چالش‌ها، تهدیدات و فرصت‌های حوزه منابع انسانی دفاع سایبر استخراج گردید.

تکیه دارد، افکار عامه از تصمیمات رهبران جامعه حمایت و به آن مشروعیت می‌بخشد. هدف تهدید نرم نیز در این سطح، ایجاد شکاف میان نخبگان سیاسی و فرهنگی و آحاد عمومی جامعه و تبدیل جماعت همراه به مردمی بی‌تفاوت با ابزارهایی مانند تشویق به نافرمانی مدنی است. در سطح تاکتیکی، رویایی قدرت نرم در نیروهای مسلح صورت می‌گیرد. این سه سطح از قدرت نرم، باید همراه باهم مورد توجه قرار گیرد تا بتواند در مقابل تهدیدات نرم مؤثر واقع شود.

در تهدیدهای پایدار پیشرفته که یکی از جدی‌ترین تهدیدهای پنهانی، خطرناک و ماندگار در سازمان‌های حاوی اطلاعات حساس و مهم محسوب می‌شود، اطلاعات به‌صورت پنهانی و در طولانی مدت استخراج می‌شود. از آنجایی که هدف‌گیری افراد از سامانه‌ها آسان‌تر است، مهاجمان از مهندسی اجتماعی استفاده می‌کنند. اشخاص هم از اطلاعات برخوردارند و هم به اطلاعات دسترسی دارند (کافی، ۱۳۹۵).^۱

در بررسی انجام شده، عوامل تهدیدات انسانی عمدی و سهوی سایبری علیه آمریکا^۲ عبارتند از: تروریست‌ها، هکرها، نیروهای دشمن، کارمندان اخراجی، گروه‌های شاکی و سارقین و مخالفان سیاسی. دفاع در برابر مهندسی اجتماعی، به‌عنوان بخشی از امنیت فضای سایبری مورد توجه قرار می‌گیرد. برخلاف باور مردم که بیشترین آسیب‌پذیری در سیستم‌های اطلاعاتی را در حوزه نرم‌افزار می‌دانند، این عامل انسانی است که بیشترین میزان ریسک را دارد (پاوکوویچ و همکاران، ۲۰۱۱). در شبکه‌های اجتماعی نیز با ترفندهای روان‌شناسانه و بهره‌برداری از نیاز انسان‌ها، به اعتمادسازی کاذب در سطح وسیعی ترغیب و به کسب اطلاعات و تغییر عادات مبادرت می‌ورزند. در کشورهای آمریکا و اسرائیل، در برخی رده‌های لشکری عضویت در این شبکه‌ها ممنوع شده و در سایر رده‌ها با اسامی غیرواقعی و بدون اشاره به نوع و محل خدمت مجاز است (ویشه، ۱۳۹۰).

در برابر تهدیدهای موجود در حوزه منابع انسانی دفاع سایبری، فرصت‌هایی نیز برای جمهوری اسلامی ایران در این عرصه وجود دارد که برخی از مهم‌ترین آن‌ها بر اساس مصاحبه با نخبگان عبارت است از: امکان فعال‌سازی منابع انسانی جوان و باانگیزه برای حضور در دفاع سایبری با توجه به جذابیت‌های آن، آسیب‌پذیری منابع انسانی حوزه سایبری حریف و افزایش ضربه‌پذیری آن، امکان آموزش فعالان اپوزیسیونی حوزه سایبری حریف توسط منابع انسانی خودی، امکان بهره‌گیری از آموزش‌های حریف در فضای مجازی و بازتولید آموزش‌های تقابلی و

۱ - عضو هیئت‌علمی دانشگاه جامع امام حسین(ع)

۲ - <http://uscyberlabs.com>

پدافندی، امکان ایجاد امواج سایبری (بمباران گوگلی و...) توسط منابع انسانی خودی در راستای منافع ملی، تسهیل در ارتباطات و کسب اخبار حوزه‌ی دفاع سایبری به دلیل گسترش فناوری اطلاعات (کارگروه مطالعاتی شهید صیاد شیرازی، ۱۳۹۳/۰۱/۲۱). همچنین آموزش مستمر و به‌روزرسانی این آموزش‌ها، تأیید صلاحیت و شناخت سابقه به همراه نظارت پیگیر از عوامل فرصت‌ساز نیروی انسانی به‌شمار می‌آیند.

هم‌اکنون، ارتباطات فردبه‌فرد وب‌محور که علاوه‌بر مخاطبین خاص به تفاوت‌ها، علایق و ویژگی‌های فردی نیز تأکید می‌کند، روش‌های سنتی فعالیت‌های رسانه‌ای را به چالش کشیده است. ارتباطات رسانه‌ای برخط افراد سازماندهی‌شده و نیروهای متخصص با هدف آگاهی‌رسانی داخلی و بین‌المللی، سبب ایجاد قدرت توزیعی دیپلماسی در راستای تبدیل تهدید عامل انسانی به فرصت و دستیابی به اهداف دیپلماسی عمومی کشور می‌گردد.

با توجه به تهدیدات و فرصت‌های شناسایی شده در حوزه منابع انسانی دفاع سایبری برخی پارامترهای راهبردی عبارتند از: طراحی نظام جامع آموزش، توانمندسازی و تربیت منابع انسانی، طراحی و عملیاتی‌سازی نظام جامع منابع انسانی، ارتقاء و نهادینه‌سازی فرهنگ حفاظتی، درونی‌سازی ظرفیت‌های منابع انسانی، طراحی و پیاده‌سازی نظام انگیزشی منابع انسانی، هوشمندسازی سامانه‌های نظارتی و امنیتی، طراحی نظام جذب و ارتقای بومی اساتید، تهاجم سایبری توأمان با رعایت اولویت‌های دفاع سایبری (کارگروه مطالعاتی شهید صیاد شیرازی، ۱۳۹۳/۰۱/۲۱).^۱

روش‌شناسی تحقیق

تحقیق حاضر کاربردی، توسعه‌ای بوده که با بهره‌گیری از روش ترکیبی (سه بعدی) با استفاده از روش‌های کمی و کیفی و ترکیب آن و روش هدفمند جهت جمع‌آوری اطلاعات از نخبگان در حوزه سایبری و روش اکتشافی در مراجعه به اسناد و مدارک استفاده شده است. در تبیین متغیرهای کلیدی، با توجه به اهمیت موضوع، عوامل خارجی موثر، صرفاً به عوامل خارجی پرداخته شده و برای تبیین عوامل داخلی مشتمل بر ضعف‌ها و قوت‌های نظام در این عرصه، نیاز به پژوهش‌های دیگری می‌باشد. بر این اساس در این تحقیق سعی شده است علاوه‌بر تصویرسازی درست از فضای سایبر و بیان رابطه‌ی آن با فضای واقعی (منابع انسانی) به تشریح و تبیین مرزها

^۱ به دلیل گستردگی موضوع، عوامل داخلی مؤثر مشتمل بر ضعف‌ها و قوت‌های منابع انسانی در حوزه دفاع سایبری در این پژوهش مورد بررسی قرار نگرفته و نیازمند پژوهش مستقل دیگری می‌باشد.

۱۳۶ فصلنامه امنیت ملی، سال هفتم، شماره بیست و ششم، زمستان ۱۳۹۶

در این فضا پرداخته و چگونگی و اهداف استفاده از این مرزها در دفاع سایبری بیان شود. در این راستا برای تبیین مرزهای سایبری سعی گردید با تکیه بر استدلال‌ها و نظراتی که از سوی صاحب‌نظران مختلف منابع انسانی در این زمینه ارائه شده است، به تجزیه و تحلیل داده‌ها پرداخته و براساس این داده‌ها، نتیجه‌گیری صورت گیرد. لازم به ذکر است در این تحقیق، برای گردآوری داده‌ها از پرسشنامه، اطلاعات اسنادی و اینترنتی استفاده شده است.

همچنین جامعه‌ی آماری موردنظر این پژوهش، اعضای خبرگی گروه مطالعاتی شهید صیاد شیرازی اعم از اساتید و دانشجویان، اساتید و دانشجویان دانشگاه عالی دفاع ملی، مدیران و کارشناسان ارشد و عالی اداره کل فضای مجازی در معاونت فنی وزارت اطلاعات، شورای عالی فضای مجازی کشور، گروه مدیریت راهبردی و منابع انسانی مرکز تحقیقات راهبردی دفاعی ستادکل نیروهای مسلح و مدیران امنیتی وزارت کشور بوده‌اند. این پژوهش با استفاده از دیدگاه نخبگان صاحب‌نظر که از ویژگی‌های جامعه آماری برخوردار بودند، به روش غیرتصادفی و اشباع هدفمند و با حجم محدود ۴۰ نفر، به‌عنوان جامعه‌ی خبرگی اجرا شده است.

در این پژوهش برای بررسی روایی و پایایی تحقیق نیز از آلفای کرونباخ استفاده شد که ضریب آلفای کرونباخ برای تهدیدات ۰/۸۰ و برای فرصت‌ها، ۰/۸۴ محاسبه گردید.

تجزیه و تحلیل و یافته‌های تحقیق

جدول ۱. اهمیت تهدیدات منابع انسانی دفاع سایبر

ردیف	درجه اهمیت هر سوال از صد درصد									تهدیدات منابع انسانی دفاع سایبر
	۱	۲	۳	۴	۵	۶	۷	۸	۹	
۱	۲۳	*	*	*	۶۸	۱۵۹	۶۸	۶۸	۶۸	نفوذ عوامل سرویس‌های اطلاعاتی در سیستم خودی
۲	۲۳	*	*	*	۴۵	۱۱۴	۹۱	۱۸۲	۵۴۵	عامل‌گیری منابع انسانی خودی توسط سرویس حریف
۳	۲۳	*	۶۸	۲۳	۹۱	۱۵۹	۹۱	۱۳۶	۴۰۹	نفوذ به منظور دستیابی و افشای اطلاعات منابع انسانی توسط حریف
۴	*	*	*	*	۱۱۴	۲۳	۱۸۲	۳۱۸	۳۶۴	آثار تهاجم فرهنگی و جنگ‌نرم دشمن بر منابع انسانی
۵	۲۳	۲۳	۶۸	۶۸	۲۳	۲۳	۲۹۵	۲۵	۲۲۷	کانالیزه نمودن متخصصان دفاع سایبری به ارائه‌ی آخرین دستاوردهای علمی کشور در قالب مقالات ISI
۶	۲۳	۲۳	۶۸	۶۸	۴۵	۱۱۴	۱۳۶	۱۸۲	۳۴۱	راهبرد دشمن مبنی بر تشویق و تسهیل مهاجرت نخبگان
۷	*	*	*	۲۳	۱۵۹	۶۸	۱۱۴	۲۷۳	۳۶۴	فروش تجهیزات و سامانه‌های آلوده و

متغیرهای کلیدی منابع انسانی در تقویت دفاع سایبری جمهوری اسلامی ایران ♦ ۱۳۷

ردیف	تهدیدات منابع انسانی دفاع سایبر	درجه اهمیت هر سوال از صد درصد								
		۱	۲	۳	۴	۵	۶	۷	۸	۹
	ضدحفاظتی به سازمان دفاع سایبر خودی									
۸	آموزش‌ها و مرجع‌سازی‌های علمی غیربومی	۷۵.۳	۲.۳	*	۲.۳	۶.۸	۱۸.۲	۴.۵	۲۹.۵	۱۳.۶
۹	ترویج قابلیت‌های شبکه‌های اجتماعی برای عضویت	۷۴.۲	۶.۸	*	۲.۳	۶.۸	۱۳.۶	۱۱.۴	۱۵.۹	۱۵.۹
۱۰	امکان عضوگیری و به خدمت گرفتن منابع انسانی در سفرهای خارجی	۷۶.۸	۲.۳	۲.۳	۹.۱	۴.۵	۶.۸	۴.۵	۱۳.۶	۲۹.۵
۱۱	عدم هماهنگی و انسجام واحدهای مختلف دفاع سایبری	۸۸.۴	۲.۳	*	*	۲.۳	۴.۵	۱۱.۴	۱۸.۲	۲۲.۷
۱۲	رشد ناهماهنگ دانش دفاعی منابع انسانی با تهدیدات توسعه‌ی سایبری در سطوح مختلف	۷۹.۸	*	*	۲.۳	۶.۸	۴.۵	۱۸.۲	۲۰.۵	۲۰.۵
۸۱/۱						میانگین کل				

از مجموع میانگین (۸۱/۱ درصد) حداقل تعداد نخبگان (۷۴/۲ درصد) شاخص ترویج قابلیت‌های شبکه‌های اجتماعی برای عضویت را مهم‌ترین تهدید در زیرساخت‌های منابع انسانی دفاع سایبر تشخیص داده و در نقطه مقابل، بیشترین نخبگان (۹۰/۹ درصد) در تشخیص خود، نفوذ عوامل سرویس‌های اطلاعاتی در سیستم خودی و در حوزه زیرساخت‌های منابع انسانی دفاع سایبر کشور را مهم‌ترین تهدید در حوزه مزبور اعلام کرده‌اند.

جدول ۲. اهمیت فرصت‌های منابع انسانی دفاع سایبر

ردیف	فرصت‌های منابع انسانی دفاع سایبر	درجه اهمیت هر سوال از صد درصد									
		۱	۲	۳	۴	۵	۶	۷	۸	۹	
۱	امکان فعال‌سازی منابع انسانی جوان و بانگیزه برای حضور در دفاع سایبری با توجه به جذابیت‌های آن	۸۹.۴	*	*	۲.۳	*	۶.۸	۶.۸	۱۸.۲	۲۷.۳	۳۸.۶
۲	آسیب‌پذیری منابع انسانی حوزه‌ی سایبری حریف و افزایش ضربه‌پذیری آن	۷۹.۳	۴.۵	*	۴.۵	۲.۳	۱۳.۶	۴.۵	۱۱.۴	۲۵	۳۴.۱
۳	امکان آموزش فعالان اپوزیسیونی حوزه‌ی سایبری حریف توسط منابع انسانی خودی	۷۹	۲.۳	*	۲.۳	۶.۸	۱۱.۴	۹.۱	۱۸.۲	۱۵.۹	۳۴.۱
۴	امکان بهره‌گیری از آموزش‌های حریف در فضای مجازی و بازتولید آموزش‌های تقابلی و پدافندی	۸۰.۳	۲.۳	*	۲.۳	۴.۵	۱۳.۶	۲.۳	۲۰.۵	۲۲.۷	۳۱.۸

ردیف	درجه اهمیت هر سوال از صد درصد										فرصت های منابع انسانی دفاع سایر	میانگین
	۱	۲	۳	۴	۵	۶	۷	۸	۹	میانگین		
۵	۷۴	۲۳	۴۵	۹۱	۴۵	۹۱	۶۸	۱۵۹	۱۸۲	۲۹۵	امکان ایجاد امواج سایبری (بمباران گوگلی و...) توسط منابع انسانی خودی در راستای منافع ملی	۵
۶	۷۸	*	*	۹۱	*	۱۸۲	۲۳	۱۵۹	۲۵	۲۹۵	تسهیل در ارتباطات و کسب اخبار حوزه دفاع سایبری به دلیل گسترش فناوری اطلاعات	۶
۷	۹۲	*	*	*	*	۲۳	۶۸	۱۱۴	۱۱۴	۶۸۲	طراحی نظام جامع آموزش، توانمندسازی و تربیت منابع انسانی	۷
۸	۸۸	*	*	*	۲۳	۶۸	۶۸	۱۱۴	۲۲۷	۵۰	طراحی و عملیاتی سازی نظام جامع منابع انسانی	۸
۹	۸۶	*	*	*	*	۲۳	۱۱۴	۱۳۶	۲۵	۴۷۷	ارتقاء و نهادینه سازی فرهنگ حفاظتی	۹
۱۰	۸۴	*	*	۲۳	۶۸	۲۳	۴۵	۱۵۹	۳۶۴	۳۱۸	درونی سازی ظرفیت های منابع انسانی	۱۰
۱۱	۸۰	۲۳	*	۲۳	۲۳	۶۸	۹۱	۲۲۷	۳۴۱	۲۰۵	طراحی و پیاده سازی نظام انگیزشی منابع انسانی	۱۱
۱۲	۸۲	۲۳	*	۲۳	۴۵	۱۳۶	۱۳۶	۳۱۸	۳۱۸	۲۳	هوشمندسازی سامانه های نظارتی و امنیتی	۱۲
۱۳	۸۴	۳	*	۴۵	۶۸	۲۳	۱۱۴	۱۱۴	۱۳۶	۵۰	طراحی نظام جذب و ارتقای بومی اساتید	۱۳
۱۴	۸۵	۲۳	*	۲۳	۴۵	۲۳	۶۸	۱۳۶	۲۵	۴۳۲	تهاجم سایبری توأمان با رعایت اولویت های دفاع سایبری	۱۴
۸۳/۲							میانگین کل					

از مجموع میانگین (۸۳/۲ درصد) کمترین تعداد پاسخگویان (۷۴ درصد) شاخص امکان ایجاد امواج سایبری (بمباران گوگلی و...) توسط منابع انسانی خودی در راستای منافع ملی را به عنوان فرصت در زیرساخت های منابع انسانی دفاع سایبر کشور اعلام کرده اند و از سوی دیگر، بیشترین تعداد پاسخگویان (۹۲/۹ درصد) در اعلام نظر خود شاخص طراحی نظام جامع آموزش، توانمندسازی و تربیت منابع انسانی را به عنوان پارامتر فرصت از متغیرهای کلیدی منابع انسانی در تقویت دفاع سایبر کشور ارزیابی کرده اند.

نتیجه‌گیری

بر اساس آنچه که در این پژوهش گذشت، متغیرها با اولویت میانگین شاخص‌ها به ترتیب زیر مشخص شده‌اند:

الف) تهدیدات منابع انسانی دفاع سایبر عبارتند از:

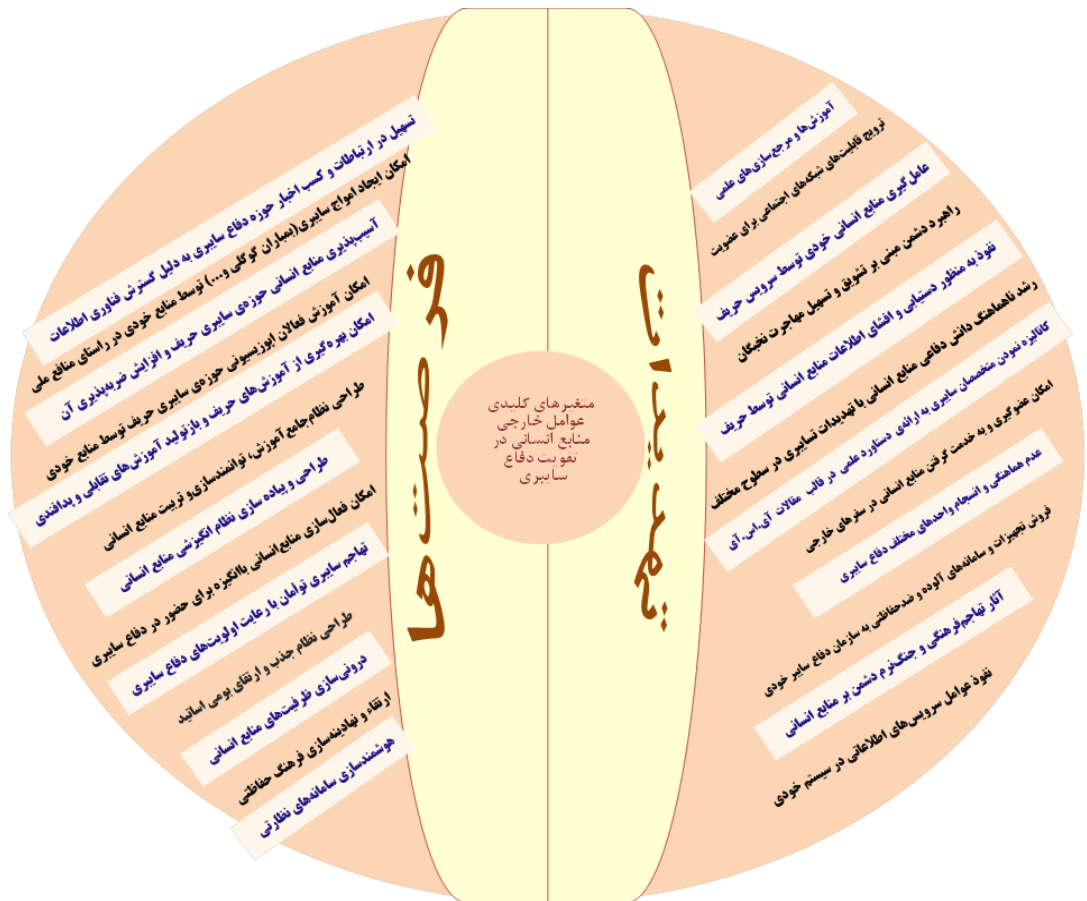
- ۱- نفوذ عوامل سرویس‌های اطلاعاتی در سیستم خودی؛
- ۲- نفوذ به منظور دستیابی و افشای اطلاعات منابع انسانی توسط حریف؛
- ۳- آثار تهاجم فرهنگی و جنگ نرم دشمن بر منابع انسانی؛
- ۴- راهبرد دشمن مبنی بر تشویق و تسهیل مهاجرت نخبگان؛
- ۵- ترویج قابلیت‌های شبکه‌های اجتماعی برای عضویت؛
- ۶- عدم هماهنگی و انسجام واحدهای مختلف دفاع سایبری؛
- ۷- عامل‌گیری منابع انسانی خودی توسط سرویس حریف؛
- ۸- کانالیزه نمودن متخصصان دفاع سایبری به ارائه‌ی آخرین دستاوردهای علمی کشور در قالب مقالات آی.اس.آی؛
- ۹- فروش تجهیزات و سامانه‌های آلوده و ضدحفاظتی به سازمان دفاع سایبر خودی؛
- ۱۰- آموزش‌ها و مرجع‌سازی‌های علمی غیربومی؛
- ۱۱- امکان عضوگیری و به‌خدمت گرفتن منابع انسانی در سفرهای خارجی؛
- ۱۲- رشد ناهماهنگ دانش دفاعی منابع انسانی با تهدیدات توسعه‌ی سایبری در سطوح مختلف.

ب) فرصت‌های منابع انسانی دفاع سایبر عبارتند از:

- ۱- امکان فعال‌سازی منابع انسانی بانگیزه برای حضور در دفاع سایبری با توجه به جذابیت‌های آن؛
- ۲- آسیب‌پذیری منابع انسانی حوزه‌ی سایبری حریف و افزایش ضربه‌پذیری آن؛
- ۳- امکان ایجاد امواج سایبری (بمباران گوگلی و...) توسط منابع خودی در راستای منافع ملی؛
- ۴- طراحی نظام جامع آموزش، توانمندسازی و تربیت منابع انسانی؛
- ۵- درونی‌سازی ظرفیت‌های منابع انسانی؛
- ۶- هوشمندسازی سامانه‌های نظارتی و امنیتی؛
- ۷- طراحی نظام جذب و ارتقای بومی اساتید؛

۱۴۰ فصلنامه امنیت ملی، سال هفتم، شماره بیست و ششم، زمستان ۱۳۹۶ ←

- ۸- امکان آموزش فعالان اپوزیسیونی حوزه‌ی سایبری حریف توسط منابع خودی؛
 - ۹- امکان بهره‌گیری از آموزش‌های حریف و بازتولید آموزش‌های تقابلی و پدافندی؛
 - ۱۰- تسهیل در ارتباطات و کسب اخبار حوزه دفاع سایبری به دلیل گسترش فناوری اطلاعات؛
 - ۱۱- طراحی و عملیاتی سازی نظام جامع منابع انسانی؛
 - ۱۲- ارتقاء و نهادینه‌سازی فرهنگ حفاظتی؛
 - ۱۳- طراحی و پیاده سازی نظام انگیزشی منابع انسانی؛
 - ۱۴- تهاجم سایبری توأمان با رعایت اولویت‌های دفاع سایبری.
- بنابراین می‌توان متغیرهای کلیدی منابع انسانی در تقویت دفاع سایبری جمهوری اسلامی ایران را به شکل زیر (شکل شماره ۱) ارائه نمود:



شکل ۱. متغیرهای کلیدی منابع انسانی در تقویت دفاع سایبری جمهوری اسلامی ایران

منابع و مآخذ:

الف) فارسی

- ابطحی، حسین (۱۳۸۶). مدیریت منابع انسانی (اداره امور کارکنان). کرج: مؤسسه تحقیقات و آموزش مدیریت.
- ازکیا، مصطفی؛ جاجرمی، حسین (۱۳۹۰). روش‌های کاربردی تحقیق، چاپ اول، تهران: شرکت انتشارات کیهان.
- البرعی، محمد؛ مودود رحمان (۱۳۷۷). بررسی نظارت‌های سازمانی و ارزیابی رفتار سازمانی از دیدگاه اسلام با به کاربردن فرآیند تحلیلی، مجموعه مقالات نگرشی بر مدیریت در اسلام، تهران: انتشاران مرکز آموزش مدیریت دولتی.
- جاهد، حسینعلی (۱۳۸۴). «سلامت سازمانی»، ماهنامه تدبیر، شماره ۱۵۹.
- حسن‌بیگی، ابراهیم (۱۳۸۴). «توسعه شبکه ملی دیتا، چالش‌های فراروی امنیت ملی»، فصلنامه مدیریت، شماره ۴۸.
- حسن‌بیگی، ابراهیم (۱۳۸۸). حقوق و امنیت در فضای سایبر، تهران: دانشگاه عالی دفاع ملی.
- حیدری تفرشی، غلامحسین (۱۳۸۱). نگرشی نوین به نظریات سازمان و مدیریت. تهران: انتشارات فراشناختی اندیشه.
- رادمن، تام؛ ویلکینسون، آدریان (۲۰۰۶). مدیریت منابع انسانی پیشرفته، تهران: مه کامه.
- رسول‌زاده، مهدی (۱۳۸۸). «سازمانهای مجازی»، ماهنامه تدبیر، شماره ۱۲۶.
- سعادت، اسفندیار (۱۳۸۰). مدیریت منابع انسانی، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- سنگه، پیتر (۱۳۸۶). فرمان خلق سازمان‌های یادگیرنده. ترجمه حافظ هدایت و محمد روشن، تهران: سازمان مدیریت صنعتی.
- سیدجوادین، سیدرضا (۱۳۸۲). مبانی مدیریت منابع انسانی، تهران: دانشگاه تهران.
- فاستر، جرج.م. (۱۳۷۵). جوامع سنتی و تغییر ساختی، ترجمه مهدی ثریا، تهران: مرکز پژوهش‌های بنیادی وزارت ارشاد.
- فرزین، علی (۱۳۸۹). منشور منابع انسانی (نگرش به منابع انسانی در غرب و اسلام)، تهران: مجتمع مطالعاتی شهید بهشتی.
- گیدنز، آنتونی (۱۳۷۳). جامعه‌شناسی، ترجمه منوچهر صبوری، تهران: نشر نی.
- ورزشکار احمد (۱۳۸۲). برنامه‌ریزی استراتژیک نیروی انسانی، تهران: دانشگاه امام حسین (ع).

منابع انگلیسی

- Alberts, David S. Garstka John J. Hayes, Richard E. Signori, David A. ; "Understanding Information Age Warfare". CCRP Publication Series, 1999.
- Bas Barrett. Man'Work'Organization. boston: Allyn and baconinc, 1972.
- Garvin, David A. "Building a Learning Organization". Harvard Business Review. July - August 1993. pp 78-91.
- Gunasekaran, A, McGaughey, R and Wolstencraft, V; Agile manufacturing: Concepts and framework, Agile Manufacturing: The 21st Century Competitive Strategy, Elsevier Science, 2001, 25-49
- Metes, George, Gundry, John, Bradish, Paul; Agile Networking, 1998, Prentice Hall
- Hubrt Herenger ,ReneHeek and Ronald Kubert" Operation virtual organizations using bipartite service level agreements "(2007)
- yanis Vergadis ,Dimitris Apostohou and Gregori mentzos "a Collaboration Pattern Model For Virtual organization "(2005)