ارائه الگوی راهبردی مدیریت تحولات برآمده از توسعه فناوری اطلاعات و ارتباطات بر امنیت داخلی جمهوری اسلامی ایران

ابراهیم حسن بیگی[1]

ابراهیم کولیوند[2]

تاریخ دریافت: ۱۳۹۶/۰۳/۶ تاریخ پذیرش: ۱۳۹۵/۱۱/۱۸

چکیده:

در این تحقیق با استفاده از روش داده بنیاد و فرایند تحلیل شبکه‌ای تلاش شده است برای مدیریت تحولات برآمده از توسعه فناوری اطلاعات و ارتباطات بر امنیت داخلی جمهوری اسلامی ایران الگوی راهبردی ارائه شود. در این تحقیق تهدیدات چهارگانه تروریسم، خرابکاری، براندازی و جاسوسی به‌عنوان تهدیدات اصلی امنیت داخلی در نظر گرفته‌شده‌اند. این الگو شامل ابعاد، مؤلفه‌ها و شاخص‌هایی است که باهم ارتباطات مفهومی نیز دارند. برای حصول به این هدف، توسعه فاوا در پنج سال آینده مدنظر قرارگرفته است و با کمک جمع‌آوری کتابخانه‌ای، مصاحبه با ۱۱۰ نفر از متخصصان، تشکیل ٦٤ جلسه نخبگی و شرکت در چهار اجلاس بین‌المللی در اروپا، اطلاعات لازم جمع‌آوری گردید. در مرحله بعد این اطلاعات مورد غربالگری و دسته‌بندی قرار گرفت که حاصل این مرحله در قالب جدول کدگذاری ارائه گردیده است. به کمک نرم‌افزار ابر تصمیم‌ساز وspss اطلاعات جمع‌آوری‌شده، موردبررسی و تحلیل قرار گرفت. مدل مفهومی و نتایج تحقیق برای تائید مجدد در قالب پرسشنامه‌ای، بین ۲۱ نفر از جامعه نخبگان توزیع گردید و نتایج مورد تائید قرار گرفت. هفت بعد اقدامات اطلاعاتی، اقدامات اجتماعی- سیاسی، ظرفیت‌سازی، هماهنگی ملی و بین‌المللی، ساختارهای اجرایی و پیاده‌سازی، اقدامات فنی و قوانین و مقررات به‌عنوان ابعاد مدیریت راهبردی تحولات برآمده از توسعه فاوا بر امنیت داخلی پیشنهاد گردید. برای هر یک از ابعاد تعدادی مؤلفه و برای هر مؤلفه نیز دو شاخص انتخاب گردید. درمجموع این الگو دارای ۳٤ مؤلفه و ٦٨ شاخص است. همه این ابعاد، مؤلفه‌ها و شاخص‌ها از جدول کدگذاری استخراج‌شده‌اند و تلاش شده است روند استخراج منطقی آن‌ها از منابع اولیه اطلاعات حفظ گردد.

کلیدواژه‌ها: الگوی راهبردی مدیریت، فناوری اطلاعات و ارتباطات، تروریسم، خرابکاری، براندازی، جاسوسی نوین

---

[1] استاد و عضو هیئت‌علمی دانشگاه عالی دفاع ملی

[2] دانش آموخته دوره دکتری امنیت ملی دانشگاه عالی دفاع ملی ونویسنده مسئول:

مقدمه: با بررسی ماده ٤٦ قانون برنامه پنجم توسعه جمهوری اسلامی ایران می‌توان تأثیرات شگرف و عمیق جامعه را از فناوری اطلاعات و ارتباطات مشاهده نمود. در این سند تکلیف شده است با رعایت موازین شرعی و امنیتی، کلیه دستگاه‌های اجرایی و واحدهای تابعه و وابسته تا پایان سال دوم و ٦٠٪ خانوارها و کلیه کسب‌وکارها تا پایان برنامه بتوانند به شبکه ملی اطلاعات و اینترنت متصل شوند. با بررسی اجمالی این سند به‌وضوح در کنار بهره‌برداری از فرصت‌های، کنترل تهدیدات برآمده از فناوری اطلاعات و ارتباطات نیز در نظر گرفته‌شده است. در این ماده، حداقل در ۷ مورد ملاحظات امنیتی و کنترل تهدیدات برآمده از توسعه فناوری اطلاعات و ارتباطات گوشزد شده است.

نه‌تنها در کارهای تحقیقاتی و دانشگاهی بلکه در اسناد بالادستی و راهبردی کشور نیز به‌ندرت به تهدیدات نوین برآمده از فناوری اطلاعات و ارتباطات در حوزه‌هایی نظیر تروریسم، جاسوسی نوین، براندازی و خرابکاری پرداخته‌شده است. عدم شناسایی، بررسی و ارائه الگوی راهبردی مدیریت تهدیدات می‌تواند ضربات سنگینی بر پیکره نظام مقدس جمهوری اسلامی ایران وارد نماید. به نظر می‌رسد افق روشنی برای کنترل تحولات برآمده از فناوری اطلاعات و ارتباطات در حوزه امنیت داخلی جمهوری اسلامی ایران وجود ندارد. هرچند مدیران بخش‌های حوزه فناوری بیشتر متوجه تحولات شده‌اند و با فرصت‌ها و تهدیدات نوینی که حاصل فناوری است به‌صورت عمل‌گرایانه درگیر شده‌اند اما حوزه سیاست‌گذاری امنیت داخلی و به‌طور خاص الگوی راهبردی مدیریت آن ، فاصله‌ی زیادی با تجارب مدیران دارد. این موضوع مهم‌ترین مسئله این تحقیق است. در این تحقیق تلاش شده است با در نظر گرفتن تجارب موجود که نزد مدیران اجرایی جمهوری اسلامی ایران است و همچنین نگاه به تحولات ابعاد چهارگانه امنیت داخلی یعنی تروریسم، خرابکاری، براندازی و جاسوسی نوین برآمده از فناوری اطلاعات و ارتباطات، الگوی راهبردی مدیریت تحولات(ابعاد، مؤلفه‌ها و شاخص‌های مدیریت این تحولات و چگونگی رابطه بین آن‌ها)، متناسب با نظام مقدس جمهوری اسلامی ایران، تدوین و ارائه گردد. این مهم با احصاء شاخص‌های ابعاد چهارگانه امنیت داخلی ازیک‌طرف و در نظر گرفتن آن دسته از تحولات فناوری اطلاعات و ارتباطات که بر ابعاد چهارگانه فوق بیشترین تأثیر رادارند و اعمال رویکردی کنترلی، راهبردی، آینده‌نگر و بومی جمهوری اسلامی ایران صورت خواهد گرفت.

مبانی نظری: تحقیق موسسه گارتنر (Gartner, 2014)، نتایج جالبی در خصوص اولویت‌های

فناوری و شغلی مدیران ارشد فناوری اطلاعات این شرکت‌ها داشته است. برای تهیه این گزارش بزرگ‌ترین نمونه آماری جهان از میان مدیران ارشد فناوری اطلاعات شرکت‌ها و سازمان‌ها موردمطالعه قرارگرفته‌اند. هدف اصلی از این تحقیق، جمع‌آوری نظرات مدیران، در خصوص چگونگی ایجاد توازن در میان اولویت‌های مدیریتی، فنی، راهبردی و کسب‌وکار است. در این گزارش از اطلاعات حاصل از مطالعات پیمایشی، مطالعات موردی، نظرات خبرگان استفاده‌شده است. در سال ۲۰۱٤ تعداد ۲۰۵۳ نفر از ۳٦ زمینه شغلی مختلف در ۲۱ کشور دنیا موردمطالعه قرارگرفته‌اند. گردش مالی این شرکت‌ها در حوزه فناوری اطلاعات بالغبر ۲۳۰ میلیارد دلار بوده است.

جدول۱: ده اولویت فناوری و شغلی مدیران ارشد فناوری اطلاعات

رتبه	اولویت فناوری	رتبه	اولویت شغلی
۱	***تجزیه‌وتحلیل داده‌های انبوه***	۱	تسریع رشد شرکت
۲	***فناوری‌های همراه***	۲	عرضه‌ی یافته‌ها
۳	***رایانش ابری***	۳	کاهش هزینه‌های سازمان
٤	**نرم‌افزارهای گردش کار**	٤	جذب و حفظ مشتریان جدید
۵	**نوسازی فناوری‌های موجود**[1]	۵	بهبود زیرساخت و نرم‌افزارهای کاربردی
٦	**مدیریت فناوری اطلاعات**[2]	٦	خلق محصولات و خدمات نوین
۷	**مدیریت تعامل با مشتری**[3]	۷	افزایش راندمان
۸	**مجازی‌سازی**	۸	جذب و حفظ نیروی کار
۹	**امنیت**	۹	پیاده‌سازی تحلیل داده‌های بزرگ
۱۰	**سیستم برنامه‌ریزی منابع سازمان**[4]	۱۰	توسعه بازار

یکپارچه شدن[5] چهار نیرو

محققین در طول چند سال گذشته نظاره‌گر تحولات مستقل و جدای از هم چهار نیروی قدرتمند یعنی فناوری‌های اجتماعی[6](همانند وب ۲)، فناوری‌های همراه[1] (همانند فناوری تلفن همراه)،

[1] Legacy modernization
[2] IT management
[3] Customer relationship management
[4] EPR applications
[5] Nexus
[6] Social

رایانش ابری[2] و اطلاعات[3] (منظور اطلاعات انبوه و تحلیل آن است) بوده‌اند. به‌واسطه تغییر ذائقه مردم و تحولات اتفاق افتاده در ابزارهای هوشمند، این نیروها همگرا شده‌اند. این همگرایی با محوریت مصرف‌کننده باعث شده است که مدیران سازمان‌ها، شاهد منسوخ شدن معماری موجود در سازمان‌ها باشند.

در این یکپارچه شدن نیروهای چهارگانه، اطلاعات نقش بستر و زمینه[4] را برای وقوع رفتارهای اجتماعی و سیار ایجاد می‌نماید. تجهیزات همراه خود یک سکو[5] برای شبکه‌های اجتماعی هستند که راهه‌ای نوینی را برای انجام امور ارائه نموده‌اند. رفتارهای اجتماعی اخیر، به‌گونه‌ای بی‌سابقه افراد را به‌طور هم‌زمان به مشاغلشان و دیگر افراد جامعه مرتبط نموده است. فناوری‌های ابری امکان ارائه اطلاعات و خدمات را به مصرف‌کنندگان و سیستم‌ها فراهم نموده‌اند. یکپارچه شدن این چهار نیرو منجر به ایجاد زیست‌بوم[6] ابری با محوریت مشتری شده است. این چهار نیروی درهم‌تنیده و یکی شده آن‌چنان فضایی ایجاد نموده‌اند که در آن ابزارها و نرم‌افزارهای چندمنظوره، افراد، اطلاعات و دارایی‌های مردم در تعامل دائمی‌اند.(عصاریان، چین ۱۳۹۱)

مردم چه بدانند و چه ندانند به‌واسطه آنکه در تلاش‌اند امور مختلف را یکپارچه مدیریت نمایند وابستگی‌شان به زیرساخت‌های ابری افزایش‌یافته است. این امر در مورد کارمندان باعث تحول در ادارات و سازمان‌ها شده است. سازمان‌های پیشرو از فرصت ایجادشده به‌واسطه این چهار نیرو، جهت خلق محصولات و خدمات بهره می‌گیرند. در مقابل، سازمان‌های سنتی هم در فناوری اطلاعات مورداستفاده و هم در کسب‌وکارشان دچار سردرگمی و آشفتگی شده‌اند. کارایی ابزارها در حال بهبود است و دسترسی به اطلاعات، وسیع‌تر و عمیق‌تر خواهد شد.

فناوری–محوری[7] جای خود را به انسان–محوری[8] خواهد داد. مردم مصرف‌کننده‌های پیچیده‌تری خواهند شد و نه‌تنها پدیدآورندگان فناوری بلکه جزئی از آن خواهند بود. این فرایند همراه با افزایش پیچیدگی است. این در حالی است که همین پدیده پیچیده باید برای مصرف‌کننده ساده و

---

[1] Mobile
[2] Cloud
[3] Information
[4] Context
[5] Platform
[6] Ecosystem
[7] Techno-centered
[8] Human-centered

دل‌چسب باشد. اغلب فناوری‌ها در فرایند بلوغ خود پیچیده‌تر و کارآمدتر می‌شوند. تلاش می‌شود ساده‌ترین راه و مؤثرترین آن‌ها بکار گرفته شود تا استفاده از آن برای مصرف‌کننده ساده‌تر شود. این در حالی است که پیچیدگی آن برای تولیدکننده افزایش می‌یابد. مدیریت این پیچیدگی کل زیست‌بوم ارائه‌کنندگان فناوری را متأثر می‌نماید(از فروشگاه‌های ابزار گرفته تا ارائه‌کنندگان خدمات ابری).

جنبه دیگر تحول برآمده از یکپارچه شدن این چهار نیرو، عدم نیاز به محل خاص با امکانات پیچیده برای انجام امور است. قبلاً مردم می‌بایست برای انجام امور رایانشی[1] خود به محلی با فناوری مناسب می‌رفتند ولی امروزه در دسترس بودن ابزارها، حد واسط‌ها و نرم‌افزارهای کارآمد، این وابستگی را از بین برده است. گوشی‌های هوشمند و تبلت‌ها به همراه نرم‌افزارهای متعدد، زیست بومی فناورانه ایجاد نموده‌اند. این زیست‌بوم هر آنچه را که فردی برای انجام امورش لازم دارد در میان دستانش قرار داده است و او را از انجام مقدمات زائد بی‌نیاز کرده است. از طرفی همین پیشرفت باعث شده است که مردم مصرف‌کننده‌های پیچیده‌تری شوند. به عبارتی افراد توانمندتر شده‌اند. مردم انتظار دارند تمایز میان شغل و فعالیت‌های شخصی خود در شبکه را از بین ببرند و آن‌ها را یکی کنند. برای ایجاد یک فعالیت با این سطح از تعامل مقدمات ذیل باید فراهم شود.

۱- برای دسترسی به اطلاعات موردنیاز لازم است سرویس‌های ابری ایجاد شود.
۲- مردم دائم در حال جابجایی و تحرک‌اند لذا به تجهیزات و نرم‌افزارهایی نیاز دارند که در دستانشان جا بگیرد نه بر روی میز کارشان.
۳- اطلاعات مکانی(مثلاً اطلاعات مربوط به تجهیزات بکار رفته)خود حجم فراوانی از اطلاعات را ایجاد می‌کنند که باید مدیریت شود.
٤- دسترسی به شبکه‌های اجتماعی نیازمند سکوهای اجتماعی(مثل فیس بوک) می‌باشند.

سایبر تروریسم: باید توجه داشت که هیچ تعریف پذیرفته‌شده جهانی درباره سایبر تروریسم وجود ندارد. اما برخی مفاهیم وجود دارد که با ترکیب کردن آن‌ها می‌توان یک تعریف کاربردی برای سایبر تروریسم ارائه کرد." مرکز حفاظت زیرساخت‌های ملی امریکا تروریسم مجازی را به‌عنوان یک عمل غیرقانونی اجراشده از طریق رایانه‌ها که به خشونت، مرگ یا تخریب منجر

[1] Computing

می‌شود و به‌منظور وادارسازی یک دولت به تغییر سیاست‌گذاری‌اش استفاده می‌شود، تعریف می‌کند.(Clay ,2010,31)

در این تعریف چهار محور اصلی وجود دارد: اول اینکه عمل سایبر تروریسم یک کار غیرقانونی است دوم انجام آن از طریق رایانه انجام می‌شود سوم دارای مؤلفه خشونت است و چهارم به تغییر در سیاست‌گذاری دولت تأکید می‌ورزد. اما تعریف دیگری نیز وجود دارد و آن این است که تروریسم مجازی، استفاده از رایانه باانگیزه سیاسی به‌عنوان سلاح یا اهدافی توسط گروه‌های فرو ملی یا عواملی غیرقانونی است که قصد خشونت داشته و به‌منظور ایجاد تغییرات در سیاست‌گذاری‌های دولت انجام می‌شود.(Clay ,2010,18) دورتی دنینگ تعریف دیگری ارائه می‌دهد او می‌گوید سایبر تروریسم عبارت است از تلاقی تروریسم و فضای رایانه‌ای. (Denning, 1999,27)

تروریسم مجازی به معنای حملات غیرقانونی ضد رایانه‌ها و اطلاعات ذخیره‌شده در آن‌ها است که هدف از آن ارعاب یا اجبار یک دولت یا اتباع آن به‌منظور پیشبرد اهداف سیاسی یا اجتماعی است.این حملات باید به اعمال خشونت بر ضد اشخاص یا دارایی‌ها شود یا دست‌کم موجب وارد آمدن آن اندازه آسیب به آن‌ها گردد که ایجاد ترس نماید.(طیب،۱۳۹۰)

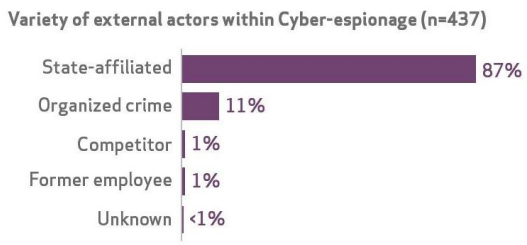
پیتر فلمینگ و مایکل استون سایبر تروریسم را این‌گونه تعریف می‌کنند: هرگونه عمل تروریستی که در آن از سیستم‌های اطلاعاتی یا فناوری دیجیتال(رایانه‌ها و شبکه‌های رایانه‌ای) چه به‌عنوان ابزار حمله و چه به‌عنوان آماج حمله استفاده شود(طیب، ۱۳۹۰)

تعامل فضای مجازی با تروریسم به سه طریق صورت می‌گیرد: وسیله تسهیل‌کننده اقدامات تروریستی، هدف اقدامات تروریستی و یک سلاح تهاجمی در دستان تروریست‌ها. با این اوصاف تعریف ذیل به‌عنوان سایبر تروریسم ارائه می‌گردد: " هرگونه استفاده از فضای مجازی، چه به‌عنوان تسهیل‌کننده اقدام‌های تروریستی و چه به‌عنوان هدف جهت تخریب و نابودی و یا ابزار حمله تروریستی، سایبر تروریسم تلقی می‌گردد." (عصاریان، چین، ۱۳۹۲)

جاسوسی مجازی: منظور از جاسوسی مجازی بیشتر دسترسی غیرمجاز به شبکه و سیستم‌های رایانه‌ای با حمایت دولت‌ها است. بیشتر آماج جاسوسی مجازی، بخش‌های دولتی(مراکز نظامی، خدمات عمومی، ادارات و زیرساخت‌ها) می‌باشند. در سال ۲۰۱۳، ۵۱۱ واقعه امنیتی در این خصوص گزارش‌شده است که در ۳۰۶ مورد جاسوسی مجازی تائید شده است. (Verizon,

(2014 در میان روش‌های نفوذ در شبکه، بیشترین آمـار رشـد در چنـد سـال گذشـته مربـوط بـه جاسوسی مجازی بوده است به‌طوری‌که در سال ۲۰۱۳ سه برابر شده است.

در جاسوسی مجازی طیف وسیعی از تکنیک‌ها و ابزارهای فنی بکار گرفته می‌شـود. یکـی از ایـن ابزارها که به‌سرعت توسط دولت‌ها بکار گرفته‌شده است روش "نفوذ راهبردی به شبکه[1] " اسـت. است. جمع‌آوری اطلاعات در خصوص جاسوسی مجازی به دو دلیل با محـدودیت روبـرو اسـت یکی آنکه قربانیان دلیلی برای بیان نفوذ و سرقت اطلاعات خود نمی‌بینند و دیگری آنکه الگـوریتم و سیستم خودکاری جهت تشخیص جاسوسی مجازی ابداع نشده اسـت. افـزایش آمـار جاسوسـی مجازی در چند سال اخیر را می‌توان به افزایش حساسیت سازمان‌ها و تبـادل بهتـر داده‌هـا در ایـن خصوص مرتبط دانست (عصاریان، چین، ۱۳۹۱)



شکل ۱- حامیان جاسوسی مجازی

همان‌گونه که انتظار می‌رود اغلب جاسوسی مجازی توسط بازیگران دولتی و یا منتسـب بـه آن‌هـا، صورت گرفته است. دومین بازیگران این عرصه گروه‌های جنایتکار سازمان‌یافته مـی‌باشـند. رقبـا و کارمندان سابق در رتبه‌های بعدی قرار دارند. هرچند اهداف مالی در جاسوسی مجازی وجود دارد ولی دستیابی به انواع گواهی‌ها و مجوزهای دسترسی که امکان تسلط بر سیستم‌ها را فراهم می‌کنـد بیشتر مدنظر می‌باشند. یکی از ویژگی‌های فنی جاسوسی مجـازی، اسـتفاده وسـیع از تکنیـک‌هـای نفوذ است. به نظر می‌رسد به‌واسطه حمایت دولت‌ها از جاسوسی مجـازی، ابزارهـای مورداسـتفاده برای این کار بسـیار متنـوع اسـت. حملـه‌کننـدگان معمـولاً بـه دنبـال اطلاعـات حسـاس و دارای طبقه‌بندی می‌باشند ولی اطلاعات مربوط به سیسـتم، مجوزهـای دسترسـی، اطلاعـات شخصـی و اطلاعات مالی از اهداف آن‌ها می‌باشند. فقط در ماه مارس ۲۰۱۳ آژانـس امنیـت ملـی آمریکـا ۹۷

[1] Strategic website compromises (SWCs)

میلیارد داده گوناگون از طریق جاسوسی مجازی، از سراسر جهان به دست آورده است که از این میزان ١٤ میلیارد داده و گزارش(١٥٪ کل داده‌ها) مربوط به ایران بوده است. پاکستان با حدود ۱۳ میلیارد، اردن با حدود ۱۲ میلیارد و مصر با حدود ۷ میلیارد به ترتیب در جایگاه بعدی قرارگرفته‌اند.(The guardian, 2013:P23)

براندازی مجازی: به‌طورکلی تأثیر فناوری اطلاعات و ارتباطات بر براندازی را می‌توان در سه قالب اصلی دسته‌بندی نمود. نخست تأثیرات عمیق، خزنده و درازمدت است که لایه‌های ارزشی و هنجاری افراد و جوامع را آماج خود قرار می‌دهد. در دومین تأثیرگذاری، بحث‌های شبکه‌سازی که می‌توان آن را میان‌مدت در نظر گرفت، مطرح می‌شود. سومین مورد، تأثیرات تاکتیکی و عملیاتی(کوتاه‌مدت) این فناوری‌ها در استراتژی‌های نوین براندازی است که فناوری اطلاعات و ارتباطات بیشتر به‌عنوان ابزار و کاتالیزور، درصحنه اغتشاشات بکار گرفته می‌شود.

هویت‌سازی: در طول سالیان گذشته مقام معظم رهبری در سخنرانی‌هایی که به مناسبت‌های مختلف ایراد فرموده‌اند همواره خطر تحرکات نرم را در قالب‌های مختلفی ازجمله تهاجم فرهنگی، شبیخون فرهنگی، ناتوی فرهنگی و جنگ نرم گوشزد فرموده‌اند که این بیانات نشان از دغدغه و حساسیت‌های ایشان به اهمیت موضوع است.

فناوری اطلاعات و ارتباطات فقط یک ابزار فنی ساده به دست ما نمی‌دهد بلکه چه‌بسا نگاه‌ها و ارزش‌ها و عادتواره‌ها را و اصولاً مدل ذهنی افراد را متحول نماید. شاید اگر گوتنبرگ دستگاه چاپ را اختراع نکرده بود، جنبش اصلاح دین و پروتستان تیزم نیز در اروپا روی نمی‌داد. آدام شاف، بحث کرده است که چگونه انقلاب میکروالکترونیکی، به انقلاب انفورماسیون (اطلاعاتی شدن) و رقم خوردن جامعهٔ پسانوین اطلاعاتی انجامید (شاف، ۱۲،۱۳۷۵). جهانی‌شدن از پیامدهای فناوری اطلاعات و ارتباطات بود. گیدنز جهانی‌شدن را بسط اجتناب‌ناپذیر تجدّد در گسترهٔ بین‌المللی می‌داند(Giddens, 1990,P49) و آلبرو، آن را پنجمین مرحله جامعه‌شناسی دانسته است.(Albrow, 1990,P65) مانوئل کاستلز، با شرح تازه‌تر و مشروح‌تر این تحولات، از شکل‌گیری «جامعهٔ شبکه‌ای» بحث کرد. جامعه‌ای بسیار متفاوت از جامعه سنتی و جامعه صنعتی(کاستلز، ۲۵،۱۳۸۰).

شبکه‌سازی:

دیپلماسی عمومی به‌عنوان یکی از برنامه‌های آمریکا جهت شبکه‌سازی ناظر به برقراری ارتباط با

مردم و تحت تأثیر قرار دادن آن‌ها در جوامع موردنظر است. در این رابطه تشخیص شرکا بالقوه، حائز اهمیت فراوان است. ازنظر آمریکایی‌ها مسلمانانی که به دموکراسی و حقوق بشر موردقبول نهادهای بین‌المللی احترام می‌گذارند و نیز معتقد به تنوع فرهنگی، قوانین غیر فرقه‌ای، مخالف با تروریسم، انتخاب آزاد، احترام به حقوق زنان و اقلیت‌های مذهبی باشد، به‌طور بالقوه متحد محسوب می‌گردند.

ایجاد اغتشاش و بحران

اثرگذاری مطلوب رسانه‌های اجتماعی در عالم خارج و اقدام عملی برای تغییرات اجتماعی(مثل انقلاب‌های رنگی) مستلزم وجود سه عامل مشخص است: اولین مسئله وجود ارتباطات است. این عامل به معنای استفاده از رسانه‌های اجتماعی به‌منظور انتقال پیام است. این مرحله می‌تواند شامل مذاکره، محاوره و دریافت بازخورد باشد. دومین مسئله همکاری است که همراهی دیگران در رسانه‌های اجتماعی به‌منظور رسیدن به هدفی مشخص در عالم واقعی است. این عامل با انتقال و اشتراک‌گذاری دانش و ایجاد زیرساخت‌های عمل جمعی عجین شده است. عامل سوم فراگیری و گسترش تجربیات افراد از طریق اقدامات بر خط و در فضای مجازی است. مجموعه این شرایط باعث افزایش کارآمدی عمل اجتماعی مردم در دنیای واقعی با بهره‌گیری از امکانات دنیای مجازی است. به‌عبارت‌دیگر، رسانه‌های اجتماعی از طریق چهار فرایند کلی می‌توانند اثرگذاری خود بر تحولات اجتماعی را سبب شوند. این چهار فرایند به‌تدریج از دنیای مجازی به دنیای واقعی سیر می‌کنند. (گوهری،۱۳۹۰،۱۲۵)

خرابکاری:

قسمت عمده سامانه‌های فیزیکی- مجازی با محوریت ایمنی فیزیکی طراحی و آزمایش می‌شوند و دراین‌بین امنیت مجازی مورد غفلت قرار می‌گیرد. عمر مفید تجهیزات بکار رفته در سامانه‌های حیاتی فیزیکی- مجازی نظیر سدها و نیروگاه‌های هسته‌ای بسیار زیاد و در حدود ۳۰ سال است. به علت قیمت بسیار بالایی این تجهیزات، امکان تعویض آن‌ها وجود ندارد. از این بدتر آن است که اغلب این سامانه‌ها یکپارچه بوده و قابلیت ارتقا ندارند. ولی سامانه‌های کامپیوتری را می‌توان با ارتقا و افزودن بسته‌های تکمیلی در مقابل تهدیدات پیش‌آمده، ایمن کرد. ارتقاء یک سیستم به ماه‌ها برنامه‌ریزی نیاز دارد بعلاوه برای مدت زیادی زیرساخت موردنظر غیرفعال خواهد بود. (Cardenas et al :2009)

تفاوت عمده سازمان‌های فیزیکی- مجازی با سامانه‌های صرفاً مبتنی بر فناوری اطلاعات، مربوط

به نحوه تعامل سامانه‌ها با محیط خود است. در یک سامانه معمولی، در صورت قطع شبکه یا خرابی کامپیوتر، ضرر و زیان مالی و تأخیر در سرویس روی می‌دهد و احتمال خطرات جانی وجود نخواهد داشت درصورتی‌که در سامانه‌های فیزیکی- مجازی که اغلب داری بخش‌های کنترلی بلادرنگ[1] می‌باشند قطع شدن شبکه یا کامپیوتر می‌تواند خطرات جانی به دنبال داشته باشد. نمونه‌ای از این نوع، انفجار در لوله گاز شهر واشینگتن است که در سال ۱۹۹۹ اتفاق افتاده است. وابستگی و تعامل سامانه با محیط در سامانه‌های فیزیکی- مجازی یک مزیت هم دارد و آن امکان تشخیص حملات مجازی از طریق مشاهده اثرات عینی است. این ملاحظات بسترهای آزمونی جدیدی را می‌طلبد. مراکز تحقیقاتی به دنبال طراحی آزمون‌های متناسب با تهدیدات فوق می‌باشند. تمرکز این آزمون‌ها باید طیف وسیعی از زیرساخت‌ها را شامل شود. حملات مجازی برای تروریست‌ها بسیار جذاب است زیرا می‌توانند آسیب‌های جدی فیزیکی ایجاد نمایند بدون آنکه خطری برای نیروهای متخاصم ایجاد نماید. البته تولید سلاح‌های مجازی کار هرکسی نیست و به توان و امکانات بالایی نیاز دارد که در اغلب گروه‌های تروریستی غیردولتی وجود ندارد. به‌عنوان‌مثال ساخت استاکس نت که علیه تأسیسات هسته‌ای جمهوری اسلامی ایران بکار رفته است تنها از عهده ابرقدرتی مثل آمریکا برمی‌آید که مهم‌ترین سرنخ برای دخالت آمریکا هم همین پیچیدگی است. به‌واسطه پیچیدگی طراحی و تولید سلاح‌های مجازی به نظر نمی‌رسد در آینده نزدیک، گروه‌های تروریستی غیردولتی از عهده ایجاد خسارت جانی جدی برآیند. البته از گروه‌های تروریستی غیردولتی انتظار حملات مجازی برای مقاصد محدودتری نظیر از کار انداختن سیستم‌های حفاظتی یک ساختمان و یا یک واحد سازمانی جهت تسهیل حملات فیزیکی و یا ایجاد ترافیک ساختگی جهت ممانعت از حضور به‌موقع نیروهای عملیاتی درصحنه دور از ذهن نخواهد بود(عصاریان، چین،۱۳۹۱).

در این موارد استفاده از راهکارهای معمولی حفاظت مجازی نظیر آنتی‌ویروس، دیوار آتش، سامانه تشخیص نفوذ می‌تواند مجموعه را نسبت به حملات فیزیکی- مجازی محافظت نماید. مهم‌ترین اقدام، ترویج فرهنگ بهداشت و مراقبت مجازی در سازمان است این موضوع شامل پیروی از سیاست‌های حفاظتی سازمان توسط افراد و مدیران، اعمال مرتب پیوست‌های امنیتی و نظایر آن است. این امر اجرای اقدامات تروریستی در فضای مجازی را بسیار مشکل می‌نماید.

---

[1] Real- time

مدیریت تهدیدات:

امروزه داشتن مدیریت مشترک و عدم تفکیک مدیریت تهدیدات چهارگانه امری اجتناب‌ناپذیر است.(PWC, 2014) سرعت بسیار بالای تحولات فناوری اطلاعات و ارتباطات منجر به تغییرات شدید محیط امنیتی بسیاری از کشورها شده است. جهت هماهنگی ظرفیت‌های ملی با پدیده‌های نوین، چابکی بسیار بالایی موردنیاز است. از معماری کنونی سازمان‌ها نمی‌توان انتظار شناسایی بهنگام تهدیدات نوین و ارائه راهکارهای مدیریت آن‌ها را داشت. لذا وجود ساختارهای منعطف که شرح وظایف ثابت و محدودی ندارند امری اجتناب‌ناپذیر است. بسیاری از مؤلفه‌ها و شاخص‌های ارائه‌شده جهت مدیریت راهبردی تحولات برآمده از توسعه فاوا بر امنیت داخلی نیاز به ظرفیت‌سازی دارند لذا زمان‌بر می‌باشند. هدف، ایجاد توان پیشگیری و مقابله با تهدیدات چهارگانه به نحوی است که پدیده‌ها تبدیل به بحران ملی نشوند. این مؤلفه‌ها و شاخص‌ها بسیاری از سازمان‌ها و نهادها را درگیر می‌نماید. علاوه بر این ایجاد نهادهای جدید جهت تقسیم‌کار و اجتناب از دوباره‌کاری، امری ضروری به نظر می‌رسد. ازآنجاکه منشأ تهدیدات فضای مجازی در اغلب موارد خارج از مرزهای سیاسی یک کشور قرار دارد، هیچ کشوری به‌تنهایی قادر به مدیریت آن‌ها نیست. همکاری‌های بین کشورها در قالب انواع قراردادهای دو یا چندجانبه و ایجاد ساختارها و نهادهای بین‌المللی جهت مدیریت مشترک تهدیدات از نیازهای قرن حاضر می‌باشند.

قوانین و مقررات کیفری جهت حمله‌کنندگان و ایجاد بازدارندگی قضایی در کنار الزامات حقوقی و دستورالعمل‌های واضح و به‌روز که راهنمای رفتار مناسب و ایجاد بهداشت مجازی است مکمل یکدیگر می‌باشند.(Global Cybersecurity Index: 2014)

بعد قوانین و مقررات تنها محدود به مرزهای یک کشور نیست و باید در سطح جهانی طیف وسیعی از مجرمین را از افراد تا دولت‌ها پوشش دهد. ایجاد نهادهای بین‌المللی جهت تدوین قوانین و اعمال آن‌ها از دیگر الزامات است. جهت ایجاد ظرفیت‌های ملی برای مدیریت تهدیدات چهارگانه امنیت داخلی سرمایه‌گذاری و تقویت تحقیقات در ابعاد مختلف در کنار آموزش و ایجاد رشته‌های تخصصی دانشگاهی اجتناب‌ناپذیر است. ایجاد توانایی مدیریت حوادث و افزایش توان بازیابی خدمات را می‌توان با انجام مانورهای مناسب تعقیب نمود. اهمیت وجود گروه‌های پاسخگویی و مدیریت حوادث امنیتی در سطح ملی در حملات مجازی چند سال گذشته، خود را نشان داده است. بدون اعزام گروه‌های خبره و مجهز برای کاهش دامنه حملات و بازیابی سریع

خدمات، امکان ایجاد بحران‌هایی در سطح ملی دور از ذهن نخواهد بود. وجود راهبردهای ملی مناسب به همراه ملزومات پیاده‌سازی آن نظیر ساختارهای اجرایی و نهادهای نظارتی و کنترلی می‌تواند امنیت مجازی را در درازمدت نهادینه سازد(عصاریان، چین،۱۳۹۱).

هر اقدام امنیتی باید مبتنی بر برآورد مخاطرات باشد. بازه زمانی پنج سال در اغلب اسناد راهبردی کشورها به‌عنوان بازه زمانی مناسب در نظر گرفته‌شده است. همکاری در تمام سطوح برای مدیریت مخاطرات امنیت داخلی برآمده از تهدیدات مجازی باید تقویت شود. در پایین‌ترین سطح، همکاری بخش خصوصی با نهادها و سازمان‌های دولتی قرار دارد. در سطوح بالاتر، همکاری‌های بین دستگاهی، همکاری بین دو یا چند کشور و درنهایت همکاری بین‌المللی قرار می‌گیرد که همگی مکمل یکدیگر خواهند بود و جایگزین یکدیگر نمی‌شوند. امروزه مهم‌ترین نوع براندازی، براندازی نرم است، همان‌گونه که مقام معظم رهبری بارها فرموده‌اند هدف اصلی دراین‌بین، مردم و ارزش‌های و باورهای آن‌ها است. تأثیر فضای مجازی به‌عنوان رسانه‌ای قوی و تأثیرگذار طیف وسیعی از متغیرهای اجتماعی و سیاسی را تحت تأثیر قرار می‌دهد. عمیق‌ترین لایه هر جامعه، هویت فردی، اجتماعی و ملی است که شکل‌گیری آن درازمدت و تدریجی است. رسانه‌های دیجیتال با تأثیر بر ارزش‌ها و باورها افراد هویت فردی و جمعی آن‌ها را دستخوش تغییر می‌کند. در سطح بعدی جذابیت و قدرت اقناع‌کنندگی که همان قدرت نرم است به‌شدت با فضای مجازی به‌عنوان یک رسانه عجین شده است. امروزه تصور افراد از یک پدیده می‌تواند با واقعیت فاصله داشته باشد و مهم‌ترین علت آن مدیریت اطلاعات و اخبار است. تقویت مشروعیت یک نظام سیاسی و مشروعیت زدایی از گروه‌های برانداز، به کمک رسانه‌ها از جمله رسانه‌های دیجیتال صورت می‌گیرد. بسیج نیروهای پراکنده و مدیریت آن‌ها جهت تحقق اهداف یک گروه یا نظام تنها از طریق شبکه‌سازی میسر می‌شود. از گذشته تاکنون از شبکه‌های حقیقی نظیر مساجد جهت بسیج نیروها استفاده‌شده است و امروزه این کارکرد به شبکه‌های اجتماعی مجازی منتقل‌شده است. بهره‌برداری از فضای مجازی به‌عنوان ابزاری جهت اطلاع‌رسانی و مدیریت بحران‌های سیاسی از دیگر توانایی‌های فن‌آوری اطلاعات و ارتباط است که در مواقع ضروری باید مدیریت شود. استفاده از ظرفیت‌های سلبی فضای مجازی نظیر فیلترینگ، مقابله با شایعه‌سازی و عملیات روانی در مواقع خاص می‌تواند از گسترش بحران‌های سیاسی–اجتماعی بکاهد.یکی از ابعاد مدیریت تهدیدات برآمده از فاوا بر امنیت داخلی، اقدامات اطلاعاتی است بازنگری در مفاهیمی مثل

تروریسم، جاسوسی، خرابکاری، براندازی، محرمانگی و حریم خصوصی در قرن حاضر امری ضروری است. تعاریف کلاسیک و موردپذیرش همگان دیگر کارایی ندارند. مرز میان جاسوسی و جمع‌آوری آشکار، تضارب آراء و براندازی نرم، هک و نفوذ با خرابکاری صنعتی و استفاده قانونی و یا سوءاستفاده از فضای مجازی برای مقاصد تروریستی واضح نیست و نیازمند تحقیقات، قانون‌گذاری و ایجاد اشتراک ادراک میان بازیگران عرصه امنیت داخلی است.امروزه مأموریت سرویس‌های اطلاعاتی تغییر کرده است و مقابله با خرابکاری در فضای مجازی، ارتقاء امنیت زیرساخت‌های حیاتی، پیشگیری و مقابله با سوءاستفاده از فضای مجازی برای اقدامات تروریستی، مبارزه با براندازی نرم، مقابله با جاسوسی مجازی و ایجاد ظرفیت‌های لازم برای بازدارندگی مجازی به دستور کار سازمان‌های اطلاعاتی اضافه‌شده است. ساختارهای سنتی سازمان‌های اطلاعاتی از چابکی لازم برای مدیریت محیط امنیتی بسیار متغیر کنونی برخوردار نیست(عصاریان، چین،۱۳۹۱).

عمر پدیده‌های امروزی بسیار کوتاه است لذا هیچ سازمانی با ساختار سلسله مراتبی و مبتنی بر شرح وظایف ثابت، توان رویارویی با تهدیدات نوظهور را نخواهد داشت. ایجاد سازمان‌های مجازی چابک، مبتنی بر شبکه‌های اطلاعاتی، ساختار خود سازمانده و بین‌رشته‌ای امری ضروری است.نقش منابع آشکار به‌واسطه تأثیر فناوری اطلاعات و ارتباطات به ۸۰٪ در میان منابع اطلاعاتی رسیده است. حتی منابع غیر آشکار نیز، به‌شدت از فناوری اطلاعات و ارتباطات متأثر شده‌اند. امروزه استفاده از ابزار بسیار قدرتمند داده‌کاوی برای تحلیل داده‌های انبوه امری جاافتاده در سازمان‌های اطلاعاتی است. استفاده از سلاح‌های مجازی برای حمله به دشمنان و یا بازدارندگی سایبری در سازمان‌های اطلاعاتی و امنیتی، ابزاری شناخته‌شده است و جای بسیاری از ابزارهای سنتی را گرفته است.

روش‌شناسی تحقیق:

در این تحقیق از روش آمیخته به‌صورت ذیل استفاده‌شده است که ابتدا از سازوکارهای روش نظریه مبنایی صرفاً جهت به دست آوردن مفاهیم (ابعاد، مؤلفه‌ها و شاخص‌ها مدیریت راهبردی تحولات) استفاده‌شده است و سپس نتایج به‌دست‌آمده را به شکل پرسشنامه بسته و نیمه‌باز به خبرگان ارائه نموده و نظر آن‌ها کسب گردیده است. به عبارتی بخش کیفی تحقیق کاملاً مبتنی بر

نظریه مبنایی است این کار با ایجاد جدولی از مفاهیم (گزاره‌های) استخراج‌شده از منابع مختلف اطلاعات اعم از اطلاعات کتابخانه‌ای در اسناد فارسی و انگلیسی، مصاحبه‌های عمیق، پنلهای خبرگی، مشاهدات مستقیم سازمان‌ها و نهادها و همچنین شرکت در اجلاس‌های داخلی و خارجی صورت گرفته است. تلاش شده است استخراج مفاهیم با در نظر گرفتن سؤالات اصلی و فرعی تحقیق صورت بگیرد. گزاره‌های هم مفهومی که در منابع مختلف تکرار شده‌اند به‌عنوان نشانه‌ای از اهمیت مفهوم در نظر گرفته‌شده است. حاصل بسط منابع به گزاره‌ها، جدولی پنج ستونی است که در ستون اول مشخصاتی از منبع، در ستون دوم گزاره‌های پدیده‌شناسی پنج متغیر اصلی(فناوری ارتباطات و اطلاعات، تروریسم، خرابکاری، براندازی، جاسوسی و تروریسم)، در ستون سوم تحولات برآمده (فرصت‌ها و تهدیدات) از فاوا بر تهدیدات چهارگانه امنیت داخلی (تروریسم، خرابکاری، براندازی، جاسوسی و تروریسم)، در ستون چهارم گزاره‌های مدیریتی ذکرشده در منابع و در ستون پنجم عناصر مدیریت راهبردی (ابعاد، مؤلفه و شاخص) استخراج‌شده است.

بعد از تهیه جدول فوق، کار دسته‌بندی مفاهیم هم‌خانواده و استخراج مفاهیم انتزاعی صورت گرفت که حاصل آن جدول دسته‌بندی مفاهیم به ابعاد، مؤلفه و شاخص‌ها است. درنهایت، گزاره‌ها در قالب ۷ بعد و ۳٤ مؤلفه، دسته‌بندی شدند و نتیجه‌ی آن مدل مفهومی ذیل است.

قسمت کمی تحقیق با تبدیل مدل مفهومی به سؤالاتی در دودسته صورت گرفته است در دسته اول، سؤالاتی در قالب طیف لیکرت مطرح‌شده است و از پرسش‌شوندگان خواسته‌شده است اعتبار ابعاد و مؤلفه‌های ادعاشده را تائید یا رد نمایند. در دسته دوم سؤالات که استخراج‌شده از نرم‌افزار سوپردسیژن است، مقایسه زوجی ابعاد و مؤلفه‌ها صورت گرفته است که حاصل آن رتبه‌بندی عناصر الگوی راهبردی مدیریت است.

جامعه آماری در این پژوهش عبارت‌اند از کلیه خبرگان و صاحب‌نظران کشور که در زمینه‌های ذیل دارای تخصص یا تجربه می‌باشند. فناوری اطلاعات و ارتباطات (فاوا)، حوزه‌ی امنیتی-اطلاعاتی[1] و مدیریت راهبردی

این افراد مسئولین و کارشناسان نهادهای امنیتی و اطلاعاتی، اعضاء هیئت‌علمی دانشکده‌های مرتبط، اعضاء سازمان‌های حفاظت اطلاعات، نیروهای مهم اطلاعات سپاه و بخش‌هایی از نیروی انتظامی(پلیس فتا) باشند در طول این تحقیق ازنظر ۱۱۰ نفر از متخصصین و

[1] Intelligence and Security

صاحب‌نظران استفاده‌شده است که دراین‌بین، با حدود ٤٥ نفـر از ایـن متخصصـین، مصـاحبه عمیق صورت گرفته است.

جدول۲: مدیریت راهبردی تحولات برآمده از توسعه فاوا بر امنیت داخلی

اقدامات اطلاعاتی	اقدامات اجتماعی- سیاسی	همکاری	ظرفیت سازی	ساختاردهی اجرایی و سازمانی	اقدامات فنی	قوانین و مقررات
مفاهیم اطلاعاتی	هویت سازی	همکاری‌های دو یا چند جانبه بین کشورها	تحقیقات	راهبردها و سیاست‌های کلان	تیم‌های پاسخگویی به حوادث رایانه-ای	قوانین و مقررات کیفری
ماموریت اطلاعاتی	قدرت نرم	همکاری بین دستگاهی	آموزش و تحصیلات تکمیلی	نقشه راه و طرح‌های پیاده سازی	استانداردها	مقررات و الزامات رسمی و حقوقی
ساختار سازمان و جامعه اطلاعاتی	مشروعیت زدایی	همکاری بخش خصوصی و دولتی	افراد، مشاغل و سازمان‌های مورد تأیید	سازمان‌ها و نهادهای مسئول اجرا	اعتبار سنجی و اعطای گواهی	قوانین و مقررات کیفری و حقوقی بین‌المللی
منابع اطلاعاتی	شبکه سازی	همکاری بین‌المللی	مانورهای امنیتی	نهادهای نظارتی و کنترلی	فناوری‌های بومی و اختصاصی	
ابزار اطلاعاتی	بحران های سیاسی		رونق کسب و کار فاوا		سازوکارهای تحلیل مخاطرات	
					سامانه‌های مراقبتی و هشداردهی	

تجزیه‌وتحلیل داده‌ها:

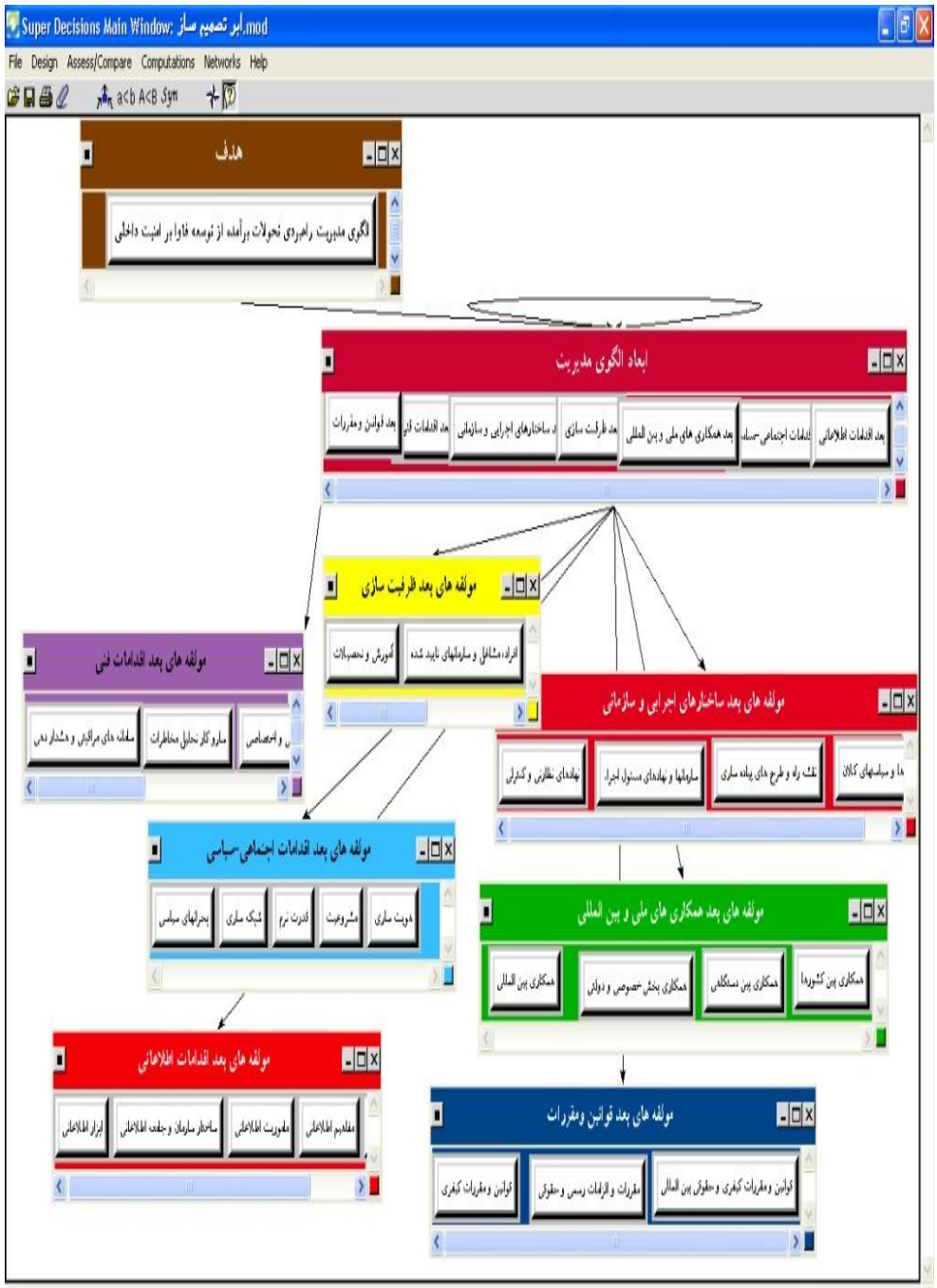
ردیف اول مدل مفهومی که شـامل اقـدامات اطلاعـاتی، اقـدامات اجتمـاعی- سیاسـی، همکـاری، ظرفیت‌سازی، ساختارهای اجرایی و پیاده‌سازی، اقدامات اطلاعاتی و قوانین و مقررات است ابعـاد

هفتگانه مدیریت تحولات برآمده از توسعه فاوا بر امنیت داخلی است. در ذیل هر بعد مؤلفه‌های آن‌ها ذکرشده است که درمجموع ۳٤ مؤلفه ارائه گردید. برای هر مؤلفه نیز دو شاخص از جدول کدگذاری انتخاب‌شده است. همه عناصر این مدل، از طریق توزیع پرسشنامه طیف لیکرت مورد تائید جامعه آماری قرار گرفت.

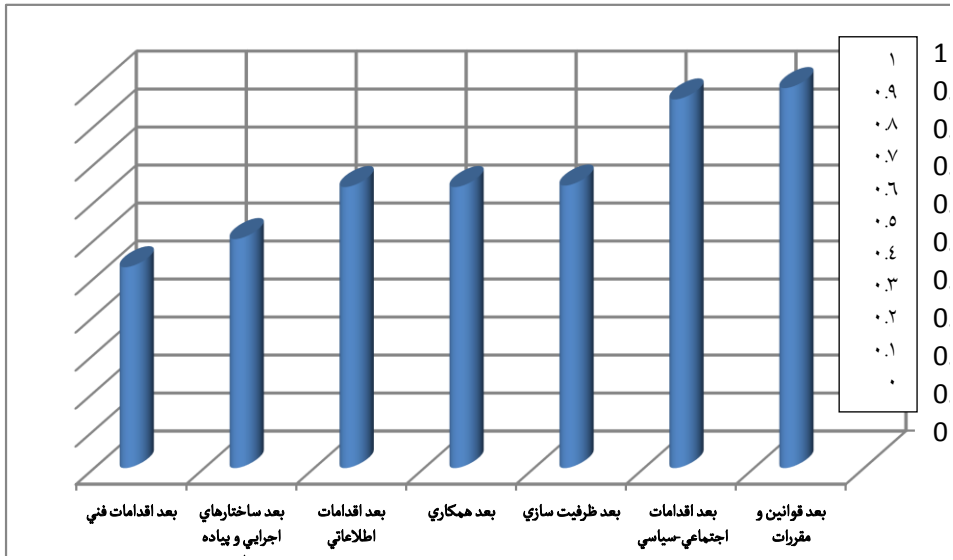
جدول ۳- نتایج پرسشنامه در خصوص ابعاد الگو

ردیف	پرسشنامه	کاملاً موافقم	موافقم	نظری ندارم	مخالفم	کاملاً مخالفم
۱	"اقدامات اطلاعاتی"به‌عنوان یکی از ابعاد مدیریت راهبردی امنیت داخلی	71.4	28.6	0	0	0
۲	"اقدامات فنی" به‌عنوان یکی از ابعاد مدیریت راهبردی امنیت داخلی	81	19	0	0	0
۳	"ساختارهای اجرایی و سازمانی" به‌عنوان یکی از ابعاد مدیریت راهبردی امنیت داخلی	47.6	42.9	9.5	0	0
٤	"همکاری" به‌عنوان یکی از ابعاد مدیریت راهبردی امنیت داخلی	71.4	23.8	4.8	0	0
٥	"ظرفیت‌سازی" به‌عنوان یکی از ابعاد مدیریت راهبردی امنیت داخلی	47.6	38.1	14.3	0	0
٦	"قوانین و مقررات" به‌عنوان یکی از ابعاد مدیریت راهبردی امنیت داخلی	57.1	42.9	0	0	0
۷	"اقدامات سیاسی - اجتماعی" به‌عنوان یکی از ابعاد مدیریت راهبردی امنیت داخلی	42.9	57.1	0	0	0

اولویت‌بندی ابعاد از طریق تحلیل پاسخ پرسشنامه‌ی حاصل از نرم‌افزار سوپردسیژن و بر مبنای مدل صفحه بعد به دست آمد.



شکل ۲- مدل نرم‌افزار تصمیم گیری متعالی



نمودار ۱- اولویت‌بندی ابعاد الگو

نتیجه‌گیری و پیشنهاد:

مهم‌ترین نتیجه این تحقیق مدل مفهومی آن است زیرا حاصل تحلیل حجم بسیار زیادی از اطلاعات جمع‌آوری‌شده از منابع مختلف است. در این مرحله کلیه اطلاعات حاصل از منابع مختلف اطلاعات یعنی اطلاعات کتابخانه‌ای(مرور و فیش بندی ۸۰۰۰ صفحه متن فارسی و انگلیسی و ترجمه بیش از ۳۰۰ صفحه متن انگلیسی) ، مصاحبه(۱۱۰ مصاحبه با افراد و سمینار گروهی)، پنل‌های خبرگی(٦٤ جلسه)، شرکت در اجلاس‌های داخلی و خارجی(حضور در سه اجلاس اروپایی) و بررسی‌های میدانی(حضور در ۳۰ سازمان و نهاد دولتی) در قالب جدولی دسته‌بندی و کدگذاری شد. فرایند جمع‌آوری اطلاعات تا زمان رسیدن به اشباع نظری نسبی (فقدان مطالب جدید و تکراری شدن اطلاعات) پیش رفت. در جدول کدگذاری، پنج ستون وجود دارد. ستون اول نشان‌دهنده منبع اطلاعات است. در ستون دوم متغیرهای پنجگانِ تحقیق یعنی توسعه فاوا، تروریسم، خرابکاری، براندازی و جاسوسی نوین، پدیده‌شناسی شده‌اند. در ستون سوم تحولات(فرصت‌ها یا تهدیدات) برآمده از توسعه فاوا بر تروریسم، خرابکاری، براندازی و جاسوسی نوین موردبررسی قرارگرفته است. در ستون چهارم روش‌های مدیریت تحولات برآمده از توسعه فاوا بر ابعاد چهارگانه امنیت داخلی(تروریسم، خرابکاری، براندازی و جاسوسی نوین)

موردبررسی قرارگرفته است. در ستون پنجم عناصر اصلی مدیریت راهبردی(ابعاد، مؤلفه و شاخص‌ها) از منابع استخراج و ذکر گردیده است.

در مدل مفهومی عناصر اصلی مدیریت راهبردی تحولات برآمده از توسعه فاوا بر امنیت داخلی ذکرشده است بعلاوه روابط بین آن‌ها نیز بیان‌شده است در مرحله بعدی می‌توان اولویت‌بندی این عناصر را ازنظر جامعه آماری مشاهده نمود. همان‌گونه که در شرح روش فرآیند تحلیل شبکه‌ای ذکر شد بسیاری از ابعاد و مؤلفه‌های ارائه‌شده ترکیبی می‌باشند و با یکدیگر همپوشانی‌هایی دارند. البته هریک از ابعاد و مؤلفه‌ها، تأثیر مدیریتی یکسانی بر تک‌تک تهدیدات ندارند و از بار مدیریتی متفاوتی برخوردار می‌باشند. مثلاً بعد مدیریتی "اقدامات اجتماعی- سیاسی" بیشتر متوجه براندازی است و بعد "اقدامات فنی" بیشتر گرایش به مدیریت خرابکاری دارد. بااین‌حال در بسیاری از موارد تهدیدات چهارگانه هم‌راستا شده و عوامل، ابزار و اهداف یکسانی خواهند داشت.

پیشنهادها کاربردی:

- ایجاد مرکز سنجش ملی برای تعیین وضعیت امنیت داخلی با در نظر گرفتن شاخص‌های مطرح‌شده در این تحقیق.
- شناسایی متولیان قانونی ابعاد مختلف امنیت داخلی و در صورت لزوم ایجاد ساختارهای نوین.
- ایجاد هماهنگی‌های لازم بین بازیگران مختلف امنیت داخلی از طریق وضع قوانین و مقررات فرادستگاهی.
- تقویت جایگاه شورای عالی فضای مجازی به‌عنوان نهاد ارشد رصد، سیاست‌گذاری و مدیریت کلان تحولات برآمده از توسعه فاوا بر امنیت داخلی.

پیشنهادها پژوهشی:

- تدوین راهبرد ملی در حوزه‌های ضد تروریسم، ضد براندازی، ضدخرابکاری و ضد جاسوسی توسط وزارت اطلاعات و جامعه اطلاعاتی به‌عنوان یک طرح پژوهشی ملی.
- تدوین راهبرد کلان نظام در حوزه تحولات برآمده از توسعه فاوا بر تروریسم، خرابکاری، براندازی و جاسوسی. در تحقیق حاضر، عناصر اساسی این راهبرد و اولویت‌بندی آن‌ها مشخص‌شده است به کمک این عناصر(ابعاد، مؤلفه‌ها و شاخص‌ها)

می‌توان راهبرد کلان در حوزه تحولات برآمده از توسعه فاوا بر امنیت داخلی جمهوری اسلامی ایران را تدوین نمود.

- تدوین سیاست‌های دستگاهی در حوزه مدیریت تحولات برآمده از توسعه فاوا بر تروریسم، خرابکاری، براندازی و جاسوسی به کمک عناصر ارائه‌شده در این تحقیق.
- به‌روزرسانی سند فتا با در نظر گرفتن کاستی‌های موجود در این سند نظیر فقدان بخش‌های اجرایی و نظارتی، نگاه تک‌بعدی به تهدیدات برآمده از توسعه فاوا بر امنیت داخلی(صرفاً خرابکاری در زیرساخت‌های حیاتی) و بی‌توجهی به تهدیدات نوین براندازی، تروریسم و جاسوسی در فضای مجازی.

منابع و مآخذ:

منابع فارسی:

- امام خامنه‌ای(مدظله العالی) (۱۳۸۹)، سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات، قابل‌دسترس در:http://www.khamenei.ir و http://www.csri.ac.ir/618
- حافظ نیا، محمدرضا (۱۳۹۰)، جغرافیای سیاسی فضای مجازی، سمت، تهران.
- طیب، علیرضا(۱۳۸۲)، تروریسم، تاریخ، جامعه‌شناسی، گفتمان، حقوق، نشر نی، تهران.
- کاستلز، مانوئل(۱۳۸۰) ، عصر اطلاعات، اقتصاد، جامعه و فرهنگ، ترجمه حسن چاوشیان و همکاران، انتشارات طرح نو، تهران.
- گوهری مقدم، ابوذر(۱۳۹۰) ، رسانه‌های اجتماعی و انقلاب‌های اخیر خاورمیانه، ارائه مدل مفهومی، رسانه، شماره پیاپی ۸۵.
- عصاریان نژاد، حسین،الگوی مدیریت استراتژیک تحولات و تغییرات فناورانه در امنیت داخلی کشور، مجموعه سخنرانی های تخصصی در داعا ۲-۱۳۹۱، تهران

منابع انگلیسی:

- Albrow, M. (1990), Globalization, Knowledge & Society, London.
- Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A.,Sastry, S.S.(2009). Challenges for Securing Cyber.
- Chen, Hsinchun, (2012), Dark Web, Exploring and Data Mining the Dark Side of the Web, Integrated Series in Information Systems Volume 30, Springer Science+Business Media, LLC 2012.
- Clay, Wilson (2010), Cyberterrorism: in Theory or in Practice, Defenses Against Terrorism Review, Vol.3, no.2.
- Conway, M.(2002). Reality Bytes: Cyberterrorism and Terrorist Use of the Internet, available at:
- http://www.firstmonday.org/issues/issue7_11/conway/index.html.
- Denning, D. (1999), Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Washington D.C.: Nautilus Institute, available at: http://www.nautilus.org/info-

Policy/workshop/papers/ denning.html.

- Gartner (2014), Top 10 Strategic Technology Trends For 2014 available at: http://www.forbes.com/sites/peterhigh/2013/10/14/gartner-top-10-strategic-technology-trends-for-2014/#undefined.
- Giddens, A. (1990), The Consequences of Modernity, Standford University.
- Global Cybersecurity Index (2014), available at:
- http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.
- PWC(2014), The convergence of everything digital, Avaialable at:
- pwc.com/cybersecurity
- The guardian (2013), Boundless Informant: the NSA's secret tool to track global surveillance data, available at:
- http://www.guardian.co.uk/world/interactive/2013/jun/08/nsa-boundless-informant-data-mining-slides.
- Verizon (2014), data breach investigation report, available at:
- www.Verizon.com.