سامانه های حفاظت اطلاعات در نبردهای آینده

ابراهیم رحیمی [1]

چکیده

حفاظت اطلاعات ازجمله سازکارهای نیروهای مسلح برای حفظ اقتدار و اعتبار امنیت کارکردهای نیروهای مسلح تلقی می گردد، تغییرات ناگهانی قطب های موجود و بهم ریختن وضعیت دوقطبی (بلوک شرق و غرب). کشورها را بر آن می دارد تا پیش از وقوع حوادث فناورانه مروری برآینده داشته باشند، این پژوهش در ارتباط با سامانه های حفاظت اطلاعات در نبردهای آینده به منظور پیش بینی منطقی و پیشنهاد راهبردی متناسب با محیط امنیتی موجود و تهدیدات آینده تنظیم گردیده است.

اگرچه این پیش بینی در دوران پیشرفت پرشتاب تکنولوژی و دگرگونی متناسب با زمان و فضا بویژه در عملیات نظامی کار ساده ای نمی باشد ولی این مقاله با یک تحقیق کتابخانه ای و با دسترسی محدود و مبتنی بر حقایقی پیرامون فرضیات حاکم بر محیط جنگهای زمینی آینده از تجربیات عملی و مدارک به دست آمده در جنگ خلیج فارس و منطقه کوزوو، نشان می دهد که می توان به نیّات دشمنان آینده و بررسی تهدیدات آنها پی برد، در این راستا تلاش می شود ضمن ارائه چارچوب نظری، برخی از الگوهای مطرح در انتخاب سامانه های حفاظت اطلاعات و برخورد با فرصت ها و تهدیدات (نبردهای آینده) را بر می شماریم و چالش های فراروی نیروهای مسلح را مورد بررسی قرار دهیم تا بتوانیم راه کارهای مناسب جهت اعتلای اعتبار و مطلوبیت سازمان حفاظت اطلاعات را ارائه کنیم.

واژه های کلیدی

تهدیدات،فرصت ها،سامانه،محیط امنیتی،حفاظت اطلاعات،اطلاعات.

---

۱ - دانشجوی دانشگاه دفاع ملی

مقدمه

آینده اساساً فرصتی برای یک کشور یاکشورهایی است که در عرصه سیاست جهانی، پیروزی بدون خونریزی را، بتوانند با برتری آرمان های خود درآمیزند، هر چند که این فرصت همیشگی نخواهد بود. با این که هیچ یک از دستاوردهای بشری جاودانه نیست، اما در چند سال آینده مثلاً بیست وپنج سال آینده، کشورها به منظور بیمه کردن دستاوردهای حاصل از موفقیت های خود به همراه مردم آن کشور در جهانی که پیچیده تر می شود وارد میدان خواهند شد. به فرض این که کشوری با همه توانایی هایی که دارد، در بیست و پنج سال آینده نخواهد توانست بر این جهان پهناور تسلط و نظارت پیوسته ای داشته بلکه در یک وضعیت نسبتاً ایده آل و در حال پیشرفت باقی مانده به راه خود ادامه دهد.

تاریخ هنوز راه دور و درازی در پیش دارد، گوناگونی فرهنگ های بشری همچنان پابرجاست و دلبستگی و تمایل به قدرت و نیز جاذبه های شورانگیز احساسات همانندگذشته در زندگی و حیات سیاسی ملتها جای خواهند داشت. بنابراین گونه ای پراکندگی قدرت، اما نه الزاماً از نوع کلاسیک آن در برابر ما قرار گرفته است، بدین اوصاف سامانه های حفاظت اطلاعاتی می بایستی با پیچیدگی خاصی نه تنها همپای تغییرات بلکه پیشتر و هوشیارتر تهدیدات را کشف و ضمن تشخیص سمت و سوی آن متناسب با شدت تهدید اقداماتی پیشگیرانه پیشنهاد بدهند و با هماهنگی هرچه تمام تر در جهت نهادها و واحدهای درونی گام بردارند که در بخش های آتی به آن پرداخته خواهد شد.

بیان مساله

به طور کلی برای فهم سیاست های حفاظت اطلاعاتی اولاً می توانیم به تحلیل کارکردها و مسایل ناشی از سیاست ها بپردازیم و بررسی کنیم که چه سازمانها و گروه هایی چه رفتاری را چگونه در حوزه امنیت و حفاظت اطلاعات یا اطلاعات انجام داده اند. ثانیاً برساختار، فرآیندها و منابع سازمان ها و گروه ها برای تبیین تصمیمات تأکید گردد و بررسی نحوه تشخیص و تعریف مسائل امنیتی، چگونگی درک و تعیین موقعیت ها و راه کارها که چگونه طرح و ارزیابی می شوند، مورد توجه قرار گیرد.

نحوه دستیابی به بهترین سامانه ها چگونه است؟ چگونه ذهنیت ها و تصورات و باورها بر سامان ها و کارکردها تأثیر می گذارد؟ نقش تأثیرگذار شخصیت ها به عنوان موتور محرک در ساختارها و فرآیندها و تأثیر ارتباطات رسمی و غیررسمی و نحوه ارتباط ساختارها بر فرهنگ سازمانی و مانند آن مورد توجه قرار داده می شود.

ثالثاً محیط عینی و ذهنی امنیتی و تأثیر آن در سیاست حفاظت اطلاعات بایستی مورد توجه قرار گیرد. در حوزه ذهنی شخصیت های تصمیم ساز و تصمیم گیرنده با باورها، هنجارها، تمایلات، تصورات و ارزش های مختلفی حضوردارند و مطالعه روان شناختی سیاست سازی حفاظت اطلاعات جنبه های بسیار مهم به شمار می آید، همچنان که مطالعه زمینه های تهدیدات، آسیب ها، فرصت ها و اولویت ها مورد تأکید قرار می گیرد.

ضرورت تحقیق

انقلاب اطلاعاتی چهره جنگ های امروزین را دگرگون کرده است، دیگر ارتش های عظیم در سنگرها به جنگ های فرسایشی اشتغال ندارند بلکه جای آنان رانیرو های مکانیزه کوچکی گرفته اند که براساس اطلاعات لحظه به لحظه دریافتی از ماهواره ها و حسگرهای درون میدان نبرد باسرعتی شگفت آور به نقاط استراتژیک دشمن یورش می برند، برنده در نبردهای آینده کسی است که بتواند با استخراج دقیق ترین اطلاعات و تحلیل به موقع آنها نیروهای خودی را به سمت نیروهای دشمن هدایت نماید و پیروزی را نصیب نماید، لذا کسب و جمع آوری اطلاعات و حفاظت از آن یکی از ضروریات می باشد در غیر این صورت دشمن هر چه سریعتر به اطلاعات دسترسی پیدا نموده با غافلگیری، هواپیماها و موشک ها را در آشیانه ها زمین گیر نموده، ارتباط فرماندهان را در تمام رده های فرماندهی قطع و فرامین شبیه سازی شده ای جایگزین خواهد نمود.

اهداف تحقیق

اهداف، نیازها و مطلوبی است که تعیین صحیح آنها در قالب کوتاه مدت، میان مدت و بلند مدت با تبیین نتایج مطلوبی که کارکنان، بخش ها و سامانه های حفاظت اطلاعاتی می بایستی در جهت آن کار کنند انجام می شود.

سؤال تحقیق

چه عواملی نقش اساسی در سیاست ها و سامانه های حفاظت اطلاعاتی دارند؟

در پاسخ به این پرسش اهتمام به سطوح تحلیل و ماهیت سازمان حفاظت اطلاعات در سطح خرد، اصلی ترین عامل رفتار و کارکرد سازمانی را باید در سطح خرد جستجو نمود و در سطح کلان با نگرش سیستمی، محیط امنیتی را عامل مؤثر بر سیاست های حفاظت اطلاعات شناخت. به عبارتی مهم ترین عامل رفتار سازمان های حفاظت اطلاعاتی محیط امنیتی است که بیشترین تأثیر را بر سیاست های حفاظتی دارا است واین تأثیر می تواند در حدی باشد که نقش شکل دهنده و پدیدآورنده سیاست های جدید حفاظتی باشد.

فرضیه تحقیق

۱ - اگرچه تکنولوژی در خدمت اطلاعات درآمده ولی به نظر می رسد که علوم و فنون با ایجاد موانعی باعث می شوند اطلاعات شدیداً مراقبت شده و جمع آوری وکشف تهدید مواجه با اشکال گردد.

۲ - پرورش اخبار به علت وسعت موضوعات فریبنده و ارزیابی دقیق منابع گوناگون که از کنترل ستاد خارج است، از مراحل پیچیده اطلاعات و حفاظت اطلاعات می باشند که مستلزم کارشناسان ورزیده ای است.

روش اجرای تحقیق

پژوهش در زمینه سامانه های حفاظت اطلاعات در نبردهای آینده به منظور رعایت اصول حفاظتی به صورت کتابخانه ای صورت گرفته است، در کتابخانه ها نیز معمولاً کتب اطلاعاتی که حاوی حقایقی باشد به ندرت یافت می شوند. آنچه که موجود است نویسندگان بیشتر پیش بینی نموده اند. بنابراین انتخاب نوشتجاتی که در این تحقیق مفید واقع شود به دشواری صورت گرفته است.

بدین جهت با ترجمه کتاب های مستند خارجی سعی شده است که حقایق استخراج و به رشته تحریر درآید.

غالب این کتب را کارشناسان که سال های متمادی در این حرفه خدمت کرده اند و دارای تجربیات وسیعی بوده اند، تألیف نموده اند. لذا نسبت به امور اطلاعاتی صاحب نظر هستند. به علت این که ممکن است کتب مزبور خوانندگانی نداشته باشد، نسبت به ترجمه آنها اقدامی به عمل نیامده است.

تعاریف و مفاهیم اساسی در تحقیق

۱ - تعریف اطلاعات: اخبار پرورش یافته را اطلاعات گویند.

۲ - امنیت ملی: عدم تهدید به ارزش های اساسی و علایق و مصالح ملی در یک کشور، حفاظت یک ملت در مقابل انواع تجاوزات خارجی،جاسوسی، عملیات خصمانه، براندازی و نفوذهای دشمنانه.

۳ - تعریف حفاظت اطلاعات: عنصری از عملیات نظامی است که وظیفه آن خنثی کردن یا از بین بردن تأثیر سیستم های اطلاعاتی دشمن است.

محیط تحقیق

جامعه اطلاعاتی که بتواند حوزه این تحقیق در آینده مدنظر قرار گیرد به علت محدودیت

زمانی و عدم دسترسی به منابع آن موجود نبود لذا در یک محیط فرضی و شبیه سازی شده در آینده، با منابع کتابخانه ای محیط مورد تحقیق قرار گرفته است.

محدودیت های تحقیق

با توجه به طبقه بندی موضوع مورد بررسی (وضعیت کنونی و عدم امکان مقایسه)، تنها روش جمع آوری اطلاعات، کتابخانه ای امکان پذیر بوده است.

ادبیات نظری تحقیق

تحلیل سیاست های حفاظت اطلاعات به لحاظ ماهیت پنهان سازمانی، یک رشته گویا در مباحث تئوریک نیست و تاریخ قابل دسترسی ندارد. لیکن در نظریه های مرتبط با سیاست، آنچه مورد بررسی قرار می گیرد این است که چگونه بازیگران ونقش آفرینان راه هایی را برای تحلیل موقعیت خود انتخاب می کنند، اهداف خود را تعیین ودر مورد آنها تصمیم می گیرند.

در واقع، اهداف سیاست حفاظت اطلاعات، ابزار آن، فرآیند تصمیم سازی و تصمیم گیری، تجزیه و تحلیل قدرت سازمانی و آثار محیط امنیتی بر سیاست های حفاظت اطلاعات مورد بررسی قرار می گیرد.

برای رسیدن به نظریه هایی جهت سیاست حفاظت اطلاعات و برای فهم کارکردها و رفتارهای حفاظتی- اطلاعاتی سرویس های مختلف به نحو علمی، نیازمند موارد مهمی هستیم از جمله:

۱ - اطلاعات قابل مقایسه عملکرد سرویس های حریف و هدف و به عبارت دیگر بررسی نتایج عملکرد سرویس های حفاظت- اطلاعاتی ضروری است.

۲ - مطالعه ساختار، فرآیندها، شخصیت ها و فرهنگ سازمان های حریف و هدف و سازمان های خودی برای فهم چرایی کارکرد سازمان ها، ضروری است.

۳ - مطالعه زمینه ها و بُعد ذهنی محیط امنیتی.

فهم نتایج حاصله از سیاست های حفاظت اطلاعاتی نیازمند فهم محیط روانی و تأثیری که اقدامات برادراک افراد و بخش های تصمیم ساز و تصمیم گیرنده در سازمان های حفاظت اطلاعاتی دارد می باشد.

۴ - شناخت تصمیم سازان و تصمیم گیران سیاست های حفاظت اطلاعاتی در فهم ماهیت تصمیم هایی که می گیرند بایستی حائز اهمیت قرار گیرد و از ویژگی های آنان برای نظریه سازی استفاده گردد.

۵ – فهم فرآیند سامانه ها ، تصمیم سازی و تصمیم گیری سیاست های حفاظت اطلاعاتی به میزان فهم نتایج حاصله از سیاست های حفاظت اطلاعاتی اهمیت دارد.

۶ – رویکردهای مطالعه سیاست های حفاظت اطلاعاتی:

رویکردهایی که در بررسی و مطالعه سیاست های حفاظت اطلاعاتی قابل طرح می باشد عبارتند از:

۶-۱ رویکرد روانشناختی:

در سازمان های حفاظت اطلاعات نظامی، سیاست های حفاظت اطلاعاتی معادل تشخیص و تفکر رؤسای سازمانی است. فلذا براین اساس برای فهم سیاست های یک سازمان حفاظت اطلاعاتی در هر کشوری شناخت ویژگی های رؤسا و مدیران اصلی آن ضروری است و متغیرهای تأثیرگذار دیگر از اهمیت درجه اول برخوردار نیستند، سیاست های سازمانی مساوی با ارزش ها باورها و تصمیم گیری رؤسا بدون تأثیر محیط امنیتی (عینی و ذهنی) است.

۶-۲ رویکرد انفعالی:

سیاست های حفاظت اطلاعاتی در این رویکرد بازتاب و انعکاس عملکرد و سیاست های سرویس های حریف و هدف است، این گونه سیاست ها از پویایی درونی و استقلال برخوردار نیست.

۶-۳ رویکرد پیشتاز:

در این رویکرد سیاست های حفاظت اطلاعاتی دارای استقلال از محرک های محیط امنیتی و مبتنی بر پویایی های سیستم امنیتی نظام هستند و به نحو دقیق و طی فرآیندهای علمی شکل می گیرند.

عوامل مختلف داخلی و خارجی در محیط امنیتی کاملاً مورد توجه قرار می گیرد و حتی عوامل روان شناختی محاسبه می گردد.

در مطالعه و سیاست سازی تمایل به رویکرد اول ودوم و کم توجهی به رویکرد سوم اثر بخشی سازمانی را دچار تردید می نماید و خارج شدن از چارچوب علمی و پرداخت ایدئولوژیک و غیر تئوریک به سیاست ها، سازمان و کارکردها را دچار آسیب می نماید.

سیاست های حفاظت اطلاعاتی بارویکرد غلط به شکل توصیفی و تبلیغی، متلّون و فلسفی نمایان می گردد.

مطالعه سیاست های حفاظت اطلاعات همواره با موانع اساسی روبروست که برخی از

آنها عبارتند از:

– سیاست های حفاظت اطلاعات حوزه های انحصاری و با دسترسی محدود محسوب می گردد و طرح عمومی آن افشای اسرار طبقه بندی تلقی خواهد شد.

– سیاست های حفاظت اطلاعاتی در کشور غیر متمرکز و متفرق است.

– امکان دسترسی به اطلاعات ومنابع تصمیم گیران با دشواری همراه است و بعضاً غیر ممکن می باشد.

– ماهیت سیاست گذاری در این حوزه با پیچیدگی و اعمال قدرت توأم است و بازشناسی سیاست ها هزینه خواهد داشت.

– اولویت های اساسی و عمده سیاست های حفاظت اطلاعاتی در هر حوزه مبتنی بر زمان و مکان متفاوت با یکدیگرند.

– ابهام و کلی گرایی و بی سیاستی، سیاستی سابقه دار و مورد استفاده در این حوزه است.

در نتیجه این موانع، اهتمام لازم به این بحث مهم صورت نمی گیرد و مطالعات علمی دقیق و مؤثر به ندرت انجام می شود.

طرح اولویت های برتر در سیاست های حفاظت اطلاعاتی جهت توجه به چالش های موجود ضروری است و به نظر می رسد سازمان های حفاظت اطلاعاتی با چند مسأله اساسی مواجه اند.

اول مسأله اصلاح ساختار و توسعه حرفه ای سازمانی است.

دوم مسأله امنیت و منافع ملی است که حفظ منافع نیروهای مسلح مقدمه این مهم می باشد، و سازمان های حفاظت اطلاعات به عنوان مجموعه ای تخصصی باید از نیروهای مسلح که مدافع نظام است دفاع کند و کلیه سیاست ها و خط مشی های خود را در این راستا جهت دهی کند.

سوم مقابله با سرویس های اطلاعاتی آمریکا و اسرائیل و متحدین آن به عنوان سلطه طلب درمنطقه و نظام بین الملل، این مسائل در شرایطی کاملاً متغیر در پیش روی ما است و دگرگونی های اطراف ما موجب تغییر در اهداف، ابزار،فرآیندها و سامانه امنیتی می گردد و آثار متنوعی را بر جای می گذارد. اهداف سازمانی نیازها و مطلوب سازمان و ابزارها و تکنیک ها بیانگر مقدورات و امکانات سازمانی هستند و سامانه ای که در واقع محیط امنیتی را در بر می گیرد بر تعیین اهداف و دسترسی به ابزارها تأثیر دارد. در این بحث موضوع

مهم این است که میزان و نحوه تغییر و تحول در اهداف و ابزارها درشرایط امنیتی کنونی تعیین گردد و چنانچه این مهم انجام پذیرد می توانیم مدعی باشیم که سیاستگذاری حفاظت اطلاعاتی دارای پویایی است و از روزمره گی و ایستایی خارج شده است.

پیوند ساختاری تعریف شده بین اطلاعات و حفاظت اطلاعات امری الزامی و محتوم است و اصالتاً این دو بخش غیر قابل تفکیک اند واگر در تفکیک از یکدیگر عمل کنند در راستای تأمین منافع امنیت ملی حرکت نکرده اند و به عبارتی منافع قشری و صنفی را بر مصالح ملی ترجیح داده اند.

پیوند ساختاری مؤثر و کارآمد مستلزم شرایط و مقدماتی است که بایستی مورد توجه قرار گیرند.

از جمله مسائل مهم در مباحث امنیتی این است که چه عواملی نقش اساسی در سیاست های حفاظت اطلاعاتی دارند؟

در پاسخ به این پرسش اهتمام به سطوح تحلیل و ماهیت سازمان حفاظت اطلاعات در سطح خرد، اصلی ترین عامل رفتار و کارکرد سازمانی را باید در سطح خرد جستجو نمود و در سطح کلان بانگرش سیستمی، محیط امنیتی را عامل مؤثر بر سیاست های حفاظت اطلاعات شناخت. به عبارتی مهم ترین عامل رفتار سازمان های حفاظت اطلاعاتی محیط امنیتی است که بیشترین تأثیر را بر سیاست های حفاظتی داراست و این تأثیر می تواند در حدی باشد که نقش شکل دهنده و پدید آورنده سیاست های جدید حفاظتی باشد.

در این راستا چنانچه سازمان های حفاظت اطلاعات بی توجه به تحولات محیط امنیتی دچارعادت و روزمره گی شوند و تغییر و تحولات را نادیده بگیرند به نقط ها ی می رسند که باید تغییرات بنیادی در ساختار، فرآیندها، فرهنگ سازمانی و دیگر زمینه های برجسته سازمانی را در زمانی کوتاه و با شتاب تند تجربه کنند و به جای پیش بینی و تحولات برنامه ریزی شده با ریسک و خطر پذیری هزینه های کلان و خسارات جبران ناپذیری را باعث گردند.

محیط امنیتی و استراتژی های سازمانی بیشترین اثر را برفرهنگ سازمانی بر جای می گذارد. و فرهنگ سازمانی فضا و بستری است که سازمان برای دستیابی به کارآمدی در مقابله با ناامنی ها و درک محیط امنیتی به آن نیاز دارد.

پیش بینی، پیشگیری، تجسس، شناسایی و خنثی سازی از الزامات کارآمدی سازمان های حفاظتی است و این فرهنگ سازمانی است که باید این قدرت و توان را

فراهم سازد و این عملی نیست مگر آن که ارتباط خردمندانه ای میان ارزش ها و باورها از یک سو و استراتژی ها و محیط امنیتی از سوی دیگر فراهم گردد. به عبارت دیگر سازمان نیازمند فرهنگی است که کارکنان و بخش های مختلف را برای رویارویی و پاسخگوئی به محیط امنیتی آماده نماید.

۷ - تقسیم بندی محیط های امنیتی

محیط امنیتی بنا به (بافت) و بستر آرام، ساده و یا پیچیده ای که دارد قابل طبقه بندی است.

مؤلفه های این طبقه بندی شامل، پیچیدگی محیط، تنوع سازمان های اطلاعاتی کشورهای حریف و هدف، میزان تغییر و تحول و نامعلومی در محیط با قابلیت پیش بینی، می تواند باشد.

مشخصات کلی و انواع محیط می تواند به شرح زیر باشد:

الف- محیط متلاطم و ناامن

ب- محیط ناآرام و حضور فعال حریف

پ- محیط نسبتاً آرام با پیچیدگی زیاد

ت- محیط آرام و با ثبات

۱--۷محیط متلاطم و ناامن و دشوارترین موقعیت:

در این شرایط حضور گروه ها و سازمان ها موجد ناامنی فراوان و خودجوش است و ائتلاف و اتحادسازمان ها و گروه ها علیه سرویس های خودی قوی است. در این شرایط مجهولات برای سازمان مجهول است وعلم بروجود مسائل امنیتی وجود ندارد.

۲-۷ - محیط ناآرام:

پیچیدگی بیش از دو محیط بعدی است و محیط دچاربحران است و دشمن در مقابل حرکات تاکتیکی و استراتژیکی سازمان واکنش نشان می دهد و ما را دچار انفعال و عکس العمل می کند.

فشار برروی تصمیم گیرندگان بسیار سنگین است، اما استراتژی و حرکات استراتژیکی همچنان اهمیت دارد. در این محیط دشمن مسلط عمل می کند وبه نحو آفندی و فعال برای رویارویی و خنثی نمودن عملیات سازمان اقدام می نماید. عکس العمل های حفاظتی و ممانعتی افزایش می یابند و سازمان های اطلاعاتی از بستر ها و امکانات محیط محروم می گردند.

۳-۷ - در محیط نسبتاً آرام و پیچیده:

فرصت ها و تهدیدات با یکدیگر پیوند خورده و توأم با هم عمل می کنند و توزیع این دسته بندی ها در محیط یکنواخت نیست و تلاش برای استفاده از فرصت ها همواره توأم با خطر برخورد با تهدیدات است و فاصله گرفتن از تهدیدات معادل از دست رفتن فرصت ها است، استراتژی و حرکات استراتژیکی اهمیت بیشتری دارند. طرح ها و اولویت ها باید به دقت تنظیم شوند و نیروها باید حرفه ای و با قابلیت های بالا تلاش نمایند.

۴-۷ - در محیط آرام و با ثبات:

فرصت ها و تهدیدات به طور یکنواخت در محیط پراکنده است و برخورد با آنها برحسب اتفاق خواهد بود. سازمان براساس آزمون و خطا عمل می کند.

حرکات تاکتیکی از اهمیت بیشتری برخوردار است و تلاش برای به دست آوردن امتیاز و استفاده از فرصت ها بدون خطرپذیری مسأله اصلی سازمان است.

۸ - شرح نمونه ای از نبردهای امروزی که بی ارتباط با آینده نمی باشد:

۱-۸ - جنگ در عصراطلاعات: [فن آوری اطلاعات امنیت ص ۲۲]

در طول تاریخ، با پیشرفت تکنولوژیک، نظریات نظامی، سازمان ها و استراتژی آن دائماً تغییر یافته به پیش رفته است. صنعتی شدن در جنگ جهانی اول به وجود آورنده جنگ های فرسایشی و ارتش های بسیار بزرگ بودکه مدت های طولانی در برابر یکدیگر سنگربندی کرده، با تلاش در از بین بردن قسمت های مختلف ارتش حریف، سعی می کردند وی را تضعیف کرده، در نهایت نابود کنند. از طرفی اکتشافات علمی منجر به ایجاد ارتش های مکانیزه جنگ جهانی دوم شد که به خصوص هواپیماها و تانک ها نقش مهمی در آن بازی می کردند.

انقلاب اطلاعاتی هم نوعی جنگ را پایه ریزی کرده (و خواهد کرد) که درآن نه تعداد و نه حتی قدرت آتش نتیجه را تعیین نمی کنند. در این جنگ طرفی که بیشتر می داند بهتر می تواند بر همه سایه افکنده بر میدان نبرد غلبه کند، نیروهای خودی، دشمن و موقعیت ها را دقیق تر ببیند و از برتری مطلق خود برای غلبه ای راحت و کم تلفات بر حریف یاری جوید.

۲-۸ - جنگ شبکه ای [فناوری اطلاعات امنیت ص ۲۴]

در فشرده ترین تعریف، جنگ شبکه ای گسترده و مرتبط با اطلاعات میان ملت ها و یا جوامع است. تعریف فوق به این معناست که تلاش برای از بین بردن و یا خدشه دار کردن

اطلاعات جامعه ای که هدف تهاجم است و تغییر سطح هر نوع آگاهی وی از خود و جهان اطراف می باید به عنوان جنگ شبکه ای طبقه بندی شود. این جنگ می تواند برروی عقاید نخبگان، تمامی جامعه و یا هر دو متمرکز شده باشد. جنگ شبکه ای ممکن است شامل اعمال تکنولوژیکی، تبلیغات و عملیات روان شناسانه ای باشد که به منظور تخریب فرهنگی و سیاسی، از اعتبار انداختن ویا مقابله با رسانه های محلی، نفوذ در شبکه های کامپیوتری ودسترسی به بانک اطلاعاتی و تلاش برای گسترش عقاید مخالف و حرکت های اعتراضی با استفاده از بستر شبکه های اطلاعاتی صورت می پذیرد.

جنگ شبکه ای می تواند صورت های گوناگونی داشته باشد. بعضی مواقع ممکن است بین دو دولت- ملت در بگیرد وگاهی میان دولت ها و گروه های مستقلی مانند شورشی ها و یا تروریست ها. برای مثال می توان به جنگ اطلاعاتی میان کوبا و قاچاق چیان مواد مخدر در آن کشور و یا به جنگ دولت های مرکزی آفریقا علیه خرید و فروش ممنوع اسلحه میان کشورهای همسایه و نیروهای شورشی داخلی اشاره کرد. درمورد اخیر، تمامی تلاش دولت مرکزی به دست آوردن اطلاعاتی از زمان و مکان فروش اسلحه به شورشیان است تا با استناد به آن بتواند جلوی اقدام غیرقانونی کشورهای همسایه را بگیرد. لازم به ذکر است که براساس تعاریف کلاسیک جنگ، جنگ های شبکه ای را نمی توان جنگ هایی واقعی دانست اما شاید بتوان آنها را ابزاری برای ایجاد و یاپیشگیری ازاین جنگ ها قلمداد کرد.

۳-۸ - جنگ رایانه ای: [فناوری اطلاعات امنیت ص ۲۴]

جنگ رایانه ای اشاره به وضعیتی دارد که در آن عملیات نظامی براساس اطلاعات رایانه ای کنترل شود ویا به منظور جلوگیری از عملیات دشمن، برای ایجاد اختلال در ارتباطات و جلوگیری از دسترسی وی به اطلاعات تلاش شود. معنای دیگر جنگ رایانه ای، تلاش برای کسب اطلاعات هرچه بیشتر درباره دشمن و جلوگیری نمودن از کسب اطلاعات توسط وی درباره شماست، یا به تعبیری تلاش برای تغییر توازن اطلاعات ودانش به نفع شما به خصوص در وضعیتی که توازن نیروهای نظامی به نفع شما نیست و در نهایت جنگ رایانه ای به معنای استفاده از اطلاعات برای به حداقل رساندن سرمایه، جنگ افزار و نیروی انسانی مورد نیاز برای کسب پیروزی در جنگ است.

۴-۸ - شبکه ها در خدمت سلسله مراتب:

در طول تاریخ و حداکثر دیدگاه های سنتی به ارتش، تمامی ارتش ها دارای سلسله مراتب کاملاً دقیق بوده، نیروها به اجرای دقیق و بی چون و چرای دستورات مافوق افتخار

می کرده اند، در این ارتش ها تمامی دستورات دقیقاً از بالا دیکته می شد و سربازان پایین تر بدون چون و چرا آن ها را اجرا می کردند. اما امروزه انقلاب اطلاعاتی باعث ایجاد تغییراتی در این وضعیت شده است. امروزه سلسله مراتب ارتشی در معنای قدیمی خود منسوخ شده و برای فرمانبرداری نظامی، مرزهای جدید در حال تعریف است.

برای مثال مغول ها که در قرن سیزدهم براساس جنگ اطلاعاتی امروزین خود را سازمان داده بودند، بیشتر شبیه به یک شبکه بودند تا سلسله مراتبی منظم به عنوان مثالی امروزی تر می توان از ویت کنگ هایی که در جنگ آمریکا و ویتنام می جنگیدند نام برد. نیروی نظامی نسبتاً کوچکی که در برابر یکی از بزرگترین نیروهای نظامی قرن حاضر به خوبی ایستادگی کرد. ویت کنگ ها نیز بیشتر به نظامی شبکه ای شبیه بودند تا سیستمی مبتنی بر سلسله مراتب رسمی درهر دو مثال بالا نیروهایی که در برابر مغول ها و ویت کنگ ها می جنگیدند، مؤسساتی بزرگ و نهادینه شده بودند که برای جنگ های فرسایشی و منظم تربیت شده، از سلسله مراتب نظامی دقیقاً تبعیت کرده و در آنها تمامی دستورات از فرماندهان رده بالا صادر می شد.

۵-۸ - جنگ اطلاعاتی:

جنگ اطلاعاتی یا IW را به سادگی می توان استفاده از اطلاعات برای رسیدن به اهداف ملی تعریف نمود. جنگ اطلاعاتی نیز همانند ارتش های رسمی، سیاست اقتصاد و دیگر نهادهای ملی در تلاش برای تأمین اهداف ملی هستند. برای جلوگیری از سوء تفاهم تعریف بالا را می توان به دو بخش مجزای جنگ رایانه ای و جنگ شبکه ای تقسیم بندی نمود.

جنگ اطلاعاتی شامل جنگ شبکه ای نیزمی شود، این جنگ با تعاریف معمول جنگ تفاوت داشته، دائماً باید با حمایت (احیاناً غیرعلنی) دولت ها با دو هدف جریان داشته باشد:

الف) به دست آوردن اطلاعات از فعالیت ها، موجودی ها و تصمیمات دولت های دیگر

ب) جلوگیری از دسترسی دشمن به اطلاعات خودی از طریق تقویت سیستم های دفاعی موجود در شبکه. در این جنگ میدان نبرد امواج ماهواره ای و اینترنت است. کشورها برای آن که اطلاعات خود را در تمامی کشور قابل استفاده سازند اجباراً آن را روی اینترنت قرار می دهند و در نتیجه متخصصین رایانه ای کشورهای دیگر خواهند توانست از طریق نفوذ در شبکه ها، به آنها دسترسی پیدا کنند. جنگ امروز، جنگ برای حفظ اطلاعات خودی

و به دست آوردن اطلاعات دیگران است. جنگجویان رسمی و غیررسمی این جنگ دیگر افراد نظامی نخواهند بود بلکه جاسوس هایی خواهند بود که حتی بدون خروج از منزل، به اطلاعاتی حیاتی دسترسی پیدا خواهند کرد و یا سیستم های حفاظتی شبکه های خودی را در برابر نفوذ دیگران ایمن تر خواهند نمود

۶-۸ - جنگ الکترونیک [۳ص۱۸۸]

آمریکایی ها یک بار دیگر هم از تکنیک جنگ الکترونیک برای منهدم ساختن تأسیسات ارتباطی عراق در جنگ اول خلیج فارس در سال ۱۹۹۱ استفاده کرده بودند. در جنگ سال ۲۰۰۳ موضوع مهم، نابودی یا بی خاصیت کردن سیستم های اطلاعاتی کلیدی عراق با روش های الکترونیک یا فیزیکی بود. در ساعات اولیه آغاز عملیات توفان صحرا، سلاح های ضد تشعشع که از هلی کوپترها و هواپیماها شلیک می شدند. شبکه دفاع هوایی عراق را فلج کردند.

نوارهایی از فیبر کربنی که از موشک های تام هاوک برفراز سیستم سوئیچینگ شبکه برق عراق تخلیه شد، باعث اتصال برق و خاموشی های گسترده در شبکه برق عراق گشت . یک بمب هدایت شونده که توسط بمب افکن آمریکایی رها شد از هواکش سیستم تهویه مطبوع مرکز تلفنی عراق در بغداد وارد شد و تمام شبکه زیرزمینی کابل کواکسیال که فرماندهی عراق را به واحدهای زیر دستش مرتبط می ساخت، از بین برد. پس از این که مراکز فرماندهی و کنترل از کار افتادند نیروهای مهاجم درصدد نابودی سیستم های رادار عراق برآمدند، در حالی که رادارها نمی توانستند فضای نبرد را ببینند، بنابراین عراق شانس کمی برای پیروزی داشت. ویروس های کامپیوتری نیز از جمله عوامل اختلال در سیستم ارتباطی عراق بودند. براساس یک گزارش، ویروسی که در یکی از IC های چاپگر جاسازی شده بود چاپگرها و مانیتورهای تحت سیستم عامل ویندوز را از کار انداخت. این چاپگر از فرانسه خریداری شده و در مقر دفاع هوایی عراق نصب گشته بود. گفته می شد که ویروس مذکور توسط آژانس امنیت ملی آمریکا و CIA طراحی شده بود که به نام ویروس AF/۹۱ بود.

۷-۸ - محیط امنیتی:

ما در عصری به سر می بریم که از بارزترین ویژگی های آن پیچیدگی، تنوع و پیوندهای درهم تنیده امنیتی است به گونه ای که تهدیدات و فرصت ها با وابستگی به هم درصدر مسایل امنیتی کشور قرار گرفته است.

در عصر کنونی «مفهوم بندی های مسلط از فضای سیاسی درروابط بین الملل تغییر نموده

و درنتیجه تقسیم خارجی- داخلی در عرصه بین المللی از بین رفته است. [۹]

محیط امنیتی با بسترها و امکاناتی که جهانی شدن در اشکال مختلف به وجود آورده همراه است و پیوند خورده است و درهر بخش چالش ها و پیامدهای خاصی را داشته است.

در بعد اقتصادی بر اثر تحولات چشمگیر در فناوری، اطلاعات، تصمیم گیری، تجارت و سرمایه گذاری خارجی ودیگر فعالیت های وسیع اقتصادی دولت ها و سازمان های بین المللی، بنگاه های تجاری، سرمایه داران خصوصی، بانک ها و مانند آن بستری از امکانات و شرایط را برای سازمان های اطلاعاتی فراهم آورده که بسته به قدرت سازمانی حاصل آثار مثبت و منفی در بخش امنیت بوده است. از طرفی تخصصی بودن مسائل اقتصادی و اهمیتی که کشورها به سود و ثروت می دهند سازمان های حفاظتی را دچار انفعال در این عرصه نموده و بخش های اطلاعاتی توانمندتر، از این بستر نهایت بهره برداری را در جمع آوری اطلاعات و اعمال نفوذ می نمایند. در بعد فرهنگی که پیوندی دیرینه با اقتصاد و فناوری داشته، سازمان های اطلاعاتی با سوار شدن برجریان کالاها و ایده ها که به سرعت گسترش می یابد بهره برداری خود را نموده اند و سازمان های حفاظتی با خوش بینی و ساده انگاری به سیاست های انفعالی و انزوا روی آورده اند و یا با نگاه امنیتی به جریان های فرهنگی پرداخته اند. در بعد سیاسی با پیوندهای ایجاد شده بین سیاست، اقتصاد و فرهنگ و نقش بازیگران غیردولتی و شبکه های فراحکومتی که وظایف خاص دولت ها و از جمله مسأله مهاجرت ها و برقراری امنیت را انجام می دهند و نقش سازمان های اطلاعاتی در ظهور نهادهای خصوصی که علی الظاهر نه دولتی هستند نه مربوط به یک ملت خاص قمداد می شوند مانند پزشکان و وکلای بدون مرز، عضو بین الملل، گروه سبز و مانند آن، بسترها و امکانات گسترده ای جهت بهره برداری اطلاعاتی و حفاظت اطلاعاتی ج.ا.ا نیز می باشد. امروزه محیط امنیتی کشورها به عنوان یک واقعیت حاوی مشخصات ذیل است:

۱) حصر و محدودیت مناسبات امنیتی.

۲) تشدید پنهان کاری جریان ها و شبکه های موجد ناامنی با هدایت و پشتوانه آمریکا.

۳) افزایش آسیب پذیری امنیتی.

۴)گسترش فناوری های عملیات پنهان.

۵) محدودیت زمان و افزایش سرعت عمل حریف.

۶) فرسایش پنهان و توهم قدرت سازمان های حفاظت اطلاعاتی.

۷) اولویت جمع آوری انسانی.
۸) درک مبهم از تهدیدات.
۹) تداخل حوزه های گوناگون جاسوسی (جاسوسی سیاسی، صنعتی، نظامی)
۱۰) عدم موازنه هزینه های سرمایه گذاری شده و نتایج قابل پیش بینی.
۱۱) ایمن نبودن ساختار و پراکندگی جمعیت مرزی.
۱۲) وجود بحران های منزلتی در گروه های مختلف جامعه.
۱۳) ضعف شم اطلاعاتی و مشارکت مردمی در جمع آوری اطلاعات.
۱۴) هوشمند نبودن سیستم های حفاظتی و دفاعی کشور.
۱۵) ضعف سرمایه گذاری در آموزش، تحقیقات و فناوری در بخش حفاظت اطلاعات.
۱۶) ضعف سیاستگذاری استانداردسازی سامانه حفاظتی و امنیتی کشور.
۱۷) ناهماهنگی و کارهایی موازی در امور اجرای اطلاعات و حفاظت اطلاعات.

براساس این شاخصه ها محیط امنیتی عصر کنونی محیطی جدید به شمار می آید. این وضعیت باعث گردیده تا سازمان های حفاظت اطلاعاتی به تبعیت از تضعیف اختیارات، قدرت و حاکمیت سرزمینی دولت های همسایه منفعل عمل نمایند و با عقب ماندگی خود آینده را از دست بدهند. این شرایط الزاماتی را باعث می گردد و چالش هایی را به وجود می آورد که تهدید امنیت ملی است و شرایطی که با فرسایش جدی حفاظت اطلاعات ها همراه است و چنانچه به شناخت این شکاف ها و چالش ها نپردازیم نمی توانیم با اتخاذ سیاست های مؤثر و کارآمد ایفای نقش نمائیم.

در این راستا چنانچه سازمان های حفاظت اطلاعات بی توجه به تحولات محیط امنیتی دچار عادت و روزمره گی شوند و تغییر و تحولات را نادیده بگیرند به نقطه ای می رسند که باید تغییرات بنیادی در ساختار، فرآیندها، فرهنگ سازمانی و دیگر زمینه های برجسته سازمانی را در زمانی کوتاه و باشتاب تند تجربه کنند و به جای پیش بینی و تحولات برنامه ریزی شده، ریسک و خطرپذیری را باعث گردند.

محیط امنیتی و استراتژی های سازمانی بیشترین اثر را بر فرهنگ سازمانی بر جای می گذارد. و فرهنگ سازمانی فضا و بستری است که سازمان برای دستیابی به کارآمدی در مقابله با ناامنی ها در یک محیط امنیتی به آن نیاز دارد. پیش بینی، پیشگیری، تجسس، شناسایی و خنثی سازی از الزامات کارآمدی سازمان های حفاظتی است و این فرهنگ

سازمانی است که باید این قدرت و توان را فراهم سازد و این عملی نیست مگر آن که ارتباط خردمندانه ای میان ارزش ها و باورها از یک سو و استراتژی ها و محیط امنیتی از سوی دیگر فراهم گردد. به عبارت دیگر سازمان نیازمند فرهنگی است که کارکنان و بخش های مختلف را برای رویارویی و پاسخگویی به محیط امنیتی آماده نمایند.

نتایج کلی

الف) سازمان های اطلاعاتی و حفاظتی به عنوان مجموعه ای پیچیده با افراد، گروه ها، سازمان ها و بخش های متنوع و متعددی که هریک دارای مضار و منافع ویژه ای هستند سروکار دارند. تحولات و مسایل امنیتی چه تهدید باشد یا فرصت برکارکرد و نقش این سازمان ها تأثیر میگذارند و این در حالی است که سازمان های اطلاعاتی و حفاظتی زیر سیستمی از دولت محسوب می شوند که دارای وابستگی چند جانبه ای هستند و بدین لحاظ طراحی و بهره گیری از استراتژی هایی که امکانات و قدرت لازم را در برخورد صحیح با محیط امنیتی به وجود آورد یک اولویت برجسته به شمار می آید.

ب) سازمان های اطلاعاتی ج.ا.ا با اتخاذ استراتژی های ذیل و یا ترکیبی از آنها می توانند ازتحولات امنیتی محیط بهره برداری نمایند:

۱) تمرکز تلاش های جمع آوری و تحلیل اطلاعات از آمریکا و متحدانش.

۲) ائتلاف و اتحاد اطلاعاتی و هم سوئی با کشورهایی که دشمن با آمریکا، دوستان دشمن آمریکا و یا حریف و هدف آمریکا محسوب می گرددند و از توان لازم برخوردار هستند.

۳) مذاکره اطلاعاتی- امنیتی که طی آن تلاش می گردد برای تضادها و رقابت های مخرب راه کار به وجود آید.

۴) اعمال نفوذ بر گروه های سیاسی ذی نفوذ در سیاست ها و تصمیم سازی های آمریکا.

پ- سامانه های حفاظت اطلاعاتی می بایستی در سه سطح فنی، عملیاتی و استراتژیک مطرح شوند:

۱) در سطح فنی، نحوه بهره برداری از منابع و نوع تولیدات اطلاعاتی و حفاظتی که باید ارائه گردد مطرح می باشد. در این سطح هماهنگی مدیریت عملیاتی و ایجاد ارتباط با کاربران اطلاعات پنهان مطرح است و به عبارتی باید اطمینان حاصل شود که عملیات و تولیدات سازمان در راستای نیازهای واقعی و منافع امنیت ملی است.

۲) در سطح عملیاتی نحوه انجام وظیفه مدیریت عملیاتی مطرح است که بدون تردید اتخاذ این استراتژی ها از یک طرف مستلزم شناخت ویژگی های سازمانی مانند توانایی های مدیریت، سطح دانش کاربری کارکنان، قابلیت های فنی، ساختار، سیستم های کنترل و نظارت، الزامات خط مشی ها و سیاست ها، امکانات و تجهیزات و فرآیندهای کار حفاظتی می باشد و از طرف دیگر به تحلیل دقیق فرهنگ سازمانی و الگوهای رفتاری بستگی دارد.

سامانه های حفاظتی در سطح عملیاتی بر کار ویژه های سازمانی تاکید دارند و در این راستا جریان اطلاعات و مدیریت عملیات تولید اطلاعات نقش اصلی را داراست و مؤلفه های تکنولوژی تجهیزات، فرآیندهای عملیاتی، نیروی انسانی و به طور کلی مدیریت عملیات در آن دخالت دارند.

۳) در سطح استراتژیک، کل سامانه حفاظت اطلاعاتی مطرح است و هدف آن اطمینان از سلامت عملکرد سطح فنی است. در این سطح برپایی ارتباط مناسب میان سازمان و محیط تعیین استراتژی های کلی در سطح سازمان، برنامه ریزی دراز مدت، سمت گیری های اساسی، جلب پشتیبانی نهادها، گروه ها و یا افراد نسبت به عملکرد سازمان و تداوم شناخت و مراوده با محیط امنیتی مورد توجه است.

ت- پایگاه های تهدید: اهم تهدیدات و مسایلی را که در این وضعیت متوجه سامانه های حفاظت اطلاعاتی و مسؤولیت های خطیر آنهاست، از آنجا که درک معقول از ماهیت تهدیدات و آسیب پذیری ها با امنیت ملی کشور ارتباط دارد و فقدان امنیت بازتاب ترکیبی از تهدیدات و آسیب پذیری ها است، که تفکیک معنادار آنها ممکن نیست.[۵] سازمان های حفاظت اطلاعاتی برای ارتقای کارایی خود در افزایش امنیت ملی لازم است سیاست هایی را به کار گیرند که باعث کاهش آسیب پذیری ها در حیطه مسئولیت حفاظتی خود باشند و ثانیاً سازمان های اطلاعاتی با تلاش های متمرکز و کسب قدرت لازم و پیوند طرح ریزی شده با سازمان های حفاظتی و تصمیم گیران باعث کاهش تهدیدات گردند. در این عرصه سازمان های حفاظتی و اطلاعاتی بایستی متحد و متمرکز باشند وبا سرعت عمل نمایند.

بدون تردید درک معقول تهدیدات امنیتی به لحاظ جنبه های ذهنی و عینی و دشواری هایی که وجود دارد کاری بسیار سخت و دشوار است خصوصاً تهدیداتی که متوجه امنیت نظامی است، یعنی میزان قابلیت نیروهای مسلح یک کشور برای حفاظت از حکومت و مردم در مقابل تهدیدات قهرآمیز.[۶]

در محیط امنیتی کنونی توجه به نقش یک جانبه گرایی ایالات متحده آمریکا و سیاست های این قدرت جهانی و نقش فعال سازمان های اطلاعاتی این کشور و متحدانش در منطقه ضروری است. مهم ترین پایگاه ها و ابزار سازمان های اطلاعاتی آمریکا در منطقه را در کشورهای ترکیه و اسرائیل باید جستجو کرد. چرا که این دو کشور علاوه بر سابقه دیرینه همکاری اطلاعاتی دردهه ۱۹۹۰ به عنوان کارگزاران آمریکا در منطقه عمل کرده اند. [۷]

پیشنهادات

الف- محیط امنیتی فعلی تأثیر بارزی برکارکردها و رفتارهای سازمانی داشته است، شرایط امنیتی ضرورت تغییراتی اساسی را در سیاست های حفاظت اطلاعاتی باعث گردیده است. در شرایط کنونی به سبب عمق و گستره خصومت ایالات متحده آمریکا و قدرت مضاعف ساختارهای اطلاعاتی این کشور با متحدانش، سازمان های خودی با مسایل و دشواری های جدی مواجه می باشند. سرویس های ایالات متحده با اتخاذ سیاست های آفندی همه جا به دنبال جمع آوری وسیع و عمیق اطلاعات می باشد که وجود این تلاش در طرح های آینده مؤثر است.

چنین وضعیتی سازمان های اطلاعاتی و حفاظتی کشور را به سوی سمت گیری و تمرکز تلاش ها رهنمون می سازد. خود اتکائی و کسب قدرت درونی و حرفه ای شدن سازمان های حفاظتی و اتحاد و ائتلاف با کشورهای مؤثر در حوزه جمع آوری علیه آمریکا می تواند بر قدرت کشور بیفزاید.

ب- ارتقای توان سازمانی و تحکیم پایه های قدرت حفاظت اطلاعاتی در امنیت، توانمندسازی این سازمان از طریق، جمع آوری در هدف، همکاری سازمان های داخلی ، کارآمدی، مسؤولیت پذیری، حیطه بندی، قانون گرایی، حرفه ای گرایی و ....می باشد.

پ- در وضعیت کنونی که تهدیدات ملموس اند به دلیل آسیب پذیری در مقابل تهدیدات است که ناامنی و مسائل حاد امنیتی به وجود می آید. در این شرایط اگر اجازه ندهیم که سیاست گذاری در حوزه حفاظت اطلاعات دچار سیاست زدگی و انواع تمایلات و فشارها گردد در جهت کاهش آسیب پذیری های سازمانی گام برداشته ایم.

ت- تلاش برای مقابله و رویارویی جهت حذف یا تقلیل تهدیدات در تدبیر اول: سیاست های حفاظت اطلاعات متوجه تقلیل آسیب در نیروهای مسلح و سازمان های وابسته خواهد بود که لازمه آن قدرتمند شدن حفاظت اطلاعات است. متغیرهای عمده ای که بر سیاست امنیت ملی به طوراخص مؤثر است را بر شمرده و برخی نتایج را درباره نحوه تأثیر

این متغیرها بر مساله امنیت ارائه نموده. [۵ ص ۳۹۵]

در تدبیر دوم: سیاست های حفاظت اطلاعات بر منشاء و علل تهدیدات متمرکز است و هدف خود را اقدامات اطلاعاتی- سیاسی جهت کاهش یا حذف تهدیدات قرار می دهد، ترکیب مناسب این دو تدبیر با توجه به مؤلفه های داخلی و خارجی مؤثر و بسیار حائز اهمیت می باشد.

ث- اتخاذ سیاست های اطلاعاتی و حفاظت اطلاعاتی قوی و معتبر و غیرتحریک آمیز در بستر اعتمادسازی و با ایجاد بصیرت سیاسی و حرفه ای امکان پذیر است و ایجاد چشم انداز روشن و درست از حفاظت اطلاعات در نظر نیروهای اطلاعاتی، فرماندهان و کارکنان بسیار اهمیت دارد، چرا که دیدگاه های منفی و ذهنیت های غلط و تنگ نظرانه به حفاظت اطلاعات، محدودیت ها و موانع جدی را در اتخاذ سیاست ها و اقدامات امنیتی بر جای می گذارد.

ج- افکار عمومی کارکنان و تصمیم گیران درباره سیاست های حفاظتی بسیار مهم است و اگر بصیرت واعتماد لازم به وجود آید موضع گیری های افراطی و جزمیت های شکننده به حداقل می رسد، ایجاد احساس ضرورت حیاتی تعاون اطلاعاتی و وابستگی متقابل اطلاعات و حفاظت اطلاعات و بخش های تصمیم گیر باعث تأثیر مثبت در سیاست گذاری های حفاظتی است و دور نمای بهتری را به دست می دهد.

نتیجه گیری

سیاست سازی و سیاستگذاری و به طور کلی تعیین سامانه های حفاظت اطلاعات با توجه به تهدیدات فعلی و آینده امری اساسی است که تأثیر مستقیم بر منافع امنیت ملی دارد و اگر تصمیم گیری در این حوزه به شیوه ای خردمندانه صورت نگیرد، ضایعات جبران ناپذیری را به وجود می آورد و در این راستا درک محیط امنیتی که نقش موثر و برتر را در سمت گیری سیاست های سازمانی دارد از اهمیت ویژه ای برخوردار است و مطالعه علمی و مستمر آسیب ها، تهدیدات، فرصت ها و اولویت ها ضرورتی حیاتی است.

توجه به محیط امنیتی تأکیدی برفعل و انفعالات درون سازمانی است، به نحوی که درک محیط امنیتی باعث ایجاد تعادل و توازن مناسب میان قدرت اطلاعاتی و ضد اطلاعاتی در برخورد و رویارویی بامسائل امنیتی محیط گردد و به طور کلی در هنگام سیاستگذاری، هدف گذاری و تعیین استراتژی، شناخت عوامل داخلی و خارجی و تعیین آثار ناشی از آن در رسیدن به تعادل مطلوب بسیار مهم است.

منابع و مأخذ

1- F. E Emery and E. L. Trist, << The Causal Texture of organizational Environments>>

Printedinto morrow, s organization, by Jun and storm, opcit, P.P141- 1510.

۲ – فناوری اطلاعات و امنیت صفحه ۲۲ و صفحه ۲۴.

۳ – ضیائی پرور، حمید، جنگ نرم- ویژه جنگ رایانه ص ۱۸۸.

۴ – Krause, J and n. ren wick (eds), Identities in International relations (Hound mills: ۱۹۹۶) p.xii.

۵ – بوزان، باری، مردم، دولت ها و هراس ، ترجمه ناشر، تهران، پژوهشکده مطالعات راهبردی فصل سوم – ۱۳۷۸

۶ – ماندل، رابرت، چهره معتبر امنیت ملی، ترجمه ناشر، پژوهشکده مطالعات راهبردی ۱۳۷۷/ص۵۲

۷ – ملکی، محمدرضا «روابط ترکیه و اسرائیل و آثار آن در آسیای مرکزی و قفقاز»

فصلنامه مطالعات آسیای مرکزی و قفقاز شماره ۲۴ زمستان ۱۳۷۷

8 - Buzan, bary, South Asia Moving Towards Transformation: Emergence of india as a Great Power International Studies 39, 1 (2002). P13

9- karuse, j and n, renwick (eds), Identities in international relations