

حفاظت و اطلاعات؛ جستاری در ماهیت یک نظارت استراتژیک

مهدی لطفی^۱

چکیده

نهادهای نظارتی را می‌توان به دو شاخه تقسیم کرد که از نظر دامنه نظارت و حدود اختیارات از یکدیگر متمایزند. بعضی از نهادهای نظارتی جنبه عمومی دارند و گستره نظارت وسیعی برای آنها تعریف شده است و دسته دیگر جنبه اختصاصی و محدوده متمرکزتری دارد. ولی اختصاص‌گرایی در این گونه دسته‌بندی، حاکی از نقش ضعیف و دامنه کوتاه آن نهاد نظارتی خاص نیست؛ بلکه ممکن است این ساختار متمرکز در یک سیستم و سازمان، دامنه نظارت پرنفوذ و پرارزشی داشته باشد که اثرگذاری و عمق استراتژیک آن بیشتر از نهادهای نظارتی عام باشد. پرداختن به موضوع نهادهای نظارتی خاص از جمله سازمان حفاظت و اطلاعات در مراکز نظامی و امنیتی و اداری مانند مرکز حفاظت و اطلاعات در قوه قضائیه و سازمان‌های تابعه آن که جزئی از کل هستند، از نظر اهمیت، هم‌تراز با نهادهای نظارتی عام از جمله سازمان بازرسی کل کشور و جامعه اطلاعاتی در قالب کلی از جز هستند. وظایف یک نهاد نظارتی خاص در سیستم، جهت تحقق سلامت و صیانت از سازمان است. هویت و جایگاه یک نهاد حفاظتی در زمان بحران و شرایط آشفته سیستم به‌خوبی خود را نشان می‌دهد؛ زیرا اهتمام مدیران و رؤسا، بیشتر تمرکز بر اجرا و سرعت در حصول نتیجه است تا دوران مدیریت متفاوت و موفق در رزومه مدیریت خود ثبت نمایند. این امر محقق نمی‌شود جز اینکه منویات مدیران و رؤسا توسط یک شبکه تیزبین و مطمئن درون ساختار تالحتظہ اجرا شدن توسط مجریان، از انحراف و اهمال‌کاری مراقبت و نظارت شود. اینجا است که می‌توان از سازمان حفاظت و اطلاعات به‌منزله یک شبکه اعصاب که عیون بیدار و حصون مستحکم برای شکوفایی و تعالی یک دستگاه است نام برد. نهادهای حفاظت و اطلاعات با دو نقش صیانت از پرسنل و صیانت از سیستم می‌تواند در جایگاه نگهبان تفکر مدیر در تحقق اهداف مدیریت، نقش ایفا کند و در مقابل هر گونه برنامه‌ریزی پنهان جهت ساختار شکنی و ایجاد آشوبی سیستمی و کند نمودن سرعت رشد و تحقق آرمان و برنامه مدیر، اقدام پیشگیرانه نماید و با شناسایی پالایش و آسیب‌شناسی، قبل از وقوع بحران، نسخه اصلاح تنظیم کنند؛ این یک رفتار به‌هنگام برای یک نهاد نظارتی «استراتژیک» خاص است که بر اساس وظایف متمرکز سازمانی برای او تعریف شده است و نشان‌دهنده همان ارزش هم‌تراز با نهادهای نظارت عام در سطح گسترده صیانت از حکومت و وضعیت اجتماعی، فرهنگی، اقتصادی و سیاسی یک ملت است.

واژگان کلیدی: حفاظت و اطلاعات، نظارت عام، نظارت خاص، نظارت استراتژیک،

اطلاعات، نفوذ

۱- مقدمه

یکی از دستگاه‌های نظارتی خاص در مراکز نظامی و امنیتی و اداری، سازمان «حفاظت و اطلاعات» است که به‌منزله یک مجموعه صیانتی در کنار ساختارهای اداری و اجرایی نقش آفرینی می‌کند که از جمله ساختارهای فعال و اثرگذار در نظام اداری است. شاید حفاظت و اطلاعات را با سیمای یک تشکیلات امنیتی، اطلاعاتی پنهان بشناسیم ولی با این باطن استراتژیک هدفی متعالی را دنبال می‌کند و آن صیانت و حفظ سلامت سازمان و محیط، با هدف ایجاد فضای امن برای یک تلاش صادقانه است. اقدامات این مجموعه در گام اول پیشگیرانه است تا مچ‌گیرانه. باید با نگاه اصلاحی و رویکرد ارشادی در ابعاد و زوایای سیستم رفتار شود و این رسالت مهم تحقق نمی‌یابد جز با آگاه‌سازی و مشارکت عمومی توسط سازمان حفاظت و اطلاعات. یکی از ضعف‌های موجود در سیستم‌های اداری و مدیریتی، ایجاد خطوط فاصل با سازمان حفاظت و اطلاعات است و به آن به‌منزله مجموعه‌ای با تاروپود مجزا از شبکه اداری نگاه می‌شود. این نوع نگاه، یکی از چالش‌های مراکز حفاظت و اطلاعات در انجام مأموریت‌های سازمانی خود است؛ زیرا تشکیلات حفاظتی یک تشکیلات انحصاری و قائم به ساختار خود نیست، بلکه موفقیت‌های یک مجموعه نظارتی در گرو همکاری و مشارکت جمعی است که لازمه آن اعتماد است. رویکرد اصلاحی، یک اقدام یک‌طرفه و واحد نیست بلکه اقدامی مشترک و دوسویه است؛ زیرا شناسایی آسیب با گسترش چتر نظارت بر محیط، امکان‌پذیر است. در غیر این صورت عدم اطلاع به موقع از بحران می‌تواند ضربه جبران‌ناپذیری را بر ساختار سیستم وارد نماید که صرف این هزینه، برای کل مجموعه است. سازمان حفاظت و اطلاعات براساس مأموریت‌های استراتژیک خود برای اصلاح، مستلزم اقدام عملیاتی به‌صورت پنهان هستند، ولی در مقوله دریافت و کسب خبر رسالت و تکلیفی است که بر همه مخاطبین و پرسنل و آحاد جامعه گذاشته شده است و تکلیف انحصاری برای سازمان حفاظت و اطلاعات محسوب نمی‌شود. در بعضی مواقع این دیدگاه به وجود می‌آید که اعلام خبر و گزارش سوءجریان به نهادهای نظارتی یک نوع مداخله در امور آن‌ها است. این تلقی، اشتباه است زیرا نظارت جامع‌الاطراف، جز با جمع‌آوری اخبار از منابع سازمانی و غیرسازمانی تحقق پیدا نمی‌کند و عدم مشارکت عمومی در ارسال و اعلام اخبار و حوادث سوء می‌تواند اخبار کانالیزه شده و جهت‌داری را تولید کند که جهان‌بینی محدودی را برای تحلیل و تدبیر به سازمان حفاظت و اطلاعات بدهد، بنابراین جامعه حفاظتی مجموعه‌ای فراگیر و اجتماعی است.

۲- تعریف حفاظت و اطلاعات

حفاظت در لغت به معنای حفظ کردن، نگهداری و حراست و نگاهبانی کردن است و در اصطلاح عبارتست از همه اقداماتی که برای حفظ و نگهداری تأسیسات، اسناد و مدارک، اخبار

می‌دهد.

۱-۱-۲- اطلاعات سلبی: اطلاعاتی است که با هدف تثبیت قدرت گردآوری می‌شود و به ما امکان تدافع، پدافند و اقدام می‌دهد.^۱

عصر جدید، عصر مرگ ثانیه‌ها و فاصله‌هاست. بهره‌مندی از جدیدترین و کامل‌ترین اخبار و اطلاعات در کوتاه‌ترین زمان دست برتری تصمیم‌گیری را برای مدیران تصمیم‌ساز ایجاد می‌کند؛ این مستلزم توسعه منابع خبری است. عموم جامعه سرمایه اجتماعی قابل اعتمادی برای سازمان حفاظت و اطلاعات محسوب می‌گردند و مأموریت‌های حفاظت و اطلاعات برای عموم افراد سازمانی و غیرسازمانی آرامش، امنیت و سلامت را به ارمغان می‌آورد. منابع خطری که می‌تواند تهدیدکننده اطلاعات یک سازمان باشد را می‌توان در چهار بخش متمرکز نمود: ۱. از داخل سازمان، ۲. از خارج سازمان، ۳. بر حسب تصادف، و ۴. از روی عناد از طرف دیگران (حاجیان، و شهابی، ۱۳۸۴: ۴۸). چنانچه سازمان‌های حفاظت و اطلاعات بی‌توجه به تحولات محیط امنیتی دچار عادت و روزمرگی شوند و تغییر و تحولات را نادیده بگیرند، به نقطه‌ای می‌رسند که باید تغییرات بنیادی در ساختار، فرایندها، فرهنگ سازمانی و دیگر زمینه‌های برجسته سازمانی را در زمانی کوتاه و با شتاب تند تجربه کنند و به جای پیش‌بینی تحولات برنامه‌ریزی شده با ریسک و خطرپذیری باعث هزینه‌های کلان و خسارات جبران‌ناپذیری می‌شوند (رحیمی، ۱۳۸۷: ۱۵۸).

۳- ضرورت ایجاد سازمان حفاظت و اطلاعات

۳-۱- از منظر عقلی

حس امنیت و کرامت انسانی ایجاب می‌کند هر فردی به دنبال قرارگرفتن در فضای امن و آرام برای یک زندگی بی‌دغدغه باشد. امنیت و سلامت هر محیط و مجموعه‌ای که متشکل از گروه‌ها و تشکل‌های انسانی است، وابسته به بهره‌گیری از ابزارهای سخت‌افزاری و نرم‌افزاری برای تحقق این امنیت و آرامش هستند. هیچ‌کس نمی‌تواند در ضرورت آرامش و امنیت در جامعه تردید کند. زندگی با دغدغه و پرتلاطم، شرایط مرگ تدریجی را فراهم می‌کند. از جمله مجموعه‌های تشکیلاتی که می‌تواند آرامش و امنیت را ایجاد کند، سازمان حفاظت و اطلاعات است که ضرورتی غیر قابل انکار در یک سیستم است. نیروهای حفاظت و اطلاعات باید از روی بینایی، یقین و اطمینان حرکت کنند. نوع مأموریت نیازمند داشتن حقایق امور است نه عمل براساس شبهه و تردید که آفت‌زا و احیاناً ایمان‌سوز است. این کار در درجه اول مستلزم فکر و اندیشه است (مهدوی‌راد و صادقی، ۱۳۹۳: ۱۹). لازم است در ادامه به بعضی از این ضرورت‌ها اشاره شود:

۱-۱-۳- تشکیلاتی بودن فساد

باتوجه به رشد و توسعه فناوری و ارتقای سیستم نظارت، شبکه‌های فساد نیز تغییر ساختار داده و متناسب با این تغییر رویکرد نفوذ حرفه‌ای و مجازی خود را در دستور کار قرار داده‌اند. این خود

برگرفته از مرام‌نامه‌ای پنهان است که لازم است به اقسامی از دسته‌بندی‌های فساد اشاره شود: یک. فساد تصادفی و فساد نظام‌مند: فساد نظام‌مند در جامعه رایج است و به شکل قانده‌مند درمی‌آید. احتمال کشف و مجازات مجرم و انگیزه فساد کاهش می‌یابد؛ زیرا برخلاف حالت اتفاقی طرفین تمایلی به گزارش کردن خلاف ندارند. در این حالت نهادها و ضوابط رفتاری با الگوهای غارتگری دیوان‌سالاری تطابق می‌یابد؛ مانند رواج رشوه.

دو. فساد سازمان‌یافته و فساد فردی: در فساد سازمان‌یافته سرمایه‌گذاران می‌دانند به چه کسانی رشوه دهند و در قبال چه چیزی رشوه به دست آورند. در فساد فردی باید به چند تن مقام رسمی رشوه دهند و صفاتی هم نیست که با تقاضای رشوه بیشتری روبه‌رو نشوند. فساد سازمان‌یافته در واقع پدیده‌ای سیاسی است. یعنی کسانی که در مواضع قدرت هستند از دولت و قدرت برای انتقال منافع و عواید نامشروع به خود و وابستگان استفاده می‌کنند.

سه. فساد کلان و فساد خرد: فساد رؤسای دولت، وزیران و کارمندان عالی‌رتبه را فساد کلان و فساد کارمندان جز مثل افراد پلیس و مأموران گمرک و مالیات را فساد خرد می‌گویند. کنترل فساد کلان مقدم بر خرد است. البته بدون تردید فساد اداری همیشه با اعمال غیرقانونی تجلی نمی‌یابد. چه‌بسا تصمیماتی که در جهت انجام وظایف قانونی صورت می‌گیرد، در مقطعی باشد که منافع آن شامل افراد خاصی شود. به همین جهت در کنار مصادیق فساد اداری مثل اختلاس، ارتشا، سوءاستفاده از اموال و امکانات دولتی، کم‌کاری، تبعیض و تسریع کار دوستان و آشنایان و ... (فساد اداری غیرقانونی)، می‌توان به مصادیقی از جمله وضع قوانین تبعیض‌آمیز به نفع سیاستمداران قدرتمند و طبقات مورد لطف دولت و بخشیدن انحصارات دولتی به افراد خاص (فساد اداری قانونی) اشاره کرد (بخارایی ۱۳۸۶: ۸۵).

۲-۱-۳- تهدیدات نرم و سخت

مفهوم لغوی واژه تهدید: ترساندن، بیم دادن، بیم عقوبت دادن (بهشتی، ۱۳۶۹: ۳۱۴). در لغت‌نامه و بستر^۱ برای «تهدید» دو تعریف ارائه داده است: نخست تهدید را بیان و آن را قصد آسیب رساندن، نابود یا تنبیه کردن دیگران از روی انتقام یا ارباب می‌داند و در تعریف دوم آن را نشان دادن خطر^۲، آسیب و شرارت قریب‌الوقوع مانند جنگ تعریف کرده است (عبداله‌خانی، ۱۳۸۵: ۵۱۱-۴۹۱).

در تعریفی دیگر از واژه تهدید آمده است: «به آن دسته خطرات بالفعل و بالقوه‌ای اطلاق می‌شود که ارزش حیاتی یک کشور از جمله تمامیت اراضی، استقلال و حاکمیت ملی، نظام حاکم و نهادهای سیاسی و اجتماعی و اقتصادی و ایدئولوژی و فرهنگ و افتخارات ملی را به خطر اندازد. تهدیدها ممکن است به درون مرزی، برون‌مرزی و تهدیدهایی که مرز مشخصی ندارند تقسیم شود» (کریمایی، ۱۳۸۴: ۴۷).

1- Webster

2- Danger

همچنین کارل روپر معتقد است تهدید عبارت است از «هر گونه نشانه، حادثه یا شرایطی که توان ایجاد خسارت و ضرر علیه یک دارایی را داشته باشد (عبداله خانی، ۱۳۸۶: ۲۳). از جمله تعاریف دیگر تهدید این است: «به مجموعه خطرهای بالقوه برون سازمانی که امنیت کارکنان و سازمان را به مخاطره می‌اندازد، تهدید گفته می‌شود» (بهارى نیا، ۱۳۸۶: ۲۵).

الف. تهدیدات نرم: این نوع تهدیدات را می‌توان به دو معیار اساسی از تهدیدات سخت باز شناخت. اولین معیار غیرخشونت آمیز بودن روش تهدید و معیار دوم، نرم افزاری بودن پیامد تهدید است. بنابراین چنانچه تهدیدی از سوی عامل آن به روش غیرخشونت آمیز اجرا شود و پیامدهای ناشی از آن نیز نرم افزاری باشد، تهدید نرم نامیده می‌شود.

ب. تهدیدات سخت: عکس معیارهای تهدیدات نرم، اصلی‌ترین معیارهای تهدیدات سخت است. بنابراین خشونت آمیز بودن در روش اقدام و سخت‌افزاری بودن در پیامد اقدام دو معیار اصلی تهدیدات سخت است. این تهدیدات اغلب با ابزارهای تجهیزات مرگ‌بار انجام شده و نتیجه آن تخریب، انهدام، کشتار و وحشت آفرینی است (عبداله‌خانی، ۱۳۸۶: ۶۷).

البته مفهوم دیگری به نام جنگ نرم و جنگ سخت وجود دارد که اصطلاح جنگ نرم^۱ که در مقابل جنگ سخت^۲ استفاده می‌شود یکی از مفاهیم متداول در مکاتبات و مذاکرات استراتژیست‌ها، نظریه‌پردازان و کارشناسان علوم اجتماعی و سیاسی است (عبدی، ۱۳۸۹: ۲۴).

۳-۱-۳- نیاز به امنیت

امنیت یک مفهوم آشنا و قابل شناخت برای تمام جوامع بشری از جوامع اولیه چون قبایل کوچک گرفته تا امپراتوری‌های بزرگ جهان باستان و دولت‌شهرهای یونان بوده است و به همین قسم امروز نیز تلاش برای رسیدن به «وضعیت امن» یا «Secure Situation» اولویت نخست سیاست‌های واحدهای سیاسی مختلف را تشکیل داده و راه‌های تأمین آن از جایگاه خاصی در سیاست‌گذاری‌های امنیتی دولت‌ها در قالب امنیت ملی برخوردار است (بوزان، ۱۳۷۸: ۲۳).

به این صورت می‌توان گفت تأمین امنیت و راه‌های دستیابی به آن از جمله سنگ‌بناهای شکل‌گیری واحدهای سیاسی از نگاه تاریخی بوده تا از این طریق اعضای جوامع مذکور بتوانند به کمک یکدیگر به مهم‌ترین نیازشان که تأمین امنیت است، دست یابند. اما آنچه در جوامع اولیه و حتی تا این اواخر مطرح بود یک دیدگاه محدود به امنیت بود؛ به طوری که بحث امنیت روی موضوعات نظامی متمرکز بود. در اصل یک نوع دید تقلیل‌گرایانه نسبت به امنیت حکم‌فرما بود و امنیت را در توانایی‌های نظامی و برقراری صلح بعد از جنگ‌ها جستجو می‌کردند (بوزان، ۱۳۷۸: ۲۳).

«امنیت» از جمله مفاهیم پیچیده‌ای است که ارائه تعاریف واحدی از آن به سادگی میسر نیست. «امنیت» پیش از آنکه مقوله‌ای قابل تعریف باشد، پدیده‌ای ادارکی و احساسی است؛ یعنی این

3- Soft warfare

4- Hard warfare

اطمینان باید در ذهن توده مردم، دولت مردان و تصمیم گیران به وجود آید که برای ادامه زندگی بدون دغدغه امنیت لازم وجود دارد یا نه.

کلمه امنیت، مأخوذ از کلمه لاتین securitas است. که از secures به معنای (فراغت از نگرانی) گرفته شده است. امنیت به معنای ایمن بودن و به دور از مخاطرات است (دوستدار، ۱۳۸۸: ۱۲۱).

امنیت یکی از عناصر بنیادی بُعد سیاسی نظم اجتماعی محسوب می شود که دارای ابعاد متنوعی شامل ذهنی و عینی، داخلی و خارجی، فردی و جمعی است و از لحاظ گستره نیز شامل حیطه های ملی، منطقه ای و جهانی است از نظر سطح به سطح خرد و کلان تقسیم می شود. هریک از این ابعاد، گستره و سطوح امنیت به نوبه خود، به خرده ابعاد دیگری تقسیم می شود. به عنوان مثال امنیت در سطح خرد می تواند شامل امنیت جانی، ملی، فکری، بیانی، اخلاقی، شغلی و حقوقی باشد و امنیت در سطح کلان نیز می تواند زیر سطوح اقتصادی، سیاسی، اجتماعی، فرهنگی، نظامی و طبیعی یا زیست محیطی را در بر بگیرد (محبوبی منش، ۱۳۸۹: ۵۸).

۴-۱-۳. پدیده نفوذ

الف. معانی لغوی «نفوذ»

در کتب لغت شناسی، نفوذ به معنای اثر کردن در چیزی، داخل شدن در چیزی (فرهنگ فارسی معین)، تأثیر گذاشتن بر کسی و راه یافتن پنهانی در گروه یا جایی (فرهنگ فارسی عمید) آمده است. از سوی دیگر، معادل انگلیسی نفوذ، واژه (Influence) است که در لغت به معنی کنش یا قدرتی است که نتیجه ای را بدون اعمال آشکار زور یا بدون اعمال مستقیم فرمان، تولید می کند و در اصطلاح عبارت از اعمالی است که مستقیم یا غیرمستقیم سبب تغییر در رفتار یا نظارت دیگران می شوند (الوانی، ۱۳۸۶: ۱۴۲).

در تعریفی دیگر «نفوذ شکلی ظریف و نامرئی از قدرت است که از طریق تسخیر و مهار دستگاه محاسباتی و نظام تصمیم گیری یک فرد، گروه، دولت و ... اعمال می شود. منظور این است که آن مؤلفه ای که سبب عملیاتی شدن و عینیت یافتن قدرت می شود، نفوذ است (جمعی از نویسندگان، ۱۳۹۴: ۱۷).

ب. تفاوت رخنه و نفوذ

مسئله نفوذ اغلب با مسئله رخنه اشتباه گرفته می شود. واژه نفوذ یک مفهوم نظامی است. در تاکتیک نظامی بین دو مفهوم «رنخه» و «نفوذ» طبیعتاً یک تمایز جدی وجود دارد. برخی از این تفاوت ها عبارت اند از: ۱. رخنه مستمر اتفاق می افتد اما نفوذ نقطه ای و موضعی است؛ و ۲. غالباً رخنه توسط واحدهای ارتش نظامی کلاسیک در خط مقدم اعمال می شود، اما نفوذ توسط نیروهای ویژه در عمق مواضع کشور دشمن اعمال می شود.

از این منظر وقتی نفوذ اعم از نفوذ فرهنگی، سیاسی، اجتماعی، اقتصادی و ... سخن به میان

می‌آید منظور این است که عناصری از فکر و فرهنگ و اعتقاد و اقتصاد کشور دشمن در عقبه مواضع فرهنگی، سیاسی، اقتصادی، اجتماعی، امنیتی و نظامی خودی نفوذ کرده‌اند (جمعی از نویسندگان، ۱۳۹۴: ۱۹).

ج. انواع تقسیم‌بندی نفوذ

ج-۱. نفوذ عمودی-نفوذ افقی

ج-۱-۱- نفوذ عمودی که بیشتر سخت‌افزارانه است و حالتی آمرانه دارد، کشورهای قدرتمند به دنبال آن هستند که برتری خود را از راه‌های مختلف همچون جنگ و قدرت نظامی، اعمال فشار و تحریم و تهدید نشان دهند؛ درواقع، هر چیزی برای این کشور وسیله‌ای برای برتری طلبی و سلطه‌گری به شمار می‌آید.

ج-۱-۲- نفوذ افقی، که وجه نرم‌افزارانه آن غالب است، بازیگران به دنبال جلب اعتماد قدرت از این طریق هستند، به‌کدیگر اعتماد دارند و احساساتشان را فاش می‌کنند. در الگوی ارتباط افقی از ابزارهای مذاکره، انواع دیپلماسی و ارتباطات، سبک زندگی، ارزش‌های اجتماعی و فرهنگی و ... برای تعامل و ارتباط‌گیری استفاده می‌شود (جمعی از نویسندگان، ۱۳۹۴: ۲۳-۲۴).

ج-۲. نفوذ فردی-نفوذ جریانی

ج-۲-۱- اولین و ساده‌ترین نوع نفوذ، نفوذ موردی و انفرادی است. این تاکتیک، عمری به قدمت تاریخ دارد. در این شیوه از نفوذ به قدرت‌های تخاصم تلاش می‌کنند، با بهره‌گیری از رخنه‌های موجود در طرف مقابل، عناصر خود را وارد خانه حریف کنند تا به اهداف مورد نظر خود برسند. اهداف این نفوذ گران می‌تواند از ساده‌ترین مسائل ممکن همچون کسب اطلاع و جاسوسی گرفته تا پیچیده‌ترین هدف‌گذاری‌ها، یعنی وارد کردن نفوذگر در بدنه تصمیم‌گیری و تصمیم‌سازی سازمان حریف باشد، یا در بدنه نظام تصمیم‌گیری رخنه کنند و جایگاه فرایند کارشناسی خود را ارتقا می‌دهند، یا با بهره‌گیری از تعاملات شخصی با برخی از شخصیت‌های مؤثر، فرایند تصمیم‌سازی را به دلخواه خود هدایت و راهبرد خود را براساس عملیات «مدیریت ادراک» نخبگان بنا می‌کنند (جمعی از نویسندگان، ۱۳۹۴: ۲۴-۲۵).

ج-۲-۲- نفوذ دیگری که بسیار پیچیده‌تر و زیان‌بارتر از روش اول است، «نفوذ جریانی و شبکه‌ای» است که در جریان انسانی گسترده ولی پنهان از عناصر نفوذگر که ارتباط وسیعی میان خود دارند، وارد محیط حریف می‌شوند و با بهره‌گیری از بسترهای موجود سعی می‌کنند مسیر جامعه را تغییر دهند. اگر نفوذ انفرادی به دنبال جهت‌دهی به معدودی از نخبگان بود، نفوذ شبکه‌ای، عموم جامعه را هدف می‌گیرد و فرایندی فراگیر را تعقیب می‌کند (جمعی از نویسندگان، ۱۳۹۴: ۲۶).

۵-۱-۳- جنگ اطلاعاتی

اطلاعات یک سیستم دارای ارزش و سرمایه برای آن سیستم محسوب می‌شود. از این روی صیانت از اطلاعات از اهمیت بسیار زیادی برخوردار است و صیانت از فزای، سخت‌افزار، شبکه،

رمزنگاری، پرسنل، امنیت فیزیکی و محیطی، کنترل، بازرسی و سایر موارد ضامن سلامت، کارآیی، بقا و استمرار سیستم است.

بنابراین جنگ اطلاعات استفاده تهاجمی و دفاعی از اطلاعات و سامانه‌های اطلاعاتی برای تکذیب، تحریف یا تخریب اطلاعات، فرایندهای مبتنی بر اطلاعات، سامانه‌های اطلاعات و شبکه‌های اطلاعات دشمن با حفظ منابع اطلاعات خود است (رشیدزاده، ۱۳۸۵: ۵۰).

نبرد اطلاعات را می‌توان از دیدگاه‌ها و نقطه‌نظرهای مختلف به انواع و اقسام متفاوتی تقسیم کرد و اما معروف‌ترین تقسیم‌بندی توسط لیسکی و فلو (۱۹۹۵) از اساتید دانشگاه دفاع ملی صورت گرفته است و آن‌ها اجزای نبرد اطلاعاتی را به دو گروه تقسیم کرده‌اند: گروه اول عبارت است از فعالیت‌هایی که علیه نیروهای نظامی صورت می‌گیرد و شامل سه مورد نبرد فرماندهی-کنترل (C2W)، جنگ جاسوسی و نبرد الکترونیکی است. گروه دوم، فعالیت‌هایی است که علیه اجتماع صورت می‌گیرد و شامل جنگ روانی، نبرد اقتصادی، نبرد سایبر و نبرد اطلاع‌رسانی است در طول زمان موارد دیگری به اجزای نبرد اطلاعاتی از جمله نظارت و مراقبت، شناسایی کنترل خسارت^۱، جنگ ماهواره‌ای^۲ اضافه شده است (افضلی، ۱۳۸۷: ۷۱).

البته مفهوم استفاده از اطلاعات در جنگ قدمت طولانی دارد. ظهور اصطلاح جنگ اطلاعاتی و اهمیت روزافزون آن احتمالاً با انقلاب اطلاعات ارتباط مستقیم دارد. باور همگانی این است که چنین انقلابی آن‌قدر قدرتمند و دامنه‌تأثیر آن آنچنان گسترده است که می‌تواند بعد جدیدی در جنگ یا اصلاً سبک جدیدی از جنگ را تعریف کند. در خلال نیمه دوم دهه ۱۹۹۰ اصطلاح جنگ اطلاعاتی مطرح و بعداً توجه به آن کم‌رنگ شد (وزارت دفاع و پشتیبانی، ۱۳۸۴: ۱۷).

هیچ کارشناسی نمی‌توانست تعریف روشنی برای آن ارائه دهد، چه رسد به اینکه کارشناسان نظامی درباره یک تعریف مشخص به تفاهم برسند. اغلب به نظر می‌رسد که اصطلاح جنگ اطلاعاتی طیف بسیار گسترده‌ای را در بر گرفته و شامل موارد سنتی مانند «جنگ فرماندهی و کنترل و جنگ»^۳ الکترونیک می‌شود (وزارت دفاع و پشتیبانی، ۱۳۸۴: ۱۷-۱۸).

مارتین لیسکی، از محققان مؤسسه مطالعات استراتژیک در دانشگاه دفاع ملی، در کتاب «جنگ اطلاعاتی چیست؟» می‌نویسد: «تلاش برای درک مفهوم جنگ اطلاعاتی مانند این است که چند نفر نایبنا بخواهند با لمس کردن بخش‌های مختلف یک فیل بگویند که این موجود چیست. کسی که پیش را لمس کند می‌گوید این یک درخت است، نفر دیگری که دم آن را لمس کند می‌گوید این یک طناب است و الی آخر. بنابراین باید اذعان داشت که الگوی کلی جنگ اطلاعاتی در نگاهی عمیق‌تر در آینده شاهد تحول ماهیت جنگ خواهد بود (وزارت دفاع و پشتیبانی، ۱۳۸۴: ۱۸).

1- Damagecontrol

2- Satellite war

3- Command and Control Warfare (c2w)

۲-۳- ازمناظر آیات و روایات

آنچه در کنار مباحث عقلی می‌تواند اراده انسان را مستحکم و مصمم نماید پذیرش فطری و معرفتی است که در این موضوع با نگاه دین‌مدارانه که در بین مسلمان وجود دارد به این ایدئولوژی فکری اهتمام شده است و در کنار عقول بشری به دستورات دینی به‌منزله یک ضرورت اعتقادی توجه شود و کاملیت دین اسلام در تمامی ابعاد و شئون زندگی بر حفظ پیکره‌بندی اجتماع مسلمین دقت نظر دارد و حصون مستحکم در مقابل هرگونه گسست در جامعه اسلامی است و مراقبت و هشدارهای لازم را صادر می‌نماید، لازم است تمامی افراد جامعه به این نقطه برسند که ادامه حیات سیاسی هر جامعه برای حفظ کرامت و استقلال خود به کسب اطلاعات و حفاظت و اطلاعات از اسرار خود نیازمند است. در آیات و روایات مختلف اهمیت و ضرورت این موضوع روشن شده است که توان نظامی بدون مراقبت حفاظتی، ابزاری بی‌خاصیت است که هیچ‌گونه رخ‌نمایی برای هراس دشمن خارجی از آن وجود ندارد.

یکی از تفاوت‌های اساسی سازمان حفاظت و اطلاعات در اسلام و سازمان‌های حفاظتی غربی و شرقی با توجه به تفاوت‌های مبنایی، تمایز در مقوله‌های هستی‌شناسی، معرفت‌شناسی، انسان‌شناسی و ارزش‌شناسی است (مهدوی‌راد، صادقی، ۱۳۹۳: ۲).

خداوند سبحان در قرآن کریم به آماده‌سازی و توسعه قدرت دفاعی در مقابل دشمن و هراس به آن این‌گونه بیان فرموده است:

وَأَعِدُوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَمِنْ رِبَاطِ الْخَيْلِ، تُرْهَبُونَ بِهِ وَعَدُوَّ اللَّهِ وَعَدُوَّكُمْ و...^۱

«و هر چه در توان دارید از نیرو و اسب‌های آماده بسیج کنید تا دشمن خدا و دشمن خودتان را بترسانید.»

(رضوان‌طلب، ۱۳۹۰: ۷۳)

امیرالمؤمنین (علیه‌السلام) در مورد آمادگی در مقابل توطئه‌های دشمن می‌فرماید:

مَنْ لَمْ يَتَحَرَّزْ مِنَ الْمَكَائِدِ قَبْلَ وُقُوعِهَا لَمْ يَنْفَعَهُ الْأَسْفُ عِنْدَ هُجُومِهَا^۲

«آن‌کس که توطئه‌ها و حوادث را پیش‌بینی و پیشگیری نکند، تأسف به هنگام هجوم توطئه برای او کارآمد نیست.»

همچنین امام باقر (علیه‌السلام) در مورد بی‌توجهی به اخبار و اطلاعات دشمن این‌گونه می‌فرماید: «هر کس گزارشی را پنهان یا تعقیب نماید، اما هدفش هدر دادن خون مسلمان یا تلف کردن مال او باشد، روز قیامت با چهره‌ای سیاه و چشمانی درشت و صورتی لطمه‌دیده محشور می‌شود که همه خلایق او را می‌شناسند و هر کس گزارشی را برای احیای حق دنبال کند، با چهره‌ای نورانی و تبارنامه‌ای روشن محشور می‌شود.»^۳

(رضوان‌طلب، ۱۳۹۰: ۶۸)

۱- انفال (۸)، آیه ۶۰

۲- غررالحکم، ج ۲، ص ۷۰۱

۳- اصول کافی، ج ۷، ص ۳۸۰

در جایی دیگر امیرالمؤمنین (علیه السلام) در مورد هوشیاری اطلاعاتی می فرماید:
 «مَنْ لَمْ يَسْتَظْهِرْ بِالْيَقْظَةِ لَمْ يَنْتَفِعْ بِالْحَفْظَةِ^۱
 «آن کس که از هوشیاری اطلاعاتی بی بهره باشد، نگهبانان و سپاهیان برایش مفید نخواهد بود».
 (رضوان طلب، ۱۳۹۰: ۷۵)

همچنین مولای متقیان حضرت علی (علیه السلام) در مورد حفظ اسرار می فرماید:
 «رَأَى تَوًّا، أَسِيرٌ تَوَّسَتْ وَ أَكْرَأَ تَوًّا رَأَى تَوًّا، تَوًّا أَسِيرٌ أَوْ شَدَّ أَيْ»^۲
 «در جای دیگر حضرت امیر (علیه السلام) در مورد طبقه بندی و رعایت حفظ اسرار می فرماید:
 مَا كُنْتُ كَاتِمَةً عَدُوَّكَ مِنْ سِرٍّ، فَلَا تَطَّلَعَنَّ عَلَيْهِ صَدِيقُكَ
 «آنچه را از دشمنت پنهان می داری، دوست را نیز از آن مطلع مکن».
 (شبدینی پاشاکی، عالی نژاد، حسینی، ۱۳۹۱: ۳۸)

خداوند سبحان می فرماید:
 يَا أَيُّهَا الَّذِينَ آمَنُوا، خُذُوا حِذْرَكُمْ^۳
 «ای اهل ایمان، بیدار و مراقب باشید».
 (رضوان طلب، ۱۳۹۰: ۷۴)

لذا اهمیت و ارزش حفاظت و اطلاعات در نظام اسلامی در راستای اجرای فرامین الهی و تدابیر حضرات معصومین (علیه السلام) برای رهبری جامعه اسلامی است تا در مقابل حکام جور برای به دست آوردن اخبار و اطلاعات دشمنان و صیانت از مسلمانان عمل شود.

۴. نقش و وظایف حفاظت و اطلاعات

از جمله کارکردهای حفاظت و اطلاعات، شامل جمع آوری اطلاعات درباره سرویس های امنیتی و اطلاعاتی، از طریق منابع آشکار و پنهان، تحلیل و تحقیق در زمینه ساختار، اشخاص و عملیات های سازمان های اطلاعاتی خارجی، برای شناخت نقاط ضعف و قدرت آن ها و خنثی سازی فعالیت های خصمانه سازمان های اطلاعاتی و امنیتی کشورهای دیگر می شود. برای اجرای این وظایف، از نفوذ به درون سازمان های اطلاعاتی و دستگاه سیاست خارجی و استفاده از روش های غیرمستقیم، مانند کسب اطلاعات از پناهندگان استفاده می شود (رشیدزاده، ۱۳۸۵: ۶۲).

وظیفه خطیر حفاظت و اطلاعات از جهاتی شبیه به نهادهای بهداشتی درمانی است. این نهاد در ابتدا سعی بر آن دارد ابتدا از هر آلودگی و بیماری پیشگیری نماید و در مرحله بعد اگر احتمالاً کسی آلوده شد او را درمان نماید و در نهایت اگر دو روش قبلی مؤثر واقع نشد او را همچون یک عضو مرده و فاسد شده بدن از سیستم جدا کرده و دور بیاندازد. چنین نقشی را حفاظت و اطلاعات

۱- غرورالحکم، ج ۲، ص ۷۰۲

۲- غرورالحکم، ج ۴، ص ۱۴۶، شماره ۵۶۳۰

۳- نساء (۴)، آیه ۷۱

در سازمان ایفا می‌کند. حفاظت و اطلاعات در هر سازمان با پیش‌بینی نوع تخلف‌ها و جرایمی که ممکن است در آن سازمان به وقوع بپیوندد سعی می‌کند به انحاء مختلف، چشم و گوش کارکنان آن سازمان را به روی دام‌ها و کمین‌های سر راه بگشاید و آن‌ها را هوشیار و آگاه سازد. با این کارها اول آنکه جلوی خسارت‌های احتمالی که مسلماً هزینه‌های سنگینی برای سیستم در بر خواهد داشت، گرفته می‌شود و دوم آنکه جلوی انتشار تخلف‌ها و انحراف‌ها در بین کارکنان گرفته می‌شود. هدف حفاظت و اطلاعات، شناسایی و مقابله با تهدیداتی است که از سوی فعالیت‌های اطلاعاتی اشخاص و سازمان‌های جاسوسی، خراب‌کاری، براندازی یا تروریسم، متوجه کشور و جامعه اطلاعاتی است. تقویت امنیت، ممانعت از افشای اطلاعات، شناسایی و خنثی‌سازی جاسوسی، شناسایی تهدیدات بالقوه، و کشف و برنامه‌ریزی عملیات سازمان‌های دشمن، از جمله کارکردهای حفاظت و اطلاعات در جامعه اطلاعاتی است (رشیدزاده، ۱۳۸۵: ۶۲-۶۳).

۴-۱- اقدامات حفاظت و اطلاعات به دو بخش آفندی و پدافندی تقسیم می‌شود:

۴-۱-۱- بخش آفند، تأکید بر قدرت استفاده از اطلاعات و مانع‌سازی برای استفاده دشمن و بیگانگان دارد.

۴-۱-۲- بخش پدافندی شامل اقدامات عامل و غیرعامل در برابر جنگ اطلاعاتی دشمن و بیگانگان است که از طریق دفاع فیزیکی، حفاظت اسناد، مدارک، تجهیزات، اماکن، تأسیسات، شخصیت‌ها، تقویت موانع، ضد براندازی، ضد جاسوسی، ضد خرابکاری و مانند آن به انجام می‌رسد (رشیدزاده، ۱۳۸۵: ۶۳).

• کارکردهای حفاظت و اطلاعات در سیستم

۱. کانال ارتباطی مطمئن با مراجع تصمیم‌گیر، ۲. ارتقای نظام پاسخ‌گویی، ۳. دریافت، تجزیه و تحلیل و پردازش اخبار، ۴. پشتوانه‌ای محکم برای سلامت سیستم، ۵. مشاوره امین برای مدیر، ۶. حافظ منافع کارکنان در سیستم، ۷. اعمال رفتارهای پیشگیرانه، ۸. تحقق اهداف مدیران، ۹. اطلاع‌رسانی به هنگام، ۱۰. حفاظت کلیه کارکنان، ۱۱. مدافع حقوق مراجع کنندگان به سیستم، ۱۲. مشاوره امین در انتصابات، ۱۳. شفاف‌سازی و کارآمد سازی قوانین، ۱۴. ارزشیابی و مدیریت عملکرد کارکنان، ۱۵. شناسایی نیروهای مستعد در سیستم، ۱۶. حفاظت فیزیکی از اماکن، مقرها و اسناد و مدارک، IT، و ۱۷. ایجاد امنیت و آرامش روانی در محیط.

۴-۲- سه نقش اساسی حفاظت و اطلاعات در پیشگیری از وقوع تخلف

نقش‌های حفاظت و اطلاعات در پیشگیری از وقوع تخلف عبارت‌اند از: اول، نقش هشداردهنده یا پیشگیری‌کننده، دوم، نقش اصلاح‌کننده یا درمان‌کننده، و سوم، نقش جداکننده از سیستم.

۵- تبارشناسی مفهوم نظارت استراتژیک

۵-۱- ماهیت و مفهوم نظارت

از حیاتی‌ترین ارکان هر سیستم سالم و کارآمد وجود یک نهاد نظارتی دقیق است و وجود یک

نظم نظارتی در سیستم، می‌تواند میزان تحقق برنامه‌ها و اهداف مدیر مجموعه را ارزیابی کند، لازم است قبل از پرداختن به ماهیت نظارت با تعریف کلیدواژه «نظارت» آشنا شویم. واژه نظارت در «معجم مقاییس اللغة» این‌گونه تعریف شده است:

«نظارت از ماده نظر است که به معنای نظر افکندن و تأمل و دقت در امری است. نظر به معنای تأمل در چیزی و معاینه کردن آن نیز معنا می‌شود» (محسن شیخی، ۱۳۹۰: ۱۳).

همچنین «اقراب الموارد» می‌گوید: «النظاره» کلمه‌ای است که عجم آن را به کار می‌برد و منظور از آن، پاکیزه نمودن باغ و بستان است. بنابراین، نظارت همان مراقبت و کنترل یک چیز، از آفت و بیماری است.

تعریف‌های گوناگونی از نظارت و کنترل ارائه شده که در همه آن‌ها یک نقطه اشتراک وجود دارد و آن این است که نظارت عبارت است از «مقایسه بین آنچه هست و آنچه باید باشد». عده‌ای از نویسندگان علم مدیریت، «نظارت» را چنین تعریف می‌کنند:

«نظارت عبارت است از سنجش و اصلاح عملکرد برای به دست آوردن این اطمینان که هدف‌های سازمان و طرح‌های اجرایی آن با کامیابی به انجام رسیده است» (محسن شیخی، ۱۳۹۰: ۱۴).

بنابراین، ضرورت «نظارت» انکارناپذیر است و هر قدر این ابزار با کمال دقت، متانت، عدالت و بنا بر این، ضرورت «نظارت» انکارناپذیر است و هر قدر این ابزار با کمال دقت، متانت، عدالت و با رعایت شرایط آن به کار رود، تأثیر آن بیشتر خواهد بود. «نظارت» در سازمان‌ها نیز در جهت کمک به مدیریت و فرماندهی در جلوگیری از خطاها و غرض‌ورزی‌ها، اهمیت بالایی دارد (محسن شیخی، ۱۳۹۰: ۱۵).

اگر سیستمی برخوردار از یک نظام نظارت استراتژیک نباشد، دیر یا زود متلاشی می‌شود. هنری فایول نظریه‌پرداز معاصر، نظارت و کنترل را به منزله یک اصل منطقی که تکمیل‌کننده چهار اصل دیگر، یعنی برنامه‌ریزی، سازماندهی، هماهنگی و فرماندهی، می‌داند و می‌گوید منظور از کنترل و نظارت، سرکشی و رسیدگی به اجرای فرامین و دستوراتی است که به اعضای سازمان داده می‌شود. از این راه است که می‌توان نحوه اجرای صحیح آن را دریابیم. به خاطر همین، اگر کنترل صحیح در کار وجود داشته باشد، همیشه سیستم کنترل، باید سیستمی سریع و بادقت باشد به همه امور مربوط در اسرع وقت رسیدگی نماید و نارسایی‌ها را سریع تشخیص دهد (پارکینسون، ۱۳۶۹: ۷۰).

یکی از عوامل مؤثر در موفقیت برنامه‌ها، وجود یک نظام دقیق نظارتی است که در چارچوب سازمان حفاظت و اطلاعات در هر سیستمی قابل تحقق است. انجام فعالیت‌های یک سیستم همراه با موفقیت نخواهد بود، مگر آنکه نظارت‌های لازم نسبت به آن صورت گیرد.

وجود یک نظم نظارتی در سازمان، مدیریت را نسبت به نحوه تحقق هدف‌ها و انجام عملیات آگاه می‌کند و او را قادر می‌سازد پیگیری‌های لازم را انجام دهد. سازمان بدون داشتن یک نظام دقیق نظارت، نمی‌تواند به تمام هدف‌های مورد نظر خود دست یابد و از امکانات و منابع موجود، به نحو مؤثر و درست استفاده کند.

حصول اطمینان از اینکه اجرای برنامه و هدایت سازمان درست انجام می‌شود و در صورت مشاهده انحراف، برای تصحیح آن اقدام لازم به عمل خواهد آمد، نیازمند یک نظام مؤثر و دقیق نظارتی است (محسن شیخی، ۱۳۹۰: ۲۳). از سوی دیگر، نظارت نیز بدون وجود برنامه، مفهومی ندارد و کاری عبث و بیهوده خواهد بود.

«به دلیل این ارتباط تنگاتنگ میان نظارت و برنامه‌ریزی است که برخی از نویسندگان علم مدیریت، نظارت و برنامه‌ریزی را به دو تیغه یک قیچی تشبیه کرده‌اند که بدون هریک از تیغه‌ها، قیچی قادر به کار کردن نیست و فایده‌ای نخواهد داشت» (همان، ۲۳ تا ۲۴).

۲-۵- مفهوم استراتژی

پیش از هر اقدامی لازم است با کلیدواژه «استراتژی» در ادبیات اجرایی آشنا شویم. به همین منظور از دو منظر لغوی و اصطلاحی به این موضوع نگاه شده است.

۱-۲-۵. مفهوم لغوی استراتژی

واژه استراتژی از کلمه یونانی «استراتگوس»^۱ گرفته شده است. استراتگوس یا «استراتژ» به معنای لشکر است. «استراتگوس» به معنی فرماندهی ارتش نیز به کار می‌رفت که معنای دیگری را می‌توان برای آن تعریف کرد. «فن اداره جنگ، فن فرماندهی، فن جنگ و طرح نقشه برای جنگ» نیز از دیگر معانی آن است (علی‌بابایی، ۱۳۶۹: ۴۲).

۲-۲-۵. مفهوم اصطلاحی استراتژی

استراتژی در معنای اصطلاحی جدید به این صورت تعریف می‌شود: «به فن و علم توسعه و به کارگیری قدرت سیاسی، اقتصادی، فرهنگی و نظامی ملت، هنگام جنگ و صلح، برای تأمین حداکثر پشتیبانی از سیاست‌های ملی و افزایش احتمال و دستیابی به نتایج مطلوب برای کسب حداکثر پیروزی و حداقل شکست» (باقری کیبوق، ۱۳۷۰: ۱۹۸). اطلاق می‌شود. هرگاه قدرت سیاسی، نظامی، فرهنگی و اقتصادی، در جهت دستیابی به اهداف نظامی یک ملت به کار رود، استراتژی نظامی نامیده می‌شود. به همین ترتیب برای هریک از ابعاد فرهنگی، سیاسی و اقتصادی می‌توان تعریفی از استراتژی ارائه داد. استراتژی در معنای قدیمی خود به معنای به کارگیری همه امکانات کشور برای دستیابی به اهداف نظامی بود که بخشی از هدف‌های کلان یک کشور را تشکیل می‌داد.

البته تعاریف متعددی از استراتژی مطرح شده است که به برخی از آن‌ها اشاره می‌کنم. آندره بوفر، اهل فرانسه، استراتژی را این گونه تعریف می‌کند: «استراتژی، هنر به کار بردن زور و جبر است؛ به طوری که این زور و جبر بتواند تا حد امکان، بیشترین نتیجه را در رسیدن به اهداف سیاسی به بار آورد» (لطفی، ۱۳۹۳: ۵۱).

آنچه بوفر در تعریف خود از استراتژی دنبال می‌کند یک نوع قدرت‌نمایی جهت تطمیع و ایجاد

رعب در جبهه مقابل است تا امتیاز بیشتری از آن کسب کند ولی این نوع رفتار فارغ از هرگونه نیت سازمانی، مرزی برای مراقبت ندارد تا از سرحد قدرت‌نمایی به سمت سلطه‌گرایی سوق پیدا نکند، ولی شاید این شیوه اتخاذ استراتژی، راهبردی پرخطر باشد.

در تعریفی دیگر که از استراتژی توسط لیدل هارت انگلیسی بیان شده، آمده است: «استراتژی هنری است که با آن می‌توان با به خدمت گرفتن نیروهای نظامی، هدفی را که توسط سیاست‌های کلی دولت یا ملتی تعیین شده است، به دست آورد» (لطفی، ۱۳۹۳: ۵۱). تعریف استراتژی که توسط هارت صورت گرفته است با تعریف بوفر تفاوت‌هایی دارد. زیرا اتخاذ استراتژی متناسب با سیاست‌های کلی دولت و ملت است و وجود بازیگران فعال داخلی و خارجی محدوده رفتار آن را کنترل می‌نمایند.

امروزه ادبیات سلطه‌گری و استعمارگرایی از مفهوم واقعی خود تهی شده است و جز خاطره هولناک در ذهن جوامع بشری چیزی دیگری باقی نمانده است. امروزه مفهوم واقعی استراتژی بهره‌مندی از تمامی ظرفیت‌ها و ابزارهاست. امروزه دولت‌ها قادر نیستند فقط با استفاده از قدرت نظامی بر دشمن پیروز شوند؛ بلکه به مجموعه‌ای از ابزارها نیاز دارند که قدرت نظامی یکی از آن‌ها است (علی‌بابایی، ۱۳۶۹: ۴۴). پس می‌توان گفت موقعیت استراتژیک، موقعیتی است که مزایای قاطع نظامی، سیاسی یا اقتصادی را به دارنده آن در مقابل رقبا و دشمنانش اعطا می‌کند (ملکو تیان، ۱۳۸۳: ۲۰۷).

سیستم‌ها در مسیر تکامل خود نیازمند یک مراقبت درونی و بیرونی هستند. نهادهای نظارتی از جمله حفاظت و اطلاعات ستون فقرات یک سیستم هستند که رکن استراتژیک سیستم محسوب می‌شوند. اهداف و آرمان‌های یک سیستم محقق نمی‌شود مگر اینکه سازمان حفاظت و اطلاعات را به منزله یک جایگاه نظارت استراتژیک در سیستم بپذیریم.

۵- نتیجه‌گیری

امروزه با تحول در علم مدیریت و تخصصی شدن کارکرد سازمان‌های دولتی و غیردولتی در نظام بین‌الملل، شرایطی را برای یک نظام استراتژیک فراهم می‌کند که از ابزارهای متناسب برای رشد و پیشرفت جامعه تحت مدیریت خود استفاده نماید تا در تکاپوی رقابت‌های نابرابر قدرت‌های متخاصم جهانی، اراده مستقل و آزاد خود را در نظام سلطه‌گری و تسلط‌پذیری اعمال نماید. یکی از ابزارهایی که لازمه استواری و سرپا بودن چنین اراده مستحکمی است، اتحاد از درون و مراقبت از نفوذ بیرون است. برای مراقبت از این دو مقوله، نیازمند سازمانی تخصصی و فنی برای صیانت از اطلاعات حیاتی و سلامت نیروی انسانی کارآمد است. آنچه در این تحقیق مورد کنکاش قرار گرفت، اهمیت سازمان «حفاظت و اطلاعات» در سیستم‌های اداری، امنیتی و نظامی به منزله

یک نظارت استراتژیک بود که در ابعاد گوناگون مورد توجه قرار گرفت و به منزله یک بازوی اطمینان‌بخش و مورد وثوق در کنار مدیریت سیستم نقش آفرینی می‌کند و اهمیت این نوع نظارت خاص، در مقیاسی برابر با سیستم‌های نظارت عام است که خود جلوه هويت یک نظارت استراتژیک در قلب سیستم است و پویایی و نقش آفرینی جامع و کامل آن در مشارکت عمومی و تجانس افراد محیط با اهداف و مأموریت‌های پنهان و آشکار این سازمان سخت‌کوش است.

منابع

- افضلی، مهدی. (۱۳۸۷)، نبرد اطلاعاتی: جنگ در عرصه اطلاعات، فصلنامه اطلاع‌شناسی، شماره ۱۹. الوانی، سید مهدی. (۱۳۸۶)، مدیریت عمومی، نشر نی، تهران، چاپ سی و یکم.
- باقری کبورق، علی. (۱۳۷۰)، کلیات و مبانی جنگ و استراتژی، نشر بین‌المللی.
- بخارایی، احمد. (۱۳۸۶)، جامعه‌شناسی انحرافات اجتماعی در ایران، تهران، پژوهک جامعه.
- بوزان، باری. (۱۳۷۸)، مردم، دولت‌ها و هراس، تهران، پژوهشکده مطالعات راهبردی.
- بهارى نیا، امان‌الله. (۱۳۸۶)، حفاظت و اطلاعات رسته اداری، آموزش دانشگاه علوم انتظامی امین.
- بهشتی، محمد. (۱۳۶۹)، فرهنگ صبا (لغت‌نامه)، چاپ ششم، تهران، انتشارات صبا.
- پارکینسون، نورث کوت. (۱۳۶۹)، اندیشه‌های بزرگ در مدیریت، ترجمه مهدی ایران‌نژاد پاریزی، مؤسسه بانکداری ایران، بانک مرکزی جمهوری اسلامی ایران، تهران.
- جمعی از نویسندگان. (۱۳۹۴)، بررسی ابعاد پروژه نفوذ در جمهوری اسلامی ایران، معاونت سیاسی نمایندگی ولی فقیه در سپاه پاسداران انقلاب اسلامی، مرکز چاپ نمایندگی ولی فقیه در سپاه.
- حاجیان، محمد اسماعیل، شهابی، شهلا. (۱۳۸۴)، استاندارد مدیریت حفاظت و اطلاعات و نقش آن در عملکرد سازمان‌ها، مجله اقتصاد/تعاون، شماره ۱۷۰.
- دوستدار، رضا. (۱۳۸۸)، پلیس و امنیت، فصلنامه دانش حفاظتی و امنیتی، سال چهارم، شماره دهم.
- رحیمی، ابراهیم. (۱۳۸۷)، سامانه‌های حفاظت و اطلاعات در نبردهای آینده، ماهنامه نگرش راهبردی، شماره ۸۹ و ۹۰.
- رشیدزاده، فتح‌الله. (۱۳۸۵)، عصر اطلاعات و جنگ اطلاعاتی، فصلنامه مدیریت نظامی، شماره ۲۱.
- رضوان‌طلب، محمدرضا. (۱۳۹۰)، اطلاعات در اسلام، پژوهشکده تحقیقات اسلامی، انتشارات زمزم هدایت، قم.
- شبدینی پاشاکی، محمد، عالی‌نژاد، صمد، حسینی، غلام‌عباس. (۱۳۹۱)، سیره حفاظتی و اطلاعاتی امامان معصوم (علیه‌السلام)، انتشارات زمزم هدایت، قم.
- عبداله‌خانی، علی. (۱۳۸۵)، بررسی و نقد نظریه امنیتی ساختن، فصلنامه مطالعات راهبردی، شماره ۳۳.
- عبداله‌خانی، علی. (۱۳۸۶)، تهدیدات امنیت ملی، انتشارات مؤسسه فرهنگی مطالعات و تحقیقات

بین‌المللی ابرار معاصر تهران.

عبدی، حسین. (۱۳۸۹)، جنگ نرم، دفتر نشر معارف، قم.

علی‌بابایی، غلامرضا. (۱۳۶۹)، فرهنگ اصطلاحات روابط بین‌الملل، انتشارات سفیر.

کریمایی، علی. (۱۳۸۴)، کلیات حفاظت و اطلاعات، تهران، ساحفا ناجا، نشر حدیث کوثر.

لطفی، مهدی. (۱۳۹۳)، تنگه هرمز در ضربان انسداد، انتشارات زمزم هدایت، قم.

محبوبی‌منش، حسین. (۱۳۸۹)، امنیت، انحراف اجتماعی، پژوهشگاه علوم انسانی.

محسن‌شیخی، علی‌اصغر. (۱۳۹۰)، نظارت و بازرسی، زمزم هدایت، قم.

محمدی، حمیدرضا. (۱۳۸۴)، استراتژی قدرت‌های جهانی و تأثیر آن بر منطقه خاورمیانه (با

تأکید بر استراتژی آمریکا)، مجموعه مقالات دومین کنگره انجمن ژئوپولیتیک ایران.

ملکوتیان، مصطفی. (۱۳۸۳)، مقدمه‌ای بر جغرافیای سیاسی و اهمیت استراتژیک ایران، مجله

دانشکده حقوق و علوم سیاسی، شماره ۶۳.

مهدوی‌راد، محمدعلی، صادقی، حسن. (۱۳۹۳)، تحلیل ارزش شناختی بصیرت درحفاظت

و اطلاعات از دیدگاه قرآن و حدیث، فصلنامه پژوهش‌های حفاظتی و امنیتی دانشگاه جامع امام

حسین (علیه السلام)، سال سوم شماره ۱.

وزارت دفاع و پشتیبانی نیروهای مسلح موسسه آموزشی و تحقیقاتی صنایع دفاع-مرکز

آینده‌پژوهی علوم و فناوری دفاعی. (۱۳۸۴)، جنگ و دفاع سایبر، پروژه مطالعاتی الزامات جنگ

نوین در فضای مجازی (سایبر).