هوشمندی استراتژیک با رویکرد پدافند غیرعامل دانش محور

مصطفی امینی
کارشناس ارشد نرم افزار، کمیته مدیریت دانش، مرکز تحقیقات مبین، دانشگاه جامع امام حسین(ع)
mamini@ihu.ac.ir

حسین صابری
کارشناس ارشد نرم افزار، کمیته مدیریت دانش، مرکز تحقیقات مبین، دانشگاه جامع امام حسین(ع)
hsaberi@ihu.ac.ir

محمدرضا کنگاوری
استادیار دانشکده مهندسی کامپیوتر
عضو هیات علمی دانشگاه علم و صنعت ایران
Kangavari@IUST.ac.ir

چکیده:

برآیند پردازش هدفمند و روشمند دانش، دانش جدید، بصیرت و هوشمندی است. هوش و هوشمندی در سطوح مختلف سازمان دارای تجلی های متنوعی می باشد . نتیجه پردازش نظام مند د انش استراتژیک در سازمان ها، هوشمندی استراتژیک است. به هوشمندی استراتژیک می توان با رویکردهای متعددی نگریست . یکی از این رویکرد ها، رویکرد پدافند غیرعامل است. بخش قابل توجهی از *هوشمندی استراتژیک با رویکرد پدافند غیرعامل* را *قابلیت محوری با رویکرد پدافند غیرعامل* تشکیل می دهد. هوشمندی و هوشیاری در مقابل سیگنال های ضعیف تغییر، توان ***بقا*** و ***تعامل*** را برای سازمان های مدرن افزایش می دهد. لذا برای رسیدن به یک ضریب هوشمندی قابل قبول باید بین گذشته، حال و آینده هم افزایی های نظام مند شکل داده شود تا برآیندهایی قدرت زا برای سازمان به ارمغان آورده شوند . مقوله هوشمندی استراتژیک به دنبال دستیابی به یک ضریب هوشمندی قابل قبول با توجه به شرایط زمانی، م کانی و وضعیتی سازمان است. از آنجایی که خلق و کشف قابلیت های مدرن در سازمان ها نیازمند پردازش دانش های مرتبط با ماهیت سازمان است لذا هدف از این مقاله طرح مجموعه ای از قابلیت های پدافند غیرعامل در سطح استراتژیک سازمان می باشد. این مقاله تلاش می کند تا از *دیدگاه پردازش دانش* به این قابلیت ها بنگرد.

واژه های کلیدی:

هوشمندی استراتژیک، پدافند غیرعامل، پردازش دانش، قابلیت محوری، آینده پژوهی

۱ -مقدمه و هدف

امروزه سازمان هایی موفق و قدرتمند خواهند بود که : (۱) توانایی شکار و اداره نیازهای آشکار، (۲)توانایی شکار و اداره نیازهای پنهان و (۳) توانایی خلق و اداره نیازهای جدید را داشته باشند . قرن امروز، عصر هوشمندی در مواجهه با نیازهاست. سازمانی در فضای رقابتی امروز باقی خواهد ماند که فاصله بین شناسایی **نیاز** تا **رفع آن** را بموقع تر، هوشمندانه تر و با کیفیت تر بپیماید.

ظهور سرمایه ها و دارایی های نوین همچون دانش و همچنین پردازش های نرم [۱] همچون پردازش دانش [۲] نویدبخش شروع دوران جدیدی است که نهایتا منجر به پیدایش قدرت های نرم هوشمند [۳] خواهد شد. از جمله لوازم رسیدن به یک قدرت نرم هوشمند، تلاش برای دستیابی به **هوش و هوشمندی**[۴] در سطوح مختلف سازمان است.

در همین راستا، از جمله مفاهیم مدرن مرتبط با هوش و هوشمندی، مفهوم هوشمندی استراتژیک [۵] در سازمان است. هوشمندی استراتژیک ارتباطات تنگاتنگ و معناداری با مفاهیم *آینده*، *قابلیت محوری*، *سناریو*، *کانون تفکر*، *دانش* و *تنوع* دارد. هوشمندی استراتژیک به دنبال معنابخشی، عمق بخشی و بعد بخشی به راهکارهای بلند مدت سازمان می باشد . هوشمندی استراتژیک به معنای مجموعه ای از اعمال جستجو، پردازش، انتشار و حفاظت از اطلاعات و دانش با هدف ارائه آنها به فرد صحیح در زمان صحیح جهت اتخاذ تصمیم صحیح است. این نوع هوشمندی بدون وجود یک ساختار یکپارچه بین نیاز، مخاطب سازمان، دارایی ها و سرمایه های سازمان و سطوح مختلف مدیریت حاصل نخواهد شد . پیامد فرآیند هوشمندی استراتژیک، تحلیل و کشف نیازهای کلان و راهکارهای رفع آنهاست . در حقیقت هوشمندی استراتژیک، محصول پردازش نظام‌مند دانش استراتژیک است. به عبارت بهتر، هوشمندی هم فرآیند است و هم محصول.

هدف از این مقاله بیان مجموعه ای از قابلیت های استراتژیک با رویکرد پدافند غیرعامل در راستای دستیابی به هوشمندی استراتژیک است. برای نیل به مجموعه ای از قابلیت های پدافند غیرعاملی در سطح استراتژیک باید خصیصه-ه‌ای جدید تهدیدات نوظهور را شناخت تا بتوان راهکارهای پدافندی متناسب با ماهیت تهدید ارائه داد . لذا این مقاله بعد از بیان مفاهیم مرتبط با هوشمندی استراتژیک، مجموعه ای از روندهای پیدایش تهدیدات نوظهور را مطرح می کند. سپس با توجه به این روندها، مجموعه ای از قابل یت های پدافند غیرعاملی نوین را تشریح می کند . نهایتاً پس از بیان ارتباط میان توان پردازش دانش های استراتژیک با خلق قابلیت های پدافند غیرعاملی، از مباحث مطرح شده نتیجه می-گیرد.

---

[1] Soft Processing
[2] Knowledge Processing
[3] Intelligence Soft Power
[4] Intelligence
[5] Strategy Intelligence

۲ -مواد و روش ها

۲ ۱ - هوشمندی استراتژیک

هوشمندی استراتژیک با موضوعات گسترده ای همچون ارزیابی های اقتصادی و سیاسی، نیات و توانمندی های نظامی کشورهای خارجی (و بالاخص عوامل غیردولتی) در ارتباط تنگاتنگی است. چنین هوش و هوشمندی امکان دارد علمی، فنی، تاکتیکی، دیپلماتیک ، و یا جامعه شناختی باشد، اما این تغییرات در ترکیب با واقعیت‌های شناخته شده درباره یک حوزه مورد نظر و مشخص همچون توانمندی های جغرافیایی، جمعیتی و صنعتی تحلیل می شوند. توجه به خصیصه‌های بومی در هوشمندی استراتژیک بسیار حائز اهمیت است.

هوشمندی استراتژیک یعنی هوشمندی در سطح استراتژیک . از آنجایی که سطح استراتژیک بر سیاست های کلان تاکید دارد پس می توان گفت هوشمندی استراتژیک یعنی هوشمندی در تجویزهای آینده نگرانه، هدفمند، نظام مند، روش‌مند و یکپارچه در سطح استراتژیک.

هوشمندی استراتژیک از جنس "**خرد**[1]" یا "**حکمت**" است که پشتوانه‌ی انتخاب راه و مقصد است. در حقیقت ***خرد کاربردی کردن دانش است*** . یک سازمان می تواند به اتکای خرد تصمیم بگیرید که "*خدمت مناسب برای سازمان چیست؟* "در حالی که با اتکا به دانش می‌تواند "*آن خدمت را به نحو احسن بسازد*". تولید خرد از شؤون رهبری یک سازمان است، و حال آن‌که تولید خدمت در زمره وظایف بدنه اجرایی سازمان قرار می‌گیرد. به عبارت دیگر، سئوال اصلی در هوشمندی استراتژیک یک سازمان این است که برای حفظ موقعیت سازمان و ارتقای جایگاه ملی و جهانی آن بر چه "***قابلیت‌هایی***" متمرکز شویم. به عبارت دیگر، هوشمندی استراتژیک به دنبال بسط قابلیت محوری و کشف مزیت های رقابتی جدید در محیط پویا و متغیر امر وزی است. بنابراین هوشمندی استراتژیک دارای ارتباط تنگاتنگ و معناداری با آینده نگری و آینده نگاری می باشد.

هوشمندی استراتژیک به دنبال معناسازی[2] و معنابخشی است. درباره فرآیند معناسازی و معنابخشی بیان چند نکته لازم است: (۱) معناسازی و معنابخشی یکی از پیچیده ترین وظایف انسانی است، (۲) فرآیند معناسازی به دنبال نمایش و آشکارسازی یک کلان ساختار[3] (همچون یک داستان یا سناریو) از مجموعه ای از موجودیت‌های ریزساختار[4] است، و (۳) معناسازی و معنابخشی بدون وجود دانش و پردازش آن ناممکن است ، (۴) انسان یکی از اصلی ترین پردازنده های دانش است.

---

[1] Wisdom
[2] meaning-making
[3] macro-structure
[4] micro-structure

در حقیقت هوشمندی استراتژیک به دنبال حرکت از *تحلیل درخت ها* به *تحلیل جنگل* است. یعنی انتقال از سطح درخت ها (مولفه های خُرد) به سطح جنگل (مولفه های کلان) و دور شدن از مباحث ناچیز ، کم اهمیت و روزمره است. هوشمندی استراتژیک دربرگیرنده تلاش هایی برای درک کردن یک "تصویر بزرگ" از هستی سازمان بر مبنای منابع دانشی می باشد.

۲-۲- مولفه های هوشمندی استراتژیک

هوشمندی استراتژیک یعنی جمع آوری، پردازش، آنالیز و توزیع هوش به همان صورتی که برای شکل دهی طرح‌های کلان در سطح ملی و بین المللی مورد نیاز است. امروزه اکثِ (و نه همه) اطلاعات موردنیاز از انعکاس‌های استراتژیک از هوشمندی متن باز[1] بدست می آیند.

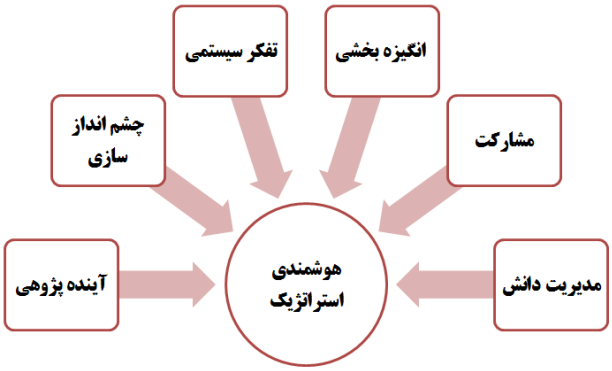
به عقیده عده ای از صاحبنظران بعضی از خصیصه های اکثر رهبران موفق، توجه آینده نگارانه به دولت و کسب و کار است. بنابر این دیدگاه، می توان گفت هوشمندی استراتژیک با مجموعه ای مولفه ها و قابلیت های نظام مند زیر مرتبط است (شکل ۱):

- **آینده نگلوی**[2]: قابلیت فهمیدن روندهایی که تهدیدات یا فرصت هایی را برای سازمان فراهم می کنند.
- **چشم انداز سازی** [3] : قابلیت مفهوم سازی یک حالت ایده آل مبتنی بر آینده نگری و ایجاد یک فرآیند برای تحقق و پیاده سازی آن.
- **تفکر سیستمی**[4]: قابلیت درک، سنتز و یکپارچه سازی عناصری که به عنوان یک کل برای رسیدن به یک هدف مشترک عمل می کنند.
- **انگیزه بخشی**[5]: یعنی قابلیت انگیزه دادن به افراد مختلف برای کار کردن با همدیگر در راستای پیاده سازی چشم‌انداز. درک کردن اینکه چه چیزی موجب انگیزش افراد می شود. این موضوع با مقوله هوش شخصیتی[6] ارتباط معناداری دارد.
- **مشارکت**[7]: قابلیت توسعه دادن اتحادهای استراتژیک با افراد خاص، گروهها و سازمان ها. این مقوله نیز به هوش شخصیتی وابسته است. مشارکت یک فاکتور کلیدی در توانایی پردازش دانش است.

---

[1] Open Source Intelligence
[2] Foresight
[3] Visioning
[4] System Thinking
[5] Motivating
[6] Personality Intelligence
[7] Partnering

- **مدیریت دانش**[1]: منظور توانایی اخذ، حفاظت و بکارگیری دانش در راستای اهداف کلان سازمان است . بخشی قابل توجهی از هوشمندی استراتژیک به توانایی به اشتراک گذاری دانش و دستیابی به به یک ضریب توان پردازش دانش قابل قبول در سازمان دارد.



شکل ۱. هوشمندی استراتژیک با تاکید بر مدیریت دانش

بنابراین درباره *هوشمندی استراتژیک* می توان چند نتیجه گرفت:

۱ - هوشمندی استراتژیک یک مقوله ***وابسته با دانش*** است.

۲ - هوشمندی استراتژیک محصول ***پردازش دانش استراتژیک*** است.

۳ - برآیند فرآیند هوشمندی استراتژیک، ***قابلیت محوری*** است.

۴ - قابلیت محوری می تواند ***جنبه های گوناگونی*** داشته باشد.

۵ - تاکید هوشمندی استراتژیک بر ***یک نگرش بلند مدت*** است.

۶ - یکی از لوازم هوشمندی استراتژیک ***دیده بانی آینده و آینده پژوهی*** است.

۳ -یافته ها

۳ ۱ - روندها در تهدیدات نوظهور

از دیدگاه مدیریت تهدید[1]، امروزه یکی از هنرهای ضروری مدیریت استراتژیک سازمان ها توانایی تبدیل کردن تهدید به فرصت (فرصت سازی)، مهندسی معکوس تهدید و پدافند بومی و خوداتکاء است. از جمله لوازم دستیابی به این گونه قابلیت ها، شناخت روندهای جدید برای خلق تهدیدات نوظهور است. بعضی از این روندها عبارتند از:

[1] Knowledge Management

- **روند پویاسازی تهدید:** یکی از روندهای مهم در خلق تهدیدات نوظهور توجه به تغییرات محیطی و دخالت دادن این تغییرات در رفتارهای تهدید است . توانایی خودجوششی و پویایی تهدید در شرایط مختلف و توجه به عدم قطعیت محیطی در تحلیل، طراحی و پیاده سازی تهدیدات نوظهور موجب پیدایش تهدیدات پویا شده است.
- **روند خودمدیریتی تهدید:** نگاه استقلال گرایانه به تهدیدات موجب پیدایش روند خودمدیریتی تهدید شده است . امروزه تهدیدآفرین ها به دنبال ایجاد تهدیداتی هستند که می توانند خوداتکا، خود انتشار و خودترمیم کننده باشند. حضور ربات های نرم افزاری در توسعه تهدیدات و توانایی خودتکثیری آنها، مصداقی از این روند است.
- **روند هوشمندسازی تهدید:** تلاش دانشمندان علوم شناختی و هوش مصنوعی برای افزایش ضریب هوشی، ضریب عاطفی، ضریب تجربی و ضریب شخصیتی ماشین ها و ربات ها موجب هوشمندتر شدن تهدیدات و افزایش ضریب هوشی تهدید، حاملان تهدید و تهدیدآفرین ها شده است. یکی از پیامدهای این موضوع افزایش ضریب تطبیق‌پذیری تهدید با شرایط محیطی می باشد.
- **روند نرم سازی تهدید :** ظهور فناوری های نوین همچون فناوری نرم [۲] و نگاه برخاسته از علوم اجتماعی و علوم انسانی در خلق تهدید ات موجب نرم تر شدن تهدیدات شده است . این گونه از تهدیدات ممکن است پیامدهای سخت و نرم داشته باشند.
- **روند چابک سازی تهدید:** سرعت خردمندانه بخشی از هوشمندی است. امروزه با افزایش سرعت تغییرات محیطی و ظهور تجهیزات و فناوری های پرسرعت تر و قوی تر یکی از روندهای موردنظر تهدیدآفرین ها افزایش سرعت تکثیر تهدید و تسریع در واکنش های تهدید می‌باشد.
- **روند شکاف سازی:** اصل نخستین برای نفوذ تهدید، وجود شکاف است . این شکاف می تواند در عرصه های مختلف وجود داشته باشد. از وجود شکاف بین استراتژی های سازمانی و قوانین گرفته تا شکاف موجود در بین سیستم های اطلاعاتی. هدف از روند شکاف سازی تلاش برای برهم زنی هماهنگی، ایجاد فاصله و استفاده از گپ ها و فاصله های موجود برای نفوذ تهدیدات به عمق های بیشتری از سیستم است.

در ادامه با توجه به روندهای مذکور مجموعه ای از قابلیت های پدافند غیرعاملی در سطح استراتژیک را مطرح می کنیم.

۲-۳- قابلیت محوری با رویکرد پدافند غیرعامل

حفاظت، تشخیص و واکنش مولفه های تشکیل دهنده چرخه پدافند غیرعامل هستند . همواره باید به خاطر داشت که حفاظت، تشخیص و واکنش مولفه های حساس به دانش هستند . به عنوان مثال، یک حفاظت آگاهانه، در حقیقت یک حفاظت مبتنی بر مهارت است. پس بدون دانایی، آگاهی و دانش نمی توان به آن صفت آگاهانه را داد.

---

[1] Threat Management
[2] Soft Technology

از طرف دیگر در حوزه پدافند غیرعامل، تهدیدکننده برای ***عملیاتی کردن تهدیدات*** از سه مورد زیر استفاده می‌کند:

- شکاف
- غفلت
- جهالت

به عنوان مثال، یکی از راهکارهای نفوذ بدافزارها مثل نرم افزارهای جاسوسی در زیرساخت های وابسته به فضای سایبر ابتداً شناسایی نقاط مستعد نفوذ و نقاط ضعف طرف مقابل است . یکی از این نقاط ضعف، وجود شکاف بین سیستم های اطلاعاتی سازمان هاست که به علت پارادایم پروژه های جزیره ای در سازمان ها به وجود آمده اند . به عنوان مثال دیگر، یکی از روش های نرم نفوذ در زیرساخت های حیاتی- اجتماعی کشور توسط نیروهای تهدیدآفرین، استفاده از شکاف‌های موجود بین راهبردها می باشد.

اگر به سه مورد فوق به عنوان سه **تهدید مادر** بنگریم، بنابراین هوشمندی در پدافند غیرعامل بر مبنای دانش های فناورانه، انسانی، اجتماعی و دیج یتالی در تمام سطوح مدیریتی بالاخص سطح استراتژیک سازمان می تواند مفید باشد . همچنین می توان گفت : توجه به دانش می تواند در هر سه مورد فوق الذکر ضریب شکاف، غفلت و جهالت را کاهش دهد.

در همین راستا، می توان با تاکید بر مبادی ارزشی و بومی ، یک پارادایم نوین تحت عنوان پارادایم هوشمندی استراتژیک با تاکید بر پدافند غیرعامل دانش محور[1] پیشنهاد داد. طبق تحقیقات انجام شده و مشاهدات محیطی، معتقدیم یکی از پارادایم های آتی و پیش روی سازمان ها، **پارادایم پدافند غیرعامل دانش محور** است. علت این ادعا این است که از آنجایی که: (۱) بخش قابل توجهی از مقوله حفاظت از جنس پدافند غیرعامل است، (۲) پدافند در مقابل تهدید مطرح می شود، (۳) یکی از دغدغه های سازمانها در عصر دانش حفاظت و صیانت از دانش و سرمایه های دانشی خود می باشد، (۴)اقدامات امنیتی و ایمنی، فعالیت هایی حساس به دانش هستند، و (۵) برای حفاظت از دانش نمی توان پدافند بدون دانش داشت؛ بنابراین می توان به وظایف و ماموریت های سازمان ها از دیدگاه پدافند غیرعامل نگریست . لازم به ذکر است امروزه کانون های تولیدکننده و اداره کننده تهدیدات به دانش های جدید برای تولید و اداره تهدیدات نیازمندند . بسیاری از دانش های جدید، دانش هایی میان رشته ای یا چند رشته ای هستند . از این رو هر یک از دانش های سازنده آنها، با علاقه مندی ها و نگرش های خود به موضوع می نگرند . پس *امروزه تهدید می تواند بار دانشی داشته باشد و این دانش قابل بازیافت است* . همچنین به دانش های نهفته در تهدید می توان از جنبه های متعددی نگریست . بر همین اساس سازمانهای امروزی برای تبیین و تسری دیدگاه *پدافند غیرعامل دانش محور* در تصمیمات و اقدامات هوشمندانه

[1] Knowledge-based Passive Defense

خود در سطح استراتژیک باید به قابلیت های پدافندی زیر توجه داشته باشد. هر کدام از این قابلیت ها را می توان به عنوان یک تجلی جزیی از هوشمندی استراتژیک در سازمان ها دانست.

(۱) قابلیت مهندسی معکوس تهدید: در قرن اخیر تهدیدات قصدمند، مقولاتی وابسته به مهارت هستند که سازمانها می توانند با شکار تهدیدات و مهندسی معکوس آنها فر صت های جدیدی را خلق کنند . به عبارت دیگر، کنترل و مدیریت تهدید نیازمند مهارت است. اگر تهدید بصورت صحیح مدیریت و هدایت شود موجب خلق فرصت خواهد شد . یعنی می توان به تهدید، به عنوان چشمه فرصت نگریست. بنابراین تهدید می تواند با رعایت نکات و اصولی خاص، بطور غیرمستقیم منفعت زا باشد. **تهدید می تواند به عنوان مبدا نوآوری برای رفع زیان های تهدید باشد** . این روال بدون دانش تخصصی و موضوعی در حوزه تهدید میسر نیست . تهدید می تواند سبب ارتقاء مخاطب تهدید شود . در این نگرش به تهدید ، اصلی ترین راهکار توجه به خودحفاظتی و خودپایشی [1] برای جلوگیری از تکثیر ناخودآگاه تهدید است. این سخن به معنای استقبال از تهدید نیست بلکه به معنای **"عصاره کشِیِ دانشی "** از تهدید است.

(۲) قابلیت تغییر هوشمندانه: وجود تهدید می تواند مبدایی برای واکنش های پدافندی باشد . یعنی پدافند در مقابل تهدید، را می توان به ع نوان مبداء *تغییر منفعت زا* دانست. بنابراین پدافند را می توان شروعی برای تغییرات هدفمند سازمانها دانست. به عبارت دیگر، از آنجایی که وجود تهدید، وجودی تداومی در طول زمان دارد و ***تا زمان هست، تهدید هم هست*** ، بنابراین واکنش نظام مند و هوشمند به تهدیدات از لوازم ح یات و بقا خواهد بود . واکنش به تهدیدات موجب افزایش *ضریب تجربی* خواهد شد و افزایش ضریب تجربی موجب تغییر موقعیت و وضعیت مخاطبان تهدید به موقعیت و وضعیت جدید خواهد شد. این انتقال وضعیت مملو از بار دانشی خواهد بود. اگر این انتقال وضعیت درست مدیریت شود می تواند باعث رشد و در غیر این صورت باعث تنزل شود . واکنش پدافندی به تهدید، مخاطب تهدید را در وضعیت جدیدی قرار می دهد. میزان سودمندی این وضعیت جدید وابسته به توانمندی های پدافندی قبل از بالفعل شدن تهدید است. پیشرفت مخاطب تهدید تابعی است از نحوه واکنش او در برابر تهدید.

(۳) قابلیت توسعه توانمندی های پدافندی: بی شک پیشگیری مقدم بر درمان است. به عبارت دیگر می توان گفت، پدافند مقدم بر آفند است. پس بی شک توسعه توانمندی های پدافندی راه حلی عقلانی و منطقی می باشد . به عبارت دیگر، از آنجایی که موفقیت در برابر تهدیدات تابعی از توا نمندی های پدافندی مخاطب تهدید است بنابراین توسعه و بهبود مداوم و پایدار این توانمندی یک راه حل پدافندی معقول محسوب می شود. سفارشی کردن این توانمندی ها در شرایط مختلف و محدودیت های متنوع موجب افزایش توان پدافندی مخاطبان تهدید خواهد شد . به عنوان مثال، یکی از توانمندی های موردنیاز برای مقابله با تهدیدات بالفعل، *مشارکت هدف دار با تهدیدآفرین* است. و یا هدایت و تلاش برای تغییر مسیر تهدید یکی از راه های مدیریت تهدید است.

---

[1] Self-Monitoring

(۴) قابلیت شناخت نقاط ضعف تهدید : همواره ماهیت تهدیدات دارای ویژگی فازی است . یعنی نمی توان هیچ تهدیدی را کامل دانست زیرا به یک تهدید می توان از دیدگاه ها و جنبه های مختلفی نگریست . لذا اگر حتی در شرایطی استثنایی، تهدیدی کامل باشد این کاملیت فقط از یک یا چند جنبه است. پس اگر از جنبه های دیگری نیز به آن تهدید نگریسته شود می توان نقاط ضعف آن را کشف کرد . کشف نقاط ضعف یک تهدید، یکی از مراحل کلیدی شناخت تهدید است. شناخت نقاط ضعف تهدید، شاه کلید تهدیدشناسی است که بدون دانش، ممکن نیست. به عبارت دیگر، بدون شک پیشگیری از تهدید، بدون شناخت تهدید و تهدیدآفرین میسر نیست . یکی از تاکتیک های مهم در تهدیدشناسی شناخت نقاط ضعف تهدید است . شناسایی این نقاط می تواند یکی از راهکارهای مناسب برای اقدام پدافندی موثرتر باشد. اگر شناخت مخاطب تهدید از نقاط ضعف تهدید هدف گرا و مسئله گرا باشد بنابراین می تواند با استفاده از نوآوری و خلاقیت راه حل های پدافندی مناسبی را مشخص کند . پس تهدید می تواند موجب شکوفایی قدرت نوآوری و خلاقیت در مخاطب تهدید شود . در آینده همین ایده های خلاقانه و نوآورانه به عنوان سرمایه های دانشی محسوب خواهند شد.

(۵) قابلیت خودشناسی از دریچه تهدید: تهدید علاوه بر مضرات دارای مزایایی نیز هست . اساساً یکی از راه های شناسایی نقاط ضعف، شبیه سازی و ساخت تهدیدات مصنوعی و تحلیل واکنش سیستم ها و سازمان ها در مقابل آن است. یعنی می توانیم تهدید را به عنوان ***اسبابی*** برای شناخت نقاط ضعف خود بدانیم. پس سازمانها می توانند با شبیه‌سازی تهدیدات مصنوعی، نقاط ضعف‌های خود را شناسایی کنند. به عبارت دیگر، با یک نگرش مثبت گرایانه می‌توان گفت، ***وجود تهدید، مثبت مشروط است*** . وجود تهدید بهانه ای برای شناخت نقاط ضعف مخاطبِ تهدید از خودش است. تهدید می تواند موجب *ارتقای شناختی* مخاطب تهدید شود. اگرچه وجود تهدید باعث افزایش ضریب نوآوری و خلاقیت مخاطب تهدید خو اهد شد اما معتقدیم ***تهدید تا زمانی مثبت است که بالقوه باشد*** . زیرا در این صورت مخاطب تهدید را مجبور به خودپایشی و تلاش برای تهیه راه‌حل های بدیل برای رفع نقاط ضعف خود می کند. شناخت نقاط ضعف اقدامی پیشگیرانه در پدافند غیرعامل است.

(۶) قابلیت اقدام پیش کنشانه [1]: همواره آمادگی بهتر از واکنش های لحظه ای است . همواره هزینه اقدامات پیشدستانه و پیش کنشانه پدافندی مقرون به صرفه تر از اقدامات مقطعی و لحظه ای به تهدیدات بالفعل است . یعنی اقدام پیش کنشانه، بهترین اقدام پدافندی است. منظور از اقدامات پیش کنشانه مجموعه ای از اقدامات پدافند غیرعامل است که موجب پیشگیری از خلق تهدید می شود. جلوگیری از خلق تهدیدات بالقوه و تبدیل تهدیدات بالقوه به بالفعل، موجب کاهش هزینه های پدافندی خواهد شد. یکی از مزایای اقدامات پیش کنشانه برملا شدن تهدیدات بالقوه قبل از بالغ شدن آنهاست . بلوغ تهدید مقدمه هزینه آفرینی تهدید است . بنابراین در بعضی از شرایط خلق حوادث مصنوعی

[1] Proactively Action

اقدامی پدافندی و مناسب محسوب می شود. بهترین موقع برای مقابله با تهدید، ***پیشگیری از خلق تهدید*** است. بعد از این مرحله، موقعیت بهتر، ***پیشگیری از بلوغ تهدید*** است.

پس می توان از مطالب مذکور چند نتیجه گرفت که یک سازمان در عصر دانش اولاً تهدید را می تواند به عنوان یک ***منبع دانش*** بداند که او را قادر می کند تا با مهندسی معکوس تهدیدات به فرصت های جدید دست یابد، ثانیاً تهدیدآفرین یک کارگر دانشی است، ثالثاً برای رسیدن به یک تصمیم و اقدام پیش کنشانه در سط ح استراتژیک، به قابلیت محوری مبتنی بر هوشمندی استراتژیک نیاز دارد.

۳ ۳ -پردازش دانش استراتژیک و خلق قابلیت های پدافند غیرعامل

به نظر ما ایده ***پدافند غیرعامل دانش محور*** می تواند در سطح استراتژیک سازمانها موجب شکل دهی هوشمندی استراتژیک مبتنی بر قابلیت های پدافند غی‌رعاملی شود. از این طریق سازمانها می‌توانند به چند نتیجه ارزشمند برسند : (۱) تمرکز به ***قابلیت محوری*** به جای سردرگمی در فعالیت های روزمره، (۲)جهت‌دهی به اقدامات روزمره در راستای رسیدن به قابلیت های مدرن، (۳) هوشمندی در سطح استراتژیک با رویکرد پدافند غیرعامل به چند مولفه نیاز دارد : (الف) سرمایه: منظور تمامی سرمایه های فناورانه، انسانی، اجتماعی و دیجیتالی متناسب با سطح استراتژیک است . (ب) دانش: منظور مجموعه دانش های استراتژیک از دیدگاه دانش فناورانه، دانش انسانی، دانش اجتماعی و دانش دیجیتالی است. (پ) پردازش دانش: منظور پردازش نظام مند دانش با رویکرد پدافند غیرعامل است که می تواند قابلیت های خردمندانه و جدیدی را برای سازمان ها به ارمغان بیاورد . (ج) درک صحیح: درک صحیح از مفهوم پدافند غیرعامل متناسب با خصیصه های منحصربفرد سطح استراتژیک در مدیریت سازمان و دانش های پدافندی هم سنخ با تهدیدات این سطح می تواند موجب افزایش ضریب صحیح بودن قابلیت های پدافندی باشد.

قابلیت محوری بدون پردازش نظام مند، موضوع گرا، هدفمند و روشمند دانش حاصل نخواهد شد. انسان به عنوان اصلی-ترین پردازنده دانش در سازمان ها می تواند کمک قابل توجهی به دستی ابی به ضریب هوشمندی قابل قبولی در سطح استراتژیک داشته باشد. در همین راستا، اتاق های فکر و اندیشکده ها به عنوان یکی از اصلی ترین ***کانون های تولید قابلیت*** می توانند جایگاه استراتژیک و ارزشمندی در هوشمندی استراتژیک داشته باشند . به عبارت بهتر، بخش قابل توجهی از ضریب هوشمندی سازمان ها در سطح استراتژیک وابسته به اشتراک گذاری و پردازش دانش در اتاق های فکر و کانون های اندیشه است . از طرف دیگر، در هوشمندی استراتژیک برای دستیابی به یک سطح قابل قبولی از انعطاف پذیری در قابلیت های پدافند غیرعامل، به یک خیزش استراتژیک پویا مبتنی بر سناریونگاری نیاز است . بنابراین تدوین مجموعه ای از سناریوها برای قابلیت های مذکور می تواند برای سازمان مفید باشد.

۴ -بحث و نتیجه گیری

یکی از تهدیدات بالقوه در سطح استراتژیک، غافلگیری استراتژیک است . یکی از راهکارهای پدافند غیرعاملی برای این تهدید، دستیابی به یک ضریب هوشمندی مناسب در سطح استراتژیک است . به عبارت دیگر، هوشمندی استراتژیک موجب پیشگیری از غافلگیری استراتژیک خواهد شد. هوشمندی استراتژیک حاصل به اشتراک گذاری نظام مند دانش در اتاق های فکر و اندیشکده ها با تاکید بر قابلیت محوری است.

توجه به چند نکته درباره هوشمندی استراتژیک با تاکید بر قابلیت های پدافندی ضروری به نظر می رسد: (۱)هوشمندی استراتژیک ایده آل، یک هوشمندی حاصل از یکپارچگی مولفه های آینده نگاری، چشم اندازسازی، تفکر سیستمی، انگیزه بخشی، مشارکت و مدیریت دانش می باشد، (۲) یکی از جدی ترین تهدیدات در تحقق هوشمندی استراتژیک وجود شکاف ماموریتی و فناورانه بین این مولفه ها و همچنین عدم وجود ادبیات مشترک میان پردازنده های دانش می باشد، (۳) بهترین گزینه برای پوشش شکاف های بین این مولفه‌ها و یکپاچه سازی آنها استفاده از دانش می‌باشد و (۴) استفاده از دانش برای یکپارچه سازی این مولفه‌ها علاوه بر یکپارچگی و چابکی، انعطاف پذیری را نیز برای سازمان به ارمغان خواهد آورد.

بنابر تعبیری می توان گفت : هوشمندی استراتژیک ذاتاً دارای ماهیتی از جنس پدافند غیرعامل است . زیرا هوشمندی استراتژیک اساساً به دنبال *آماده شدن برای آینده* با تاکید بر قابلیت سازی و قابلیت محوری است و آمادگی یکی از اصول پدافند غیرعامل می باشد . لذا از آنجایی که سناریوها به عنوان بستری برای خلق قابلیت ها و استراتژی های گوناگون هستند که هر کدام می توانند متناسب با شرایط و اقتضائات مختلف پدید آیند بنابراین برای دستیابی به هر قابلیت فوق الذکر (قابلیت مهندسی معکوس تهدیدات، قابلیت تغییر هوشمندانه، قابلیت توسعه توانمندی های پدافندی، قابلیت شناخت نقاط ضعف تهدید، قابلیت خودشناسی از دریچه تهدید و قابلیت اقدام پیش کنشانه) بهتر است تعدادی سناریو تدوین شود. در تدوین سناریوها باید به خاطر داشت که بخش قابل توجهی از هوشمندی استراتژیک را ارزش و توانایی ارزش آفرینی شکل می دهد.

منابع

امینی، مصطفی (۱۳۸۹). مدیریت انتقال دانش با توجه به زمینه کاربر برای سازمان های مجازی در محیط گرید . پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد اراک.

امینی، مصطفی (۱۳۸۸). لجستیک دانش. گزارش سمینار کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد اراک.

خداداد حسینی، سید حمید؛ صفری کهره، محمد (۱۳۸۷). هوشمندی استراتژیک در سیاست گذاری حوزه آینده نگری فناوری، سومین کنفرانس بین المللی مدیریت استراتژیک. تهران: گروه ناب، موسسه مدیریت و توسعه.

لیندگرن، ماتس؛ باند هولد، هانس (۱۳۸۶). طراحی سناریو: پیوند بین آینده و راهبرد (عبدالعزیز تاتار، مترجم). فرزانه میرشاه-ولایتی، مسعود منزوی (ویراستاران)، چرا طراحی سناریو لازم است؟ دلایلی از حوزه تحقیقات راهبردی (ص ۱۷-۳۴). تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی (نشر اثر اصلی ۲۰۰۳).

لیندگرن، ماتس؛ باند هولد، هانس (۱۳۸۶). طراحی سناریو: پیوند بین آینده و راهبرد (عبدالعزیز تاتار، مترجم). فرزانه میرشاه-ولایتی، مسعود منزوی (ویراستاران)، روش ها (ص ۱۴۷-۱۸۲). تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی (نشر اثر اصلی ۲۰۰۳).

سرفرازی، مهرزاد؛ قربانی، امیر و دیگران (۱۳۸۷). مدیریت دانش، به عنوان یک سرمایه استراتژیک هوشمند، اولین کنفرانس جهانی بانکداری الکترونیکی. تهران: موسسه مطالعات بهره وری و منابع انسانی.

شوارتز، پیتر (۱۳۸۸). هنر دورنگری: برنامه ریزی برای آینده در دنیایی با عدم قطعیت (عزیز علیزاده، مترجم). مسعود منزوی و حمید رهنما (ویراستاران)، انسان، سناریوساز بالفطره (ص ۳۱-۴۵). تهران: مرکز آینده پژوهی علوم و فناوری دفاعی، موسسه آموزشی و تحقیقاتی صنایع دفاعی (نشر اثر اصلی ۱۹۴۶).